IT-retten

Mads Bryde Andersen

IT-retten

2. udgave

Gjellerup
København 2005

Mads Bryde Andersen
IT-retten
2. udgave, 1. oplag
er sat med Times af Dedicated PrePress, Virum,
og trykt og indbundet af BookPartner, København.
Omslaget er tilrettelagt af Jens Hage.

ISBN 87-13-04906-2 (trykt bog)
ISBN 87-13-04907-0 (e-bog)

Gads Forlag
Klosterstræde 9
1157 København K
Tlf. 77 66 60 00
Fax: 77 66 60 01
www.gjellerup.com

INDHOLDSOVERSIGT

INDHOLD

ANDEN DEL: RETSBESKYTTELSE

TREDJE DEL: REGULERING

FORORD

Igennem 1990'erne er der sket en gennemgribende forandring af det emneområde, der tidligere gik under betegnelsen "edb-retten". Hvor man dengang beskæftigede sig med de juridiske problemer, der opstår, når edb-systemer udvikles, anvendes og overdrages, er fokus nu skiftet, så man i højere grad interesserer sig for den digitale informationsanvendelse i *alle dele* af samfundslivet. Denne massive udvidelse af det IT-retlige emneområde har gjort det til lidt af en udfordring at samle disse forskelligartede emner under ét.

Det er denne bogs ambition at give en samlet præsentation af de retsregler, der har størst praktisk betydning for IT-anvendelsen i bred forstand, hvad enten der er tale om private, erhvervsmæssige eller offentligretlige sammenhænge. Som samfundet ser ud i dag, har nærmest alle retsregler en eller anden IT-dimension. Emneafgrænsningen er lagt om de regler, der i særlig grad *præges* af IT. Enten fordi de udtrykkeligt drejer sig om IT. Eller fordi de netop ikke gør det, men i deres møde med IT-fænomenerne giver anledning til særlige vanskeligheder ("beskrivelsesproblemer" mv.). Visse retsområder er dog udeladt, herunder beskatning, konkurrenceforhold, strafferetlige efterforskningsspørgsmål og international privat- og procesret. Fremstillingen er så vidt muligt ført ajour til 1. juli 2001.

Bogen har flere målgrupper. Den første, og væsentligste, er den praktiserende jurist, der er med til at træffe de praktiske dispositioner mv. Men en mindst ligeså væsentlig målgruppe er den IT-ansvarlige, som i praksis ofte står overfor den praktiske IT-rets problemer, og som måske ligefrem – frivilligt eller ufrivilligt – er sat til at rådgive nogen herom.

Det er ikke let at ramme to så forskellige målgrupper. For at overkomme de problemer, den *ikke-juridiske* læser står overfor, har jeg forsøgt at skrive teksten i et ikke alt for indforstået juridisk fagsprog, ligesom jeg har forklaret nogle af de mere vanskelige juridiske begreber i ordlisten. Samme ordliste skulle omvendt gøre det lettere for *juristen* at dykke ned i de relevante tekniske problemer.

Flere foreløbige udgaver af denne bog har været anvendt i undervisningen i IT-ret i årene fra 1996-2001. Jeg har fået god feedback fra mange af de jurastuderende, der har fulgt disse kursusfag, og fra gode venner og kolleger, som jeg har arbejdet med under mine mange gøremål gennem årene, bl.a. i Dansk Datafor-

ening, Dansk Internet Forum, det nordiske retsinformatik-miljø, EU, IT-sikkerhedsrådet, UNCITRAL, OECD, og i de lovforberedende og rådgivende udvalg, jeg har deltaget i. Det ville føre for vidt her at nævne dem alle.

I projektets sidste fase har jeg fået gode forslag om forbedringer af mine ph.d.-studerende, Kim Frost og Henrik Udsen. En særlig tak retter jeg til stud.jur. Anja Jørgensen, der har gjort mig den store tjeneste at gennemgå det manuskript til bogen, der anvendtes i "Udvidet IT-ret" ved Københavns Universitet i forårssemesteret 2001, og påpeget en række passager, der var fejlbehæftede eller vanskeligt forståelige. Det færdige manuskript er med stor dygtighed korrekturlæst af forlagsredaktør Susanne Falck.

Men, som man siger i den slags forord: Det endelige ansvar for bogen er naturligvis mit. Bogen er tilgængelig fra hjemmesiden www.it-retten.dk, hvor den – med henvisning til ophavsretslovens § 12, stk. 1 – kan læses og kopieres til "privat brug". Fra denne hjemmeside kan man også finde links til store dele af det baggrundsmateriale, der omtales i bogen, ligesom der – inden for visse grænser – vil blive givet meddelelse om ny lovgivning og praksis eller anden væsentlig information, der kan understøtte læserens arbejde med IT-rettens problemverden.

København i august 2001

Mads Bryde Andersen
mads.bryde.andersen@jur.ku.dk

FORORD til 2. udgave

Som forventelig er der siden 1. udgave af denne bog udkom for 4 år siden sket mangfoldige ændringer i såvel lovgivning, retspraksis som i den juridiske litteratur. Som følge heraf er retsopfattelsen inden for mange af de områder, denne bog dækker, ændret. Fremstillingen er derfor grundlæggende revideret i lyset af denne retsudvikling.

Der er ikke taget højde for forhold, der er kommet til efter 1. juli 2005.

København i juli 2005

Mads Bryde Andersen

IT-ordbog

Foruden de ordforklaringer, der fremgår af bogen, henvises til følgende IT-ordbøger og leksika, der er tilgængelige fra nettet:

- <www.it-dansk.dk>: IT-terminologisk ordbog udarbejdet af IT-terminologiudvalget under Dansk Sprognævn
- <www.wikipedia.org>: Et af de største net-baserede leksika med over 600.000 grundige artikler, der udarbejdes under en kontrolleret proces under deltagelse af brugere mv.
- <www.wepopedia.com>: Netbaseret ordbog og søgemaskine, der særligt omhandler IT- og internet-relaterede begreber og problemstillinger.

ABA: American Bar Association. Den amerikanske advokatsammenslutning. Har bl.a. igangsat og gennemført en række initiativer på IT-området, herunder en EDI-standardaftale og et sæt guidelines for digital signatur.

ADAPSO: Association of Data Processing Service Organisations (amerikansk brancheorganisation).

Adgangskontrol: Foranstaltninger, der indebærer et indblik i og efter omstændighederne filtrering af, hvem der opnår fysisk eller kommunikativ forbindelse med en lokalitet eller et system. For at opnå dette kan man f.eks. afkræve besøgende særlige legitimationsbeviser eller pasord (se **password**).

ADSL: Forkortelse for *A*symmetric *D*igital *S*ubscriber *L*ine. Teknik til overførelse af digital kommunikation med stor båndbredde via eksisterende kobberlinjer. Hastigheden på en ADSL-forbindelse afhænger af, om der sendes eller modtages data. ADSL-standarderne giver mulighed for at modtage mellem 1,5-9 mbit/s (såkaldt *downstream*), medens der kan overføres mellem 16 og 640 kbit/s (*upstream*). Computeren tilsluttes et særligt ADSL-modem, der i modsætning til tidligere telefonmodems ikke betjener sig af telefonnettet. ADSL-teknologiens store udbredelse skyldes bl.a. at kunden typisk betaler et fast beløb for sin ADSL-opkobling, uanset brug. Dermed kan man lade sin computer være "tilsluttet internettet" døgnet rundt..

AES: Advanced Encryption Standard. Ny NIST-standard til asymmetrisk kryptering, planlagt til afløsning af DES-standarden, først og fremmest i USA, men på sigt formentlig også i andre dele af verden.

Afleveringsprøve: Den prøve, der ifølge aftale skal "bestås" af en IT-leverandør, for at dennes ydelse kan siges at være præsteret kontraktsmæssigt. Typisk indgås aftaler om afleveringsprøve kun i mere komplekse IT-transaktioner, hvis der indgår et ikke ubetydeligt element af udvikling og installation.

Agent: Se **Intelligent agent**.

Agil Programudvikling: Af engelsk: *Agile Software Development.* Samlebetegnelse for forskellige metoder til udvikling af programmel hvis fælles kendetegn er, at man reducerer risikoen for problemer i udviklingsprocessen ved at koncentrere udviklingsindsatsen om små forløb (kaldet iterationer), der typisk varer mellem 2 og 4 uger. Hvert forløb udgør i sig selv et miniprojekt, der afleveres, vurderes og efter omstændighederne også markedsføres. Se også Extreme programming.

AI: Se **artificial intelligence**.

AIPI: Association Internationale pour la Protection de la Propriaté Industrielle.

Alfanumerisk: Et **tegn**sæt, der både indbefatter bogstaver, tal og specialtegn.

Algoritme: En matematisk defineret serie af instruktioner, der kan løse et specifikt problem. Inden for IT-retten anvendes ordet i to betydninger. For det første om det idégrundlag, der ligger til grund for et **edb-program**, og som almindeligvis ikke kan beskyttes ophavsretligt, sml. ophl. § 36, stk. 1, nr. 3. En anden og mere snæver anvendelse knytter sig til de eksakte matematiske fremgangsmåder, der tilsigter at udvirke specifikke funktioner, f.eks. i forbindelse med **komprimering** af tekst eller **kryptering**.

Analog datarepræsentation: Betegnelse for **data**, der er repræsenteret ved et ikke på forhånd givet antal tilstande (f.eks. temperaturforandringer), modsat **digitale** data, der alene kan repræsenteres ved kendte talstørrelser ("nuller og et-taller"). Sondringen mellem analog og digital datarepræsentation er iøjnefaldende på TV-området. Et analogt TV-signal ændrer sig kontinuerligt, hvorved det repræsenterer varierende grader af lys, farve og kontrast. I modsætning hertil repræsenterer et digitalt tv-billede (som man f.eks. kan se i TV's tekst-tv-sider) et antal absolutte farveværdier og -flader mv.

Andenordens-domænenavn, se **domænenavn**.

ANSI: American National Standards Institute – nu NIST (s.d.).

Ansvar: Den retsstilling, der foreligger, når der kan rettes en sanktionspræget retsfølge (f.eks. straf eller erstatningspligt) mod nogen pga. en handling eller undladelse der er resultatet af dennes valg. Begrebet anvendes i flere betydninger. At være "ansvarlig" kan således dels pege på den retsfølge, der gøres gældende, dels på den situation, der foreligger, når den *potentielt* ansvarlige har muligheden for at vælge og dermed udvirke retsfølgen.

AntiPiratGruppen: En sammenslutning af organisationer inden for film og musikbranchen, der bekæmper ulovlig kopiering og distribution af film og musikværker. AntiPiratGruppens medlemmer er IFPI Danmark, Foreningen af Danske Videogramdistributører, Foreningen af Filmudlejere i Danmark, KODA, NCB, Dansk Artist Forbund og Dansk Musiker Forbund.

APNIC: Organisation med basis i Tokyo, der har ansvaret for tildeling af IP-adresser i Asien og stillehavsområdet.

Applikation: "Anvendelse", underforstået: IT-anvendelse. Benyttes ofte med tilføjelsen "-programmel" (applikationsprogrammel) for at markere en forskel til **systemprogrammel**. Kan også betegne en given, bruger-rettet IT-løsning. Et **edb-program** til tekstbehandling er et eksempel på en applikation.

AQAP: Allied Quality Assurance Publications – NATO-publikationer om kvalitetssikring. For IT-produktudviklinger, der tager sigte på militær anvendelse inden for NATO-samarbejde, anvendes denne standard ofte, ligesom den spiller en mere generel rolle på IT-området.

Arbejdsstation: Se workstation.

Artificial intelligence: Se **kunstig intelligens**.

ASCII: Forkortelse for American Standard Code for Information Interchange. ASCII-koden er en international **standard**, der udpeger et tal for hvert af de alfabetiske og numeriske **tegn**, der anvendes under **edb**-behandling. Bogstavet "E" har f.eks. ASCII-værdien 69.

ASP: Application Service Provision: Moderne udtryk for en totalleverance, hvorved en IT-leverandør præsterer såvel drift, vedligeholdelse og undertiden udvikling til brugeren. På nær arbejdspladsudstyret befinder al hardware og software sig hos leverandøren, hvorfra det stilles til rådighed gennem en telekommunikationsforbindelse med den fornødne kapacitet og driftseffektivitet. Foruden finansieringsmæssige fordele på kort sigt kan brugeren herved opnå fordel af ikke selv at skulle stå for drift, vedligeholdelse og opdatering af programmet: IT-funktionerne kommer så at sige ud af et stik i væggen. Den væsentligste fordel for ASP-leverandøren (der pga. telekommunikationsdelen optræder i samspil med en teleleverandør) ligger i muligheden for at knytte kunderne tættere til sig ved de løbende betalinger. ASP-konceptet forudsætter, at leverandøren i videst mulig udstrækning kan (gen-)bruge standardiserede opsætninger af sine produkter.

ASP-licens: Licens til edb-program, der stilles til rådighed som led i en ASP-løsning. Programmet afvikles fra den server, hvorfra ASP-tjenesten stilles til rådighed, og kan følgelig ikke kopieres. Licensen er derfor typisk klausuleret for en bestemt periode med ret for et vist antal brugere til at anvende det pågældende programmel i denne periode.

Assembler-kode: Betegnelse for **formalsprog**, der alene består af symboler for de **binære** kommandoer, der kendes af en given **computer**. Betegnes ofte som symbolsk maskinsprog.

Asymmetrisk kryptering: Se **Public Key Krypteringssystem**.

Autenticitet: Rigtigheden af en påstået identitet, f.eks. afsenderen af en digital meddelelse. Sikkerhed for autenticitet kan f.eks. opnås gennem brug af **digital signatur**.

ATM: 1. Automated Teller Machine. Amerikansk – og efterhånden også dansk – betegnelse for pengeautomat, dvs. en elektronisk eller mekanisk enhed, der på anfordring kan udbetale kontantbeløb i form af sedler eller mønter. Den mest velkendte danske ATM er Dankort-automaten ("Kontantautomaten"). 2. Asynchronous Transfer Mode: Transmissionsmetode, hvorefter data inddeles i celler med en fikseret størrelse, som kan sendes mere effektivt via et transmissionsnet. Hermed opnås en mere sikker og effektiv transmission af data.

Banner: Egl. flag. Betegnelse for den angivelse af et varemærke, der sker ved placering af et symbol for det pågældende varemærke.

Bannerannonce: Annonce på en hjemmeside, der synliggør en leverandørs ydelse. Typisk er bannerannoncen forbundet med en **link**.

Baud: Modulationsenheder pr. sekund. Udtryk for en digital kommunikationshastighed. Hver modulationsenhed kan overføre en eller flere **bit**.

BBS: Bulletin Board System, også kaldet elektronisk opslagstavle. **Database** med **information** inden for en nærmere angiven emnekreds, der via det offentlige telefonnet står til fri rådighed for **brugere** med interesse inden for den pågældende emnekreds. BBS'et fungerer således, at brugerne dels kopierer nogle **informationer** fra det ("downloader") dels lægger andre ind ("uploader"). Den kommunikation, der foregår på BBS'et, kontrolleres almindeligvis af en systemoperatør (også kaldet "sysop"), der efter et nærmere udøvet skøn henholdsvis tilstår og nægter adgang for nye og eksisterende brugere. BBS'er tjener almindeligvis nyttige funktioner, f.eks. som "konferencer" for meningsudvekslinger mellem de tilknyttede brugere, men har i enkelte tilfælde været anvendt til illegitime formål, f.eks. formidling af hemmelige **password**s og teknikker til **Hacking**.

Benchmark-test: (Bench = høvlebænk). Analysemetode til at godtgøre beskaffenheden af et IT-system med udgangspunkt i en kendt belastning, som dets ydeevne herefter sættes i forhold til. Bruges primært til sammenligninger af IT-systemers ydeevne.

Beta-version: Tidlig test-udgave af et program. Anvendes både om programmer, der omsættes på kommercielt grundlag som på ikke-kommercielle programmer (freeware) og almindeligvis med en klausul, der forbyder videreoverdragelse. Beta-versioner kan være mere eller mindre stabile og funktionsdygtige.

Binært talsystem: Talsystem, hvis cifre kan antage to ("bi") værdier (1 og 0). 10-talssystemet kan til sammenligning antage 10 værdier (0-9). Det binære talsystem er den logiske grundenhed i moderne computere, der netop kan håndtere elektromagnetiske høje henholdsvis lave elektriske impulser.

Biochip: Betegnelse for et **lagermedium**, hvis bestanddele består af organiske molekyler. Udviklingen af biochips er endnu på det eksperimenterende stadium. Bliver forskningen succesfuld, vil biochippen kunne sprænge alle kendte grænser for, hvor megen **information** der kan lagres på et givet areal. De organiske molekyler (herunder navnlig DNA-molekylet) er nemlig det mindste kendte medium for information.

BIOS: Basic Input Output System. Den del af en computers **styresystem**, der varetager den basale kommunikation med computerens forskellige enheder. Foreligger ofte i maskinens hardware og er følgelig integreret med den pågældende maskine. BIOS-systemet sætter en grundlæggende **grænseflade** for computerens programkompatibilitet.

Bit: Eng.: *Bi*nary Digi*t,* dvs. binært tal. Den mindste informationsmængde, der kan lagres og håndteres i en **digital** computer. Repræsenteres ved en valgfrihed med to muligheder – logisk som 0 eller 1; fysisk som en høj eller lav elektrisk spænding.

Bitmap: Digitalt billede hvis enkelte punkter er repræsenteret ved et tal (bit).

Black box-analyse: Den analyse af et edb-program, der alene udføres ved, at data sendes til og fra programmet. En sådan analyse kan udføres lovligt i medfør af ophl. § 36, stk. 1, nr. 3, fordi den alene indebærer en besigtigelse eller afprøvning, men derimod ikke en oversættelse, sml. herom ophl. § 37.

Blog, se Weblog

Bluetooth: Standard for trådløs kommunikation mellem IT-komponenter (f.eks. mobiltelefoner, hovedtelefoner, computere, printere, eller PDA'ere). Standarden anvender 2,45

GHz-frekvensbåndet, der kan anvendes uden særlig godkendelse. Ved brug af en sådan teletransmission kan man kommunikere inden for en afstand på mellem 2 og 10 meter mellem de kommunikerende enheder. I første generation af standarden vil overførelseshastigheden være 1 Mbps. For den praktiske IT-anvendelse vil en indarbejdet brug af Bluetooth-standarden kunne blive et farvel til mange af de kabelføringer, der hæmmer den praktiske brug af IT-systemer.

Boilerplate: Kogeplade. Betegnelse for aftalevilkår, der indgår som fast ingrediens i forskellige typer af aftaler, uanset deres indhold. Bestemmelser om misligholdelse, konfliktløsning, lovvalg mv. betegnes undertiden som aftaleretlig "boilerplate language".

BOLERO: Akronym for "**B**ill **O**f **L**ading for **E**u**RO**pe". Oprindelig et projekt, støttet af EU under EUs INFOSEC-program. Projektet tilbyder en fuldstændigt papirløs håndtering af søtransporten. The Bolero User Association har i 1996 indgået aftale med SWIFT, hvorefter SWIFT skal implementere og drive BOLERO-løsningen. Nærmere oplysninger på .boleroltd.com.

Bot: Internet slang for **søgero*bot***.

Browser: **Klient**-program, der er beregnet til at læse WWW-dokumenter fra en Web-server. De fleste browser-programmer er baseret på den standard, der blev skabt ved Mosaic – en freeware applikation udviklet ved det amerikanske National Center for Supercomputer Application (NCSA).

Bruger: Upræcis betegnelse for (1) den fysiske person, der betjener et IT-system (ofte også kaldet operatør) og/eller (2) den fysiske eller juridiske person, der gør brug af et IT-system til et givet formål. I sidstnævnte betydning, som ofte anvendes i IT-kontrakternes sprogbrug, markerer brugeren modparten til "Leverandøren".

Brugergrænseflade: Se **grænseflade**.

BSA: Business Software Alliance. International organisation af programproducenter, der via et netværk af nationale advokat-repræsentanter står for retsforfølgning af ulovlig kopiering verden over.

Buffer: eller bufferlager. Betegnelse for fysisk **lagerenhed** eller område i RAM, der bruges til midlertidig opbevaring af **data**. Et bufferlager kan kompensere for den forskel i behandlingstid, der er mellem to enheder i et IT-system. Bufferlagre kan f.eks. være indbygget i **printere** og skærme med henblik på midlertidig lagring af de data, der udprintes, henholdsvis vises på skærmen.

Bug: Programmeringsfejl (også kaldet "lus") der skaber en uhensigtsmæssighed i et IT-system. Ordet stammer fra computerens tidlige barndom, hvor en hyppig fejltype var forårsaget af små insekter mv., der satte sig fast i maskineriet.

Bulletin Board: Se BBS.

Bundling: Betegnelse for det forhold, at en leverandør kun sælger flere produkter, når de indgår i et samlet hele – i et "bundt" (eng.: *bundle*). Bundling rejser vanskelige konkurrenceretlige spørgsmål. I mange tilfælde vil leverandørens ønske om at bundle flere produkter være konkurrenceskadelig. Ofte vil der dog ikke være en sådan klarhed over, hvad et "produkt" er på IT-området, at det er åbenbart, at der foreligger en retsstridig "bundling".

Bus: Den elektroniske kommunikationskanal i en **computer**, hvorigennem CPU, **lager** og øvrige komponenter udveksler **information** med hinanden, og hvorpå der kan tilsluttes yderligere enheder. En bus har samme centrale funktion for et IT-system som vejnettet har for et transportsystem. Derfor har det stor betydning, hvilke regler der gælder for **transmission** af **data** over bussen, da disse regler bestemmer den **kompatibilitet**, der vil være gældende for de enheder, der skal tilsluttes computeren.

Buzzword: Trylleord. Betegnelse om ord, der anvendes om noget nyt og "smart", ofte uden noget klart kendskab til hvad der nærmere bestemt menes, og undertiden med henblik på at imponere.

Byte: En informationsmængde bestående af et antal bits, der kan indeholde et tegn. En byte er typisk på 8 bit, hvoraf dens betegnelse kommer ("By eight"). Dette danner 256 kombinationsmuligheder (2 i ottende).

Båndbredde: Den mængde information (ofte målt i bits per sekund) som kan transmitteres gennem et datanet. Henvisningen til "bredde" stammer fra tv-området, hvor kapacite-

ten beror på, hvor mange frekvenser der er til rådighed for transmissionen.

CA: Certification Authority. Den instans (eller tjenesteyder) i et **Public Key Krypteringssystem**, der registrerer de offentlige **nøgler**, som anvendes af systemets kommunikerende parter, og som på grundlag af denne registrering efterfølgende erklærer (certificerer), at den offentlige nøgle hører til den pågældende kommunikerende part. I loven om elektroniske signaturer omtales CA som "Nøglecenter".

Cache-memory: Hukommelse, der gør det muligt at lagre information "tæt på brugeren" for dermed at kunne optimere systemets funktionalitet. Alternativet til at "cache" vil ofte være at hente eller bringe de pågældende data fra og til medier, som det måske er forbundet med tid og omkostninger at nå. *Caching* anvendes såvel *internt* i det enkelte system, f.eks. ved at der opbygges mellemlagre på harddisken for at frigøre information for RAM-hukommelsen for derimod at optimere dens funktionalitet som *eksternt*, f.eks. når en Internet-leverandør lagrer information fra hyppigt efterspurgte hjemmesider på sit eget udstyr.

CAD/CAM: Sammenskrivning af de to forkortelser for henholdsvis Computer Aided Design og Computer Aided Manufacturing. Almindeligt anvendt betegnelse for brug af IT til frembringelse af industrielle emner. Ved CAD tegnes emnet på skærmen, og tegningen raffineres og optimeres ved dertil indrettede programfunktionaliteter. CAM-systemerne muliggør en efterfølgende produktion baseret på CAD-tegningerne.

CAFC: Court of Appeals for the Federal Circuit – amerikansk føderal appelret, der bl.a. behandler patentsøgsmål.

CASE: Computer Aided Software Engineering. Betegnelse for teknikker, der er i stand til at udvikle eller vedligeholde et IT-system uden detaljeret programmering. Det særlige ved CASE-værktøjer – sammenlignet med programoversættere mv., der jo også "selv" tilvejebringer et programresultat (objektkoden) – ligger i CASE-værktøjets overtagelse af en række af de strukturelle opgaver, der kan belaste programmeringen (f.eks. konsekvensrettelser, diagramanvendelse etc.).

CCITT: Comité Consultatif International de Téléphonique et Télégraphique – Den Internationale Rådgivende Komité for Telegraf og Telefon. Henhører under den Internationale Telekommunikations Union (ITU), der er hjemmehørende i Genève og beskæftiger sig med teleselskabers internationale standardiseringsarbejde.

CC, se Creative Commons.

CCPA: Court of Customs and Patent Appeals, nu: CAFC (s.d.) – amerikansk føderal appelret, der, inden CAFC kom til, pådømte sager hvor USPTO (s.d.) havde truffet afgørelse.

CCTLD: Country code Top Level Domain. Den del af navnehierarkiet på Internet, der defineres ved de enkelte landebetegnelser, forkortet i henhold til ISO 3166-standarden, f.eks. .dk for Danmark.

CD: Se **Compact Disc**.

CD-I: Compact disc interactive, en kommunikationsstandard foreslået af Philips og Sony med henblik på **interaktiv** præsentation af video-, tekst-, audio- og data-information.

CD-ROM: Se **compact disc**.

CD-TV: Compact Disc TeleVision. Tidligere, og nu forladt, teknologi, der gjorde det muligt at afspille videosekvenser ved hjælp af CD-skiver. Den teknologi, der i dag løser disse problemer, er DVD.

CD-WORM: Compact Disc – Write Once, Read Many. Betegnelse for digitalt lagermedium baseret på den optiske CD-teknologi, og som giver mulighed for at lagre information én gang med henblik på efterfølgende læsninger.

CEC: Commission of the European Communities – EU-kommissionen.

CECUA: Confederation of European Computer User Associations – Sammenslutning af europæiske edb-brugerforeninger. CECUA har bl.a. udsendt et antal standardkontrakter på IT-området.

Celle: Se **regnearksprogram**.

CEN: Comité Européen de Normalisation – Europæisk standardiseringsorganisation bestående af medlemmer fra EU- og EFTA-lande.

CENELEC: Comité Européen de Normalisation Electrotechnique. Den Europæiske Komité for Elektroteknisk Standardisering.

CEPIS: The Council of European Professional Informatics Societies. Europæisk sammenslutning af professionelle IT-foreninger, der

har til formål at koordinere disses synspunkter overfor de europæiske institutioner.

CEPT: Conférence Européenne des Administrations des Postes et des Télécommunications. Den Europæiske Konference af Post- og Teleadministratorer.

CERN: Den Europæiske organisation for nuklearforskning. Fordi "opfinderen" af www-teknologien, *Tim Berners-Lee* var ansat hos CERN, da han udviklede de principper, der siden har været centrale for www-anvendelsen på **Internet** spiller CERN en vis rolle i nettets udvikling.

Certification Authority: Se CA.

Certificere: At udstede **certifikat**.

Certifikat: En erklæring om et produkts, en persons eller en procedures faktiske beskaffenhed, der er udstedt af en uafhængig person eller myndighed, og som tilsigter at skabe tillid til bestemte aspekter af det pågældende produkt mv.

Certifikatudbyder, se CA.

Chat: Slangudtryk for kommunikation, der formidles digitalt og i realtid, f.eks. via en Internet-baseret nyhedsgruppe ("chat-room").

Chip: Populær betegnelse for **halvlederchip**.

CIM: Computer Integrated Manufacturing. Betegnelse for produktionskoncept, hvori processer, der ellers forudsætter menneskelige beslutningsfaktorer, styres af IT.

Clean room-teknik: Fremgangsmåde, som anvendes ved udvikling af program, der ønskes gjort **interoperabelt** med et eksisterende program gennem brug af grænsefladeinformation frembragt ved **dekompilering** eller reverse engineering af det eksisterende program: For at minimere risikoen for påstande om, at den gennemførte reverse engineering går videre end tilladt, afsondres de programudviklere, der skal frembringe det nye program, fuldstændigt fra de medarbejdere, der forestod arbejdet med at **dekompilere**, hvorved deres udviklingsarbejde kan siges at finde sted i et afsondret – "clean" – rum.

Click wrap-aftale: Aftale, der indgås uden parternes samtidige tilstedeværelse, ved at den ene part – f.eks. en forbruger – med et klik på et ikon el.lign. manifesterer sin vilje til at være bundet af vilkår, der optræder i tilknytning til ikonet. Se også **point-and-click-aftale** og **shrink wrap-aftale**.

Client/server-arkitektur: Arkitektur for databehandling, der fordeler opgaverne mellem flere computere, der henholdsvis opfylder rollen som bruger af programmer og data ("klient") og som leverandør heraf ("server"). I dag er det den almindelige regel, at databehandling sker efter dette princip. Når man betjener sig af systemer til elektronisk post udføres en del af databehandlingen via brugerens e-post **klient** (f.eks. installeret på en bærbar computer), medens andre dele af den sker fra den e-post server, der f.eks. drives af en arbejdsgiver og/eller en Internet-leverandør.

COCOM: The Coordinating Committee for Multilateral Export Control; vestligt samarbejdsforum, der tidligere fastlagde regler om eksportkontrol vedrørende udstyr med militær betydning. Nu afløst af Wassenaar-arrangementet af 13. juli 1996.

Compact Disc: – også kaldet CD. Optisk medium til lagring af data i **digital** form. Data fra en CD overføres ved hjælp af en laserstråle, der belyser disken og dermed reflekterer dennes strukturer. Når CD-mediet bruges til lagring af lyd (således som det kendes fra musikverdenen), billede og tekster og dermed anvendes til datalagringsfunktioner, betegnes det ofte som CD-ROM. Se også **DAT.**

Compiler: Oversætterprogram. Program beregnet til **kompilering** (oversættelse) af programmel fra **kildetekst** til **objektkode**.

Computer: (af engelsk: to compute = at beregne). Teknisk indretning, der er i stand til at lagre, sammenligne og beregne data. Med udviklingen af den **digitale** teknik er begrebet i praksis begrænset til **data**, der repræsenteres digitalt. For at kunne udføre de nævnte funktioner må en computer omfatte en centralenhed (også kaldet CPU) og et hertil hørende internt **lager**. Nu om dage er de fleste computere indbygget i **halvlederchips**. I daglig tale henviser begrebet til den overordnede fysiske indbygning af computeren.

Computervirus, se **programvirus**.

Cookie: Generel betegnelse for teknik til registrering af, hvad en **klient** har foretaget sig på en **server**, som finder sted hos klienten. Cookie-teknologi anvendes navnlig i client/server-sammenhænge, hvor detaljer om klientens benyttelse ikke registreres på serve-

ren. Et væsentligt eksempel herpå er benyttelse af www-teknologi, hvor en web-server sørger for, at der på brugerens harddisk gemmes oplysninger om f.eks. e-mailadresse, identitetsoplysninger, foretrukket sprog eller andre præferencer, med henblik på næste benyttelse af web-serveren. Når brugeren (klienten) kobler sig op på serveren næste gang spares der transmissionstid til udveksling af disse oplysninger, ligesom serveren uden en ny registreringsprocedure kan verificere, at der er tale om en berettiget bruger. I www-anvendelse er cookie-teknologien udviklet af det amerikanske firma Netscape til HTTP/1.0-protokollen og med det formål at gøre den ellers tilstandsløse http-kommunikation fleksibel overfor brugerens krav.

Copyleft: Almindelig betegnelse for en licenstype, der gør det muligt at genbruge værker af forskellig slags, herunder litteratur, programmel og kunst. Hvor ophavsretten (the copy*right*) tjener til at begrænse udbredelsen af et værk går copy*left*-tanken i modsat retning: Gennem en copyleft-licens forpligter den person, der bearbejder et værk, sig til at give almenheden adgang til at lade disse bearbejdninger genudgive og viderebearbejdes af andre. Der er flere metoder til at opnå en sådan "copylefting". Et udbredt eksempel herpå er GNU-GPL (s.d.).

CP: Certification Policy. Et regelsæt fastsat af en certifikatudbyder (CA), og som angiver, hvorledes et certifikat skal anvendes samt, hvilke sikkerhedsmæssige egenskaber det besidder. Se også CPS.

CPS: Et regelsæt fastsat af en certifikatudbyder (CA), som angiver, hvilke procedurer CA'en gennemfører i forbindelse med udstedelsen af et certifikat.

CPU: Central Processing Unit. Den centrale del af et IT-system, hvor systemets data behandles i overensstemmelse med en række indlæste **programmer**.

Cracker: Ofte anvendt betegnelse for en person, der bryder en kopibeskyttelse, f.eks. på et spil eller et edb-program.

Creative Commons: Betegnelse for en amerikansk privat organisation, der blev stiftet i 2001 under deltagelse af blandt andre den amerikanske juraprofessor Lawrence Lessig med det formål at skabe et sæt alment accepterede licensvilkår, der gør det muligt at genbruge værker, der har været offentliggjort på nettet. Første version af de licenser, der udgør kernen i projektet, blev udsendt den 16. december 2002, men siden er kommet senere ændringer til. Selv om CC-licenserne er konciperet på baggrund af amerikansk ret og amerikansk juridisk terminologi, har bevægelsen oplevet en betydelig international bevågenhed. Blandt andet kan nogle af de mest udbredte søgemaskiner begrænse søgninger efter information (og værker), der på forhånd er genstand for en cc-licens.

Cursor: En elektronisk pegepind (markør) på et skærmbillede. Kan enten flyttes ved "piletaster" på et **tastatur** eller med en **mus**.

Cyberspace: Populær betegnelse for den oplevelse af computeren som et "rum", der f.eks. mærkes ved brugen af visse spil og ved kommunikation over og søgninger i det verdensomspændende **Internet**. Betegnelsen blev første gang foreslået af den amerikanske science fiction-forfatter *William Gibson*, der fik inspirationen til det efter at have iagttaget børn i en spillearkade. Præfikset "cyber" stammer fra "cybernetics", se **kybernetik**.

DA: Dansk Arbejdsgiverforening.

DAB: Digital Audio Broadcasting. Metode til at transmittere lyd i digital form. Lyden kan dermed transmitteres uden kvalitetstab, men teknikken kan kun anvendes på frekvensbånd, hvor der ikke er for stor afstand mellem afsender og modtager.

Dankort: Betegnelse for det betalingskort, der blev indført af danske pengeinstitutter i 1983. Kan anvendes i såvel ATM-automater som POS-automater.

Danmønt: Småpengekort udviklet af danske pengeinstitutter i samarbejde med enkelte større betalingsmodtagere.

Dansk Dataforening: Forening stiftet i 1958 med det formål at udbrede kendskabet til informations-teknologien og dens anvendelse, at fremme anvendelsen af IT til gavn for samfundet og den enkelte bruger af teknologien og at samle IT-brugere, IT-professionelle og IT-interesserede om disse opgaver. I 2001 har foreningen godt 5.000 medlemmer.

Dansk Internet Forum: Forkortet DIFO. Forening stiftet i 1999 af en kreds af organisationer og virksomheder med interesse for Inter-

nets udvikling i Danmark. DIFO er et eksempel på selvregulering inden for den del af Internet-aktiviteterne, der styres og kontrolleres af **DK-hostmaster**-funktionen. Ifølge vedtægterne for DIFO kan DIFO etablere eller være deltager i et paritetisk klagenævn for Internet i Danmark: Klagenævnet for Domænenavne.

Dansk Standard: Selvejende institution under Erhvervsfremmestyrelsen, der understøtter udvikling af danske standarder og deltagelse i det internationale standardiseringsarbejde.

DAT: Digital Audio Tape. Magnetbånd, der anvendes til lagring af **data**, der er repræsenteret **digitalt**. Dataene lagres ved elektromagnetisme, men repræsenteres på samme måde som på en **compact disc**. Et DAT-bånd kan derfor både anvendes til lagring af tekster, lyd og billeder.

Data: Af latin: datum, dvs. noget givet. Betegnelse for **tegn**, der er beregnet til overførelse af **information** efter et særligt regelsæt (format).

Data mining: Nutidigt udtryk for den maskinelle bearbejdning af en database, der sker med henblik på at uddrage adfærdsmønstre eller andre sammenhænge af datamaterialet, som ellers ikke ligger lige for, f.eks. med henblik på direkte markedsføring. Den bruger, der ønsker at "data mine" et datamateriale, er nødt til at definere en række faktorer, som datamaterialet herefter undersøges for, f.eks. indkomstforhold og forbrugsmønstre i en kundedatabase.

Data warehouse: Oprindeligt udtryk for en database med informationer, der er indsamlet over en længere periode, og som anvendes til **data mining**. Udtrykket anvendes også om et system til effektiv lagring og anvendelse af data, hvorved den enkelte PC-bruger kan trække de samme data fra en central server, men i et format, der svarer til det enkelte behov.

Database: En organiseret mængde af **data**, der er konstrueret således, at data kan fremkaldes efter brugerens nærmere instruktioner. Dette sker gennem brug af en dertil indrettet **applikation** (et såkaldt database management system også kaldet DBMS).

Databehandling: Se **edb**.

Datafangst: Betegnelse for den situation, hvor et IT-system modtager **data**.

Datamat: Ældre synonym for **computer**.

Datamatik: Læren om automatiseret behandling af **data**, dvs. – i praksis – IT-videnskab.

Datanet: (1): Betegnelse for de offentlige ledningsnet, der står til rådighed for offentlig datakommunikation. (2): Se **netværk**.

Datasikkerhed, se IT-sikkerhed.

DBMS: Databasemanagementsystem. **Systemprogrammel** til at organisere, styre og lagre komplekse mængder af **data**.

DBS: Direct Broadcasting via Satellite. Ny teknologi, der gør det muligt for forbrugere at modtage tv-programmer fra en parabolantenne på størrelse med en pizza, der låses fast på en bestemt satellit. Signalet fra denne satellit er digitaliseret og reduceret ved såkaldt **komprimering**. Ved hjælp af et apparat, der er monteret i tilknytning til tv-apparatet, dekoder forbrugeren herefter tv-signalet, så det passer til hans tv-apparat.

DCS-1800: System til mobiltelefoni, der er baseret på GSM-standarderne, men som anvender 1800 Megahertz frekvensbåndet. Kapaciteten i DCS-systemet er dobbelt så høj som i GSM-systemet. Til gengæld er rækkevidden kun den halve, hvorfor brugeren må være tættere på sendestationerne ("cellerne").

DECT: Digital European Cordless Telecommunications. Fælleseuropæisk standard for trådløs digital kommunikation over korte afstande, f.eks. inden for en virksomhed. Standarden tager sigte på, at en DECT-terminal (f.eks. en lommetelefon) kommunikerer med en basisstation, der er forbundet med det almindelige faste telefonnet. DECT har en høj kapacitet (dvs. giver mulighed for intensiv dataoverførelse), men kun en begrænset rækkevidde, typisk på under 200 m. Standarden er derfor mest velegnet som grundlag for lokaltelefoni i virksomheder eller som grundlag for "fællestelefon" i boligejendomme.

Dekompilering: Betegnelse for en proces, der til dels indebærer det modsatte af en **oversættelse**; gennem studier af **objektkodens** bestanddele beregner man sig frem til, hvilken struktur **kildeteksten** må antages at have haft. Dekompilering er reguleret ved artikel 6 i Rådsdirektivet om retlig beskyttelse af edb-programmer.

DES: Data Encryption Standard. Krypteringsalgoritme, der blev udviklet af IBM i 1974. DES er en offentlig algoritme, der er offentliggjort som NIST-standard. Man opdeler meddelelsen i blokke på hver 64 bits, der i overensstemmelse med algoritmen erstattes med 64 andre bits. Sikkerheden ved at bruge den beror altså ikke på, at algoritmen holdes hemmelig, men derimod på indholdet af den kode, kaldet **nøgle**, som anvendes til at aktivere den. DES bygger på symmetrisk kryptering, men anvendes ofte i samspil med en asymmetrisk krypteringsalgoritme, f.eks. således at selve teksten krypteres under DES, hvorefter den anvendte DES-nøgle krypteres under en langt mere ressourcekrævende asymmetrisk krypteringsalgoritme, f.eks. **RSA**.

Desktop: Almindelig betegnelse for computer, der står på bordet, f.eks. en stationær PC. Udtrykket bruges ofte som modsætning til **laptop**, hvor billedet er, at computeren befinder sig i brugerens skød (lap).

DIF: Dansk Ingeniørforening.

DIFO: Dansk Internet Forum, s.d.

Digital datarepræsentation: Betegnelse for **data**, repræsenteret ved tal. Ved digital datarepræsentation er informationen altid knyttet til en kendt talstørrelse. Se også **analog datarepræsentation**.

Digital meddelelse: Meddelelse, hvis informationsindhold er repræsenteret ved digital teknik, dvs. ved brug af nuller og éttaller.

Digital signatur: En talværdi (numerisk værdi), der fastlægges på grundlag af en meddelelse i digital form og i overensstemmelse med en procedure (**algoritme**), som gør det muligt entydigt at verificere, at talværdien er udvirket på grundlag af den digitale meddelelse og med den private krypteringsnøgle i et nøglepar. Teknikken betjener sig af public key-**kryptering**. Den numeriske værdi fastlægges ved hjælp af afgiverens *hemmelige* **nøgle**. Hvis modtageren kan verificere den numeriske værdi ved hjælp af afgiverens *offentlige* nøgle, kan han slutte, at meddelelsen må stamme fra afgiveren (se **autenticitet**), og at den ikke siden afgivelsen er blevet ændret (se **integritet**). Det store praktiske problem med systemer til **digital signatur** er sikkerheden for, at det virkelig er afgiveren, der står bag det anvendte nøglepar. Til at sikre dette anvender man en certificeringsinstans (også kaldet CA), der med sit certifikat om afsenderens identitet mv. tilvejebringer denne sikkerhed. Se også **elektronisk signatur**.

Disk: **Lager**-medium baseret på roterende magnetisk skive. Omfatter bl.a. diskette og harddisk.

Diskette: Se disk.

Display: Betegnelse for en skærm eller et panel – f.eks. på en PC, en telefon, et ur eller en personsøger – der kan vise **data** i en eller anden form.

Distancearbejde: Arbejde som en person (være sig ansat eller selvstændig) udelukkende eller for en væsentlig del af sin tid udfører på et sted, der ikke har karakter af en traditionel arbejdsplads for en arbejdsgiver eller klient, og hvor brugen af telekommunikation og avanceret IT indgår som en væsentlig del af arbejdets udførelse.

DivX: Format til komprimering af film, som i dag ofte anvendes til en (ofte ophavsretsstridig) komprimering af spillefilm på Internet. Ved hjælp af formatet kan en film lægges ned på en enkelt CD i en kvalitet, der er bedre end kendt fra det almindelige VHS-format. Formatet har også lovlige anvendelsesformer, f.eks. som grundlag for hjemmevideo.

DK-Hostmaster, se **hostmaster**.

DNS: Domain Name Service. Betegnelse for en databasetjeneste, der til brug for den løbende Internet-kommunikation afgiver information om, hvilke computere der står bag hvilke **domænenavne** på **Internet**. DNS-servere findes på forskellige niveauer i Internet-hierarkiet. På øverste, internationale niveau findes der 13 DNS-servere, hvoraf den nærmeste er placeret i Stockholm. På trinnet lavere – dvs. toplevel-domæneniveauet (f.eks. .dk) – findes der et antal DNS-servere, for Danmarks vedkommende i alt 6. Disse DNS-servere peger videre på de enkelte Internet-leverandørers DNS-servere. Hver DNS-server afgiver enten de pågældende oplysninger selv eller foranstalter kontakt til de DNS-servere, der tilhører den pågældende Internet-leverandør. Uden DNS-tjenesten ville det være umuligt at kommunikere på nettet (da man i så fald ikke ville kende adresserne på de computere, der skulle kommunikeres til).

Dokumentation: Sprogligt nedfældet beskrivelse af en **funktion** eller egenskab. Det kan være både hensigtsmæssigt og nødvendigt at "dokumentere" funktioner, der er komplekse eller forgængelige. Således er en programdokumentation nødvendig både for den, der benytter et **edb-program**, og for den, der udvikler eller vedligeholder det. Dernæst kan det være af værdi at dokumentere (i betydningen rapportere) et forløb, om hvilket der efterfølgende kan tænkes at opstå bevistvivl. Se også **logning**.

Domæne: Teleteknisk adresse for en del af Internets navnerum (f.eks. "www.ku.dk"), der gør det muligt for andre Internet-brugere at finde frem til den bestemte severe (f.eks. til www-kommunikation eller elektronisk post). I det angivne eksempel er toplevel-domænet "dk" for Danmark og secondlevel-domænet "ku" for Københavns Universitet.

Domænenavn: Det navn (udtrykt i bogstaver fra A til Z og/eller tallene fra 0 til 9 med mulighed for adskillelse med bindestreg(er) og med et karakterantal fra 1 til og med 63), der i henhold til registrering i en central instans forbindes med en IP-adresse. Domænenavnet vælges af den person, der under den pågældende IP-adresse knytter en computer (server) til nettet og udformes derfor typisk på en måde, der associerer med vedkommende – f.eks. som personnavn, firma eller forkortelse. Af samme grund knytter der sig en betydelig markedsføringsmæssig interesse til at erhverve sådanne navne. Domænenavne optræder i vekslende niveauer på Internets navnehierarki. Øverst som topleveldomæner (f.eks. .dk eller .com). I almindelig tale refererer begrebet "domænenavn" almindeligvis til de såkaldte andenordens-domænenavne (f.eks. ku.dk).

Dongle (også kaldet hardware-nøgle): Lille hardware-anordning, der anvendes til kopibeskyttelse. Donglen fremtræder som en lille hardware-komponent med en indbygget halvlederchip, der ved at blive indsat i det udstyr, hvorfra et hertil hørende informationsprodukt kan anvendes lovligt, afgiver de nødvendige koder for at få produktet til at fungere. Donglen tilsluttes typisk en ledig port i det pågældende udstyr, f.eks. printerporten. Dongles anses for at udgøre det mest sikre middel mod kopibeskyttelse – omend også det mest besværlige. Derfor anvendes denne teknik primært til mere kostbare programpakker.

DOS: Disk Operating System. Navnet på et tidligere **styresystem**, der bl.a. anvendtes i IBM's PC samt PC'er, der tilsigter at opnå **kompatibilitet** hermed.

DoS-angreb: Denial of Service-angreb. Hærværkslignende angreb mod Internet-baserede servere. Angrebet sker ved, at gerningsmanden programmerer et antal computere, som han ofte vil have opnået kontrol over på retsstridig vis, til at sende et stort antal indholdsløse **requests** til offerets web-server, der som følge heraf overbelastes og går ned.

Downloading: Levering af digitale data ved kopiering fra afsenderens medium, f.eks. en hjemmeside på Internet. Downloading af en fil vil således indebære levering af en digital ydelse. I modsætning til uploading er det karakteristisk for downloading, at dataoverførelsen udvirkes af modtageren.

Driftssystem: Se **styresystem**.

Driver: (Udtales på engelsk). Også kaldet drivprogram. Betegnelse for **systemprogrammel**, der styrer **grænseflade** og **kommunikation** til computerens ydre enheder, f.eks. printer eller skærm.

Drop dead-anordning: Program, hvis funktion det er at fratage et system dets arbejdsevne, f.eks. for det tilfælde, at visse kontraktsbetingelser ikke opfyldes. Anvendelse af drop dead-anordninger må understøttes af kontraktsvilkår, der ledsages med en klar vejledning om, hvilke faktiske handlinger – f.eks. indtasting af en kode, der udleveres af leverandøren – der imødegår anvendelsen af anordningen, hvis ikke de skal føre til ansvar for leverandøren.

DS: 1. Forkortelse for standardiseringsorganisationen Dansk Standard. 2. Ofte anvendt forkortelse for **Digital Signatur**.

DTV: Digital Television. Metode til transmission af TV-signaler i digital form. Hvis DTV anvendes i kombination med teknikker til **komprimering**, kan der gives plads til 10 kanaler, hvor der i analog form kun er plads til en.

Dum terminal: Betegnelse for IT-terminal, der ikke er indrettet til at udføre selvstændig be-

handling af **data**, men som alene virker som enhed til præsentation og **transmission** til et andet – intelligent – system, hvor databehandlingen foregår. Se også **intelligens**.

DVA: Dansk Varekode Administration. En privat forening dannet af 7 erhvervsorganisationer og del-foreninger med henblik på administration af **EAN**-stregkoder i Danmark.

DVD: Oprindelig forkortelse for Digital Video Disk, men nu for Digital Versatile Disc (versatile = alsidig). Standard, der oprindelig tog sigte på at skulle understøtte lagring af videoinformation på en CD, men som på grund af dette mediums ringe udbredelse på videoområdet nu er konstrueret til at kunne håndtere enhver form for information på CD-mediet med det sigte, at DVD'en med tiden kommer til at erstatte video- og lydbånd, CD'er mv. Ved at anvende nye teknikker til **komprimering**, flere spor på skiven og en anden lagringsmetode (såvel et "reflektivt" lag, som et "semitransmitterende") kan man på en DVD lagre op til 12 gange så megen information som på en CD, bl.a. ved at anvende begge skivens sider. DVD, der understøttes af den internationale plade-, film- og IT-industri, blev lanceret i januar 1997 og foreligger i forskellige sub-standarder med forskellig lagerkapacitet og hertil hørende typisk informationstype, f.eks. DVD-Video (for film mv. lagret under MPEG2-standarden) og DVD-ROM (for data). Den oprindelige standard understøtter lagring af op til 4,7 Gigabytes data. En senere standard (DVD-RAM), der understøtter gentagen lagring af data, vil kun have en kapacitet på 2,6 Gigabytes. Lagerkapaciteten for den såkaldte DVD-R, der vil give mulighed for lagring af data én gang, vil være på 3,95 Gigabytes. For at hindre ulovlig kopiering af den ophavsretligt beskyttede information på DVD'er er den indlagte information **krypteret** under en særlig algoritme (CSS-algoritmen), som således skal være implementeret for afspilningsudstyret under anvendelse af en såkaldt hovednøgle.

DVI: Digital Video Interactive. Varemærke registreret for den amerikanske chip-producent Intel Inc.

EAN: European Article Numbering Association. En forening, der beskæftiger sig med **standarder** for stregkoder. Omfatter i dag ca. 45 medlemslande.

ECE: [United Nations] Economic Commission for Europe.

Edb: Forkortelse for elektronisk databehandling, dvs. behandling af **digitalt** repræsenterede **data** ved hjælp af **processorer** og elektroniske **lager**medier. Da edb i dag anvendes som et begreb snarere end som en forkortelse, er det mest korrekt at skrive det med små bogstaver. Begrebet er dog efterhånden afløst af det bredere IT.

Edb-program: En række af instruktioner ("koder") til en **processor**, der under forudsætning af et korrekt samspil med andre programmer, regne- og lagerenheder mv. sætter processoren i stand til at behandle en given type **data**.

Edb-sikkerhed: Se IT-sikkerhed.

Edb-system, se IT-system.

Edb-terminal: Ordet terminal markerer afslutningen på et **system**. Anvendes oftest om de ydre enheder af et IT-system, der vil sætte en bruger i stand til at kommunikere med systemet. Begrebet omfatter dermed arbejdspladsterminaler ligefuldt som Dankort-terminaler.

Edb-virus: Se **programvirus**.

EDEL: Svensk aftaleformular for IT-overdragelser, udsendt af Föreningen Svensk Programvaruindustri.

EDI: Electronic Data Interchange. Direkte oversat: elektronisk data-udveksling. Oversættelsen er dog ikke betegnende. Det centrale ved den udveksling af **data**, der sker ved EDI, er, at data, der ellers er beregnet til at blive læst af mennesker (f.eks. fakturaer, bestillinger, mv.), læses af et modtagende IT-system, der initierer en **kommunikativ** proces svarende til deres indhold; fakturaen bogføres automatisk, købsordren effektuerer automatisk en produktionsgang etc. Dette forudsætter, at de pågældende data er struktureret i nøje overensstemmelse med **standarder** for såvel indhold som struktur, og arbejdet med at udvikle EDI består da også primært i at vedtage og implementere disse standarder. EDI-konceptet tager i første række sigte på den information, der udveksles i forretningsmæssige samkvem (f.eks. faktureringer, aftaler, bekræftelser etc.), men der er principielt intet

til hinder for, at EDI-løsningerne også kan gøre deres indtog inden for den private sfære.

EDIA: Electronic Data Interchange Association. Britisk EDI-sammenslutning, der bl.a. har markeret sig ved at udgive en standard kommunikationsaftale.

EDIFACT: Forkortelse for Electronic Document Interchange for Administration, Commerce and Transport. Serie af **standard**er, der understøtter elektronisk udveksling af handelsdokumenter ved EDI. EDIFACT blev foreslået i april 1987, og opnåede allerede i september s.å. enstemmig vedtagelse som ISO 9735. Nogle af EDIFACT-standarderne, der knytter sig til 6. og 7. lag i OSI-referencemodellen, fastslår bl.a. retningslinjer for strukturering af brugerens data og tilknyttede servicedata i et åbent EDI-system. Det må ventes, at brugen af EDIFACT-standarder i de kommende år vil blive meget udbredt, ikke blot inden for **elektronisk handel**, men også i relation til udveksling af oplysninger i digital form med offentlige myndigheder.

e-handel: Se **elektronisk handel**.

e-handelsdirektivet: Direktiv 2000/31/EF om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked, EFT 2000 L 178/1.

Ekspertsystem: Almindeligt udbredt betegnelse for **system**, der på grundlag af avancerede programmer og information udfører beslutninger eller danner grundlag for at udføre beslutninger ved at simulere de overvejelser og handlingsvalg, som en ekspert ville træffe i en given situation. Grundlaget for ekspertsystemets beslutninger mv. er en vis viden, hvorfor sådanne systemer ofte også betegnes "videnbaserede systemer".

Elektronisk handel: Eller "e-handel". Eng.: Electronic Commerce. Samlebetegnelse for anvendelse af digital teknologi ved indgåelse af aftaler, betaling samt levering af ydelser. Begrebet er ikke afgrænset til den kommercielle sfære, men omfatter også private forbrugeres anvendelse af digital teknologi til de nævnte formål. Begrebet udsondres undertiden. For det første sondres ofte mellem direkte e-handel, hvor både aftaleindgåelse og -opfyldelse sker digitalt, og indirekte e-handel, hvor kun aftaleindgåelsen sker digitalt (f.eks. fra en hjemmeside), medens opfyldelsen sker konventionelt (f.eks. ved, at den købte bog leveres med posten). Ligeledes sondres mellem *business-to-business*-e-handel (også kaldet "B2B"-e-handel), hvor begge parter er erhvervsdrivende, og *business-to-consumer*-e-handel ("B2C"-e-handel), hvor den ene part er forbruger. Undertiden betragtes kommunikation mellem borgere og myndigheder (*consumer-to-administration*) og mellem erhvervsdrivende og myndigheder (*business-to-administration*) også som omfattet af begrebet e-handel.

Elektronisk post: Betegnelse for enhver form for elektronisk overførsel af data mellem **elektroniske postkasser**.

Elektronisk postkasse: En facilitet, hvorved en telekommunikations-bruger kan placere sine **filer** ("pakker") på en "adresse", f.eks. hos en tredjepart (netværksleverandør), hos hvem adressaten for de pågældende pakker herefter kan hentes. Elektronisk post understøttes bl.a. af CCITT-standarden X.400.

Elektronisk signatur: Enhver fremgangsmåde til signering af meddelelser, der er egnet til at sikre meddelelsens **autenticitet** og **integritet**. Et praktisk vigtigt eksempel herpå er en **digital signatur**, s.d. En elektronisk signatur, der ikke også er en digital signatur, kan f.eks. afgives ved brug af en metode, der identificerer biologiske forhold ved afgiveren, f.eks. ved at lade ham tiltræde meddelelsen ved brug af biometriske teknikker (f.eks. genkendelse af stemme, fingeraftryk eller iris).

Elektroniske penge: Almindelig betegnelse for den elektroniske registrering af en værdi, der kan anvendes bredt til betaling, men som ikke er knyttet til en individualiseret konto, f.eks. **Danmønt**.

e-mail: Se **elektronisk post**.

EN: Europäische Norm, dvs. Europæisk Standard. Betegnelse for standard, der er blevet godkendt efter vedtægterne i et standardiseringsorgan, som EU har indgået aftale med (f.eks. CEN og CENELEC).

Enkeltbrugerlicens: Licens til et edb-program, giver brugeren ret til selv at anvende programmet. Er andet ikke aftalt, vil enkeltbrugerlicensen være afgrænset i overensstemmelse med bestemmelsen i ophl. § 36, stk. 1, nr. 1 ("den legale programlicens").

ENV: Europäische Norm für Versuchungsweise Anwendung. Betegnelse for foreløbig Europæisk Standard (EN).

e-post: Se **elektronisk post**.

EPK: Den Europæiske Patentkonvention.

EPO: European Patent Office.

EPROM: Erasable Programmable Read Only Memory. **Lager**-enhed beregnet til opbevaring af **data**, der alene kan ændres ved hjælp af særligt udstyr (ultraviolet lyspåvirkning), hvorved dataene (f.eks. **programmer** og **databaser**) "brændes" ind i lagerenheden eller lagres permanent ad elektronisk vej (EEPROM, Electronically EPROM).

ERMES: European Radio MEssaging System. Ny standard for personsøgning, udviklet af ETSI og understøttet ved rådsdirektiv 90/544/EØF, der etablerer et harmoniseret frekvensbånd for dette net. Når ERMES er udbygget, vil det tillade overførelse af såvel tal, bogstaver som lydsignaler til personsøge-terminaler i hele Europa.

ERP: Enterprise Resource Planning. Moderne betegnelse for administrative IT-systemer, der systematiserer og nyttiggør de data, der indgår i virksomhedens administrative funktioner, f.eks. regnskabs-, løn- og kundedatabaser. Tidligere anvendte betegnelser herfor er ADB (Administrativ Data Behandling) og administrativ edb.

Escrow-løsning: Løsning på et kontrolproblem, der består i, at det kontrollerede deponeres hos en troværdig tredjepart (se **TTP**), idet begge parter har tillid til at den pågældende tredjepart kun vil frigive det deponerede under særskilt angivne og anerkendte betingelser. I IT-retten drøftes ofte to former for escrow, key escrow (se **nøgledeponering**) og source code escrow (se **kildetekstdeponering**).

ESF: Edb-systemleverandørernes forening – nu en del af IT-brancheforeningen.

ESPRIT: European Strategic Programme for Research and development in Information Technology.

ETSI: European Telecommunications Standards Institute. Europæisk institut for standardisering af telekommunikation, oprettet i 1988. ETSI har bl.a. fastsat standarderne for det europæiske digitale telefonsystem GSM, der gradvis er ved at vinde global anerkendelse. Blandt det standardiseringsarbejde, ETSI foreståar i dag, er udviklingen af standarder for elektronisk signatur, herunder signaturgenereringssystemer (*smartcards* mv.), se nærmere <http://portal.etsi.org>.

EUREKA: European REsearch Coordination Agency. Europæisk samarbejdsprogram, der under deltagelse af 19 deltagerlande har til hovedformål at styrke det europæiske samarbejde inden for det højteknologiske område.

Extreme Programming: Metode til udvikling af edb-programmel, der ved brug af en række principper for løbende kvalitetskontrol, aftestning og brugerevaluering sikrer kvaliteten af den udviklede kode. Ofte begynder man med små og simple dele af det færdige program, som man derefter aftester og vurderer sammen med brugerne, uden på forhånd at føle sig bundet af en fast plan for udviklingsprocessen. Gradvis vokser projektet sig større og større, idet såvel udvikleren som brugeren bevarer kontrollen med det. Metoden blev i sin tid foreslået af Kent Beck, Ward Cunningham og Ron Jeffries i en bog (med samme titel) fra 1999 (2. udg., 2005). Blandt de grundlæggende værdier, forfatterne fremlagde som bærende for denne form for programmering, er kommunikation, simpelhed, feedback, mod og respekt. Extreme programming, kan anskues som et eksempel på Agil Programudvikling (s.d.).

EØS: Det Europæiske Økonomiske Samarbejdsområde.

Facility Management, se **FM**.

FAT: File Allocation Table, dvs. filfordelingstabel. Tabel, der findes på et lagermedium, og som rummer **information** om, hvilke **filer** der findes på det pågældende **medium**.

FDS: Forum for Digital Signatur. Initiativ under Dansk Standard, hvor virksomheder, myndigheder og organisationer med interesse for den praktiske implementering af teknologier til digital signatur i Danmark, mødes for at drøfte tekniske, herunder implementeringsmæssige, anliggender vedrørende digital signatur af fælles interesse. FDS blev oprindeligt etableret som et underudvalg til udvalg S142u27 under Dansk Standard.

Fil: Mængde af **data**, som logisk har noget at gøre med hinanden, og som derfor håndteres som en enhed.

FIL: Foreningen af Internet Leverandører. Dansk sammenslutning af Internet-leverandører.

Filoverførsel: Også kaldet filtransport, eng.: file transfer. Overførsel af **fil** fra en del af et IT-system til et andet eller fra et IT-system til et andet.

Firewall: Computer, der fungerer som barriere mellem et internt net og omverdenen ved at kontrollere mulighederne for at sende informationer fra og til det interne net. Der findes forskellige former for firewalls. De hyppigst anvendte er *filtrerende gateways* (der undersøger de kommunikerende IP-adresser i overensstemmelse med regler fastsat på forhånd), *applikations-gateways* (der kontrollerer enkelte former for kommunikation (e-post, FTP-overførelser etc. og sikrer, at den afvikles som planlagt) og *proxy-servere* (der fungerer som egentligt mellemled ved at identificere og autorisere de enkelte kommunikationstyper fra og til det interne net, eventuelt ved brug af kryptering).

Firmware: Betegnelse for **hardware**, der indeholder **edb-programmer** og **data**, som ikke kan ændres under en sædvanlig brugeranvendelse.

Fjerdegenerationsprogrammel: **Program**-værktøj til udvikling af **applikationer**. Kendetegnet ved, at programmøren kan nøjes med færre programinstruktioner sammenlignet med andre udviklingsapplikationer. Der er ingen absolut grænse mellem fjerdegenerationsprogrammering og anden programmering i **højniveausprog**.

Fleksibel information: Information, som kendetegnes ved ubesværet at kunne fæstne sig på medier af enhver art, f.eks. et forretningskoncept, der kan formuleres mundtligt, nedfældes på skrift eller udøves i praksis.

Flerbrugerlicens: Licens til et edb-program, der giver flere brugere ret til at anvende programmet, enten samtidigt eller forskudt. Er der tale om licens til samtidig brug vil licensen ofte være maksimeret, således at programmet ikke kan anvendes af mere end et bestemt antal brugere, uanset disses identitet. Flerbrugerlicenser anvendes typisk af virksomheder med op til 50 ansatte.

FLOP: Floating Point Operation – betegnelse for en regneoperation, f.eks. en addition, subtraktion, division eller multiplikation, som finder sted i en **processor**. En FLOP – og **Megaflop** (s.d.) er den grundlæggende bestanddel – og måleparameter – for alle edb-beregninger og ækvivalerer for såvidt begreberne bit og byte, der er tilsvarende grundbestanddele for informationsmængder.

Flow-chart: Grafisk afbildning af de funktioner eller datastrømme, der finder sted i et IT-system. Flow-charts kan hjælpe overblikket over et system under udviklingsprocessen.

FM: Facility Management. Drift af IT-system ved ekstern leverandør. At mange virksomheder i dag vælger FM skyldes bl.a. IT-systemernes stadigt mere vigtige rolle for mange virksomheder og den heraf følgende nødvendighed af, at ledelsen befatter sig med vanskelige og teknisk prægede IT-spørgsmål, som f.eks. valg af maskinplatform mv. I lyset af disse vanskeligheder og af de stadigt lavere omkostninger ved at skulle drive IT-systemet ved FM, vælger mange virksomheder denne løsning, f.eks. ved beslutning om **outsourcing**.

FN: De Forenede Nationer.

Font: Betegnelse for en bestemt udgave af en skrifttype. I IT-systemer vil fonte ofte være defineret **digitalt**, således at det enkelte **tegn** fremtræder som en såkaldt bitmap. I mange printere kan man indlægge fonte og dermed gøre det muligt at skrive forskellige skrifttyper. Sådanne fonte kan dels høre til printere eller tekstbehandlingssystemer, dels kan de erhverves som separate IT-produkter.

Formalsprog: Betegnelse for **sprog**, hvis syntaks og semantiske opbygning kan fastlægges ad matematisk vej og med matematisk præcision. De **programmeringssprog**, der anvendes ved programmering af en computer (f.eks. BASIC, ALGOL, COBOL, C, FORTRAN, Pascal, PROLOG og mange andre) er eksempler på formalsprog. Se også **naturligt sprog**.

Fortrolighed: Hemmeligholdelse. I privatlivssfæren kan ønsket herom have rod i et personligt behov for at have visse oplysninger for sig selv ("privatlivets fred" mv.). På det erhvervsmæssige område kan der være en åbenlys økonomisk interesse i at bevare information som virksomhedens erhvervshemmelighed. En sådan opretholdelse af en for-

trolighedstilstand er i øvrigt afgørende for, om hemmeligheden kan beskyttes i henhold til markedsføringslovens § 12. For offentlige myndigheder gælder der almindelige og specielle regler om tavshedspligt og persondatabeskyttelse – sidstnævnte regelsæt gælder også for private virksomheder mv. Foruden de retsregler, der beskytter interessen i fortrolighed findes der talrige tekniske metoder til at opnå fortrolighed, herunder **adgangskontrol** og **kryptering**.

Frame: I HTML-standarden betegnelsen for en inddeling af en web-side, inden for hvilken der kan foregå en særskilt kommunikation, f.eks. visning af data fra en anden web-side eller animation.

Framing: Ofte anvendt betegnelse for den form for (gen)-brug af data fra en hjemmeside, der sker ved brug af HTML-standarden, se **frame**. Da framing ofte gør det muligt at genanvende disse data i en form og på en måde, som den oprindelige besidder ikke havde tænkt sig, giver framing anledning til særlige immaterialretlige problemer.

Free Software: Programmel, som sættes på markedet med en markering af, at visse immaterialretlige eneretspositioner ikke vil blive gjort gældende. F.eks. kan det være fastsat, at brugere af programmet har ret til at kopiere, ændre og videredistribuere det. At et program markedsføres som "frit" er ikke ensbetydende med, at ophavsretten hertil er opgivet (se hertil Public Domain).

Free Software Foundation: Også kaldet FSF. Amerikansk baseret organisation, der arbejder for udbredelse af *open source*-programmel. FSF beskæftiger sig bl.a. med vedtagelse og tilpasning af de licenser, der i dag ligger til grund for distribution af dette programmel, bl.a. the GNU-GPL (s.d.).

Freeware: Almindeligt brugt betegnelse for programmel, som rettighedshaveren har opgivet enhver ret til, hvorved programmet er gratis ("free").

FSF, se Free Software Foundation.

FSR: Foreningen af Statsautoriserede Revisorer. Da revisionsarbejdet bl.a. indebærer en pligt til at revidere klientens IT-systemer, spiller FSR en rolle for fastlæggelsen af god praksis på dette område. FSR har bl.a. udsendt to revisionsvejledninger om IT-revision, som dets medlemmer har pligt til at følge.

FTP: File Transfer Protocol. Protokol, der anvendes til at transmittere information over Internet.

Funktion: Se **system**.

FWA: Forkortelse for "Fixed Wireless Access". Standard for datakommunikation, der baseres på radiobølger udvekslet mellem fikserede sende- og modtagestationer. En FWA-bruger placerer en boks på sit hus. Boksen er udstyret med en sender, en modtager samt en antenne på størrelse med en madpakke, der peger direkte mod en anden (fikseret) basisstation. Herefter kan de brugere, der hører til huset, deles om transmissionskapaciteten, som for den enkelte bruger kan ligge et sted mellem 256 Kbit/s og 34 Mbit/s. Telestyrelsen udbyder for tiden (2001) FWA-licenser i licitation.

G7: The Group of Great Seven. Forum, hvor verdens syv førende industrinationer (USA, Japan, Canada, Frankrig, UK, Tyskland og Italien) jævnlig mødes for at diskutere spørgsmål af global betydning for dem.

GATT: General Agreement on Tarifs and Trade, se WTO.

GB: Gigabyte(s). Måleenhed for lagerkapacitet. I den oprindelige tekniske betydning udgør måleenheden 1.073.741.824 bytes svarende til 2 opløftet i 30. potens. Siden december 1998 har International Electrotechnical Commission (IEC) dog vedtaget, at GB betyder 1 millard bytes, svarende til angivelsen af meter mv., se http://physics.nist.gov.

Generation: Fordi IT udvikles så hurtigt, kan det være hensigtsmæssigt at systematisere forskellige teknologier efter det tidsforløb, hvori de henholdsvis blev frembragt og implementeret. Hertil ses ordet generation ofte anvendt. Baseret på de anvendte processorteknologier taler man f.eks. om forskellige maskingenerationer (begyndende i 1950'erne og med efterfølgende ca. 10-årige intervaller).

Gigabyte: Se **GB**.

GIGO: "Garbage In, Garbage Out" – En populær talemåde, der markerer den sammenhæng, der er mellem inddata og uddata: Er systemets inddata ikke korrekte, vil dets uddata heller ikke være det.

GII: Global Information Infrastructure, den internationale informations-infrastruktur. Ofte benyttet betegnelse ("**buzzword**") for den sammenkobling af hele verdens informationssystemer, man forsøger at realisere i disse år, og som bl.a. vil indebære en udvidelse og forstærkning af eksisterende netforbindelser (telefonnettet, **Internet** etc.).

GNU: Forkortelse for den cirkulære sætning "Gnu is not Unix". Almindelig betegnelse for en programkerne, som er baseret på **open source**-filosofien, og som sammen med en række tilknyttede programmer (i praksis **Linux**) kan fungere som styresystem. GNU-kernen blev skrevet i 1980'erne af en række personer i UNIX-miljøet med tilknytning til open source-bevægelsen. Den er i dag integreret i Linux-styresystemet.

GNU-GPL: GNU general public license. Alment kendte licensvilkår som oprindeligt knyttedes til GNU-kernen, men som efter at denne kerne blev indbygget i Linux-operativsystemet nu også anvendes som grundlag for distribution af dette system. Vilkårene giver brugeren ret til fri anvendelse af programmet til selvvalgt formål, fri ret til at undersøge programmet, frihed til at kopiere programmet samt sprede kopier af det til tredjeparter – med eller uden betaling – samt frihed til at forbedre programmet og kopiere og sprede eksemplarer af det forbedrede program.

Gnutella: Princip for udveksling af datafiler mellem Internet-brugere baseret på **peer-to-peer**-teknologi. Fra en Gnutella-website henter den bruger, der ønsker at gøre brug af teknologien, et program, der gør det muligt at knytte kontakt til andre Gnutella-brugere (hvis identitet også kan hentes fra Gnutella-websites) med henblik på afgivelse og modtagelse af information. Når den enkelte bruger på grundlag af Gnutella-programmet knytter kontakt med en anden, udvalgt, Gnutella-bruger afgiver han herved en invitation til, at alle andre Gnutella brugere kan anvende en afgrænset del af hans computer til udveksling af information, når computeren er online. Resultatet bliver dermed, at den enkelte Gnutella-bruger "deler filer" med alle andre registrerede Gnutella-brugere, der er online i brugsøjeblikket.

GPRS: General Packet Radio Service. Overbygning på GSM-standarden, der vil gøre det muligt at transmittere data med op til 150 kbit i sekundet, i praksis dog mindre. Samtidig tillader GPRS-standarden brugeren konstant at have en linje åben, således at han kan modtage data (f.eks. e-mails) med det samme de afsendes. GPRS-telefoner og abonnementer kan købes i handlen, men teleselskaberne gør ikke meget ud af at markedsføre denne løsning.

GPS: Global Positioning System. Satellit-baseret system, der bl.a. anvendes til navigering og stedbestemmelse for sø-, luft- og land-trafikken. Grundlaget for et GPS-system er en lille radiomodtager, der kommunikerer med 24 satelliter, som kredser om jorden i en afstand af ca. 22.000 km. i en fast bane. Satellitterne er placeret således, at man kan se fra fem til otte satellitter fra et vilkårligt punkt på jorden, hvor hver satellit passerer over samme sted for hver 24 timer. Ved hjælp af signaler herfra kan man fastsætte radiomodtagerens geografiske placering med ca. 5 meters nøjagtighed. Systemet har hidtil været anvendt til navigation inden for sø- og luftfarten, men anvendes i stigende grad – navnlig fordi tidligere militært begrundede usikkerheder nu er fjernet – også til jordbaseret transport, herunder ved gods- og hyrevognstransport.

Groupware: Programmel, der understøtter gruppearbejde og dermed effektiviserer det arbejde flere personer (kolleger eller samarbejdspartnere) skal udføre i samarbejde, f.eks. ved at strukturere ellers ustruktureret information således, at den enkelte bruger ubesværet kan finde rundt i den, samtidigt med at den til enhver tid er fuldt opdateret.

GRUR: Gewerblicher Rechtsschutz und Urheberrecht. Zeitschrift der Deutschen Vereinigung für gewerblichen Rechtsschutz und Urheberrecht. Tysk ophavsretligt tidsskrift.

Grænseflade: Samlebetegnelse for den **information**, der må udveksles mellem to kommunikerende enheder for at etablere grundlaget for at iværksætte en **kommunikationsproces** mellem disse enheder. Man sondrer sædvanligvis mellem brugergrænseflader og tekniske grænseflader. En teknisk grænseflade defineres bl.a. af de **protokoller**, som

transmitterede bits skal fremtræde i, og som for så vidt "læses" af en teknisk komponent. Et **programs** brugergrænseflade er indbegrebet af den **information**, **brugeren** må være i besiddelse af for at bruge programmet. Hvor en skrivemaskines "brugergrænseflade" består af de enkelte tasters placering, består et IT-systems brugergrænseflade af den måde, de enkelte kommandoer præsenteres på.

GSM: Europæisk standard for digital mobiltelefoni, udviklet af ETSI. Forkortelsen stod oprindelig for Groupe Spéciale Mobile, men da man i takt med systemets udbredelse i resten af verden fandt den europæiske henvisning mindre adækvat, har man i nyere tid ladet forkortelsen referere til Général Système Mobile eller "Global System for Mobile (communication)". GSM-systemet er allerede videreudviklet med det såkaldte DCS-**1800**-system. Herudover planlægges en ny og endnu mere kraftfuld standard, kaldet UMTS, Universal Mobile Telecommunications Services.

GTLD: Generic Top Level Domain. Den del af navnehierarkiet på Internet, der defineres efter generiske – modsat nationale – betegnelser. Det væsentligste eksempel herpå er .com, der oprindeligt alene tog sigte på kommercielle brugere, men som i dag også er navnerum for en række private brugere.

GUI: Graphical User Interface, grafisk brugergrænseflade. Betegnelse for det **sprog** for kommunikation, der sker mellem bruger og IT-system, der kendetegnes ved at anvende visuelle udtryk, f.eks. ikoner, grafer og andre symboler, som brugeren kan genkende uden særlige IT-forudsætninger.

GUIDEC: Forkortelse for en publikation med titlen: General Usage for International Digital Electronic Commerce. Der er tale om en vejledning om praktisk brug af teknikker til digital kommunikation i handelsforhold. Vejledningen er udsendt af ICC og foreligger senest i en 2. udgave fra 2001.

Hacking: Betegnelse for den aktivitet, der består i, at en person ("hackeren") forsøger at skaffe sig uberettiget adgang til et IT-system, som han ingen lovlig adgang har til, ved – typisk via det offentlige telenet – at udnytte sikkerhedsmæssige svagheder i dette system. I mange tilfælde drives hacking som en slags sport, og da hackeren ofte er en yngre, teknisk kyndig person, som ikke i øvrigt har kriminelle vaner, har der været en tendens til at betragte hacking som "drengestreger". Der er imidlertid tale om en strafbar handling, jf. strfl. § 263, stk. 2, og hacking har i visse tilfælde været praktiseret som led i grovere forbrydelser (spionage mv.).

Halvleder: (Eng.: semi-conductor). Materiale (f.eks. silicium), der under givne omstændigheder reagerer forskelligt på elektromagnetisme, og som derfor er velegnet til at håndtere **data** repræsenteret **binært**.

Halvlederprodukt: En komponent bestående af et stort antal transistorer placeret på et mikroskopisk areal. Transistorerne opbygges her gennem en proces, hvor en række materialelag med vekslende ledeevne placeres ovenpå en skive (eng.: "chip") af et halvledermateriale (f.eks. silicium eller germanium). Herved fremkommer en tredimensionel struktur, der også kaldes en **topografi**. En chip er udstyret med ledere (ben), der muliggør **kommunikation** af de **data**, den genererer, til omverdenen.

Handshake: Teknisk betegnelse for den indledende udveksling af tekniske oplysninger, der igangsætter en digital kommunikationsproces, f.eks. overførelse af en telefax eller afsendelse af e-mail. Afsenderapparatet fremsender en besked om, hvilken type udstyr der er tale om, og hvilken type information der ønskes overført. Modtagerapparatet behandler denne besked og kvitterer i givet fald med en besked om, at selve transmissionen af information kan indledes.

Hard copy: Betegnelse for **medium**, hvorpå informationerne er knyttet i bestandig form. Udskrift af tekst på papir, transparent eller film er eksempler på hard copies. Udskrift til skærm eller diskette – der typisk bliver overskrevet – udgør soft copies.

Harddisk: Se disk.

Hardware: Også kaldet maskinel. Betegnelse for de materielle dele af et IT-system. Sondringen mellem hardware og software er ikke altid klar. Det maskinel, der behandler IT-systemets informationer, må nødvendigvis være designet i overensstemmelse med visse grundlæggende principper for **programmering**, ligesom enhver programmering sker

under respekt af de tekniske grænser, der ligger i hardwaren.

Hashværdi: Også kaldet hash-total eller nonsenstotal. En datamængde (bit-streng), der i sig selv ikke rummer nogen **information**, men som besidder den egenskab éntydigt at kunne henføres til en anden datamængde. Hash-værdier kan anvendes bl.a. til at påføre en datamængde såkaldt **digital signatur**, hvilket sker gennem **kryptering**. I stedet for at kryptere en lang digital meddelelse (hvilket tager tid og maskinressourcer) kan man nøjes med at kryptere den kortere hash-værdi og dermed reducere tidsforbruget ved kryptering og **transmission** samt lagerplads. Der findes en række vedtagne standarder for hashværdier, herunder MD2, MD5 og NIST Secure Hash Algorithm.

HDTV: High Definition Television. Højopløsnings-tv. Standard, der er under udarbejdelse, for transmission af højkvalitets tv-signaler. Standarden giver bl.a. mulighed for et tv-billede med højere opløsning (med heraf mulighed for lettere læsbar tekst og billeder) og surround sound.

Hexadecimal: Betegnelse for talværdier, angivet i 16-talssystemet (af græsk hexa = 6), idet tal efter 9 repræsenteres med bogstaverne A, B, C osv. I IT-sammenhæng kan det være nyttigt at benytte dette talsystem, fordi det korresponderer med værdien af den binære værdi 2 multipliceret med sig selv 4 gange. Hexadecimale angivelser benyttes undertiden til at repræsentere kodeværdier, der ellers forekommer i ren binær form. Selv om det ikke er enkelt at overskue en hexadecimal talrække – for en person med de rette forudsætninger! – er det trods alt lettere end at overskue en binær talrække. En styrekode angivet med den binære værdi 00001101 kan hexadecimalt udtrykkes med værdien 0D.

Hjemmeside: Database tilsluttet **Internet**, og som i overensstemmelse med almindeligt udbredte standarder, herunder navnlig HTML-, og http-standarderne, præsenterer sin information i hypertekst-format og i en opsætning, der gør det muligt for brugeren at springe fra en del af hjemmesiden til en anden eller fra en hjemmeside til en anden. Den information, der fremvises på en hjemmeside, vil ofte foreligge i en kombination af grafiske udtryk og tekst. Ved hjælp af **hypertekst**-links på hjemmesiden kan brugeren fra enkelte punkter (fremhævet skrift) springe hen til andre hjemmesider. Der er ingen grænser for, hvilken type information der kan holdes tilgængelig fra en hjemmeside eller for, hvordan denne kan stilles til rådighed for almenheden. Visse hjemmesider tjener rent markedsføringsmæssige formål (reklamer for produkter, omtale af virksomheden mv.). Andre virker som fora for personer med fælles interesser. Og endnu andre, f.eks. hjemmesider, der drives af akademiske institutioner eller offentlige myndigheder, tjener almennyttige formål.

Home banking: IT-system, der giver bankkunder mulighed for via en personlig, hemmelig kode eller andet lignende legitimationsmiddel digitalt at overføre pengebeløb, købe eller sælge valuta eller værdipapir eller foretage andre bankforretninger og -transaktioner, uden at være i personlig kontakt med det pågældende pengeinstitut.

Homepage, se hjemmeside.

Hostmaster: Betegnelse for den virksomhed, der inden for et toplevel-domæne (f.eks. ".dk" eller ".com") står for tildeling af subdomænenavne. I Danmark optræder virksomheden DK-Hostmaster A/S som hostmaster for .dk-domænet. Fra og med efteråret 1999 har DK-Hostmaster A/S været et helejet datterselskab under foreningen **Dansk Internet Forum** og styret af denne. De adresser, som Hostmaster tildeler domænenavne, erhverves fra den pågældende regionale registrator, i Europa RIPE.

Hotfix: Slang for en hurtig – men ikke nødvendigvis optimal – udbedring af en opstået programfejl. Det forekommer hyppigt, at programleverandører søger at afhjælpe mangler ved leveret programmel ved at stille hotfixes til rådighed for kunderne på Internet.

Hotspot: Almindelig betegnelse for område (f.eks. café, hotel eller lufthavnslounge), hvor de tilstedeværende kan koble sig op på Internet via en Wi-Fi-forbindelse. Visse kæder, f.eks. den amerikanske Starbucks-restaurationskæde, er kendt for sine hotspots.

Hukommelse: Ofte anvendt betegnelse for IT-medium, der er beregnet til at lagre data. Et bedre ord er **lager**.

HTML: HyperText Markup Language. Standard for **opmarkering** af hypertekst-dokumenter på World Wide Web. Standarden, der vedligeholdes af www Consortium, foreskriver bl.a. hvorledes font-størrelser, indholdsfortegnelser og linjeskift mv. i disse dokumenter skal fremtræde.

http: HyperText Transfer Protokol. Standard for udveksling af hypertekst-dokumenter på **Internet**. De fleste hjemmesider på World Wide Web kan nås ved hjælp af http-kommunikationsprotokollen, der derfor også er angivet som indledning til adressen, f.eks. "http://www.fsk.dk".

Hypertekst: Tekst struktureret efter kriterier, der ikke nødvendigvis læses lineært. På grundlag af et antal koder, der er lagt ind i teksten på forhånd efter redaktionelle overvejelser kan brugeren springe rundt i teksten som han vil (alt efter, hvad koderne tillader). Hypertekst-applikationer har tidligst været anvendt som grundlag for digitale ordbøger og leksika: Når brugeren befinder sig i et ordbogsopslag på en digital ordbog og ser en henvisning til et andet ord, "klikker" han med sin mus på dette ord, hvorefter den bagved liggende kode bringer ham hen til det sted i ordbogen, hvor det er forklaret.

Hypertekst-link, se **link**.

Hæftelse: Juridisk begreb, der beskriver den måde, hvorpå en pligt kommer til at påhvile den forpligtede, dvs. antage en form, der gør pligten gennemtvingelig over for den pågældende. Hovedreglen er, at man hæfter for sine egne handlinger, hvad enten disse handlinger udmønter sig i løfter (hvorved man selv skaber den retsregel, der giver hjemmel for pligten) eller i skadegørende handlinger (hvorved pligten udspringer af et erstatningsretligt regelsæt, som man ikke selv har skabt). Man kan enten hæfte middelbart, således at hæftelsen først udløses via et middel (f.eks. et særskilt løfte, som afgives efterfølgende, som ved fuldmagt) eller umiddelbart, således at hæftelsen straks indtræder, når en situation indtræffer (f.eks. at selvskyldnerkautionisten ikke betaler).

Højniveausprog: **Programmeringssprog**, som må **oversættes** til **objektkode**, før det kan eksekveres af **computeren**.

IANA: Internet Assigned Numbers Authority. Privat, international organisation, der har ansvar for uddeling af IP-adresser på Internet. IANA blev oprindelig etableret som en privat selvejende institution af en enkeltperson ved University of Southern California, nu afdøde *Jon Postel*, men indgår i dag som en del af ICANN. Det daglige arbejde med uddeling af IP-adresser er delegeret til RIPE NCC, med basis i Amsterdam og ansvar for Europa, InterNIC med basis i Washington D.C. og ansvar for Amerika og APNIC med basis i Tokyo og ansvar for Asien og stillehavsområdet.

IBF: Internet-brancheforeningen. Dansk sammenslutning af Internet-leverandører, som indtil etableringen af DIFO primært varetog interessen for de Internet-leverandører, der uden at være medlemmer af FIL ønskede ret til at oprette domænenavne under .dk-domænet. Se også FIL.

ICANN: The Internet Corporation for Assigned Names and Numbers, se .icann.org. Amerikansk baseret organisation, der styrer fordelingen af toplevel-domænenavne på Internet. ICANN's arbejde er nærmere beskrevet i den internationale vedtagelse, der er nedfældet i dokumenterne RFC 1591 og IPC1.

ICC: International Chamber of Commerce. Det Internationale Handelskammer, med hjemsted i Paris.

ICP: ICANN Policy Document. Dokument udstedt, af ICANN med angivelse af, hvilken politik man agter at følge på et bestemt område – f.eks. tildeling af landedomæner for omstridte territorier.

ICT: Information and Communications Technologies, tidligere benyttet betegnelse, der forudsætter en sondring mellem informationsteknologi (dvs. teknologi til informationsbehandling) og teknologier til overførelse af kommunikation (f.eks. ved hjælp af **Internet**).

IDA: Interchange of Data between Administrations. Ofte anvendt EU-betegnelse for digitale systemer, der sikrer udveksling af data mellem offentlige myndigheder. Electronic Data Interchange between Administrations. Kan for så vidt ses som forvaltningens pendant til handelslivets EDI.

ID-MOU: Se MOU.

IEEE: Institute of Electrical and Electronics Engineers, Inc. Faglig forening for elektroingeniører, hjemmehørende i USA.

IETF: Internet Engineering Task Force. Det organ i Internet Society/ICANN, der fastlægger standarder for **Internet**.

IFIP: International Federation for Information Processing.

IIC: International Review of Industrial Property and Copyright Law. Internationalt orienteret immaterialretligt tidsskrift, udgivet af Max Planck Instituttet i München for international patent-, ophavs- og konkurrenceret.

Indlæsningsenhed: Systemkomponent konstrueret til **datafangst**.

Information: I kommunikationsteoretisk betydning betegnelse for det samlede valg af **tegn**, som en kommunikerende enhed foretager i overensstemmelse med reglerne i et givet **sprog** med henblik på at påvirke en anden enhed, når denne ved at knytte fysisk forbindelse med det anvendte **medium** genskaber de trufne valg og dermed får mulighed for at erkende informationsindholdet. En sådan kommunikationsproces resulterer dermed i en overførelse af **information**, dvs. at informationen genskabes hos modtageren. Se også **data**.

Informationssamfund: Politisk talemåde, der refererer til det forhold, at nutidens samfund beror på information i så vid udstrækning, at rammerne for informationsanvendelsen og opmærksomheden på konsekvenserne heraf, er bragt højt op på den politiske dagsorden. Ethvert samfund er imidlertid et "informationssamfund", eftersom samfundslivet altid vil udspille sig mellem individer, der nødvendigvis må kommunikere med hinanden og dermed overføre information.

"Informationssamfundets tjenester": EU-retlig betegnelse for tjenester, som teleformidles ad elektronisk vej på individuel anmodning, f.eks. ved aftaleindgåelse og -opfyldelse via Internet. Betegnelsen anvendes bl.a. i visse EU-direktiver om standardisering, adgangskontrol (98/84) og elektronisk handel.

INFOSOC-direktivet: Europa-parlamentets og Rådets direktiv 2001/29/EF om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet.

Infrastruktur: Indre opbygning. Ofte anvendt betegnelse for en overordnet systemopbygning, der indbefatter komponenter og forbindelser, der hver for sig udgør omfattende og komplicerede enkeltstående systemer. Begrebet anvendes ofte om den informationsstruktur, der er opbygget i samfundet (man taler i USA om the National Information Infrastructure, eller NII) eller i hele verden (the Global Information Infrastructure, eller GII). Med tanke på de systemer, der understøtter kryptering og digital signatur ved brug af troværdige tredjeparter tales undertiden om offentlig nøgle-infrastruktur (PKI, Public Key Infrastructure).

INSTA: Det INternordiske STAndardiseringssamarbejde.

Integreret information: Information, som for de fleste praktiske formål må anses for uløseligt forbundet med sit medium. F.eks. skruelågets meddelelse til brugeren – i kraft af sin formgivning – om, hvordan flasken åbnes.

Integritet: Den egenskab ved en datamængde, at denne ikke er ændret, uden at dette uden videre kan opdages.

Intel: Amerikansk virksomhed, der har udviklet og produceret hovedparten af de halvlederprocessorer, der er indbygget i PC'er baseret på styresystemerne DOS, **Windows** og OS/2. Intel har i disse udviklingsprojekter arbejdet tæt sammen med først IBM og senere Microsoft. Blandt de mere kendte produkter fra Intel er Pentium-processoren, der i dag er standard-udrustning på mange nye PC'er (eller kloner heraf). Tidligere Intel-produkter (f.eks. 80486-processoren) har båret tal-navne. Denne navngivningspraksis er nu forladt, primært fordi de har været mindre velegnede som varemærker.

Intelligens: Kvalitativ betegnelse for kompleksiteten af en given **databehandling**. En IT-terminal anses som "intelligent", hvis den rummer muligheden for selv at udføre en mængde databehandling. Den tanke, der ligger bag sprogbrugen, går ud på, at systemet i disse tilfælde optræder med noget, der ligner menneskelig tankekraft. Således betegner man undertiden et **program** som "intelligent", hvis det simulerer menneskelig ekspertise eller intuition. Se også **kunstig intelligens**.

Intelligent agent: Program, der er konstrueret til på brugerens vegne at betjene et andet program. Et eksempel herpå er **søgerobotter** på Internet.

Interaktiv: Vekselvirkende. Man taler navnlig om interaktion for at beskrive samspillet mellem flere kommunikerende systemer. Et interaktivt IT-baseret undervisningssystem kendetegnes ved at udføre sine funktioner i konsekvens af en række valg, som brugeren træffer, i modsætning til f.eks. et undervisningssystem, der er baseret på en bog eller et kassettebånd.

Interface: Se **grænseflade**.

Internet: En global samling af datanet, der er i stand til at udveksle data ved hjælp af visse fælles standarder. Dermed kan enhver bruger, der er koblet op på et sådant net, sættes i stand til at kommunikere enhver type af digital information med enhver anden bruger på nettet. Såvel de standarder, som der kommunikeres efter, og hvoraf TCP/IP-standarden er den vigtigste, som de principper, der anvendes for identifikation af de tilsluttede computere, fastlægges af privat baserede, men demokratisk virkende internationale forsamlinger med forankring i **ICANN** og **Internet Society**. Internet Society har officielt defineret Internet som "the global information system that (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communication using the Transmission Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses og makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein."

Internet Society: Forkortet ISOC. Privat forening, der fra et tidligt tidspunkt i Internetudviklingen har haft ansvaret for vedligeholdelse af de **standarder**, der definerer kommunikation på Internet samt uddeling af IP-numre. Sidstnævnte funktion ligger i dag hos IANA, der fungerer i samspil med ICANN.

InterNIC: Internet Network Information Center. Amerikansk organisation, der efter bemyndigelse fra **Internet Society** har ansvar for tildeling af IP-adresser i Amerika.

Interoperabilitet: Den funktionelle sammenkobling og interaktion mellem forskellige komponenter i et IT-system, der gør det muligt for disse dele at arbejde sammen. Interoperabilitet opnås gennem fælles tekniske **grænseflader**, der ofte er genstand for **standarder**.

Intranet: Lokalt datanet som baserer sig på **Internet**-teknologi og Internet-**standarder** (herunder TCP/IP-protokolstandarden), men som ikke er til rådighed for omverdenen. For brugeren ligner virksomhedens Intranet således det velkendte verdensomspændende Internet. Fordelen ved at opbygge et lokalt datanet som et Intranet ligger først og fremmest i muligheden for at udnytte de gældende standarder, der ikke er knyttet til en bestemt type udstyr.

IP-nummer: Det unikke nummer, som Internetprotokollerne anvender til at identificere computere, der befinder sig på nettet. I praksis er IP-nummeret afløst af det mnemotekniske **domænenavn**, f.eks. "cybercity.dk", der med angivelse af mindst to ord, adskilt af punktum, signalerer, hvilken virksomhed hhv. **top-leveldomæne** IP-nummeret er tildelt.

IPv4: Internet Protocol, version 4. Den **standard**, der i dag benyttes for tildeling af IP-adresser på **Internet**. Standarden giver plads for 4,3 milliarder IP-adresser, men i praksis er en stor del af dette råderum ubenyttet. Næste version af protokollen kaldes IPv6 og er baseret på en adresselængde på 128 bits, der giver plads for et astronomisk antal IP-adresser.

IPv6: se IPv4.

IRC: Internet Relayed Chat. Internet-tjeneste, der muliggør bilateral udveksling af beskeder i på forhånd udpegede grupper.

Iridium: Et af de første systemer til mobiltelefoni, udbudt af et privat konsortium – Iridium-konsortiet – og som baseres på, at man fra en mobiltelefon kobler sig op til en lavtgående satellit tilknyttet Iridium-nettet. Der har endnu ikke vist sig et økonomisk bæredygtigt marked for sådanne globale tjenester.

ISDN: Integrated Services Digital Network. Betegnelse for data**net** til offentlig **telekommunikation** i Europa, som formidler en flerhed af tjenester (f.eks. tale, tekst og billede) ved hjælp af en enkelt – eller et begrænset antal – tilslutning(er) direkte til den enkelte forbruger. Den universelle tilslutning er mulig, fordi nettet opbygges som en overbygning på eksisterende **digitale** telefoncentraler. Hvor det almindelige telefonnet alene har kunnet overføre 9600 **baud** (op til 57.600 bit i sekundet), kan man med ISDN overføre op til 128.000 bit i sekundet (svarende til to kanaler af 64.000 bit pr. sekund). Som adgangsvej til nettet er ISDN-kommunikationen i dag i nogen grad fortrængt af kommunikation via ADSL (s.d.).

ISO: International Standardization Organization – verdensomspændende standardiseringsorganisation.

ISP: Internet Service Provider. Virksomhed, der sælger adgang til Internet. I Danmark organiseres sådanne virksomheder i foreningerne FIL og **IBF**.

IT: Informationsteknologi – betegnelse for teknologier til behandling af **information** som f.eks. digitale data, tekst, grafik, billeder og lyd ved hjælp af elektroniske teknikker.

ITSEC: Information Technology Security Evaluation Criteria. EU-støttet metode til certificering af produkter ud fra IT-sikkerhedsmæssige kriterier.

IT-sikkerhed: Læren om sikkerheden ved IT-installationer mod tekniske fejl eller angreb, der kan medføre, at data tabes, ødelægges, kompromitteres eller ikke er tilgængelige.

IT-system: Betegnelse for **system**, der er opbygget på grundlag af en elektronisk **processor**, og hvis funktion det er at behandle **data** af en given karakter.

ITU: International Telecommunications Union. International organisation, der beskæftiger sig med regulering og standardisering på telekommunikationsområdet.

Java: Programmeringssprog, der er udviklet af IT-producenten Sun Microsystems, USA, og specielt med sigte på programapplikationer, der skal afvikles over **Internet** (først og fremmest www). Sproget kendetegnes først og fremmest ved at kunne afvikles uafhængigt af maskinmiljø. Derudover indeholder det en række faciliteter, der hjælper programmøren, f.eks. ved automatisk at rydde op i "glemte" programkoder mv.

Java applet: Program udviklet i Java, som er beregnet til afvikling i tilknytning til tekstuel information, f.eks. som animation på en hjemmeside.

JPO: Japan Patent Office.

Just in time-produktion: Talrige **kommunikationsprocesser** resulterer i et spild pga. omkostninger til lagerføring samt fejlskøn over behovet for at producere og indkøbe givne mængder etc. Ved at styre den **information**, der øver indflydelse på disse spildfaktorer – hvilket typisk sker ved hjælp af IT – kan man målrette produktion og produktionsopfølgning med heraf følgende effektivisering. Man producerer "lige nøjagtigt til tiden" – just in time. Ved just in time-produktion ankommer råvaren, når den skal anvendes, og færdigvaren er (først) færdig, når den skal leveres.

K18: Statens standardkontrakt for standardiserede edb-systemer.

K33: Statens standardkontrakt for edb-totalleverancer (samtidig anskaffelse af maskinel, special- og standardudviklet programmel).

KB: Kilobyte(s) = 1.000 bytes. Måleenhed for lagerkapacitet, se <http://physics.nist.gov>.

Karakter: Fordansket udtryk, der modsvarer det engelske "character", dvs. et tegn.

Key escrow, nøgledeponering. Tilstand, der giver mulighed for, at myndigheder, der er beføjet hertil, under visse betingelser kan dekryptere krypteret information ved brug af information (f.eks. deponerede nøgler), som befinder sig hos en eller flere troværdige tredjeparter. Se også **krypteringspolitik**.

Key management: Se nøgleadministration.

Keyboard: Se **tastatur**.

Kildetekst: eller **programkode**. De enkelte programinstruktioner skrevet i et givet **programmeringssprog**, der, når de **kompileres** (oversættes) til **objektkode**, sætter en **computer** i stand til at udføre dem.

Kildetekstdeponering: Den deponering af kildetekst hos en troværdig tredjepart (se **TTP**), som parterne i en aftale om softwarelicens foretager med henblik på udlevering af det deponerede til brugeren (licenstageren) med henblik på dennes egen afhjælpning af fejl

mv., såfremt leverandøren (licensgiveren) ikke lever op til sine forpligtelser i henhold til aftaleforholdet.

Killer application: Slang for edb-program, der har nået en særlig høj grad af popularitet i markedet. Ofte sættes dette kriterium der, hvor markedet vil efterspørge en computer alene med det formål at kunne afvikle programmet. Blandt de *killer applications*, vi har set i IT-historien, er det første regnearksprogrammer VisiCalc samt Lotus 1-2-3. Ligeledes kan de moderne web-browsere betragtes som Killer applications.

Klartekst: Forståelig tekst, dvs. data, hvis informationsindhold er umiddelbart tilgængelig.

Klient: Betegnelse for computer eller slutbrugerapplikation, der får en databehandlingsopgave udført af en anden computer, kaldet **serveren**. Betegnelsen er for alvor blevet indarbejdet efter den almindelige udbredelse af **client/server-teknologi**, der er en af følgerne af Internets udbredelse, f.eks. i www-sammenhæng, hvor www-brugerens udstyr optræder som klient og www-leverandørens som server. Den tekniske rollefordeling mellem klient og server har bl.a. betydning for, hvorledes ophavsretligt beskyttet programmel må anvendes og for retten til at behandle personoplysninger.

Klokke: Også kaldet "taktgiver". Den komponent, der med en fast frekvens afsender de elektriske udladninger, der igangsætter beregningerne i en **computer**. Taktgiverens frekvens bestemmer centralprocessorens hastighed og angives nu om dage i **megahertz**, f.eks. 8, 10, 16 eller 32 MHz.

Klon: Tidligere anvendt betegnelse for en **computer** eller en IT-komponent, der i henseende til **kompatibilitet** eller bruger**grænseflade** tilstræber at ligne et allerede eksisterende fabrikat. I årene efter at IBM i 1982 satte sin PC på markedet, producerede en række konkurrerende producenter PC'er med tilsvarende grænseflader til styresystemet DOS. Udtrykket havde et noget odiøst skær over sig, da de fleste af disse maskiner var produceret i fjernøsten til lave priser og ofte under en ringere grad af kvalitetssikring end man ofte finder i Europa og USA.

Kode, se **programkode** (**kildetekst**), **kryptering** og **password**.

Kommunikation: Betegnelse for en proces, hvorved **information** overføres fra en part eller et **system** til en anden part eller et andet system.

Kommunikationsproces: Se **kommunikativ**.

Kommunikativ: En proces betegnes som kommunikativ, når dens indhold eller forløb beror på **kommunikation**. En kommunikativ proces er med andre ord en kommunikationsproces.

Kompatibilitet: Betegnelse for den fælles anvendelse af regler og **medier**, der må overholdes af afsenderen og modtageren i en kommunikationsproces, og som gør det muligt for disse parter at gennemføre denne proces og dermed genskabe **information**.

Kompilering: Oversættelse. Teknisk betegnelse for den procedure, hvorved et program i kildetekstversion forandres til en objektkodeversion, der som sådan kan forstås af systemets processor. Se også **dekompilering**.

Komponent: Se **system**.

Kompression: Se **komprimering**.

Komprimering: Teknik, der reducerer det antal bits, der er nødvendigt til at lagre eller transmittere digital information. Komprimering af data anvendes ofte for at reducere omkostningerne til transmission. De programmer, der anvendes ved komprimering af audio- og videosignaler, kan ofte tilpasses, så der opstår forskellige grader af kvalitet ved dekomprimering. Et hyppigt anvendt område for datakomprimering er anvendelsen af de såkaldte MP3-filer, der anvendes ved komprimering af musikværker. Denne komprimering kendetegnes i øvrigt ved at være "lossy", idet den resulterer i et vist kvalitetstab af den komprimerede information. Lossy komprimering anvendes på områder, hvor man kan leve med et sådant kvalitetstab, således som dette eksempelvis er tilfældet ved udveksling af fotografiske billeder og lyd via Internet.

Konfidentialitet, se **fortrolighed**.

Konsol: Dataskærm der benyttes til kommunikation med en computers styresystem. Anvendes primært om arbejdspladser, hvorfra en driftsoperatør overvåger en mainframecomputers afvikling.

Kontrolspor: Revisionsteknisk betegnelse for de kontroller, der har været i anvendelse, for at sikre pålideligheden af et system, herunder navnlig et regnskabssystem. Kontrolsporet består navnlig af informationer i et bilags- eller dokumentationsmateriale, der dokumenterer, at registreringer er foretaget korrekt. Kontrolsporet gør det altså muligt at "spore" den enkelte registrering, f.eks. den udgift til indkøb af en maskine der efterfølgende kommer til udtryk i årsregnskabet. Oplysningerne i et kontrolspor kan enten være forklarende eller dokumenterende tekst eller kan udgøre dokumentation for, at nødvendige kontrolhandlinger mv. er udført (hvilket i givet fald kan komme til udtryk i et **transaktionsspor**.)

Konvergens: Grænsenedbrydning. Anvendes i IT-sammenhæng om den sammensmeltning, som den digitale teknologi har medført mellem telekommunikation, informationsbehandling (edb) og audio-visuelle tjenesteydelser. Begrebet kan dog også anvendes om den grænseoverskridning, der har fundet sted i relation til andre informationsområder, f.eks. forlags- og udgivelsesvirksomhed. For IT-retten og IT-politikken har konvergensproblemet nødvendiggjort en stillingtagen til, om de retlige begrænsninger, der traditionelt har dannet sig i relation til et medium, også skal gælde i relation til et andet, når begge medier anvendes til spredning af samme typer information.

Konvertering: Forvandling i overensstemmelse med på forhånd givne kriterier. Man taler f.eks. om, at et dokuments grafiske billede "konverteres" til bits, når dokumentet scannes, se **scanning**.

Kopibeskyttelse: Funktionalitet, der indbygges i et informationsprodukt (f.eks. en programpakke) med det formål at umuliggøre (ofte kaldet "copy protection") eller dog vanskeliggøre (ofte kaldet "copy discouragement") kopiering. Eksempler herpå er brug af **dongles** eller indbygning af funktioner, hvorved det pågældende produkt – enkeltstående eller løbende – afkræver brugeren et **password**, som skal erhverves ved en fremgangsmåde, der sikrer, at den pågældende har den fornødne brugsret.

Kryptering: eller kryptografering. Den proces, hvorved en mængde **information**, der er sammensat ved brug af et alment tilgængeligt **sprog**, transformeres til en mængde **data**, der ikke er alment tilgængelig. Transformationen sker ved hjælp af en **algoritme**, der styres af et indgangssignal, en såkaldt nøgle. Modtageren af den krypterede meddelelse kan herefter ved at gøre brug af nøglen fremkalde den oprindelige informationsmængde. Se også **Public Key Krypteringssystem** og CA.

Krypteringspolitik: Politik med hensyn til tilladeligheden af kryptering. På den ene side står hensynet til de parter, der ønsker at beskytte fortroligheden af deres data med kryptering; på den anden side hensynet til de efterforskende myndigheder, der med en udstrakt anvendelse af sådanne teknikker vil miste muligheden for at aflytte telekommunikation. Som et muligt kompromis mellem disse to hensyn har man bl.a. diskuteret muligheden for såkaldt nøgledeponering, hvorved den nøgle, der krypterer data, deponeres et sted, hvor den myndighed, der har ret til at få kendskab til disse data (f.eks. gennem aflytning) kan rekvirere den.

Kryptografi: Den lære om kodeskrift, der ligger til grund for **kryptering**. Anvendes bl.a. som grundlag for **digital signatur**.

Kunstig intelligens: Upræcist udtryk for det forskningsområde, der tilsigter at anvende IT-systemer til simulering af menneskelige intelligensfunktioner som f.eks. mønstergenkendelse, logiske konklusioner etc.

Kybernetik: Læren om styring af maskiner og andre automatiserede systemer (herunder IT-systemer). Betegnelsen blev foreslået af systemteoretikeren *Norbert Wiener*, der anvendte det græske ord "kybernetes", sømand. Når en sømand styrer et skib ved at bevæge roret, agerer han på grundlag af en løbende strøm af informationer om, hvorledes sidste rorbevægelse påvirkede skibets retning. På samme måde påvirker brugeren IT-systemet ved i et fortsættende forløb at give "inputs" på grundlag af systemets seneste "outputs".

Lager: Digitalt lagringsmedium, der er beregnet til at opbevare (modsat f.eks. at transmittere) **data**. Et lager kan tage sigte på mere eller mindre blivende opbevaring. I den ene ende af skalaen finder man CD-ROM og mag-

netbånd, hvis **data** lagres mere permanent. I den anden ende RAM-kredse (se RAM), hvis data mistes, når strømmen afbrydes.

LAN: Local Area Network, se **lokalnet**.

Laptop: Bærbar computer. Navnet er et sprogspil (lap-dog = skødehund) afledt af navnet på den "klassiske" **desktop** (dvs. skrivebords-) PC.

Laser: Ordsammenskrivning af forkortelsen for Light Amplification by Stimulated Emission of Radiation. Betegnelse for såkaldt monokromatisk – eller koherent – lys, dvs. lys, der bevæger sig på en ganske bestemt bølgelængde og altid i fase. Laserteknologi benyttes bl.a. til **transmission** af **data** via lyslederkabler.

Licens: Af engelsk: tilladelse. Anvendes oftest som betegnelse for den tilladelse, en rettighedshaver giver til at udnytte en immateriel rettighed, f.eks. en ophavsret eller et patent. I praktisk IT-sprogbrug indsnævres ordet undertiden til at angå tilladelsen til at anvende et givet **program** på en given installation.

Link: Forbindelse. Også kaldet **hypertekst**-link. I sammenhæng med **Internet** anvendes ordet hyppigst om den forbindelse, udbyderen af en **hjemmeside** kan skabe mellem sin egen hjemmeside og andre hjemmesider. For brugeren opleves en link således, at man ved at "klikke" på et bestemt sted – f.eks. en ordkombination eller en **bannerannonce** – ledes hen til en anden hjemmeside, der indeholder yderligere information herom.

LINUX: Styresystem, primært til brug i pc-miljøer, der er baseret på principper hentet fra UNIX-styresystemet. LINUX blev i sin tid udviklet af den finske studerende *Linus Torvalds* i 1991. Via Internet inviterede Torvalds hele verden til at være med i udviklingen af LINUX, og i dag er der tale om et fuldt brugbart styresystem, som bl.a. er indbygget i en række pc-producenters udstyr. Da såvel Torvalds' oprindelige version af systemet som de efterfølgende forbedringer af det er udviklet efter freeware-princippet, er dette system som udgangspunkt gratis at erhverve, ligesom **kildeteksten** er alment tilgængelig.

Livestreaming: Også kaldet "simulcasting". Betegnelse for transmission af radio eller tv via Internet samtidigt med, at udsendelsen fremføres i radio eller på tv. Lytterne og seerne kan altså høre og se udsendelsen på nettet, samtidigt med, at den sendes i radioen eller på tv. Adskiller sig fra **webcasting**, hvor udsendelsen kun udsendes på nettet, men ikke samtidig i radio eller på tv.

Logning: Registrering af hændelser. I søfarten registrerer skibets log-bog f.eks. informationer om rute og anlægshavne. I IT-sammenhænge føres der mange typer af log, f.eks. med henblik på kontrol af IT-systemets interne processer eller for at kunne genskabe en given situation. Ofte anvendes udtrykket "at logge sig på" om den handling, hvormed operatøren etablerer den forbindelse med **systemet**, som er nødvendig for hans brug af det. Man kan sondre mellem systemets egen (automatiserede) log og den logbog, der føres af den IT-ansvarlige. Sidstnævnte er navnlig af praktisk betydning under en **afleveringsprøve** og i brugerens efterfølgende registrering af fejlsituationer mv.

Lokalnet: Også kaldet LAN (Local Area Network). En flerhed af sammenknyttede databehandlingsenheder (f.eks. computere, terminaler, printere mv.), der befinder sig indenfor samme lokalitet, typisk en virksomhed. Ved opbygningen af et lokalnet anvendes forskellige strukturer (ring- eller busstrukturer).

LRA: Local Registration Authority. Den part i en Public Key Infrastruktur, der har til opgave at kontrollere identiteten af de personer, der opnår certifikater. I praksis kan LRA-funktionen tænkes henlagt til en bankafdeling, et lokalt folkeregister eller et firmas personaleafdeling.

M-handel (mobil-handel): Samlebetegnelse for dispositioner, der indebærer, at bestilling og betaling sker ved hjælp af en mobiltelefon, f.eks. således at brugeren gennem mobiltelefonen taster en pin-kode, som via en betalingsindløser udvirker en betaling til den handlende.

Mainframe: I en – nu sjældent anvendt – opdeling af **computere** i "mikro-computere", "mini-computere" og "mainframes", betegnelse for den største.

Makro: Den sammenfletning af en flerhed af instruktioner, som **brugeren** af visse **applikationer** kan sammenskrive, og som giver ham mulighed for at udføre disse instruktioner med ét kald. En makro er dermed et –

ofte lille – **program**, som brugeren skriver for at lette anvendelsen af den applikation, der rummer faciliteten til makro-programmering i sig.

Malware: Af *Mal*icious Sof*tware*. Almindelig slang for software, der er designet med det formål at ødelægge et IT-system eller gøre det funktionsudygtigt. En Orm eller en Trojansk hest (s.d.) er eksempler på malware.

Markør: Se **cursor**.

Maskinel: Se **hardware**.

Maskinkode: Se **objektkode**.

Maskwork: Se **topografi**.

Master (eller master-diskette): Det eksemplar af et digitalt lagringsmedium (f.eks. en diskette med et program eller en CD-ROM med et musikværk) som licensgiveren i en licensaftale overdrager til licenstageren, og som licenstageren herefter anvender som grundlag for eksemplarfremstillinger til slutbrugere eller underlicenstagere.

Matrixprinter: Skriveenhed, der fæstner ord og grafik til papiret ved hjælp af et skrivehoved bestykket med nåle, der danner de forskellige **tegn**, når de bevæges frem mod farvebånd og papir.

MB: Megabyte(s) = 1.000.000 bytes. Måleenhed for lagerkapacitet, se http://physics.nist.gov.

Medium: Fysisk fænomen, der besidder evnen til at lade data og informationer af en vis type fæstnes på sig. Mængden af medier er uendelig. De medier, der påkalder sig størst interesse på IT-området, er kendetegnet ved at være maskinlæsbare, hvorved menes, at de fæstnede **data** er repræsenteret **digitalt** og i denne form uden videre kan **transmitteres** til en **computer**.

Mediekompatibel information: Information, som evner ubesværet at springe til andre medier af samme art, men ikke til medier af en anden type. F.eks. information indlæst på diskette under en almindelig kendt standard.

Megaflops: Million FLOating Point instructions per Second. Måleenhed, der betegner den hastighed, hvormed en CPU arbejder, med udgangspunkt i dens beregningskapacitet. Se også MIPS.

Megahertz: Millioner svingninger pr. sekund. Anvendes bl.a. til at karakterisere hastigheden af en **processor**.

Menu: Oversigtsskærmbillede i et **program**, som præsenterer **brugeren** for et antal muligheder, hvorigennem han kan aktivere programmet eller dele af det.

Meta-tagging: Opmarkering af tekst på en hjemmeside ved hjælp af søgeord, der ikke er læsbare for hjemmesidebrugeren, men som derimod kan læses af de **søgerobotter**, der for at understøtte deres søgefunktioner indexerer hjemmesiderne på Internet. Metatags indbygges i den HTML-kode, som en hjemmeside skrives i for at kunne læses via World Wide Web-tjenester på Internet.

Microchip: se **halvlederprodukt**.

Microsoft: Amerikansk virksomhed der i 1976 blev stiftet af dens nuværende leder, *Bill Gates* og *Paul Allen* (der siden har trukket sig ud). Microsoft er i dag en af verdens førende leverandører af software til PC-baserede IT-systemer. Virksomhedens succes kan dels tilskrives dens evne til at definere de **standarder**, PC-teknologien har baseret sig på, dels ved evnen til at frembringe brugervenlige – om end ikke altid stabile – og forholdsvis billige systemer. Microsoft er i disse år ved at ændre sin strategi, således at det kan få en tilsvarende stærk betydning i det stigende marked for **Internet-**anvendelse.

Mikrocomputer: Se PC.

MIME: Multi-purpose Internet Mail Extensions. Protokol for formatering af mails, der bl.a. indeholder beskrivelser af, hvordan andre tegnsæt end ASCII repræsenteres i en e-mail, f.eks. fed tekst og kursiv. Se også **S/MIME**.

Mini: Også kaldet "minicomputer". Ældre betegnelse for computer, der i størrelse og kapacitet falder mellem den helt lille computer (PC'en) og den helt store (mainframe-computeren).

MIPS: Million Instructions Per Second. Måleenhed, der betegner den hastighed, hvormed CPU'en kan udføre instruktioner. Se også **megaflops**.

MIT: Massachusetts Institute of Technology. Amerikansk universitet, placeret i Boston, Massachusetts.

MMS: Multimedia Messaging Service. Standard for overførelse af multimedia-information via mobiltelefoni. En MMS-besked kan indeholde såvel tekst som objekter (f.eks. bille-

der, videoklip eller lyde). Som grundlag herfor anvendes eksisterende objektformater for billede eller lyd.

Mode: Udtales på engelsk. Betegnelse for en IT-komponents tilstand. Har f.eks. betydning, når man skal beskrive muligheden for at læse eller skrive til den pågældende komponent.

Modem: Udstyr beregnet til tilslutning af IT-terminaler til telefonnettet. Fungerer ved at *mo*dulere det signal, der sendes, til impulser (lydsignaler), der kan transmitteres over nettet, henholdsvis ved at *dem*odulere signaler modtaget i dette format.

Moore's lov: Den antagelse, at udviklingen af halvlederchips vil forløbe således at kapaciteten fordobles og prisen halveres ca. hvert andet år. Antagelsen, der blev gjort i 1964 af *Gordon Moore*, der var en af grundlæggerne af processor-virksomheden **Intel**, har hidtil holdt stik. Moore har siden formuleret en "Moore's anden lov", der siger, at processorernes kapacitet og funktionalitet vil stige, indtil prisen for at udvikle nye processorer bliver så høj, at det ikke lader sig gøre at finansiere den nødvendige udvikling og produktion. Moore antager, at denne grænse for Moore's anden lov vil ligge omkring år 2010.

MoU: Memorandum of Understanding. Betegnelse for en fælles hensigtserklæring, hvorved de underskrivende parter erklærer at ville løse et vanskeligt problem på frivillighedens grundlag (dvs. gennem selvregulering) efter en nærmere fastsat procedure. **Dansk Internet Forum** er f.eks. etableret på grundlag af et Internet Danmark Memorandum of Understanding, der fastslår nogle principper for, hvorledes tildeling og administration af Internet-domænenavne under .dk-toplevel-domænet skal finde sted.

MP3: Standard udviklet af MPEG til lagring af digital lyd i komprimeret form. Selv om lagringen, pga. komprimeringen, er forbundet med et vist kvalitetstab, er standarden blevet meget udbredt som grundlag for transmission af musikværker på Internet. Dette har givet anledning til rettighedsmæssige problemstillinger, når den komprimerede (og transmitterede lyd) har været ophavsretligt beskyttede musikværker, og de fornødne tilladelser ikke har foreligget.

MPEG: Motion Pictures Expert Group. Betegnelse for det standardiseringsorgan, der bl.a. har udarbejdet MP3-standarden.

Multimedia: Fælles betegnelse for IT-systemer, der integrerer behandling af tekst, grafik, lyd, billede og video, f.eks. til brug ved undervisning eller underholdning.

Mus: Betegnelse for **indlæsningsenhed** på størrelse med en tændstikæske, der flyttes rundt på en plan flade og dermed indlæser **data** svarende til **brugerens** bevægelser på denne flade kombineret med enkelte tastetryk. Musens bevægelser på fladen modsvares af de bevægelser, **cursoren** foretager på skærmen.

Nanosekund: Tidsenhed på 1/1.000.000.000 af et sekund.

Napster: Internet-virksomhed etableret i Californien i efteråret 1999 på basis af en særlig **peer-to-peer**-teknologi, hvorefter Internetbrugere henter datafiler hos hinanden baseret på et fælles index, der føres hos Napster. Filerne hentes ved hypertekst-spring fra Napsters hjemmeside til de tilknyttede Internetbrugeres hjemmesider. Teknikken har givet anledning til tvivl om, hvorvidt virksomheden Napster medvirker til at forvolde de retskrænkelser, der indtræder, når de filer, der udveksles på denne vis, indeholder ophavsretligt beskyttede musikværker eller anden information, der ikke kan spredes frit.

Naturligt sprog: Sprog, hvis syntaks og grammatik er indrettet på menneskets – i grunden ustrukturerede – tænkning, og som derfor præges af flygtige og ofte upræcise regler, sml. **formalsprog**. Naturlige sprog indgår typisk i en intelligent (i modsætning til mekanisk) **kommunikation**. Dansk, engelsk, fransk, babysprog og kropssprog er eksempler på naturlige sprog.

NC: Network Computer. Computer, der fungerer uden indlagte programmer og eksterne lagerenheder, men som i stedet udfører sine funktioner på grundlag af programmer og data, der hentes direkte ind fra et eksisterende datanet, f.eks. Internet. En række amerikanske IT-producenter har understøttet udviklingen af NC'en, bl.a. for at tage kampen op med Microsoft Inc., der p.t. dominerer markedet for PC-programmer.

NCSA: National Center for Supercomputer Applications. Amerikansk forskningsenhed, der bl.a. udgjorde rammerne for udviklingen af de første systemer til **hypertekst**-anvendelse på Internet. Se **www**.

Net: Se **netværk** og **neuralt netværk**.

Net-ID: Sikkerhedsløsning til web-baseret kommunikation udviklet og markedsført af danske pengeinstitutter. Ved hjælp af adgangskoden til en netbankløsning får brugeren mulighed for at identificere sig over for en virksomhed via en web-kommunikation, der understøttes af samme sikkerhed som den, der gælder for brugerens netbank. Virksomheder, som ønsker at udbyde sikkerhedsløsninger via Net-ID, indgår aftale herom med PBS. Se nærmere <www.pbs.dk/it-services/net-id>.

Netiquette: Internet-slang for den opfattelse af god skik, der er fremherskende ved Internetkommunikation. F.eks. anses **spamming** at være i strid med netiquette.

Netværk: En oversættelse af det engelsk/amerikanske ord "network" (net), underforstået data-net, som betegner et **system**, der forbinder en flerhed af **computere** og ydre enheder (skærmterminaler, **printere**), og som tillader alle tilkoblede brugere adgang til alle dele af systemet (evt. kombineret med logisk adgangskontrol mv.).

Neuralt net: Et **ekspertsystem** der er kendetegnet ved ikke at være udstyret med et eget symbolniveau, idet dets viden består af relationer mellem eksempler, der er indlagret i det. Ud fra visse bestemte aspekter ved en fænomentype, som operatøren på forhånd har angivet, kan det neurale net læse et antal eksempler og på grundlag heraf konkludere noget om, hvilke mønstre eller lovmæssigheder der er gældende for disse eksempler.

Newsgroup: Se **nyhedsgruppe**.

NII: National Information Infrastructure. Betegnelse for det projekt, som det amerikanske præsidentembede fremsatte i 1993 for opbygningen af en national informationsinfrastruktur. I sin oprindelige udformning skulle projektet understøtte opbygningen af såkaldte "electronic superhighways", men siden er en række andre emner, herunder ophavsretten og krypteringspolitikken, kommet på dagsordenen.

NIST: National Institute of Standards and Technology. Amerikansk standardiseringsorgan. Har bl.a. publiceret den udbredte krypteringsstandard DES.

NMT: Nordisk Mobil Telefon. System til mobiltelefoni, der er udviklet med henblik på de nordiske lande, og som baseres på datatransmission i analog form. Systemet baseres enten på 450 eller på 900 Megahertz frekvenser. Det er mindre egnet til overførelse af digitale data, men har til gengæld haft en bedre dækningsgrad end GSM-systemerne havde de første år.

Ny økonomi: Ofte anvendt betegnelse for de samfundsøkonomiske egenskaber, der gennem de seneste år har kendetegnet en række økonomier i den vestlige verden. I takt med en øget produktion af informationsrelaterede og -afhængige varer og tjenester har man – i strid med tidligere gældende økonomisk teori – på en gang oplevet høj vækst, lav ledighed, lav inflation, øget globalisering, iværksætterlyst og en (til tider) blomstrende aktiekultur. Efter sammenbruddet på markedet for de såkaldte dot com-aktier 2001 er det blevet mindre almindeligt at tale om, at vi befinder os i en sådan "ny økonomi" – ja nogen vil måske mene, at vi har fået den gamle økonomi tilbage.

Nyhedsgruppe: Betegnelse for en teknisk og organisatorisk ramme for diskussioner på Internet. Den bruger, der ønsker at deltage i en diskussion via en nyhedsgruppe, tilmelder sig denne. Herefter kan brugeren fremsende sine kommentarer mv. til nyhedsgruppen, hvorefter disse kommentarer automatisk eller efter forudgående redaktion formidles til hele gruppen.

Nøgle: Se **kryptering**.

Nøgleadministration: Den proces, hvorved nøgler frembringes, lagres, overføres, suspenderes eller tilbagekaldes med henblik på at opnå bestemte sikkerhedsmæssige funktioner.

Nøglecenter: Efter gængs terminologi, den instans, der i et system til asymmetrisk kryptering står for udstedelse af nøgler eller som udleverer det udstyr mv., der er nødvendigt for at generere nøgler og (typisk også) værktøjer til uddragelse af hash-værdier. Efter at loven om elektroniske signaturer imidlertid

har valgt at definere begrebet som svarende til CA, er der opstået en vis uklarhed om dets indhold.

Nøgledeponering, se **krypteringspolitik**.

Objektkode: – også kaldet **maskinkode**. Den version af et **program**, der er beregnet til umiddelbar afvikling i en **computer**. Objektkode kan enten foreligge i **assembler-kode** eller som en **oversættelse** af **kildetekst**.

Objektorienteret programmering: Programmeringsmetode, der bygger på et princip om, at data og tilhørende procedurer indkapsles i forskellige objekter, der under programeksekveringen behandles som et hele. I et programmeringssprog, der bygger på objektorienteret programmering, består en væsentlig del af udviklingsopgaven i at definere de pågældende objekter.

OCES: Offentlige Certificater til Elektronisk Service. Betegnelsen for en dansk offentlig nøgleinfrastruktur. IT- og Telestyrelsen har udarbejdet tre OCES-certifikatpolitikker (CP) for person-, medarbejder- og virksomhedscertifikater. Disse CP'er udgør en fælles offentlig standard, der regulerer udstedelsen og anvendelsen af den digitale OCES-signatur. CP'erne fastsætter krav til nøgleinfrastrukturen og dermed sikkerhedsniveauet for OCES-signaturen. De certifikater, der udstedes på grundlag af OCES-CP'erne, udgør ikke kvalificerede certifikater i henhold til LES.

OEM: Original Equipment Manufacturer, betegnelse for en IT-leverandør, som markedsfører en ydelse under eget navn, som består af en forædlet eller videreudviklet ydelse fra et tidligere salgsled (f.eks. en brancheløsning bestående af standard-PC'er suppleret med særligt udviklet programmel). I en OEM-leverance har den oprindelige producent intet image overfor slutbrugeren. Til forskel herfra bevarer en VAR-leverandør sit navn og image overfor slutbrugeren.

OEM-licens: Licens til et edb-program, som er præinstalleret på en pc eller anden hardware. Licensen indebærer normalt, at brugeren må anvende det præinstallerede program på den pågældende hardware men ikke andetsteds (f.eks. kopieret til anden hardware).

OIO: Forkortelse for Offentlig Information Online (på engelsk *Open Public Information Online*). Betegnelse for et dansk initiativ, der har til formål at samle formidlingen af de initiativer og aktiviteter, der vedrører de tekniske og kommunikative aspekter af digital forvaltning og elektronisk betjening af borgere og virksomheder. På <www.oio.dk> kan der hentes information om digital forvaltning og implementering af it i den offentlige sektor samt effektivisering af den offentlige kommunikation. Her finder man ligeledes en række værktøjer, der er med til at sikre grundlaget for og sammenhængen i den offentlige sektors brug af IT.

OJ EPO: Official Journal of the European Patent Office.

ONA: Se ONP.

ONP: Open Network Provision (dvs. at stille åbne net til rådighed). Betegnelse for en række EU-standarder, der benyttes inden for telekommunikation i forbindelse med tilslutning til og brug af **VANS**-ydelser. ONP er den europæiske pendant til den amerikanske Open Network Architecture (ONA). Det retlige grundlag for ONP-standarderne findes i en række rådsdirektiver, der også definerer begrebet.

Open source (eller open source-software): Åben kildetekst. Betegnelse for programmer, der udbydes således at kildetekst følger (gratis) med, hvorved brugeren selv kan foretage rettelser og – alt efter de licensmæssige begrænsninger – forbedringer. Et væsentligt eksempel herpå er **Linux**-styresystemet. Open source-princippet er altså ikke synonymt med **freeware**. Et open source program kan med andre ord sagtens overdrages under licensmæssige begrænsninger. Gennem de seneste år er der opstået en særlig open source-kultur, der bl.a. har søgt at definere nogle spilleregler for, hvorledes disse licensmæssige grænser skal lægges, se nærmere <www.opensource.org>.

Operativsystem: Se **styresystem**.

Operatør: Se **bruger**.

Opmarkering: Den kodning af en tekst, der sker med henblik på efterfølgende anvendelse i et **hypertekst**-system. Opmarkeringen kan enten fremtræde i en form, der er læsbar for brugeren (som f.eks. når man på en hjemmeside kan se, hvilke ord der kan "klikkes" på) eller skjult for brugeren, f.eks. i form af såkaldt **meta-tagging**.

Opt in: "Vælg til". Nutidigt udtryk for lovregel, hvorefter den juridiske regulering beror på, at et retssubjekt selv har truffet et valg om at være omfattet af denne regulering. Det har f.eks. været drøftet, om det offentlige som udgangspunkt (og dermed: medmindre andet var bestemt – se **opt out**) burde være underlagt en pligt til at kunne afgive og modtage forpligtende meddelelser digitalt. En sådan generel regel er ikke indført, og myndighedernes ret og pligt til at kommunikere på denne vis er derfor baseret på beslutninger og lovgivning herom i enkelttilfælde, altså efter et princip om opt in. Et andet eksempel er mfl. § 6a, stk. 1, hvorefter retten til at rette uanmodet henvendelse til kunder ved hjælp af e-post og automatiske opkaldssystemer er betinget af, at modtageren forudgående har anmodet herom.

Opt out: "Vælg fra". Nutidigt udtryk for en lovregel, hvorefter den juridiske regulering beror på, at et retssubjekt har truffet et fravalg om ikke at være underkastet en særlig pligt mv., se også **opt in**. Et eksempel herpå er reglen i mfl. § 6a, stk. 2, hvorefter retten til at rette uanmodet henvendelse til enkeltpersoner ved brug af anden telekommunikation end e-post mv. ophører, hvis modtageren har frabedt sig dette.

Optisk læser: Indlæsningsenhed, der registrerer data i form af lyspåvirkninger, f.eks. en stregkodelæser.

Orm: Almindelig betegnelse for program eller algoritme, der genskaber sig selv via et computernet, almindeligvis med henblik på at beskadige dette eller de tilsluttede systemer, eller på anden måde hindre driften.

OS/2: Styresystem til PC-baserede IT-systemer udviklet af IBM i 1987. Trods høj stabilitet og ydeevne fik OS/2 ikke den succes på desktop- og hjemme-pc-området, som IBM havde håbet på. Den sidste udgave af styresystemet, version 4.0, kom i 1996. I nogle år derefter har IBM vedligeholdt systemet med gratis opgraderinger via Internet. Der planlægges support for systemet mindst frem til 2006.

OSI: *1.* Open Source Initiative. Amerikansk organisation stiftet af *Eric Raymond*, der bl.a. i sin bog "The Cathedral and the Bazaar" (se <www.catb.org>) havde argumenteret for, at *open source*-bevægelsen burde orientere sig bort fra sine følelsesladede og ideologiske begrundelser. Raymond fremhævede den effektiviseringsgevinst, der ligger i den "bazar"-prægede programudvikling, der kan betragtes som en form for agil programudvikling, s.d. OSI virker i dag som en platform til markedsføring af denne tankegang, bl.a. ved fremlæggelse af et antal "officielle" open source-definitioner mv. OSI forestår i den forbindelse en vis certificeringsvirksomhed, idet et program kan markedsføres som "OSI Certified Open Source Software", hvis det opfylder visse krav, se <www.opensource.org>.
2. Open Systems Interconnection. Standard vedtaget af ISO for udformning af den datakommunikation, der skal forløbe, når to **systemer** sammenkobles. Standarden definerer 7 lag og betegnes oftest som OSI-referencemodellen eller blot OSI. OSI-referencemodellen er oprindeligt udviklet af ISO men siden varetaget i samarbejde med CCITT. OSI-referencemodellen specificerer de kommunikative processer mellem forskellige IT-systemer i forskellige lag: anvendelseslaget, præsentationslaget, sessionslaget, transportlaget, netværkslaget, dataoverførelseslaget og det fysiske lag. Modellen anvendes som grundlag for udvikling af standarder inden for de forskellige lag, f.eks. til brug for elektronisk post, EDI mv.

Outsourcing: Den disposition, hvorved en virksomhed vælger at lade en del af sine arbejdsopgaver – typisk sådanne, der ikke kendetegner virksomhedens produktion – udføre af en tredjepart, f.eks. gennem **FM**. I nærværende sammenhæng fokuseres primært på outsourcing af IT-funktioner. Der er imidlertid ingen grænser for hvilke virksomhedsopgaver, der kan outsources. Andre eksempler er rengøring, kantinedrift, bogholderi mv.

Oversættelse: Se **kompilering**.

Oversætterprogram: Eller oversætter, compiler. Program, der automatisk oversætter (kompilerer) en **kildetekst** til **objektkode**.

P3P: Platform for Privacy Preferences. Standard under udvikling i **World Wide Web Consortium**. Idéen er at lade web-brugerens browser gennemføre en dialog med serveren bag en hjemmeside som resulterer i en slags "aftale" om, hvilke personoplysninger der behandles på siden.

PABC: Forkortelse for Privat Automatisk Bi-Central, dvs. omstillingsbord. En moderne PABC er baseret på **digital** repræsentation af data og anvendes til at forbinde telefoner/**modems** med det offentlige telefonnet. I digitale PABC-anlæg varetages herudover faciliteter som f.eks. automatisk notering, omstilling ved optaget etc., ligesom sådanne anlæg kan give adgang til digitale **transmissioner**, f.eks. **elektronisk post** og anden datakommunikation.

PABX: Private Automatic Branch Exchange, engelsk betegnelse for PABC (omstillingsbord).

Password: Også kaldet pasord. Kodeord, f.eks. bestående af et ord eller en tal/bogstav-kombination), som en **bruger** skal afgive for at få adgang til information. Et password kan f.eks. udløse brugen af en hemmelig nøgle (se **Public Key Kryptering**), eller det kan blot udgøre det signal, der skal afgives for at få adgang til et IT-system. Dankortets PIN-kode udgør et eksempel på et password.

Patching: Teknik til fejlrettelse i programmel, hvorved der rettes i selve den binære kode. I det omfang, der er mulighed for fejlrettelse på denne måde, behøver man ikke – som ellers – at have adgang til **kildeteksten** for det pågældende program. Patching er dog vanskelig at gennemføre og anvendes primært ved brugerens egen fejlretning i **styresystemer**.

Pay-per-view: TV-system, der kun tillader seere adgang til visse programmer, hvis de har betalt.

Payware: Almindelig betegnelse for programmel, som rettighedshaveren stiller betalingskrav til. Hovedparten af den kommercielle software, der udbydes på markedet, har karakter af payware. Dog distribueres programrettelse og visse tidlige versioner (se **beta-version**) undertiden som **freeware**.

PBS: Pengeinstitutternes Betalings-service A/S. Dansk servicebureau oprettet af danske pengeinstitutter med henblik på håndtering af automatiske betalingsordninger for pengeinstitutkunder.

PC: "Personal Computer" (personlig computer). Et lille og typisk billigt IT-system beregnet til vidt forskellige **applikationer**, herunder tekstbehandling, beregning, telekommunikation etc.

PC-card: Se PCMCIA.

PCMCIA: Også kaldet PC-kort eller PC-Card. Personal Computer Memory Card International Association. Uafhængigt professionelt standardiseringsorgan, der fastlægger standarder for kort-baserede komponenter til en PC. Standarderne omfatter såvel størrelser som funktionalitet af disse komponenter. Et kort, der opfylder disse specifikationer, betegnes almindeligvis som "PC-card".

PDA: Personal Digital Assistant. Bærbar IT-baseret udstyr, der kombinerer et bredt spektrum af databehandlingsfunktioner, som f.eks. dag- og adressebog, tekstbehandling og beregning. PDA'er må med tiden forventes at blive koblet op til radio- eller kabelbaserede **datanet**. Hidtil har deres anvendelse dog været hæmmet af den manglende integration med telefoni samt af de begrænsninger, den lille skærm og det beskedne tastatur sætter.

PDP: Parallel Distributed Processing, dvs. parallel databehandling. Anvendes i et **neuralt net** (s.d.).

Peer-to-peer: Teknik til fælles brug af datafiler via web-servere. For tiden (2001) kendes to teknikker hertil, se **Napster** og **Gnutella**.

Pervasive computing: Almindeligt anvendt betegnelse for den anvendelse af IT, der indebærer, at IT-systemernes funktioner træder frem for brugeren således, at de maskinelle komponenter ikke synes. For brugeren kan dette få til følge, at almindelige brugsgenstande opfattes som "intelligente". En væsentlig teknologi, der understøtter denne form for IT-anvendelse, er RFID, s.d. I Danmark er betegnelsen "IT i alt" undertiden søgt anvendt som en dansk oversættelse af det engelske udtryk.

PGP: Pretty Good Privacy. Varemærke for **public key** krypteringsprogram, der nyder stor udbredelse for Internet, fordi det i sin tid blev udsendt som **public domain** af dets skaber, amerikaneren *Phil Zimmermann*, som siden etablerede en virksomhed, der skulle markedsføre PGP på kommercielt grundlag.

Phishing: Almindeligt anvendt betegnelse for retsstridig tilegnelse af en brugers adgangskoder eller andre identitetsoplysninger, der gør gerningsmanden i stand til at disponere på en brugers vegne. Metoden kendetegnes ved, at gerningsmanden opretter en hjemmeside, der minder om en kendt hjemmeside

(f.eks. en banks). Når brugeren kontakter denne hjemmeside, ledes han til at indtaste sine personlige oplysninger (såkaldt social engineering, s.d.), intetanende om, at gerningsmanden herefter vil gøre brug af disse til skade for brugeren. Phishing kan endvidere ske ved, at gerningsmanden installerer malware (s.d.) på brugerens udstyr, medens brugeren anvender gerningsmandens hjemmeside. Formålet er i begge tilfælde, at gerningsmanden senere retsstridigt kan gøre brug af offerets home banking-system. Ordet udtrykker, at gerningsmanden "fisker" de pågældende oplysninger fra brugeren.

PICS: Platform for Internet Content Selection, se http://www.w3.org/PICS). Standard udviklet af The World Wide Web Consortium blandt andet med EU-støtte med henblik på at understøtte muligheden for at filtrere uønsket information fra, når der surfes på Internet ved hjælp af en web-browser. Sigtet skulle altså være at give forældre mulighed for at filtrere, hvilke hjemmesider deres børn må få adgang til på nettet. Standarden udbygges løbende med en lang række "rating services" tilpasset forskellige løsninger.

PIN-kode: Forkortelse for "Personlig Identifikations Nummer"-kode; det **password**, der identificerer **brugeren** af et betalingskort i forbindelse med anvendelsen af dette kort. Benyttes undertiden også som betegnelse for enhver form for password.

Pixel: Sammenskrivning af Picture Element. Betegnelse for de lyspunkter, der tilsammen danner bogstaver og grafik på et skærmbillede. En PC-farveskærm, der følger VGA-standarden, har en opløsning på 640 x 480 pixels.

PKI, se **Infrastruktur**.

Platform: Betegnelse for det udstyr, der afvikler en bestemt **applikation**, f.eks. PC-platform. Fra gammel tid har edb-programmer kun kunne afvikles på bestemte typer af platforme, ofte defineret helt præcist til bestemte typer af maskiner og styresystemer. Med den teknologiske udvikling er et betydeligt antal applikationer imidlertid blevet platformsuafhængige, bl.a. de, der afvikles via **Internet** samt det hertil udviklede programmeringssprog **Java**.

Point and click-aftale: Aftale, der indgås uden parternes samtidige tilstedeværelse, ved at den ene part – typisk en forbruger – manifesterer sin vilje til at være bundet ved et sæt aftalevilkår ved at klikke for foden af den tekst, der angiver aftalevilkårene på en hjemmeside. I modsætning til **click wrap-aftalen** er der altså tale om, at medkontrahenten er blevet præsenteret for det fulde sæt af vilkår, før aftaleforpligtelsen påstås opstået. Se også **shrink wrap-aftale**.

Port: Almindelig betegnelse for de ind- og udgange, hvorpå man monterer kabler og andre enheder til en computer, eller i øvrigt opnår kommunikativ kontakt med computeren.

Portal: Internet-site, der leder brugeren over på et antal andre sites, der formodes at efterkomme brugerens behov for informationssøgning inden for bestemte, typiske livsområder (f.eks. indkøb, underholdning, trafikoplysninger etc.). Der findes såvel internationale (amerikansk baserede) portaler (f.eks. Yahoo.com) som nationale (f.eks. Scandinavia Online (.sol.dk) og Opasia (.opasia.dk).

POS-automat: Point of Sale-automat. Betegnelse for IT-terminal tilsluttet et betalingskortsystem placeret på et forretningssted til registrering af forbrugeres køb. POS-automaten initieres typisk ved magnetstriben på et købe- eller kreditkort.

POSIX: Forkortelse for Portable System Interface. Standard, der specificerer visse krav til et styresystems indhold og funktion. POSIX indeholder 11 dele: Posix 1: Systeminterface (et C-programs grænseflade til styresystemets kerne), Posix 2: Shell and tools (brugerens kommandoer til styresystemet), Posix 3: Testing and verification (en samling programmer til test og validering af Posix-systemer), Posix 4: Realtime (udvidelser til realtidssystemer), Posix 5: Ada language bindings (definerer hvordan programmer skrevet i sproget Ada kommunikerer med styresystemet), Posix 6: Security extensions (sikkerhedssystem), Posix 7: System administration (værktøjer til systemadministration), Posix 8: Networking (netværk), Posix 9: Fortran language bindings (definerer, hvordan programmer skrevet i sproget Fortran kommunikerer med styresystemet), Posix 10: Supercomputing (tjenester, der forventes på store

supercomputere) og Posix I I: Transaction processing (transaktionsbehandling).

Postscript: Sprog, udviklet af softwarehuset *Adobe*, der anvendes til at definere grafiske tegn, f.eks. til brug for såkaldt desktop-publishing, hvorved PC'en anvendes til at producere tekstbaseret grafisk layout. En "postscript-printer" kan dermed uden videre udprinte grafik, der foreligger under postscript.

Printer: Periferienhed, der tilsluttet **computeren** udskriver **information** repræsenteret ved tekst og grafik. Baseres på forskellige principper, f.eks. typehjulsprinter, matrixprinter og laser-printer.

Processor: Betegnelse for den eller de maskinelle enheder i et IT-system, hvori **databehandling** finder sted. For at fungere må en processor instrueres. Instruktionerne findes i et **edb-program** og kan gå ud på, at **data** f.eks. beregnes, sammenlignes, konverteres eller gentages. Nu om dage er processorer indbygget i **halvlederchips**.

Processorlicens: Licens til brug af edb-program, som er knyttet til antallet af processorer, der er til rådighed på den enkelte server eller det enkelte system. Ved at knytte licensen hertil undgår parterne besværet ved at skulle optælle eller registrere de brugere, der har ret til at benytte programmet.

Program: Se **edb-program**.

Programdokumentation: Se **dokumentation**.

Programkode: Se **kildetekst**.

Programmel: Betegnelse for det immaterielle modstykke til de materielle dele af et IT-system (dets hardware, eller **maskinel**), der udgøres af systemets **program** eller programmer.

Programmenu: Se **menu**.

Programmeringssprog: Et nøje defineret sæt af regler (formalsprog) for den kommunikationsproces, der foreligger mellem **computeren** og den, der **programmerer** den. Til et programmeringssprog hører almindeligvis en **compiler**, dvs. et program, der oversætter (kompilerer) kildeteksten til objektkode.

Programmør: Person beskæftiget med at udvikle et **edb-program**.

Programvirus: Program, som – typisk med det formål at skade eller chikanere – er udviklet med henblik på at udfolde sine funktioner uden IT-brugerens viden og ofte med ødelæggelse af data til følge. Ved f.eks. at kalde bestemte kommandoer i styresystemet, som brugeren ikke umiddelbart kontrollerer, kan en programvirus give ordrer om at slette data eller at manipulere indtastede data i strid med brugerens intentioner. En programvirus er designet således, at den på tilsvarende måde genskaber sig selv i andre programmer, ganske som en biologisk virus gør det i den mikrobiologiske celle.

Protokol: Betegnelse for det sæt af regler, som må iagttages for at gennemføre en **kommunikationsproces** mellem to IT-systemer eller moduler eller for så vidt mellem to personer. Protokollen angiver hvordan man gennemfører en **transmission** af data (i henseende til mængde, funktion, og rækkefølge), uanset informationsindholdet af disse data.

Prototyping: Princip for systemudvikling, hvorefter man undervejs udvikler et antal foreløbige løsninger (prototyper), som enten skal danne grundlag for videreudvikling eller anvendes som illustrativ anskueliggørelse af, hvordan det endelige resultat vil blive. Fordelen herved er, at brugerne kan inddrages aktivt i udviklingsprocessen ved at forholde sig til de enkelte prototyper.

Pseudokode: Betegnelse for en detaljeret **dokumentation** af en programdel, der udarbejdes af **programmøren** eller af en gruppe af programmører, inden **kildeteksten** skrives. Pseudokode minder i det ydre om **kildetekst**. Der er tale om instruktioner i skreven tekst, affattet i et "næsten" **naturligt sprog**, men med præcise notationer for de tre basiselementer, der indgår i enhver programmering: sekvens, valg og gentagelse. Men modsat kildeteksten kan pseudokoden hverken læses af computeren eller oversættes maskinelt til kildetekst. Der skal en programmør til, før den kan udmønte sig i kildetekst.

Public Domain: Direkte oversat: i almindelig ejendom. Betegnelse for produkter, hvortil der ellers måtte forventes at være knyttet en immaterialret, som almenheden desuagtet frit kan bruge, f.eks. fordi denne ret er udløbet, opgivet eller bortfaldet. En opfindelse kan f.eks. falde i the public domain, fordi et patent er udløbet eller ophørt. Den typiske årsag hertil er dog, at rettighedshaveren (typisk til et programværk) én gang for alle beslutter

sig til at opgive enhver ret og utvetydigt meddeler dette til almenheden.

Public Key Krypteringssystem: Krypteringssystem, der bygger på asymmetrisk **kryptering**. De kommunikerende parter er hver udstyret med to nøgler, der (i kraft af visse primtalsmekanismer) er således forbundet med hinanden, at en tekst (eller i øvrigt et datamateriale, der er repræsenteret i **digital** form), der er krypteret ved hjælp af den ene nøgle (uanset hvilken), kun kan dekrypteres ved hjælp af den anden nøgle. Navnet "Public Key" skyldes, at man gennem et sådant **system** kan etablere en instans, hos hvem den ene (offentlige) nøgle er registreret, og som overfor potentielle kommunikerende parter erklærer, hvilke personer der har registreret deres offentlige nøgler. Disse erklæringer kan i kombination med et troværdigt bevis for sammenhængen mellem den offentlige og den hemmeligholdte nøgle udgøre et ofte uafviseligt bevis, bl.a. for en meddelelses autenticitet og integritet. Se også CA.

Pull: Træk. Betegnelse for det princip for spredning af information, hvorefter brugeren selv vælger den enkelte informationsmængde, f.eks. ved at klikke sig ind på bestemte hjemmesider på www. I modsætning til **push**-teknologien, hvor brugeren efter bestemte kriterier blot optræder som passiv adressat for informationen, kendetegnes informationsspredning efter pull-princippet ved, at det er brugeren selv, der kontrollerer informationsstrømmen. En sådan informationsformidling – der har umiddelbare lighedspunkter med biblioteksbesøg – betragtes almindeligvis som mindre "farlig" og giver derfor anledning til færre retlige restriktioner.

Push: Skub. Betegnelse for det princip for spredning af information, hvorefter informationen selv finder frem til brugeren, f.eks. spredes til ham efter forud givne valg. Man kan f.eks. betragte TV og radio som push-medier, idet seeren og lytteren – når først han har valgt station – ikke foretager aktive skridt for at afgrænse den informationsmængde, han forbruger. Ligeledes kan man betragte den information, der udbydes fra visse nyhedsgrupper (hvor man f.eks. kan abonnere på at modtage bestemte typer af e-mails) som udtryk for push-teknologi. Sondringen mellem push- og pull-medier spiller en vis rolle for den retspolitiske håndtering af forskellige typer af medier. Traditionelt har man således betragtet push-medier som stærkere og derfor mere "farlige", hvorfor de fra gammel tid har været underlagt en mere intensiv lovregulering.

RACE: Research and development in Advanced Communications technologies in Europe. EU-forskningsprogram.

RAD: Rapid Application Development. Også kaldet Rapid Prototyping. Almindeligt brugt betegnelse for princip til udvikling af administrative IT-systemer ved hjælp af prototyping. Ved hjælp af særlige værktøjer får man hurtigt en prototype til at fungere, som herefter danner grundlag for tilpasning og videreudvikling.

RAM: Random Access Memory. Efter sin sproglige sammensætning er en RAM en **lager**enhed, på hvilken man kan lagre og læse **data** uafhængigt af, hvornår sidste lagring eller udlæsning fandt sted, og hvor man derfor kan læse og skrive til hver enkelt lagerplads uden at skulle forbi andre. I daglig tale anvendes RAM primært om lagerenheder, der er indbygget i en **halvlederchip**, og som hviler på computerens strømforsyning. Det betyder i praksis, at data fra en sådan RAM-kreds mistes ved strømafbrydelse.

Rating: Ofte anvendt betegnelse for en praksis, hvorefter en informationstjeneste (f.eks. en hjemmeside) får "karakter" for sin lødighed eller egnethed til mindreårige brugere ("forbudt for børn" etc.). Ved hjælp af dertil indrettede kriterier forsynes informationstjenesten med en markering af, hvilke typer af informationer, man kan hente fra den, hvorefter brugeren kan indrette sit udstyr til at fravælge uønskede tjenester.

Referencemodel: Betegnelse for et sæt overordnede retningslinjer givet med sigte på et sæt af standarder vedrørende en given teknisk funktion. Se OSI.

Regnearksprogram: Program, der kan foretage en række samtidige beregninger på et større antal tal. Beregningerne forberedes ved, at de enkelte tal placeres i såkaldte celler, hvor de befinder sig på linje med eller overfor andre tal – en struktur, der tilsammen danner et "regneark" (eng.: spreadsheet). Idéen i et

regnearksprogram er, at samtlige tal beregnes fra grunden, hver gang regnearket aktiveres.

Request: I www-sammenhæng betegnelse for den digitale meddelelse, brugeren af en Internet-browser fremsender til en hjemmeside for at skaffe sig adgang (modtage kopi af) information, der ligger herpå.

Reverse analysis: Betegnelse for teknisk handling, der har til formål at undersøge et programs opbygning og funktion mv. I modsætning til **reverse engineering** er en sådan foranstaltning karakteriseret ved, at der ikke sker nogen ændringer i det undersøgte program, der for så vidt anvendes i teknisk samme skikkelse som hvis formålet ikke havde været at undersøge dets funktion mv. Retten til reverse analysis uden rettighedshaverens samtykke er fastlagt ved ophl. § 36, stk. 1, nr. 3.

Reverse engineering: Betegnelse for teknisk handling, der har til formål at skille et teknisk produkt ad for at se, hvordan det er opbygget. I relation til edb-programmel anvendes betegnelsen for undersøgelser af et programs tekniske indmad, f.eks. (og typisk) den protokol eller anden kommunikationsspecifikation, der bestemmer programmets **interoperabilitet** med andet programmel. For at foretage en sådan undersøgelse er det nødvendigt at frembringe kopier af programmet i en ændret skikkelse. Ved reverse engineering kan man for så vidt siges at "arbejde baglæns" fra programmets endelige skikkelse og til dets forstadier mv. Deraf betegnelsen. Ifølge ophl. § 37 er reverse engineering tilladt uden rettighedshaverens samtykke under visse nærmere betingelser.

RFC: "Request for Comments". Egl.: udkast med henblik på kommentering. Betegnelse for en serie dokumenter, der indeholder Internet-standarder og andre dokumenter, der berører Internet. Et væsentligt eksempel herpå er RFC 1591, der definerer et sæt principper for Domain Name System Structure and Delegation, dvs. opbygningen af de nationale og generiske toplevel-domæner.

RFID: *R*adio *F*requency *I*dentification *D*evice. Betegnelse for chip-baseret teknologi, hvorved der afgives elektroniske signaler fra en chip til en læseenhed. RFID-chippen indeholder en induktionsspole og en lille kobberantenne. Når spolen rammes af radiobølger fra en skanner, lader den energi op, så den kan sende informationer tilbage til skanneren med den indbyggede antenne. Derfor behøver chippen ikke batterier. Teknologien dækkes af internationale ISO-standarder. Den information, der afgives fra en RFID, kan f.eks. fortælle, hvorfra det tilknyttede produkt stammer, samt hvilke egenskaber det har. I kombination med andre teknologier kan man herigennem tegne et mønster, der kan være nyttigt, f.eks. fordi det giver information om produktets bruger eller om andre, der kommer i kontakt med produktet. I nogle henseender minder RFID-teknologien om stregkodeteknologien, og de mest iøjnefaldende fordele ved at gøre brug af RFID er da også – som det gælder for stregkodeanvendelsen – logistiske. RFID-teknologien har dog et langt større potentiale for datalagring, bl.a. fordi det giver mulighed for at aflæse data, uden at produktet er i fysisk kontakt med en skanner. Som eksempler på praktisk anvendelse af RFID teknologi i Danmark kan nævnes Brobizz-betalingsløsningen på Storebæltsforbindelsen. Man kan ligeledes forestille sig en anvendelse, hvorefter en kunde i et supermarked, der på forhånd har identificeret sig, via RFID kunne medtage varerne uden at skulle foretage betaling ved kassen, idet oplysningen om hvilke produkter, kunden havde taget med sig, ville være tilstrækkelig for at debitere kunden. Udbredelsen af RFID afhænger bl.a. af, hvor billigt den enkelte chip kan produceres. Prisen er for tiden 10-20 øre.

RIPE NCC: Réseaux Internet Protocol Européen Network Coordination Centre. Privat organisation, der efter bemyndigelse fra **Internet Society** har ansvar for tildeling af IP-adresser i Europa. RIPE står ligeledes for en søgefunktion igennem hvilken man kan konstatere, hvilken identitet der står bag en given Internet-adresse.

ROM: Read Only Memory. Lagerenhed i en **halvlederchip**, der kun lagrer **data** én gang, typisk af producenten, således at de herefter kun kan læses ("read only"). Anvendes typisk til lagring af **computerens styresystem** eller dele heraf. Se også EPROM.

RSA: Asymmetrisk krypteringsalgoritme, der blev foreslået i 1977 af matematikerne *Rivest, Shamir & Adleman* (deraf forkortelsen). En af RSA's egenskaber består i, at information, der krypteres ved hjælp af én nøgle i et nøglepar, ikke kan dekrypteres ved hjælp af denne nøgle, men kun ved brug af den anden nøgle i nøgleparret.

Run time-licens: Licens, der giver ret til at indbygge et program i et andet program, som licenstageren udvikler. Licensen sikrer, at det indbyggede program er tilgængeligt hver gang ("time") det udviklede program afvikles ("runs"). Sådanne licenser kan være nødvendige i relation til programmer skrevet i et programmeringssprog, der kræver samtidig tilstedeværelse af et **oversætterprogram**.

Sampling: Teknisk udtryk for en digitalisering af et lydbillede i analog form, der gør det muligt at genbruge det pågældende lydbillede i det uendelige og til helt nye formål – f.eks. en korstemme som gennemgående tone i et digitalt klaver.

SCPA: The Semiconductor Chip Protection Act – amerikansk rets ækvivalent til halvlederloven.

SCSSI: Service Central de la Sécurité des Systèmes d'Information. Fransk regeringsorgan, der forvalter den franske lovgivning vedrørende kontrol med anvendelse af krypteringsteknikker.

Server: En **computer**, der gør noget for en anden computer (kaldet **klient**). Serverens betegnelse knyttes til det, serveren gør for klienten. Hvis serveren f.eks. holder styr på de filer, klienten anvender, taler man om en filserver; hvis den styrer udprintningen af den information, der håndteres på klienten, tales om en print-server, og hvis den styrer kommunikation fra en hjemmeside om en webserver. Se også **client/server-arkitektur**, **netværk** og **lokalnet**.

SET: Secure Electronic Transactions. En protokolstandard til brug ved udveksling af krypteret information, udviklet af PBS, IBM, Mastercard og Visa med henblik på sikring af elektronisk handel med kreditkort (modsat hævekort). Køberens kort skal være registreret hos en SET-myndighed (f.eks. en bank eller PBS), der optræder som CA. Heri skal sælger være registreret som SET-sælger. Ved registrering modtager kortindehaveren en krypteringsnøgle, som bruges ved SET-forsendelser. Forud for køberens betaling sender sælger en krypteret og signeret meddelelse med unik information om den indgåede transaktion til køberen, som signerer denne meddelelse og returnerer den til sælger. Når sælger har verificeret den af køberen signerede meddelelse, cleares beløbet med kortudstederen, hvorved betalingen gennemføres.

Set-top boks: Hardwareenhed, der monteret på toppen af et tv-apparat gør det muligt at anvende tv-apparatet som computer og kommunikationsenhed, f.eks. med henblik på levering af video-on-demand-ydelser eller til bestilling af varer via tv-butikker.

SGML: Standard Generalised Markup Language: En af de første standarder til **opmarkering** af **hypertekst**-dokumenter. Standarden blev formelt offentliggjort i 1986 (som ISO-standard no. 8879-1986) og var banebrydende ved at beskrive, hvorledes et dokument kan opmarkeres uanset dets øvrige (fysiske) format. SGML-standarden ligger ligeledes til grund for den meget udbredte HTML-standard for opmarkering af Internet-dokumenter. Se også XML.

SH: Sø- og Handelsretten.

Shareware: Betegnelse for **program**, som rettighedshaveren – trods sin immaterialretlige beskyttelse – ikke håndhæver samtlige rettigheder til. En af idéerne i shareware-konceptet er, at **brugeren** skal betale efter brug (og ikke efter eksemplarfremstilling) og mere eller mindre på frivillighedens grundlag. Shareware-brugere vil dermed ofte først begynde at betale for produktet, når de for alvor beslutter sig til at gøre brug af det. Se også **Public Domain**.

Shrink wrap-aftale: Trykt aftalevilkår, der fremtræder bag plasticfolien på en programpakke, og som efter sit eget indhold angiver at være bindende i det øjeblik køberen af denne programpakke åbner plasticfolien (the "wrap"). Se også **click-wrap**.

Signatur: Af "signum", lat., "tegn". Et symbol, der afgives eller anerkendes af en part som en manifestation af dennes vilje til at vedkende sig indholdet af en erklæring, f.eks. en underskrift eller et fingeraftryk. Begrebet er

ikke defineret i dansk lovgivning, se derimod UCC 1.201 (39) (1987).

Sikkerhed: Vished for, at en ønsket tilstand vil blive opretholdt. Når den pågældende tilstand har relation til IT, taler man om IT-sikkerhed. Den, der ønsker at opnå IT-sikkerhed, kan være nødt til at anskaffe sig eller udføre en række sikkerhedstjenester, f.eks. **kryptering** (f.eks. for at opnå fortrolighed og uafviselighed) og **adgangskontrol**.

SILF: Sveriges Inköps- och Logistikförbund.

Silicon Valley: Geografisk betegnelse for industriområde (region) syd for San Francisco, Californien, og hvor en række højteknologiske IT-virksomheder er beliggende, bl.a. Apple Computers, Intel, Advanced Micro Devices, Xerox (Palo Alto Research center) og mange andre. Blandt andet på grund af sin mere fragmentariske struktur har Europa endnu ingen tilsvarende region. De europæiske fællesskaber forsøger på forskellige måder at råde bod herpå, bl.a. gennem teknologiske støtteprogrammer.

SIM: Subscriber Identity Module. Det intelligente chipkort, der identificerer brugeren af en GSM-mobiltelefon.

Simulcasting: Se **livestreaming**.

Site: Forkortelse for web-site.

SITO: Svenska Informationsteknologi-Organisationer (tidligere LKD, Leverantörföreningen Kontors- och Datautrustning). Svensk IT-brancheforening.

Skanner: En **indlæsningsenhed**, der konverterer **informationer** fra en visuel flade til **digitale data**, som indlæses i en **computer**.

Skriveenhed: Betegnelse for den komponent af et **system**, hvorfra maskinlæsbare **data** konverteres til skreven tekst, f.eks. som led i tekstbehandling.

SLD: Second Level Domain – andenordens domænenavn. Se **domænenavn**.

SME: Small and Medium Enterprise, se SMV.

S/MIME: Protokol tilknyttet **MIME**-protokolsuiten. Gør det muligt at kryptere og digitalt signere elektronisk post.

SMS: Short Message Service. Teknologi til udveksling af korte beskeder via GSM-mobiltelefoni. Ved hjælp af det alfanumeriske tastatur på mobiltelefonen indtaster afsender-abonnenten en besked, som herefter befordres som en del af det digitale signal, GSM-telefonen transmitterer. Beskeden modtages kort efter – afhængigt af den aktuelle belastning på nettet – på modtager-abonnentens telefon, hvor den kan læses i et display.

SMTP: Simple Mail Transfer Protokol. Protokol for, hvordan to computere kommunikerer med hinanden, når de skal udveksle post på Internet. Protokollen, der er fra 1982, er baseret på det engelske alfabet og understøtter således ikke de danske tegn, æ, ø og å.

SMV: Små og mellemstore virksomheder. Ifølge EU-kommissionens officielle definition er en SME (Small and Medium Enterprise) en virksomhed, som har mindre end 50 (små) henholdsvis 500 (mellemstor) medarbejdere, se EFT 1996 107/4. Andre EU-definitioner er afgrænset anderledes. De særlige hensyn til disse virksomheder indgår ofte i begrundelsen for at iværksætte særlige lovgivningstiltag mv., herunder ikke mindst på IT-området.

"Social engineering": Ofte anvendt udtryk for det forhold, at en gerningsmand ved at udgive sig som repræsentant for en beføjet leverandør eller systemansvarlig franarrer en IT-bruger dennes password under foregivende af at skulle anvende det til et teknisk formål, men med den hensigt at anvende passwordet til ulovlig indtrængen i brugerens system ved **hacking.**

Soft copy: Se **hard copy**.

Soft law: "Blød lovgivning". Ofte anvendt betegnelse for den form for regulering, der ikke betjener sig af tvangsprægede sanktioner (i form af retligt bindende forbud, påbud mv.), men som i højere grad tilskynder bestemte handlemåder ud fra andre incitamenter, f.eks. forestillinger om, hvad der er etisk korrekt handlemåde eller ønsket om at opnå langsigtede fordele ved koordineret adfærd. Regulering ved branchebestemte regler om "god skik" samt standarder er eksempler på soft law-regulering.

Software: Overordnet betegnelse for den **information**, der indgår i og styrer et IT-system. Begrebet omfatter ikke blot **programmer**, men også de hertil hørende manualer mv. samt de **data**, der anvendes af det pågældende system.

SOG-IS: Senior Officials Group on Security of Information Systems. Udvalg bestående af to embedsmænd fra hvert EU- og EFTA-med-

lemsland, der rådgiver EU-kommissionen i spørgsmål om IT-sikkerhed. Etableret ved rådsbeslutning 92/242/EØF, oprindelig med et to-årigt mandat.

SOHO: Small Office/Home Office. Arbejdspladser, som ikke er dele af større virksomheder, og hvor færre end 20 medarbejdere arbejder regelmæssigt mindst én dag om ugen.

Spamming: Af engelsk: Spam = dåsekød. Internet-slang for handlinger, hvorved et stort antal enslydende e-post-meddelelser sendes *uopfordret* til et stort og ofte ukendt antal brugere, f.eks. deltagerne i en Internet-nyhedsgruppe. Spam forekommer ofte som led i markedsføring på Internet og anses generelt for at være udtryk for en tvivlsom net-adfærd.

Spoofing: Af engelsk: Spoof = svindel. Internet-slang for handlinger, hvorved en person udgiver sig for at være en anden på Internet. Muligheden herfor er tilstede, fordi Internetprotokollerne ikke i sig selv gør det muligt at identificere afsenderen af en digital meddelelse (f.eks. en e-post).

Spreadsheet: Se **regneark**.

Sprog: De regler, der i en given sammenhæng bestemmer, hvordan **information** kan overføres ved hjælp af **tegn**. Ethvert **sprog** – såvel edb-sprog som talte sprog – består af et antal ord eller ordklasser (ofte suppleret med et alfabet), en syntaks (dvs. regler for brugen af forskellige ord-kombinationer mv.) og en semantik (dvs. regler for betydningsindholdet af de enkelte ord og instruktioner). Man sondrer mellem **naturlige sprog** (f.eks. dansk og engelsk) og **formalsprog** (f.eks. BASIC, Pascal og andre edb-sprog). Hvor det med et naturligt sprog lader sig gøre at overføre **information**, selv om sprogets regler tilsidesættes, er det formelle sprog kompromisløst i så henseende. Se også **højniveausprog**.

SPU: Struktureret programudvikling. **Program**udvikling, der foregår under overholdelse af en række præcise ordensmæssige regler for, hvorledes de enkelte instruktioner i programmet skal være placeret i forhold til hinanden. Se også **pseudokode**.

SRA: Shareware Registration Agreement. Aftale, der fastslår, hvilke forpligtelser brugeren af en **shareware**-applikation er underlagt, og som f.eks. vil give brugeren fri ret til at benytte den pågældende applikation til ikke-erhvervsmæssige anvendelser i en bestemt periode. Sådanne aftaler indgås ofte, når shareware-applikationen hentes ned fra en hjemmeside på Internet.

SSL: Secure Sockets Layer. Protokol for kommunikation til og fra web-adresser, der anvender TCP/IP-protokolstandarden. SSL gør det muligt at sikre den enkelte web-adresse ved gennem kryptering at tilvejebringe sikkerhed for autenticitet, integritet og konfidentialitet. Stort set alle de Internet-browsere, der anvendes i dag, har indbygget SSL-funktionalitet: Når en bruger henvender sig til en SSL-beskyttet hjemmeside, f.eks. for at erhverve varer og tjenester, etableres der en autenticitetsprocedure mellem kundens browser og den Internet-server, der står bag hjemmesiden: Først sender serveren et certifikat til browseren. Hvis browseren godkender certifikatet (ud fra en positivliste over, hvilke CA'er der anerkendes som troværdige), foregår den videre kommunikation krypteret, hvorved det sikres, at informationen hemmeligholdes og ikke ændres undervejs. I browserens adressefelt ses dette ved, at adressen angives med forkortelsen "https".

Stand alone: Betegnelse for IT-system, der udfører sine funktioner isoleret (f.eks. en enkeltstående PC), i modsætning til systemer, der er bundet op med andre systemer i et **netværk**.

Standard: En teknisk specifikation, som er godkendt af et anerkendt standardiseringsorgan til gentagen og konstant anvendelse, men hvis overholdelse ikke er obligatorisk i retlig forstand, medmindre der foreligger særskilt hjemmel herfor. Standarder findes inden for alle livsområder og indebærer, at produkter og fremgangsmåder bliver ensartede og dermed lettere at anvende, markedsføre, sikre o.m.a.

Standardrammesystem (eller standardrammeprogrammel): Edb-program, der markedsføres som standardprogram, men hvis implementering forudsætter et betydeligt element af tilpasning til kundens særlige behov mv. I yderpunkterne mellem **specialprogrammel** og **standardprogrammel** repræsenterer standardrammeprogrammel altså en mellemform. Inden for økonomiområdet er *Navision*

Financials og *Damgaard Axapta* fremtrædende eksempler på standardrammesystemer inden for området for økonomiske systemer (ERP-systemer).

Streaming: Teknik hvorved et værk bringes frem til en bruger i en proces, der finder sted medens brugeren oplever det, f.eks. i forbindelse med at en radioudsendelse afvikles (se også livestreaming) eller ved at brugeren oplever de begivenheder, der udfolder sig foran et web-camera (s.d.).

Struktur: Ordet struktur stammer fra latin "struere" (at opbygge) og beskriver almindeligvis en indre, systematisk opbygning. Ofte kan ordet rammende oversættes med "orden". En struktureret tekst – f.eks. en ordbog – betegnes som sådan, fordi den følger et klart sæt af regler for f.eks. forkortelser, henvisninger, udtaleangivelser etc. Struktureret programmering (også kaldet SPU) er programmering, der overholder en række nøje fastlagte planer mv. I systemteorien beskriver begrebet komponenterne i et system gennem deres indbyrdes forhold.

Struktureret programudvikling: Se SPU.

Styresystem: Også kaldet operativsystem eller driftssystem. Den sammenhørende programmængde, som styrer **kommunikationen** mellem IT-systemets komponenter. Et styresystem er altid i drift, medens **computeren** afvikler et program. De vigtigste styresystemer er i PC-miljøet: Windows, DOS (MS-DOS, PC-DOS), OS/2 og UNIX.

Sui generis: "Af sin egen art". Anvendes som betegnelse for regelsystemer, f.eks. inden for immaterialretten, der ikke følger de i forvejen etablerede rettighedsformer. Halvlederbeskyttelsen og den nye særlige beskyttelse af databaser er eksempler på sui generis-beskyttelse sammenlignet med den klassiske ophavs- og patentbeskyttelse.

Swap-fil: Fil frembragt som led i en funktion, der overfører visse dele af den information, der er lagret i RAM, på harddisk, således at brugeren oplever, at RAM-lageret er større, end det virkeligt er.

SWIFT: Society for Worldwide Interbank Financial Telecommunication. International organisation til varetagelse af bankoverførelser mellem forskellige banker. Stiftet i 1973. Omfatter ca. 1500 banker i 65 forskellige lande.

Sysop: Se BBS.

System: Sammenhæng, der kan adskilles overfor en omkringliggende eller tilgrænsende sammenhæng, og som kan opdeles i bestanddele (komponenter), der i overensstemmelse med de regler, der gælder for sammenhængen, udfører en funktion. Se også IT-system.

Systemprogrammel: Betegnelse for de **programmer** i et IT-system, der ikke træder frem overfor **brugeren**, og som brugeren ikke forventes at have indflydelse på. En væsentlig del af systemprogrammellet er **styresystemet**. Som andet systemprogrammel kan nævnes de programmer, der styrer enkelte enheder, såkaldte device-drivere.

Søgerobot: Program, der afvikles fra en udbyders hjemmeside (f.eks. <www.kapow.dk>), og som i kraft af en på forhånd sket indexering af informationsindholdet på et stort antal hjemmesider er i stand til at lokalisere et antal hjemmesider svarende til de søgekriterier, brugeren angiver.

T-handel. Handel via tv. Betegnelse for handelsformer, hvor tv-apparatet anvendes som mellemled til handel via tv-butikker mv. Kommunikation til den handlende sker ved set-top bokse, monteret det enkelte tv-apparat.

Tag: Digital markør, som indsættes i en digital tekst for at identificere forskellige punkter i teksten (f.eks. en afsnitsinddeling), som efterfølgende skal understøtte en **hypertekst**-applikation (f.eks. muligheden for at linke fra én hjemmeside til en anden).

Taktgiver: Se **klokke**.

Tastatur: – også kaldet keyboard. Den del af et IT-system, hvor brugerens – manuelle – indtastning af data finder sted. Et **alfanumerisk** tastatur minder i det store hele om tastaturet på en skrivemaskine, men er suppleret med en række taster, der aktiverer særlige funktioner.

TB, se Terabyte.

TCP/IP: Transmission Control Protocol/Internet Protocol. Standard for, hvorledes elektroniske meddelelser udveksles på **Internet**.

TEDIS: Trade Electronic Data Interchange Systems. Forskningsprogram under EU-Kommissionen, der tilsigter at understøtte anven-

delsen af EDI, bl.a. ved at styrke udbredelse af EDIFACT-standarden.

Tegn: Symbol (dvs. genkendeligt billede eller lydindtryk), der i overensstemmelse med en på forhånd vedtagen orden eller konvention kan udvælges af afsenderen i en **kommunikationsproces** og som indgår i det **sprog**, der ligger til grund for denne proces.

Tekst-TV: En envejs elektronisk tjeneste til informationsformidling, i hvilken en mængde **tegn** overføres med TV-signalet og modtages på TV-apparatet.

Telearbejde: Se **distancearbejde**.

Teledata: Dansk **videotex**-system, som etableredes i midten af firserne og ophørte i 1993. Teledata blev drevet af de danske teleadministratorer, der siden genoptog tanken med Datel-systemet, der blev igangsat og ophørte få år efter.

Telefax: Udstyr beregnet til fjernkopiering af dokumenter via telefonnet, hvorigennem dokumentets **information** transmitteres som en mængde punkter.

Telekommunikation: Teknologi til samtidig **kommunikation** over afstande. Omfatter bl.a. telegraf, telefon, telex, **telefax** samt forskellige teknikker til overførelse af **information**, der er repræsenteret **digitalt**. Se også **filoverførsel**, **elektronisk post**, EDI mv.

Telematik: Betegnelse for den disciplin (branche), der er opstået ved sammensmeltningen af **telekommunikation** og **datamatik**.

Telenet: Betegnelse for de luft- og kabelbårne forbindelser, der tjener som **transmissions**medium for offentlige **teletjenester**.

TeleSec: Sikkerhedssystem baseret på **asymmetrisk kryptering**, udviklet af PBS til brug for bl.a. **home banking**.

Teleshopping: Indkøb ved hjælp af telekommunikation. Begrebet omfatter ikke alene telefonisk bestilling af ydelser, evt. via audiotextsystemer, men også bestillinger og aftaleindgåelse ved brug af **Internet**.

Teletjeneste: Tjenesteydelse, der indbefatter **telekommunikation**. En teletjeneste kan enten tilvejebringes af et selskab eller en myndighed med koncession i medfør af loven af 1897 om telegrafer og telefoner, eller – for så vidt den pågældende ydelse er liberaliseret – af en uafhængig leverandør.

Teletrust: Taleord for betegnelsen "Trustworthy Telematics" – troværdig telematik. Tidligere benyttet betegnelse for visse tidlige initiativer, der tilsigtede at udvikle en infrastruktur på frivilligt grundlag til at understøtte brug af **Public Key Kryptering** i åbne net.

Terabyte: Forkortet: TB. Betegnelse for en datamængde bestående af en trillion tegn, dvs. 1.000.000.000.000 bytes – 1000^4 eller 10^{12}. Digitale lagerarealer af en sådan størrelse er så småt ved at komme i almindelig brug, f.eks. som grundlag for systemer til digital arkivering.

TETRA: Terrestrial Trunked Radio. Betegnelse for system til digital mobiltelefoni til professionel brug (f.eks. for hyrevognskørsel, beredskabstjenester, politi, forsvar etc. – også kaldet Professionel Mobil Radio, PMR). Systemet er baseret på europæiske standarder og tillader som følge af det anvendte digitale princip integration af forskellige typer af datatransmission (herunder såvel taletelefoni som dataoverførelser).

Thesaurus: Ordbogssystematik.

Token: Egentlig stafet. Teknisk betegnelse for en digital meddelelse, der sendes i forvejen i et netværk for at give adgang til en efterfølgende datastrøm.

Toplevel-domæne: Øverste niveau af Internetadresseringssystemet. Som toplevel-domænenavne anvendes dels nationalitetsbetegnelser (f.eks. ".dk" for Danmark), se **cc**TLD, dels generiske betegnelser (f.eks. "edu" for uddannelsesinstitutioner) – sidstnævnte primært (men ikke udelukkende) med sigte på amerikanske eller internationalt orienterede brugere, se **g**TLD. Herudover anvendes bl.a. ".org" og ".int" for nationale og internationale organisationer.

Topografi: En **halvlederchip** frembringes med udgangspunkt i et halvledermateriale (f.eks. silicium). Halvledermaterialet er stanset ud i en skive (eng.: "chip") og efter at være påført et fotoresistent materiale, placeres der en maske oven på denne skive bestående af en tynd film. På denne film er der tegnet et bestemt mønster, der angiver, på hvilke (mikroskopiske) områder siliciumskiven henholdsvis skal lede strøm eller virke som halvleder (hvorved ledeevnen bestemmes af, om der tilføjes en bestemt strøm udefra). Når masken

er placeret på siliciumskiven, eksponeres den for en kraftig stråling. Det ueksponerede materiale ætses herefter bort, og tilbage kommer et kredsmønster, oven på hvilket der lægges et lag ledende materiale. Når arbejdet hermed er tilendebragt, placeres det færdige siliciumstykke i en lille plastickasse, hvor det er forsynet med ben, der transmitterer de elektriske impulser til og fra den. Topografien er det tredimensionelle mønster, der udgøres af den række af sammenhørende billeder mv., der er skabt gennem denne proces, jf. nærmere halvlederlovens § 1, stk. 2. Ordet svarer til det amerikanske ord "maskwork", men bør ikke forveksle med "topologi", således som dette ord f.eks. anvendes i relation til datanet.

Topologi: Betegnelse for den måde, hvorpå et **netværk** er bundet sammen (struktureret). Trods dets tilsyneladende lighed hermed har ordet intet at gøre med ordet **topografi**.

Transaktionsspor: Summen af de informationer, der kan "spore" en registrering, så den kan følges fra data fødes (f.eks. når en udgift faktureres) til de fremtræder i et årsregnskab – og omvendt. Se også **kontrolspor**.

Transmission: Overførelse af **data**.

Tredjepartstrafik: Visse større organisationer har opbygget **netværk** til elektronisk **kommunikation** med kunder eller mellem tilknyttede afdelinger mv. Virksomheden lejer nettet (eller rettere: adgangen til det) af televirksomhederne; men på grund af de betydelige omkostninger ved den slags lejeaftaler har de typisk kun kunnet indgås af de stærkeste markedsaktører. For de mindre er det nødvendigt med bistand fra en tredjepart, der træder ind mellem brugeren og televirksomheden: lejer kredsløbene centralt og videreudlejer dem decentralt. Den trafik, der tilvejebringes herved, betegnes tredjepartstrafik.

Trojansk hest: Ofte anvendt udtryk for program, der udfører destruktive eller utilsigtede funktioner i et andet program på en måde, der er skjult for brugeren, f.eks. i form af en **programvirus**.

TRUSTe: Betegnelse for et amerikansk system til selvregulering af elektronisk handel: Den e-handlende anfører på sin hjemmeside et ikon (TRUSTe-mærket) som manifestation af, at han er juridisk forpligtet til at efterleve bestemte krav, bl.a. vedrørende beskyttelse af kunders personoplysninger. Siden sin fødsel i USA, har systemet bevæget sig mod Europa. Nærmere oplysninger på <www.truste.com>.

TTP: Trusted Third Party (troværdig tredjepart). Betegnelse for den eller de enheder i et system til **Public Key Kryptering**, som de kommunikerende parter vælger at udvise tillid til, f.eks. et **nøglecenter** eller en CA.

Tvangslicens: En række immaterialretlige love giver hjemmel til, at en person, der under visse nærmere angivne betingelser ønsker at gøre noget, som han er forhindret i ved en immaterialret (f.eks. et patent), kan få en særlig tilladelse hertil (en licens) ved dekret fra en offentlig myndighed. For de industrielle enerettigheders vedkommende (patenter, mønstre, varemærker mv.) er det typisk Sø- og Handelsretten, der udsteder sådanne tvangslicenser. Retten fastslår dermed ingredienserne i den aftale, der skal være gældende mellem rettighedshaveren og hans bruger, herunder først og fremmest reglerne om betaling af en afgift. Inden for ophavsretten anvendes begrebet i en noget anden betydning. Her kan ophavsretligt beskyttede værker (f.eks. musik) benyttes af visse brugere (f.eks. lokalradioer) uden tilladelse fra ophavsmandens organisation, blot der betales et nærmere fastsat vederlag til denne organisation. Vederlaget kan enten være fastsat ved aftale mellem bruger og organisation eller ved en beslutning fra Ophavsretslicensnævnet. I modsætning til de industrielle rettigheders bilaterale tvangslicens rammer den ophavsretlige tvangslicens (og aftalelicens) en flerhed af rettighedshavere.

Typehjulsprinter: Skriveenhed, der har indstøbt et fast antal typer (**tegn**) i et hjul. Gennem hjulets rotering placeres det ønskede tegn foran farvebånd og papir.

Uafviselighed: I relation til data, manglende mulighed for at benægte en kobling til en datamængde, f.eks. at et dokument er underskrevet, sendt eller modtaget. I papirets verden benytter man f.eks. kvittering eller anbefalet post til at opnå sikkerhed for uafviselighed. I kraft af disse redskaber, reduceres muligheden for at fragå underskrift, henholdsvis afgivelse. I den digitale verden er **digital sig-**

natur og **tidsstempling** mulige teknikker til sikring af uafviselighed.

UBVA: Udvalget til Beskyttelse af Videnskabeligt Arbejde under AC. UBVA fungerer bl.a. som en slags forfatterforening for faglitterære forfattere og har i den egenskab bl.a. vedtaget principper for digital udnyttelse af faglitterære værker.

UCC: Uniform Commercial Code. Uniform civillovbog beregnet til vedtagelse i de amerikanske delstater, udgivet af The American Law Institute – National Conference of Commissioners on Uniform State Laws.

UDUS: Universelt Data Udvekslings System. **Standard**, der anvendes i det danske betalingsformidlingsnet og ved massekreditering og debitering på PBS og giro.

UMTS: Universal Mobile Telecommunication System. Tredjegenerationssystem til mobiltelefoni, baseret på standarder vedtaget af ETSI. Systemet, som kan håndtere transmission af kompliceret grafik, levende billeder mv., ventes prøvekørt som pilotprojekt i år 2002.

UNCID: Uniform Rules of Conduct. Standard for digital kommunikation, vedtaget af ICC.

UNCITRAL: United Nations Commission on International Trade Law. FN's handelsretskommission. Har bl.a. udsendt en modellov om International Credit Transfers (1994) og om Electronic Commerce (1996).

UNIX: Styresystem udviklet til avancerede **mikrocomputere** og **minicomputere**. UNIX betegnes almindeligvis som et åbent system, fordi dets rettighedshaver (AT&T) har fulgt en politik om at stille systemets **kildetekst** til rådighed på lempelige licensvilkår.

Uploading: Den form for levering af en digital informationsmængde (som efter omstændighederne kan udgøre en digital ydelse), som sker ved, at overdrageren transmitterer informationsmængden til erhververen f.eks. via e-mail. Den hermed udførte kopi er altså igangsat af overdrageren.

URL: Uniform Resource Locator. Et dokuments adresse på Internet. Består af mindst to ord eller forkortelser, som er adskilt af punktummer, f.eks. ku.dk for Københavns Universitet under det danske **toplevel**-domæne.

U.S.: United States Report. Amerikansk domssamling.

USB: Forkortelse for Universal Serial Bus. Standard for, hvordan en seriel bus kan kobles til en computer. Standarden beskriver dels den enhed, der fysisk placeres i computeren, dels den kommunikationsprotokol, der anvendes. Dens primære fordel ligger dels i et meget brugervenligt kontaktpunkt (uden skruer mv.), dels i en høj tolerance overfor situationer, der ellers kan fremkalde driftsforstyrrelser (f.eks. at enheden tilsluttes medens systemet er tændt). I det praktiske liv anvendes USB-enheder bl.a. til overførelse af information fra brugerens pc til andet udstyr (lagerenheder, printere, kameraer, mp3-afspillere mv.).

Usenet: Verdensomspændende Internet-baseret forum for diskussionsgrupper som på grundlag af meddelelser fra de enkelte brugere anvendes til at udveksle synspunkter og information om en mangfoldighed af emner. Ofte kan en Usenet bruger stille et spørgsmål til en diskussionsgruppe, som fremkalder kvalificerede svar fra andre deltagere. Da enkelte Usenet-grupper har været anvendt til spredning af ulovlig information, har man specielt med sigte på denne teknologi overvejet en indholdsmæssig regulering.

USPQ: United States Patent Quarterly. Amerikansk domssamling.

USPTO: United States Patent and Trademarks Office. Det amerikanske patentdirektorat.

Utility: Betegnelse for – typisk små – hjælpeprogrammer, der understøtter anvendelsen af andre **programmer**, f.eks. ved at genskabe slettede **filer**, komprimere tekst, ændre skærmens udseende, redigere i tekster lagret i andet format o.m.a. Mange utility-programmer er tilgængelige på markedet som **shareware-programmel**.

V.??: Forkortelsesform, der identificerer de tekniske standarder fra ITU-T (tidl. CCITT), f.eks. V.34, der beskriver modemkommunikation ved 28.800 bits pr. sekund.

VANS: Value Added Network Services. Tillægstjenester ydet i tilknytning til sædvanlige telekommunikationsfunktioner som f.eks. datakommunikation og telefoni. En VANS-tjeneste kan f.eks. gå ud på, at data **konverteres** eller at eksisterende teleforbindelser udnyttes mere effektivt. Potentialet i et VANS-system ligger i muligheden for at forene IT-**in-**

telligens med **telekommunikation** og derigennem levere en skræddersyet tjeneste.

VAR: Forkortelse for: Value Added Reseller. Betegnelse for IT-leverandør, der videresælger en IT-løsning, som han selv har forædlet (f.eks. ved at tilføje ekstra **programmer**), og som nu fremtræder således, at hans eget navn og image træder frem overfor slutbrugeren.

Verifikation: Den handling, hvorved der skabes sikkerhed for, at signaturen på en digital meddelelse hidrører fra den angivne afgiver af den pågældende meddelelse, og at meddelelsen ikke er ændret efter at den digitale signatur blev udvirket på den.

Videnbaseret system: Se **ekspertsystem**.

Videotex: Tovejs interaktivt IT-baseret informationstjeneste til distribution af **information** til en større skare af **brugere**. Herhjemme udbød teleselskaberne i 1980'erne et sådant system – Teledata – der dog aldrig opnået noget større gennembrud. De nævnte funktioner udføres i dag med www-teknologien.

Virtual Reality: Samlebetegnelse for teknikker, der simulerer virkelighedens verden, f.eks. til brug for underholdning eller uddannelse. Udstyret med dertil indrettede apparater (sensorer), der registrerer brugerens bevægelser, og en maske fastspændt til ansigtet, der viser et rum, der reagerer på disse bevægelser, kan brugeren opleve, at han befinder sig i en anden – virtuel – virkelighed. De fænomener, han ser omkring sig, kan han påvirke med sine organer via de fastspændte sensorer og i overensstemmelse med de love, der på forhånd er indprogrammeret i systemet. Brugeren af et VR-spil kan for så vidt siges at befinde sig i **cyberspace**.

Virus, se **programvirus**

Visual Acting: Grafisk fremførelse af en skuespillers præstation, der indebærer, at alene skuespillerens ydre fremtrædelse (krop, ansigt mv.) anvendes, men ikke hans skuespilkunst, idet bevægelserne i den færdige film fremkommer ved en digital manipulation af en række billeder af denne fremtræden.

Volumenlicens: Licens til brug af et edb-program, som indgår i en form for storkundeordning, hvor brugervirksomheden (f.eks. en offentlig myndighed) opnår ret til at anvende en lang række af producentens programmer mod betaling af et fast beløb, enten som engangsbetaling eller periodevis. Typisk vil aftalen også indeholde en storkunde-rabat. Volumenlicenser anvendes typisk over for virksomheder og offentlige myndigheder med mere end 50 ansatte. En variant af volumenlicensen er den såkaldt åbne licens (open licence), der bygger på en genforhandlingsordning, hvor aftalen og de heri indeholdte maksima for antallet af eksisterende brugere mv., revideres (f.eks. årligt).

VPN: Virtual Private Network.

VR, se **Virtual Reality**

VTU-ministeriet: Ministeriet for Videnskab, Teknologi og Udvikling. Ministeriet er nedsat ved regeringsskiftet i 2001 og viderefører bl.a. det arbejde, der tidligere blev udført af Videnskabsministeriet.

W3C: World Wide Web Consortium. Standardiseringsorganisation, der arbejder med standarder for Internet-kommunikation. Har bl.a. udarbejdet PICS-, P3P og XML-standarden.

WAN: Wide Area Network – betegnelse for **datanet**, der i sin **topologi** svarer til et **lokalnet**, men som forbinder **terminaler** over større indbyrdes afstande, hvorfor det typisk forbindes via offentlige net til **telekommunikation**.

WAP: Wireless Application Protocol. Standard, der definerer et format for overførelse af information via terminaler til mobiltelefoni og Internet, så mobiltelefonen kan bruges som Internet-terminal, f.eks. til at understøtte hurtig specifik informationssøgning, når man er "på farten", enkle bestillinger (f.eks. af flybilletter) og andre opgaver, der ikke kræver udveksling af store informationsmængder. WAP-standarden er udarbejdet af et konsortium bestående af bl.a. L.M. Ericsson, Motorola og Nokia og er baseret på TCP/IP-standarden. Med til protokollen hører programmeringssproget WML (Wireless Markup Language), som er baseret på XML.

Web: Se **World Wide Web**.

Web-browser: Se **browser**.

Web-casting: Radio- eller tv-udsendelse, der transmitteres via Internet uden samtidigt at blive udsendt i radio eller på tv. Adskiller sig fra **livestreaming**, hvor udsendelsen samtidig fremføres i radio eller på tv.

Web-kamera: Også kaldet web-cam. Almindeligt anvendt betegnelse for et kamera, der er tilsluttet Internettet på en sådan måde, at en bruger ved at koble sig op via en URL kan iagttage det, der sker foran kameraet. Webkameraer bruges såvel til video-kommunikation mellem brugere som til forskellige former for streaming (s.d.) mv.

Weblog, også kaldet Blog: Almindeligt anvendt betegnelse for en hjemmeside, der tjener som en slags offentlig dagbog for en person, og som f.eks. giver udtryk for dennes synspunkter eller personlighed. Ofte opdateres en blog dagligt med betragtninger, oplevelser el.lign.

Web-løsning: Database, der er forbundet med Internet, og som er forbundet med andre databaser ved brug af særlige principper for grafisk repræsentation af data.

Web-pact: Se **click wrap-aftale**.

Web-phishing, se Phishing.

Web-server: Computer tilsluttet Internet, og som er programmeret til at levere digitale ydelser til brugere af www-teknologien, typisk ved at afgive informationer fra en hjemmeside.

Web-site: Samling af web-sider, typisk med ensartet struktur og design. Se **hjemmeside**.

Wi-Fi (802.11-standarden): Standard for datakommunikation via lokalt trådløst net. Efter sin nuværende implementering understøtter standarden en rækkevidde på 70-100 meter, hvilket gør den velegnet til opkoblinger inden for områder, hvor personer er til stede permanent eller midlertidigt (kontorer, private hjem, lejlighedsopgange eller på såkaldte hotspots, s.d.).

Windows: Varemærke tilhørende Microsoft Corp., USA. Dækker en serie af produkter til PC-baserede IT-systemer. Blev oprindeligt udviklet som en grafisk grænseflade til DOS-styresystemet, der på samme måde som tidligere set i den populære Macintosh-computer fra Apple Computer anvendte "point and click"-teknikker baseret på **mus**. I senere versioner, herunder senest Windows 95, Windows 98, Windows NT og Windows CE, er Windows blevet et selvstændigt styresystem, hvis grænseflader bl.a. har sat standarden for, hvorledes applikationsprogrammel ("Windows-programmer") udvikles til PC'er.

WIPO: World Intellectual Property Organization. FN's særlige agentur for immaterialret.

WML: Wireless Markup Language, we WAP.

Work around: Egentlig omgåelse. Ofte anvendt teknisk udtryk for fejlrettelse, der ikke løser det tekniske problem, der ligger bag fejlen, men dog på anden måde – f.eks. ved at anvende programmet på en anden måde – gør det muligt for brugeren at løse de IT-funktioner, som fejlen ellers ville have ramt.

Workstation: Også kaldet arbejdsstation. Upræcist begreb, der i sin oprindelige betydning kunne forklares med sin direkte oversættelse og forstås som IT-terminal. Anvendes i stigende grad om **terminaler**, der alene står for en enkelt – og ofte mere krævende – type databehandling (f.eks. grafik eller CAD/CAM).

WP4: Working Party Four. Den arbejdsgruppe under ECE, der i sit arbejde med EDI bl.a. har udviklet TEDIS-standarderne.

World Wide Web: "Det verdensomspændende spindelvæv". Betegnelse for den forbindelse mellem informationsudbydende computere ("Web-servere"), der tilvejebringes via informationsforbindelser, som forskellige informationsudbydere knytter til deres databaser (**hjemmesider**). HTTP-protokollen (HyperText Transfer Protokol) angiver på forhånd den måde, de enkelte hjemmesider kommunikerer med hinanden på. Inden for hver hjemmeside er informationen typisk lagt i **hypertekst**-form under HTML-standarden.

WTO: World Trade Organization. Den organisation, der med hovedsæde i Geneve, administrerer overenskomsten om oprettelse af WTO (tidligere GATT-overenskomsterne).

www: Se World Wide Web.

X.??: Forkortelsesform, der identificerer de tekniske anbefalinger fra CCITT, f.eks. *X.21*, der beskriver **grænseflader** mellem en **terminal** og et offentligt **datanet**, *X.25*, der definerer tekniske grænseflader til offentligt kommunikationssystem, hvori **data** transmitteres som pakker, *X.200*, der giver anbefalinger for tilpasning af OSI-referencemodellen, og *X.400*, der på grundlag af OSI-referencemodellen giver en række protokolstandarder for international håndtering af **elektronisk post** og *X.509*, der beskriver opbygningen af et certifikat til brug for kryptering og digital signa-

tur. Nærmere oplysninger om disse standarder findes på <www.itu.int>.

XML: Extensible Markup Language. Standard for opmarkering af Internet-dokumenter, der bl.a. gør det muligt også at opmarkere et dokuments informationsindhold. Standarden, der blev vedtaget i 1998, understøttes af World Wide Web Consortium og forventes indbygget i fremtidens generationer af tekstbehandlingsprogrammel.

X/Open: International privat organisation, hvis formål er at hidføre såkaldt åbne IT-systemer for almene IT-applikationer baseret på internationale **standarder**.

Zone: Ofte anvendt betegnelse for den potentielle mængde af Internet-adresser, der kan befinde sig under et givet domæne. F.eks. kan man sige, at alle Internet-domæner under .dk er placeret i .dk-zonen.

Åben licens (open licence), se volumenlicens.

Kapitel 1. INTRODUKTION TIL IT-RETTEN

1.1. Emnet

1.1.a. Information som lovgivningsproblem

Det funktionelle behov

Behandling og udveksling af information spiller en central rolle for vor livsførelse. De beslutninger, der former vor tilværelse og fastslår vore relationer til omverdenen, træffes på grundlag af information i form af viden, kundskab, indsigt, erfaring eller ekspertise. Ofte er resultaterne af vore beslutninger tilmed informationsbærende, f.eks. som sproglige udtryk, meningstilkendegivelser eller lignende. For så vidt er ethvert samfund et "informationssamfund".

Ethvert samfund og enhver organisation eksisterer i kraft af en kontrolleret formidling og anvendelse af information. Statslig magt udøves ved, at direktiver og handleforskrifter kommunikeres til aktørerne. Også talrige private organisationer og virksomheder holdes sammen i kraft af deres informationssystemer. Det er almindelig kendt, at et moderne pengeinstitut vil gå konkurs, hvis det i mere end tre dage mangler adgang til sine IT-systemer. Handelen i samfundet beror på, at den enkelte aktør har kendskab til (information om), hvorledes hans med-aktører vil handle.

IT

Den digitale informationsteknologi (i det følgende kaldet IT) har givet os en række nye, kraftige værktøjer til at understøtte disse mange former for informationsbehandling. Mulighederne for at bruge IT i snart sagt alle livsforhold er så righoldige og effektive, at de på fundamental vis har ændret vor brug og afhængighed af information. I løbet af de sidste 40 år er der sket en så eksplosiv udvikling i forholdet mellem prisen og effektiviteten af sådanne teknologier, at IT i dag anvendes i alle dele af samfundslivet på en måde, der nærmest har defineret det post-industrielle samfund. Dertil skal lægges, at teknologien udbydes af en IT-industri, som i et stadigt mere intenst samspil med "informationsindustrien" er blevet vor største sektor. Det er altså ikke selve begrebet *information*, der er nyt, men derimod forestillingen om, at information i sig selv er et aktiv med en økonomisk værdi, kombineret med de

særlige måder, hvorpå denne værdi udmønter sig (f.eks. ved kopiering og påvirkning mv.).

IT-politik og IT-ret

I takt med denne udvikling er det moderne samfund blevet stillet overfor en række nye problemstillinger, der gradvis har aktualiseret sig på den politiske dagsorden og som juridiske problemer. Problemerne udspringer bl.a. af, at moderne IT har skabt nye muligheder for at samle, systematisere, afgive og modtage information og heraf følgende nye magtkonstellationer og risici.

I de nordiske lande har der været tradition for at fremstille de retlige problemer, der opstår ved brug af moderne IT, i særskilte discipliner. I Danmark taler man generelt om IT-ret. Norge og Sverige har foretrukket betegnelsen "Retsinformatik" eller "informationsret", omend svensk terminologi med *Seipel* (2001), nu i stigende grad taler om "IT-ret". I UK og USA taler man om "Computer Law/IT Law" eller – mere generelt – om "Computers and the Law/IT and the Law".

Med tiden er det blevet stadigt vanskeligere at opretholde sådanne discipliner. Hvor IT i sine tidligere udviklingsfaser hovedsagelig blev anvendt til at løse administrative og driftsmæssige beregningsopgaver, er der i dag ingen grænser for, hvordan og hvornår IT anvendes i de forskellige samfundssektorer. Som allerede antydet sker der i disse år en sammensmeltning med informationsindustrier, herunder navnlig underholdningsindustrien (film, spil mv.), forlagsindustrien og nyhedsindustrien. På medieområdet flyder IT-anvendelsen gradvis over i teleanvendelsen. I takt hermed tales i stigende grad om ICT (Information and Communication Technology).

Disse tendenser ses bl.a. ved de stadigt hyppigere fusioner, hvor "gamle" IT-virksomheder går sammen med underholdnings-, nyheds-, forlags-, tv-, radio- og televirksomheder, se neden for i afsnit 2.I.c. om det såkaldte *konvergensproblem*.

Fagelementer

På et generelt plan kan man fremdrage det fællestræk ved disse områder, at de beskæftiger sig med den juridiske regulering af *udvikling*, *anvendelse* (drift) og *overdragelse* af systemer til behandling af digital information eller af produkter og tjenester, der er således integreret med digital informationsteknologi, at kvaliteten af denne har afgørende betydning for ydelsen.

Efter en vis systematisk betragtning "begynder" dette emneområde, når ny IT udvikles, og der derfor opstår behov for immaterialretlig beskyttelse. Den *materielle* side af et informationssystem (silicium, plasticmaterialer etc.) er relativt billig, men til gengæld er der store omkostninger forbundet med at frembringe den *immaterielle* side i form af den information (programmer,

litterært og kunstnerisk indhold, knowhow mv.), der styrer systemerne og giver dem indhold for brugeren. I forhold til råvareprisen repræsenterer det færdige IT-produkt en betydelig værditilvækst, hvis værdi for rettighedshavere beror på, hvor mange eksemplarer af informationsproduktet, der kan sælges. Hvis en chip eller et standardprogram sælges i millioner af eksemplarer for en pris adskillige tusinde procent over de *variable* produktionsomkostninger (altså fraregnet de omfattende udviklingsomkostninger), kan en sådan virksomhed hurtigt vise sig profitabel. Netop denne effekt er en af hovedårsagerne til de voldsomme kurseksplosioner, visse nye informationsbaserede virksomheder har oplevet fra tid til anden.

Beskyttelsesbehovet

Kunne IT-produkter frit kopieres af enhver, ville der intet incitament være til at investere i nye udviklingsprojekter. Udviklingsomkostninger ville aldrig kunne tjenes hjem, eftersom kunderne ikke kan forventes at betale for information (og informationsbaserede produkter), som de kan få gratis. Da de fleste anser teknologisk innovation som et gode, er der almindelig enighed om behovet for retsbeskyttelse af IT. Disse problemer – der behandles i bogens anden del, kapitlerne 6-11 – er vanskelige. Har man en eneret til at udnytte information (et program, en database, halvledertopografien i en chip, en patenteret fremgangsmåde mv.), kan man dermed afskære andre fra at udnytte denne information. Er informationen noget værd, kan man sætte sine priser uden risiko for konkurrence. Den retspolitiske beslutning om, hvor stærk eneretten bør være, bliver dermed også en beslutning om, hvor fri konkurrence man ønsker.

IT er kostbar at udvikle. For små og mellemstore virksomheder kan det derfor være nødvendigt at finansiere IT-udvikling via eksterne investorer mod sikkerhed i det produkt, udviklingen resulterer i. Denne sikkerhed er vanskelig at give, når resultatet af investeringen er noget immaterielt (en immaterialrettighed eller en informationsmængde). Det immaterielle formuegode opfører sig anderledes end de fysiske aktiver, der sædvanligvis er genstand for sikkerhedsstillelse. Derfor er det nødvendigt at se på, hvorledes der skabes sikkerhed i IT-systemer med henblik på *finansiering*. Disse regler præsenteres i kapitel 12.

Regulering

Selve brugen af IT er i visse tilfælde underlagt *retlig regulering*. Lovgivningen om persondatabeskyttelse begrænser den måde, hvorpå data om enkeltpersoner lagres og anvendes; visse regler sætter grænser for, hvorledes IT-systemet kan kobles op til offentlige net til telekommunikation, andre regulerer anvendelse af IT til særlige formål (f.eks. betalingskortvirksomhed og bog-

holderi), og endnu andre lægger restriktioner i adgangen til at markedsføre IT. En lignende funktion har den erstatningsretlige regulering. Disse spørgsmål behandles i bogens anden del, kapitlerne 13-18.

E-handel og IT-aftaler

I takt med at IT-systemerne bliver brugt til at kommunikere ønsker og behov, opstår behovet for også at indgå og opfylde aftaler på denne måde. Som samlet betegnelse for sådanne former for digital samhandel taler man i dag om elektronisk handel eller e-handel. Til disse spørgsmål hører bl.a. en afklaring af, hvorledes den digitale ydelse håndteres efter køberetlige, ophavsretlige og andre regelsæt samt spørgsmålet om selve den digitale aftaleindgåelse (herunder afgivelse af tilbud og accept ved brug af digital teknologi). Disse spørgsmål behandles i kapitel 19-20.

Overdragelse af IT

IT-ydelser er blevet en handelsvare. En aftale om *overdragelse af IT* præges af, at der er tale om en kompleks ydelse, der tilmed fremstår som immateriel information. Det gør det vanskeligt at indgå, opfylde og fortolke sådanne aftaler. Retssystemet er ikke altid parat til at befatte sig med overdragelse af ydelser, der ikke kan sanses med hænder, ører eller øjne, og som tilmed kan befinde sig flere steder på en gang, ganske som anden information – tanker, idéer mv. – kan det. Derfor frembyder aftaler om IT-overdragelse særegne problemer, som nødvendiggør en særlig tilpasning af kontraktsrettens almindelige regler. Disse problemer behandles i kapitel 21-22.

Tekniske spørgsmål

Flere af bogens kapitler behandler de tekniske problemer, der opstår, når en IT-relateret sag skal præsenteres for en dømmende ret eller i øvrigt kompetent instans. I bogens indledende kapitler 2-3 beskrives visse almene aspekter af teknologien. Kapitel 4 behandler læren om IT-sikkerhed. I kapitel 16 gøres nogle bemærkninger om, hvorledes et digitalt dokumentbevis føres, og i kapitel 23 præsenteres nogle af de problemer, der opstår ved konfliktløsning ved domstole, administrative organer og gennem alternativ konfliktløsinng.

I.1.b. IT-rettens metodeproblemer

Fagets udvikling

Retsvidenskabens interesse for IT-retlige spørgsmål er gradvis vakt i takt med teknikkens udbredelse. I den amerikanske retslitteratur tog udviklingen fart i løbet af 1980'erne. Tilsvarende gælder for Danmark, der først fra og med midten af 1980'erne udviklede en egentlig edb-ret eller IT-ret. Se for en nærmere gennemgang heraf i min disputats fra 1988 Edb og Ansvar (*E&A*) kap. 2.

Selvom de fleste i dag er enige om behovet for retsvidenskabelig behandling af IT-samfundets problemer, er der ikke enighed om, hvordan denne opgave bør gribes an. I sine første år (fra slutningen af 1970'erne og fremefter) blev den metodemæssige afgrænsning af IT-retten sjældent diskuteret. IT-retten var i hovedsagen domineret af praktikere, der var mere optaget af håndgribelige resultater end af faglige grænsestridigheder, sml. forhandlingerne ved det nordiske juristmøde i Reykjavík i 1990, se NJM 1990, bd. II, s. 225 ff.. og mit indlæg i festskriftet *Suum Cuique* – retsvidenskabelige afhandlinger fra Københavns Universitet (1991).

"Edb og Ansvar"

I *E&A* betonede jeg, at IT-retten (dengang kaldet edb-retten) står overfor et *"beskrivelsesproblem"*, der hovedsagelig skyldes, at fagets emneverden ikke umiddelbart fremstår som veldefineret og klart beskrevet for fagets udøvere. Fordi information i en række henseende fremtræder anderledes end de materielle aspekter, man har været vant til at håndtere inden for rammerne af veletablerede regelgrundlag – som f.eks. købeloven, ophavsretsloven, produktansvarsretten mv. – er IT-juristen nødt til at *beskrive* de faktiske forhold og den tilhørende retlige ramme, han har med at gøre, inden han kan give sig i kast med retsanvendelsen. Denne beskrivelse er ofte vanskelig. For det første er der tale om en *kompleks* teknologi med en vanskelig terminologi. For det andet er denne teknologi for en stor dels vedkommende *immateriel* og derfor ikke rigtigt til at tage og føle på. Et digitalt informationssystem er ikke som en bygning for entrepriseretten eller en bil for færdselsretten. Information har i sig selv ingen fysiske fremtrædelsesformer. Dertil kommer, for det tredje, at IT-området ikke som andre særlige juridiske discipliner kan støtte sig til et velafgrænset *regelsæt*, der på samme måde som straffeloven for strafferetten sætter dagsordenen for fagets indhold og metode.

Analytisk metode

En anerkendelse af beskrivelsesproblemet fører til, at juristen undertiden må befatte sig med analyser, der i grunden er fremmede for den sædvanlige "lawyers law", *inden* han giver sig i kast med selve IT-rettens retsanvendelse. Dette behov opstår dels i tilfælde, hvor retskildegrundlaget er spinkelt – som det f.eks. gælder for forestillingen om, hvordan "bonus pater" handler i relation til IT – dels i tilfælde, hvor resultaterne må udledes på grundlag af almindelige retsregler, der ikke tager højde for teknologiens særpræg, og hvor regelgrundlagets forudsætninger mv. følgelig må afklares. Sådanne analyser er f.eks. nødvendige for at afklare de centrale IT-ophavsretlige spørgsmål, læren om IT-fi-

nansiering, spørgsmålene om bevisværdien af IT-medier, kontraktsretten og den almindelige erstatningsret.

Info-politik

Diskussionen om denne synsvinkel er aldrig helt blevet afsluttet. I dag er det imidlertid et faktum, at de spørgsmål, som ligger i beskrivelsesproblematikken, står meget højt på den politiske dagsorden i forsøgene på at tilrettelægge det politiske og retlige grundlag for "informationssamfundet", jf. bemærkningerne i afsnit 5.1. om lovgivning på IT-området. I mit bidrag til rapporten om Info-samfundet år 2000 (se bilagshæftet, s. 113 ff.) fremlagde jeg en række principper for, hvorledes man kunne regulere den digitale informationsanvendelse. Se ligeledes mit indlæg i rapporten om Det Digitale Danmark (November 1999), bilagshæftet s. 109 ff. og den svenske udredning i SOU 1992:110: Information och den nya InformationsTeknologin, s. 155 ff., der diskuterer spørgsmålet, om information er "egendom". En række love er allerede blevet tilpasset for at tage højde for de særlige problemer, som digital information rejser (eksempelvis ophavsretslovens regler om digital kopiering mv. samt loven om elektroniske signaturer).

Når man netop kan opretholde IT-retten som et fagområde, er det fordi visse mekanismer og egenskaber er fælles for al IT. Navnlig for den jurist, der ingen teknisk uddannelse har, er det nødvendigt at få kendskab til i hvert fald disse grundlæggende aspekter, som ofte træder frem i de IT-retlige problemer.

1.1.c. IT-rettens opgaver

Anskues IT-rettens teoretiske og praktiske opgaver på denne vis, rummer disciplinen fire bestanddele: en retsteori, en teknisk del, en retsdogmatik og en retspolitik. IT-rettens *metode* er så småt skitseret i det foregående, men uddybes i kapitel 2 med omtalen af beskrivelsesproblematikken. IT-rettens *tekniske* del analyserer bl.a. de aspekter af teknologien, der må indgå i den juridiske analyse, se kapitel 3. IT-rettens egentlige *retsdogmatik* – som er dens vigtigste bestanddel – beskæftiger sig med de retsspørgsmål, der opstår ved udvikling, anvendelse og overdragelse af IT. I nærværende fremstilling omfatter dette hovedparten af bogens anden, tredje og fjerde del.

Retsdogmatik og retspolitik

Det er vigtigt at notere, at en række af IT-rettens opgaver strengt taget ikke har retsdogmatisk karakter. En stor del af IT-juristens arbejde vil bestå i at skabe et udfyldende eller retskonstituerende regelsæt. Udfyldende i tilfælde, hvor de almindelige regler er uklare eller ikke egnede til at danne grundlag for en

påtænkt aktivitet. Konstituerende i tilfælde, hvor der indenfor en organisation eller som led i egentligt retspolitisk arbejde skal skabes et retsgrundlag for IT-tekniske foranstaltninger eller anvendelser. I en stringent juridisk systematik må disse spørgsmål siges at høre til IT-rettens *retspolitiske* del. Denne indrubricering vil dog sjældent blive opfattet således i det praktiske liv.

1.2. Historisk introduktion

1.2.a. Emnet

IT-historien kan beskrives med udgangspunkt i teknologiens forskellige aspekter, herunder de kommunikative og matematiske funktioner og den elektroniske indmad. Dermed kan man vælge at trække linier tilbage til flere og vidt forskellige forløb, der hver for sig ikke umiddelbart kan siges at have meget med hinanden at gøre. Anskuer man f.eks. IT som en teknologi til at *lagre og præsentere* data, så handler IT-historien om menneskets brug af information, se herom *Peter Blume*: Fra tale til data (1989), s. 44 ff. Tager man derimod udgangspunkt i muligheden for at foretage *beregninger* af tal, går historien helt tilbage til den græske abacus og videre til de første regnemaskiner mv. Ser man på muligheden for effektiv *informationsspredning*, er det nærliggende at føre IT-historien tilbage til de bogtrykkerteknologier, der på så afgørende vis ændrede informationsstrømmen i perioden op til oplysningstiden. Og anskuer man endelig IT som synonymt med den teknologi, der muliggør *digital databehandling* ved hjælp af elektronisk datarepræsentation, har IT-historien udspillet sig inden for godt et halvt århundrede, nemlig siden 1946, hvor den første elektroniske computer – ENIAC – så dagens lys.

Som disse eksempler viser, er IT-udviklingen ikke forløbet lineært, men nærmest som i et netværk. I dag repræsenterer IT en fusion mellem vidt forskellige vidensområder og vidt forskellige typer af teknologier, der på forskellige tidspunkter dukker op med vekslende styrke og intensitet, og som har resulteret i en lang række *konvergensteknologier*. Det er blevet mere og mere tydeligt, at nutidens forskning i ny teknologi er baseret på en vid sammensmeltning af fagområder: Programteori, avanceret matematik, viden om psykologiske reaktionsmønstre og kunstnerisk virksomhed. Denne konvergens træder klart frem, når man kaster blikket på de forskellige brancher, der i dag befinder sig på IT-markedet.

Denne flerhed af centrale aspekter gør studiet af IT-historien ganske fascinerende, men vanskeliggør en konsistent gennemgang af forløbets forskellige etaper. Følger man én tråd i netværket (anvendelsen af en bestemt teknologi), vil den undertiden slutte, hvor anvendelsen af en ny teknologi – med et ganske andet udspring – påbegyndes. I det følgende trækkes linjerne *først* fra de forskellige teknologiske komponenter, der indgår i et moderne IT-system: de maskinelle dele, programvaren, informationsindholdet. *Dernæst* fokuseres der på, hvilke funktioner IT gennem tiderne har opfyldt.

I.2.b. Hardware

Regnemaskinen

Den elektroniske computer rummer virkeliggørelsen af en tanke, der er lige så gammel som den menneskelige civilisation, nemlig at maskinen skal kunne supplere det menneskelige intellekt på de områder, hvor det enten ikke rækker eller ikke orker – ganske som værktøjer og maskiner gør det i relation til vore fysiske begrænsninger. Derfor var det navnlig arbejdet med at tælle og beregne (herunder i forbindelse med militære beregninger inden for ballistik og kryptering), der igangsatte hele denne teknologi. Beregninger består som bekendt af lange rækker af ensartede taloperationer, der gerne skulle munde ud i ét og kun ét facit. Informationsteknologiens første indsats var derfor at udvikle en avanceret talbehandler, der kunne opfylde dette formål.

I 1642 konstruerede den franske filosof og matematiker *Blaise Pascal* en simpel regnemaskine, der kunne addere og subtrahere. Den blev et forbillede for alle senere regnemaskiner, og Pascal kom til at lægge navn til et af de mest udbredte programmeringssprog i dag. I perioden fra slutningen af 1930'erne udviklede tyske og amerikanske forskere en serie ganske avancerede relæbaserede regnemaskiner. Udviklingen tog særlig fart i krigsårene, hvor der var brug for regnekapacitet til at dechifrere fjendens kodede meddelelser. Mest berømt blandt disse var den maskine, ved navn z-3, som tyskeren *Konrad Zuse* udviklede, men som blev ødelagt under et bombardement i 1944. Ligeledes kan nævnes IBM's "Mark I" udviklet under ledelse af professor *Howard Aiken*.

Datamaskinen

Den første "datamaskine", der formåede at behandle data ad elektronisk vej, og som derfor kan karakteriseres som verdens første elektroniske computer, var "the ENIAC" (the Electronic Numerical Integrator And Computer), som ingeniørerne *P. Eckert* og *J. W. Mauchley* udviklede på Moore School i Pennsylvania i

årene 1943-46. Teknikken i ENIAC var baseret på radiorør. Hvert radiorør kunne lagre og behandle den datamængde, der lader sig repræsentere i et elektromagnetisk felt, der enten er positivt eller negativt – en "bit" (fork. for *bi*nary digi*t*). Dette indebar dels en række praktiske problemer med hensyn til nedkøling, dels et problem med hensyn til den relativt svage driftssikkerhed. Maskinen vejede ca. 30 tons, fyldte et gulvareal på 135 m² og havde et gigantisk antal enkeltkomponenter: 20.000 radiorør, 70.000 modstande, 18.000 kondensatorer og 6.000 relæer. Driften forudsatte en elektricitetstilførsel på 150 kilowatt. Derfor måtte radiorørene konstant afkøles. Alligevel var teknologien i ENIAC revolutionerende. Ved at repræsentere data med elektromagnetisme kunne processerne foregå langt hurtigere, end det havde været muligt ved hjælp af de tidligere elektro*mekaniske* systemer.

Transistoren

I 1947 gjorde et hold forskere ved Bell Laboratories i USA en opfindelse, der siden skulle revolutionere efterkrigstidens samfund – transistoren. Transistoren skabte bl.a. et nyt medium for elektronisk registrering og lagring af strømudladninger og dermed også grundlag for en ny elektronisk teknologi. Mediet løste nemlig de vanskeligheder, man tidligere havde haft under driften af tidligere generationers IT og dette samtidig med, at prisen endog faldt. Se nærmere den historiske redegørelse hos *Keld Nielsen* m.fl. (1990), s. 318 ff.

Serieproduktion

I slutningen af 1950'erne og begyndelsen af 1960'erne fremkom de første serieproducerede computere. Hvor de tidligere tekniske grænser for lagring og beregning nødvendiggjorde kommunikation med maskinen i korte og eksakte matematiske instruktioner, gjorde den større regnekapacitet det muligt at lade særlige programoversættere transformere brugerens kommandoer til "maskinlæsbare" instruktioner, der som sådanne kunne eksekveres af computeren. Også kyndige med vidt forskellige uddannelser kunne nu optræde som IT-brugere og -programmører, eftersom den trælsomme indkodning af koder i maskinsprog, hvor programmøren så at sige taler i ét-taller og nuller til maskinen, nu kunne ske i såkaldte *højniveausprog*. Hermed opstod en betydelig decentralisering og spredning af teknologien. Erfaringen skulle vise, at IT-anvendelse afføder behov for yderligere IT-anvendelse.

IT-rettens problemverden fødtes med denne teknologi. De nye systemer var komplicerede og kostbare at udvikle, og de nødvendige investeringer måtte derfor hentes hjem gennem et større og bredere salg. Dette salg lod sig gøre, fordi leverandørerne havde en – relativt – billig og effektiv erstatning for intellektuel menne-

skelig arbejdskraft at tilbyde, et hidtil ukendt produkt! IT blev derfor sat til at udføre stadigt mere vitale funktioner. Samtidigt hermed steg risikoen for fejl – en risiko, der forstærkedes af en udtalt kløft mellem brugerens og leverandørens viden om teknikken. De første domme i amerikansk IT-ret hidrører fra denne periode, jf. nærmere *E&A*, s. 46.

Halvlederteknik

Omkring midten af 1960'erne begyndte man at udvikle såkaldte integrerede kredsløb – det, man i dag kalder halvlederchips eller "chips" – hvor et stort antal transistorer er indkapslet i plastic eller keramik og forsynet med ledninger til omverdenen.

Alt efter hvor tæt de enkelte komponenter er placeret i halvlederproduktet, rubriceres halvlederchips i kategorier som SSI, MSI, LSI eller VLSI: Small, Medium, Large og Very Large Scale Integration. Halvlederchips er billige og små, og chipen kom til at revolutionere IT lige så markant, som transistoren havde gjort det.

I dag er chip-teknologien ligeså basal for IT-industrien, som stålindustrien er det for bilindustrien. Halvlederchips indgår ikke blot i den elektroniske computer, men anvendes i en lang række produkter, hvor der – i videste forstand – skal registreres eller behandles data, f.eks. radioer, tv-apparater, kameraer, vaskemaskiner og biler. En mere detaljeret omtale af halvlederchipens opbygning og konstruktion findes i afsnit 10.4. under omtalen af halvlederbeskyttelsen. Produktion og anvendelse af halvlederchips illustrerer den internationale teknologiske arbejdsdeling på IT-området.

PC'en

Benævnelsen "PC" (Personal Computer) anvendes almindeligvis for et edb-system beregnet til at opfylde en enkeltpersons behov for databehandling. En PC er en såkaldt "general purpose machine", der kan programmeres til ethvert formål. F.eks. anvendes PC'er ofte som terminaler for mainframes, ligesom de bundet sammen med andre PC'er i et net ofte vil fremtræde med en kapacitet, der langt overstiger behovet for en "personlig" databehandling.

Den første PC blev sat på markedet af Apple Computer, som efter nogle underskudsgivende år ved indgangen til det nye årtusinde er ved at genvinde en stor del af markedet. Konceptet til PC'en var imidlertid formuleret af Xerox Corp. som en naturlig videreudvikling af den fotokopieringsteknologi, som selskabet – i kraft af et patent herpå – havde spundet guld på op igennem 1960'erne. Ved patentets udløb var det tanken i Xerox at udnytte den base, man havde skabt i kontormiljøerne, til det næste årtis teknologi. Trods betydelige investeringer i teknologien (men vistnok for få i markedsføringen) traf selskabet imidlertid den –

tilsyneladende fatale – beslutning at lade idéen hvile. Det brugervenlige personlige edb-system kom derfor først på markedet, da Apple Computer overtog den med sit koncept for en grafisk brugergrænseflade. Kommunikationen sker her ved, at brugeren vælger mellem en række muligheder, der fremtræder som figurer ("ikoner") og understøttes af hjælpefunktioner, der giver veje ud af blindgyder mv. Idéen er siden ført videre af talrige andre leverandører af maskinel og programmel. Dette førte til, at mange af de standardprogrammer, der markedsføres på PC-markedet, kunne anvendes helt uden forudgående undervisning, endsige manualopslag.

IBM-PC'en

Et globalt PC-marked opstod først, da IBM i 1981 efter en bemærkelsesværdig kort udviklingstid (der bl.a. var mulig, fordi man i hovedsagen gjorde brug af standardkomponenter) introducerede sin PC. Dette skabte en de facto standard for kommunikation mellem maskine og operativsystem og mellem operativsystem og programmel. Man byggede bl.a. maskinen på et operativsystem, kaldet DOS, som var udviklet af et lille nystartet firma ved navn Microsoft. Med standarden for DOS-styresystemet og den korresponderende BIOS-standard kunne uafhængige programudviklere begynde at producere software til salg i stor skala. Og dette skete. IBM var dengang verdens ubestrideligt største IT-producent, og IBM-standarder var tidligere blevet markedsskabende, alene på grund af IBM's størrelse. I løbet af 1980'erne voksede nu et righoldigt marked for hardware- og softwareløsninger frem, hvis fælles kendetegn det var, at de alle var baseret på IBM-PC'ens arkitektur.

Med udbredelsen af standardiserede styresystemer er IT blevet en masse- og forbrugsteknologi. Standardiserede programpakker markedsføres og sælges i dag som hyldevarer ("hyldeprogrammel") på linie med andet kontorudstyr fra detailforretninger eller gennem postordresalg. Samtidig er der kommet værktøjer, hvorved man uden særlig ekspertise kan udvikle egne applikationer, såkaldte "systemudviklingsværktøjer", "ekspertsystem-skaller" mv.

Lokalnet

Da den personlige computer gjorde sit indtog i begyndelsen af 1980'erne, bar den sit navn med rette. Den opfyldte netop databehandlingsbehovet for én person; var denne persons forlængede arm i henseende til beregning, strukturering, lagring og formidling af information. I dag opfyldes dette formål primært af laptops eller mappecomputere, dvs. bærbare PC'er på størrelse med en telefonbog. I dag udgør PC'en den komponent, som de fleste IT-systemer er bygget op omkring. I den enkelte virksomhed

forbindes de enkelte PC'er i lokalnet (LANs, Local Area Networks), hvis interne kommunikation og anvendelse af fælles programmer og databaser mv. styres af PC'er, der er placeret tilsvarende centralt i netværkets topologi, såkaldte *servere*.

Client/server

Den vidtstrakte anvendelse af telekommunikation, herunder ikke mindst via www (World Wide Web), har frembragt en ny arkitektur for databehandling, hvorefter opgaverne fordeles mellem flere computere, der henholdsvis opfylder rollen som bruger af programmer og data (klient), henholdsvis som udfører af databehandlingsopgaver (server). Et databaseprogram vil f.eks. ofte være opbygget således, at hele databasen lægges ned på en central server, hvorfra de enkelte data hentes til de tilsluttede maskiner (klienter). I en client/server-arkitektur vil der i vekslende omfang ske kopiering af data og programmel på henholdsvis klient- og serverniveau. Denne rollefordeling er i en række retlige henseender afgørende, bl.a. for forholdet til lovgivningen om persondatabeskyttelse og for vurderingen af det ophavsretlige behov for programlicenser. Navnlig i relation til licensreguleringen er det afgørende, hvor der befinder sig eksemplarer af det beskyttede værk (hvad enten dette fremtræder som programmel eller data).

NC'en

Mere og mere af systemets programmel indbygges i dag i dets hardware. Hardware-lagrede programmer afvikles hurtigere end programmer, der først skal indlæses fra et lagerområde til RAM-hukommelsen. Dertil kommer, at sammenbygningen sikrer rettighedshaveren, at programmet sælges sammen med maskinen og f.eks. ikke kopieres i strid med hans rettigheder over det. Bortset fra problemer med kvalitetssikring rejser denne markedsføring en række monopolretlige spørgsmål, idet sammenbygningen kan indebære en ulovlig "bundling" af flere ydelser (maskinel og programmel), hvorved kunden presses til at købe mere, end han har brug for.

"IT i alt"

Muligheden for at placere elektroniske processorer (og dermed computere) i enhver form for apparatur har ført til en række nye produkter, der fremtræder som velkendte og klassiske, men som i realiteten må betragtes som IT-systemer. Det mest velkendte eksempel på en sådan "gadget" er mobiltelefonen, der foruden selve telefonterminalen i dag ofte vil indeholde så forskellige systemer som kamera, FM-radio, spil, kalender og andre databasefunktioner, diktafon og e-mail. Men også andre eksempler kan nævnes: Armbåndsure, der indeholder tilsvarende funktioner, og programmerbart husholdningsudstyr. Udviklingen bevæger sig

med hastige skridt hen imod en tilstand, hvor der med et fordansket udtryk er "IT i alt".

I engelsk terminologi taler man i en lidt mere snæver forstand om "*pervasive computing*" om den IT-anvendelse, der indebærer, at IT-systemernes funktioner træder frem for brugeren således, at de maskinelle komponenter ikke synes. En væsentlig teknologi, der understøtter denne form for IT-anvendelsen, er RFID-brikker, der vil medføre, at almindelige brugsgenstande med tiden kommer til at udgøre komponenter i IT-systemer, som de afgiver og modtager informationer til og fra. Foruden mobiltelefonen, der gennem de seneste årtier har fået et betydeligt marked, tegner der sig enkelte meget populære forbrugsprodukter inden for dette felt, herunder den af Apple Computer producerede musikafspiller iPod og e-mail-klienten Blackberry.

1.2.c. Software

Softwarebegrebet

Begrebet software er en samlebetegnelse for den *information*, der indgår i og styrer et IT-system, hvad enten der er tale om programmel eller data. Uanset om man taler om programmel eller data, repræsenteres denne information ved *talværdier*, eftersom IT-systemet på det helt fundamentale plan udelukkende udfører beregninger af talværdier, der basalt kan udtrykkes i nuller og éttaller og repræsenteres ved "kontakter", der på mikroskopisk plan "tændes" og "slukkes".

Digital databehandling

De regnemaskiner, som blev frembragt af *Blaise Pascal* og andre af de tidligste matematikere, byggede på det 10-talssystem, som vi kender fra dagligdagens beregninger. Moderne IT-anvendelse bygger derimod på binære talsystemer, dvs. systemer (bestående af 1 og 0). Det teoretiske grundlag herfor finder man i den algebra, som den engelske matematiker *George Boole* udviklede i 1800-tallet; den "boole'ske" algebra. Den indeholder en symbolsk logik, der tager udgangspunkt i filosoffens *Gottfried W. Leibniz*' lære om, at der kun findes to logiske sandhedsværdier: sand/falsk, enten/eller etc.

Binære talsystemer er velegnede som grundlag for edb-behandling, fordi de kan knytte sig til den simple kendsgerning, om der foreligger en høj eller lav elektrisk strøm. Principielt er der intet til hinder for, at man bygger computere, der arbejder med 10-talssystemer (bestående af tallene fra 0-9), hvor hvert tal svarer til en vis strømstyrke. Dette ville imidlertid være både besværligt og kostbart, da der i givet fald skulle bruges uforholdsmæssigt mange ressourcer til de nødvendige målinger.

De basale teorier

På grundlag af Leibniz's logik opbyggede Boole et algebraisk system, som siden blev taget op af den moderne computers fædre. I 1930'erne foretog matematikeren *Claude Shannon* en sammenligning mellem Booles symbollogik og elektriske kredsløb, og i en afhandling publiceret af den engelske matematiker *Alan M. Turing* i 1937 formuleredes disse principper som en idé om, at man med dette teoretiske grundlag kunne bygge en maskine – hvis princip undertiden betegnes som en *Turing-maskine* – der principielt ville kunne foretage alle de regneoperationer, der var mulige i den menneskelige hjerne.

Turing døde en tragisk død i en relativt ung alder og nåede ikke selv at realisere sine teorier. Det var *John Vincent Atanasoff*, der knyttede det binære repræsentationsprincip til den elektroniske computer. Atanasoff var med til at udvikle de komponenter, der senere blev indbygget i den første elektroniske computer. Ophavsmanden til den første egentlige elektroniske computer anses dog almindeligvis at være den ungarsk-fødte matematiker *John von Neumann*. Den computer (ofte kaldet "von Neumann-maskinen"), som han udviklede i begyndelsen af 1950'erne, anses med sin hurtighed, kompleksitet og funktionsdygtighed for at være verdens første rigtige computer.

Programmeringssprog

Edb-programmer skrives ved hjælp af andre edb-programmer, som programmøren kommunikerer med, og som oversætter programmørens kommando til maskinlæsbare og -eksekverbare instruktioner. Kommunikationen foregår ved hjælp af såkaldte edb-sprog. Gennem teknologiens udvikling er programmeringssprogene blevet stadigt mere avancerede. Et af de første programmeringssprog – *FORTRAN* (FORmula TRANslator) – blev konstrueret i 1956. FORTRAN tager primært sigte på tekniske og ingeniørmæssige programmeringsopgaver. Sproget *ALGOL* (ALGOrithmic Oriented Language) kom til i årene 1957-60 i et samarbejde mellem repræsentanter for nogle vestlige lande og USA. Danskeren *Peter Naur* (f. 1928) – i øvrigt Danmarks første professor i datalogi (1969) – øvede betydelig indflydelse på sprogets udformning, der siden har haft betydning for udformningen af nyere sprog, såsom Pascal og PL/I. Endelig konstruerede man i 1960 til administrative beregninger sproget *COBOL* (COmmon Business Oriented Language). Endnu i dag skrives en stor del af nutidens edb-programmer i disse sprog.

I begyndelsen af 1970'erne blev en række af de gamle programmeringssprog genstand for en faglig kritik. Man påpegede bl.a., at de savnede faciliteter til strukturering af programmer og data, og at programmerne ikke blev vedligeholdt i fornødent om-

fang. Kritikken var medvirkende til, at programmeringssproget *Pascal* blev skabt. Dette sprog, der er opkaldt efter opfinderen af den første regnemaskine, blev udviklet af schweizeren *Niklaus Wirth*. Pascal er primært beregnet til undervisning i programmering på større computere og indeholder elementer, der skal opmuntre til struktureret programmering. Sproget opnåede stor popularitet, bl.a. ved udvikling af små applikationer, men har haft en række svagheder, som skiftende udbydere af Pascal-oversættere har søgt at rette. De mange rettelser er udført med udgangspunkt i forskellige maskinmiljøer, og der hersker derfor ikke fuld kompatibilitet mellem forskellige Pascal-programmer.

C

Et af de sprog, der er særligt populært blandt nutidens programmører, hedder *"C"*. C blev oprindeligt udviklet til styresystemet UNIX og indeholder relativt få restriktioner for programmøren. Selv om programmøren så at sige kan gøre, hvad han vil, stiller denne frihed store krav til hans evne til at strukturere opgaven. Til forskel fra ALGOL-programmer kan programmer skrevet i C relativt ubesværet flyttes fra en computer til en anden. Programmeringssproget C++ er en videreudvikling af C. Dets ophavsmand er danskeren *Bjarne Stroustrup*, der som så mange andre succesfulde danske IT-folk har valgt et karriereforløb uden for Danmark. Et andet hyppigt anvendt programmeringssprog i dag er *Visual BASIC*.

Java

Til at understøtte de applikationer, der afvikles fra Internet, og for at muliggøre udviklingen af Internet-PC'er, der kun har behov for en begrænset lagerkapacitet, har IT-producenten Sun Microsystems, USA, udviklet programmeringssproget *Java*. Sproget kendetegnes først og fremmest ved at kunne afvikles uafhængigt af maskinmiljø: Man behøver altså ikke at udvikle Java-oversættere beregnet til hvert enkelt maskinfabrikat. Derudover indeholder det en række faciliteter, der hjælper programmøren, f.eks. ved automatisk at rydde op i "glemte" programkoder mv. En anden forskel mellem Java-programmer og andet programmel ses på den måde, hvorpå programmet kompileres. Hvor det er hovedreglen, at edb-programmer skrives i en kildetekst-version, der herefter kompileres til objektkode, jf. nærmere herom i afsnit 3.2.c., kompileres Java-applikationer fra kildetekstversionen til en slags mellemkode, der afvikles af en "Java-virtual machine", et program, der overfor Java-programmet optræder, som om den er en selvstændig computer. Denne særenhed rejser bl.a. spørgsmål om, hvorvidt brugeren har ret til at dekompilere Java-programmet, eftersom dette er forholdsvis enkelt i dette mellemkode-stadium.

At Java-programmel kan afvikles platformuafhængigt kommer ofte til syne ved brugen af World Wide Web, hvor såkaldte "java applets" ofte vil fremtræde som animerede figurer mv. på hjemmesiden. Sådanne applets kan rejse tvivl om, hvorvidt der i ophavsretlig sammenhæng foreligger en "fiksering" eller fremførelse af værker.

Højniveausprog

Forskning indenfor kunstig intelligens har frembragt en række nye programmeringssprog, der kræver færre instruktioner pr. program, og som dermed nedbringer udgiften til edb-programmering. Et af de første sprog til dette brug – LISP (LIST Processing) – er skabt af Stanford-professoren *John McCarthy*. Danmark er godt med i udviklingen af programmeringssprog til denne type software. Således har danske firmaer som DDC International og Prolog Development Center haft succes med oversættelser til edb-sprogene ADA og PROLOG (PROgramming LOGic).

Kognitive systemer

I slutningen af 1980'erne regnede man med, at udviklingen ville tage fart inden for området for såkaldt "kognitive" systemer, dvs. systemer der kunne understøtte eksisterende vidensafhængige professioner (som f.eks. den juridiske, ingeniørtekniske eller medicinske) og måske også til en vis grad udkonkurrere disse professioner. Forskningen i disse teknologier (ofte kaldet 5. eller 6. generation) er blevet centralt placeret i den globale konkurrence. I USA, Europa og navnlig i Japan investeres der store offentlige midler i denne forskning, se hertil *E&A* s. 48 f. med henvisninger. Endnu har resultaterne dog måttet lade vente på sig. Der er stadig langt til, at IT-systemerne kan indgå i meningsfulde dialoger med deres brugere. På et forholdsvist simpelt område som talegenkendelse er de systemer, der befinder sig på markedet, forholdsvis primitive.

Neurale net

Et af de områder, hvor man er nået længst i udviklingen af kognitive systemer, er ved brug af såkaldt kunstige *neurale net*. Et neuralt net er et system, der samler information på grundlag af eksempler og efterfølgende konkluderer noget om, hvilke mønstre eller lovmæssigheder der er gældende for disse eksempler. Betegnelsen skyldes, at systemet opbygges ved hjælp af små regneprogrammer, der fungerer på samme måde som den menneskelige hjernes neuroner. Det neurale net "optrænes" gradvist til at foretage slutninger på grundlag af computerens kendskab til disse eksempler. Dette kan f.eks. benyttes til genkendelse af figurer og ord og udregning af sandsynligheder mv. At man kalder disse net for "neurale" skyldes, at de bygger på de mønstre til association mv., der foregår i den menneskelige hjerne.

CASE

En anden metode til at nedbringe omkostningerne ved programudvikling består i at anvende udviklingsværktøjer til såkaldt

Computer Aided Software Engineering (CASE). Et CASE-værktøj rummer en samlet, implementerbar og målrettet løsning til højniveauprogrammering, således at systemer kan udvikles eller vedligeholdes uden detaljeret programmering. Det særlige ved CASE-værktøjer – sammenlignet med programoversættere mv., der jo også "selv" tilvejebringer et programresultat (objektkoden) – ligger i, at de overtager en række af de strukturelle opgaver, der kan belaste programmeringen (f.eks. konsekvensrettelser, diagramanvendelse etc.).

1.2.d. Lagermedier

Formål

Hvor det er muligt at bruge en regnemaskine uden videre (man konstaterer beregningen og disponerer på grundlag heraf), kan man som regel kun få glæde af data fra et IT-system, hvis disse data holdes tilgængelige på en måde, så man senere kan få adgang til dem. På samme måde som blyanten og papiret kan tjene som grundlag for at huske regnemaskinens beregning, har man derfor brug for medier, der kan lagre resultaterne af de ofte komplicerede data, der udgår fra et IT-system.

Udviklingen af lagermedier til digital information markerer en bevægelse fra medier, der i deres ydre form og funktion var indrettet på manuel indtastning af programmel og data via hulkortlæser eller lignende, og hen imod medier, der arbejder på computerens egne præmisser, dvs. ved elektromagnetisme. Herfra går udviklingen – måske – mod helt nye former for medier; i første omgang lys, på noget længere sigt mikrobiologiske funktioner.

Hulkort

Til den første gruppe hører anvendelse af hulkort. Det var franskmanden *Joseph-Marie Jacquard*, der fik idéen med at lagre data på hulkort. I 1800 opfandt Jacquard en væv, der kunne styres af papkort med huller, hvis mønstre svarede til vævningens. Opfindelsen stødte på modstand blandt såvel fabrikanter som arbejdere, og der blev på et tidspunkt ført en sag om dens brugbarhed. Det siges, at Jacquard herunder lod opfindelsen tale for sig selv, idet han hurtigt og effektivt lod væven væve et smukt mønster i retssalen, og at dette overbeviste retten om opfindelsens værdi. Stemningen vendte nu helt, og Jacquard blev indstillet til livsvarig understøttelse ved kejserlig befaling. Se nærmere herom *Per Håkon Schmidt* (1989), s. 131 ff.

Den "moderne" hulkort-teknik er udviklet af amerikaneren *Herman Hollerith* (1860 – 1929) og bygger på et princip, hvorefter tal repræsenteres i ét hul, bogstaver og specialtegn i to eller tre huller. Et "moderne" hulkort (format 18,7 x 8,2 cm) er (var)

opbygget af 80 lodrette kolonner, hver bestående af huller i 12 vandrette positioner. Det slidsomme arbejde med indlæsning af hulkort blev udført af personale med den lidet flatterende betegnelse "hulledamer"; det første IT-proletariat. Indlæsningen af hulkortet i selve computeren foregik med særlige læseenheder, der fungerede mekanisk under en imponerende høj hastighed og præcision. Dette arbejde – der i formen svarer til rutinemæssigt maskinskrivningsarbejde – foregår i dag som såkaldt tastearbejde.

Magnetiske medier

I dag er det magnetiske medium det mest udbredte medium for lagring af digitale data i en dynamisk driftssituation. De data, som IT-systemet løbende anvender, vil som regel befinde sig på harddisks. I dag måles lageret i en harddisk almindeligvis i Gigabytes (svarende til godt en milliard tegn) men kapaciteten vokser støt, og stadigt oftere ser man lagerarealer opgjort i Terabytes (en trillion tegn, eller 1.000.000.000.000 bytes). Digitale lagerarealer af en sådan størrelse er så småt ved at komme i almindelig brug, f.eks. som grundlag for systemer til digital arkivering. Tidligere var *disketten* det format, man almindeligvis ville anvende til transport af data. Fordi et IT-system i praksis altid vil være forbundet med andre IT-systemer via telekommunikation, løses det behov for at transportere og sikkerhedskopiere data, som disketten har opfyldt, i stigende grad ved *telekommunikation*. Som medium til at opbevare data adskilt fra computeren anvender man ofte statiske RAM-enheder, der tilsluttes via computerens USB-stik. Databaser og film distribueres i stigende grad ved hjælp af optiske medier, som f.eks. CD-ROM og DVD (se herom neden for).

Digital lyd

Med den lagerkapacitet, nutidens medier tillader, er det blevet muligt at anvende IT til ikke blot at lagre data i form af tegn (tal og bogstaver), men også som billeder og lyd. *Digital lyd* registreres pr. svingning i sekundet. Hver svingning kan repræsenteres med et tal og lagres som sådant. Når man konverterer analog (dvs. naturlig) lyd til digitale data (ved såkaldt sampling), omsættes hver svingning til en værdi, hvis størrelse afhænger af, hvor præcis lyden skal være, og hvor mange spor den skal omfatte.

Samplet lyd er nærmest sterilt renset for støj og "sus" – en kvalitet, som kendere næppe nogensinde når til enighed om. Når man ved at slå et digitalt klaver an kan høre lyden af et Steinway-flygel eller et Beatles-kor, skyldes det en sådan sampling. Samplingteknikker kan kollidere med udøvende kunstneres økonomiske og navnlig personlige rettigheder.

Digitale billeder

Et *digitalt billede* er opdelt i linier, der igen er opdelt i et antal billedelementer (Pixel – picture element). Ved et pixel-antal på

800 x 600 opnås en opløsning, der er bedre end den, man kender fra tv. På en moderne CAD-CAM skærm benyttes opløsninger på 1.200 x 1.024 pixels. En almindelig fotografisk film har en opløsning svarende til 7.200 x 4.800 pixels. Billedets kvalitet beror dels på pixel-frekvensen, dels på antallet af bits pr. pixel. På en edb-skærm af sædvanlig størrelse forudsætter en acceptabel billedkvalitet 300 x 200 pixels.

Optiske medier

Som nævnt indtager det magnetiske medium en central plads ved lagring af større mængder af statiske data. Mediet understøttes af laserteknologien. Med Compact Disc-teknologien kan omfattende digitale datamængder, der ikke forudsættes ændret under en sædvanlig forbrugsproces, fæstnes som strukturændringer på en metalplade, hvorfra de træder frem, når de udsættes for reflekterende laser-lys. CD-teknologiens første boom kom på fonogramsiden, men i disse år er CD-systemer, der omfatter såvel billede som lyd og edb-data, ved at vinde indpas. Disse systemer markedsføres som tilbehør enten til IT-systemer (CD-ROM) eller til tv-apparater (CDTV). I løbet af 1990'erne har CD-ROM-teknologien vundet indpas som den teknologi, der understøtter lagring af omfattende datamængder, der forudsættes distribueret (f.eks. programmel, databaser mv.).

DVD

I slutningen af 1990'erne har den internationale fonogram-, film- og IT-industri lanceret en ny teknologi, kaldet DVD. Oprindelig var dette en forkortelse for Digital Video Disk, men nu dækker den Digital Versatile Disc. Teknologien bygger på en standard, der oprindelig skulle understøtte lagring af videoinformation på en CD. På grund af dette mediums ringe udbredelse på video-området er DVD-teknologien nu konstrueret til at kunne håndtere enhver form for information på CD-mediet. Ved at anvende nye teknikker til *komprimering*, flere spor på skiven og en anden lagringsmetode (såvel et "reflektivt" lag som et "semitransmitterende") kan man på en DVD lagre op til 12 gange så megen information som på en CD. Derfor er DVD-mediet velegnet til distribution af spillefilm, dels på grund af den høje kvalitet af billede og lyd, dels på grund af de lave stykomkostninger.

1.2.e. Telekommunikation

Behovet

Lige så længe, der har været brug for at tale sammen, har der været behov for teknikker til at overføre data. I historiens løb har man anvendt så forskelligartede medier hertil som: Røgsignaler, flag, kanonskud, budbringning, transport af mediet og meget andet. I det følgende omtales den form for dataoverførsel, der sker

ved, at databærende impulser under en tidstro proces transmitteres via et offentligt net til telekommunikation.

Bølge-transmission

De fleste af nutidens medier til telekommunikation blev skabt længe før den moderne IT. Med industrialiseringen opstod behovet for hurtig og sikker kommunikation over afstande. Mediet hertil forelå i 1820, da danskeren *H. C. Ørsted* opdagede elektromagnetismen. Det logiske grundlag fik man, da *Samuel Morse* i 1837 præsenterede sit morse-alfabet, hvis korte og lange signaler kunne konverteres til elektriske impulser. Dette førte bl.a. til opfindelsen af telegrafien i 1844. Parallelt med denne udvikling kom telefonen i 1876. Den første teknologi til ren tekstbaseret telekommunikation forelå først i 1925, da et tysk firma producerede den første skrivemaskinebetjente fjernskriver. Se nærmere om denne udvikling *Keld Nielsen m.fl.* (1990), s. 134 ff.

Udviklings-tendenser

Brugen af medier til telekommunikation har på forunderlig vis svinget frem og tilbage mellem det lednings- og æterbårne. Ved telegrafens og telefonens fremkomst i 1800-tallet var ledningsmediet i forgrunden. Dette medium afløstes gradvis – og delvis – af det æterbårne medium (telefonkommunikation via radio). Med virksomhedscomputerens udbredelse gennem 60'erne og 70'erne anvendte man også først ledningsbårne medier til overførelse af data. Disse medier er senere ved at blive erstattet af æterbårne medier (mobiltelefoni og satellit-kommunikation). Det er imidlertid edb-programmeringen, der for alvor har præget udviklingen på teleområdet. Med digitaliseringen af telesignalerne kan man ikke alene anvende en computer (f.eks. en PC) som "omstillingsbord" (PABC); de funktioner, der udføres af dette, kan gøres "intelligente", f.eks. ved forskellige former for tast-selv services.

Optisk transmission

Gennem de seneste årtier har man taget en række nye medier til telekommunikation i brug. Det drejer sig dels om opto-elektronikken (lyslederkabler, bredbåndsteknologi), dels om de nye og forfinede teknologier til radio- og satellitkommunikation. Det er bl.a. *laser*-teknologien, der har understøttet denne udvikling. Laser er såkaldt monokromatisk – eller koherent – lys, dvs. lys af én ganske bestemt bølgelængde, der altid er i fase. Da lysstrålen altid brydes ens, forbliver energien den samme, og lyset kan dermed optræde som medium for data, der repræsenterer information gennem sekvenser af lys/ikke-lys.

Disse nye teknologier til telekommunikation har sammen med satellitteknologien skabt en rygrad af effektive kommunikationslinjer, der understøtter enhver form for kommunikation: telefoni, radio og tv samt datatransmission af enhver art. Effektiviteten træder frem på flere måder. For det første er der sket en betydelig

øgning af båndbredden, dvs. af selve mængden af den kommunikation, der kan transmitteres. Medvirkende hertil har også været de teknikker, man i dag anvender til at komprimere signalerne i nettet således, at et meget stort antal kommunikationsforløb kan afvikles samtidigt. For det andet er nettene forbundne således, at trafikken kan bringes derhen, hvor den kan forløbe mest effektivt, hvilket bl.a. indebærer en mindre følsomhed overfor lokale nedbrud. Dermed er grundlaget skabt for det netværkssamfund, som vi – bl.a. på grund af Internet-udviklingen – har set gennem de sidste 15 år.

Kommissionens rolle

Teleområdet har af samme grund været et af de lovgivningsområder, som EU-Kommissionen har fulgt mest intensivt, og hvor man har haft de bedste resultater af de EU-retlige lovgivningstiltag, et arbejde der bl.a. har fundet udtryk i den igangværende, effektive, liberalisering af hele telesektoren.

I 1984 tog Kommissionen sit første initiativ på teleområdet ved at fremlægge et handlingsprogram for telekommunikation (KOM (84) 277 af 18.5.1984). Hvor Kommissionen tidligere havde anlagt en tilbageholdende holdning til teleområdet (se f.eks. Kommissionens svar i EFT 1976 C 158/27, hvor det udtales, at post- og telefonudgifter kun udgør en ringe del af de industrielle eller kommercielle udgifter), lagde den nu op til, at der skulle oprettes et EF-marked for telekommunikationsudstyr og terminaler ved en standardiseringspolitik ved gradvis at anvende procedurer for gensidig anerkendelse og ved en fri indkøbspolitik. Siden hen er der gennemført andre politiske initiativer. Se i det hele *Bing m.fl.* (2001), s. 28 ff.

1.2.f. Internet

Grundlaget for det, man i dag refererer til som Internet, blev skabt i 1969 som et forskningsprojekt under det amerikanske forsvarsministerium (Department of Defence, DoD). Projektet betegnedes *ARPA* (Advanced Research Projects Agency) og skulle tilvejebringe et decentralt datanet, som i mangel af *et* centralt knudepunkt ville være mindre sårbart overfor militære angreb eller sabotageforsøg. Dette mål blev opnået ved, at man tilvejebragte et stort antal netforbindelser mellem de mange computere, der var forbundet til nettet. En meddelelse kunne således passere fra computer A til computer B ad vidt forskellige ruter, alt afhængigt af, hvilke forbindelser der måtte være tilgængelige på transmissionstidspunktet. Der var med andre ord ikke nogen på forhånd given vej (rute) mellem to computere. Idéen var, at valget af transmissionsvej skulle bestemmes af en særskilt com-

puter, en såkaldt *router*, der fungerer adskilt fra den computer, kaldet *host*, hvorpå de pågældende programmer og data er lagret.

DoD trak sig i 1991 helt ud af Internet-samarbejdet for i stedet at opbygge det lukkede MilNet. Internet blev herefter videreført af uddannelsesinstitutionerne under en stigende kommerciel deltagelse. Internettet var – og er – ikke det eneste globale netværk. I dag findes der talrige virksomheder, der udbyder net-ydelser til sine kunder. Men da i praksis alle disse net i dag er koblet sammen med Internet, taler man ofte om "Internet", selvom der er tale om flere net: Internet består i dag af hundrede tusindvis lokalnet og millioner af enkeltstående computere, der er knyttet sammen af lokale netværk ("backbones"), der igen er knyttet sammen af udvekslingspunkter og internationale backbones.

Internet fik for alvor sit gennembrud, da det i midten af 1990'erne blev almindeligt at udveksle information via computere (servere) forbundet med Internet via den såkaldte HTTP-protokol. Denne protokol frembragte det, der i dag betegnes som "The World Wide Web" (eller blot "web'et" eller "www"). Ved at kunne hente information fra de hundrede millioner af informationsservere ("web-servere"), der er forbundet med Internet via denne protokol, er der opstået et gigantisk informationsmarked, som i sig selv har givet anledning til vanskelige retlige problemer inden for bl.a. immaterialretten og databeskyttelsesretten.

I.2.g. Fremtidsperspektiver

Standard-problemet

Skal man anskue IT-markedet under ét, præges den fremtidige udvikling af ønsket om at standardisere IT-produkterne, så de kan supplere og træde i stedet for hinanden. Hvilke konsekvenser, man skal drage af denne standardiseringsideologi, hersker der stor uenighed om. Da det helt store IT-marked åbnede sig i 1980'erne, manglede standarderne. Og hvad værre var: Med hjemmel i de immaterialretlige eneretsregler kunne den ene producent hindre den anden i at gøre brug af de produktdele, der hidfører den fornødne kompatibilitet.

Dette skisma mellem på den ene side hensynet til udvikleren og interessen i at præmiere denne med enerettigheder og på den anden side hensynet til brugeren og interessen i at værne denne mod vidtgående monopoler er et af de væsentligste samfundsmæssige problemer for IT-samfundet og rummer samtidigt en af de største retlige og retspolitiske problemfelter i IT-retten. Denne modsætning er gentagne gange kommet til udtryk gennem retspolitiske drøftelser gennem de seneste år, f.eks. forud for vedta-

gelsen af direktivet om ophavsretlig beskyttelse af edb-programmer, ved de forhandlinger der i 1996 førte til "the WIPO Copyright Treaty" og senest under de drøftelser, der førte til vedtagelsen af 2001-direktivet om ophavsret og beslægtede rettigheder i informationssamfundet ("INFOSOC-direktivet").

Åbenhed eller ikke

Inden for IT-branchen finder man en modsætning mellem to typer af leverandører af edb-programmel. På den ene side står de, der baserer deres forretning på "åbne systemer". Hertil hører f.eks. leverandører som AT&T, Sun Microsystems og en række japanske producenter. Disse leverandører har generelt ønsket, at der udvikledes *interoperable* systemer, dvs. systemer der udvikles af andre, men som kan kommunikere med virksomhedens produkter. Den, der vil udvikle produkter, der skal kunne kommunikere med et rettighedsbelagt produkt, bør – mod en betaling, der ikke er prohibitiv – kunne få adgang til programmerne til styresystemer mv. i et format (kaldet kildetekst), der gør det muligt at foretage ændringer. Heroverfor står typisk de større producenter som Apple, Amdahl og Digital samt på programområdet ikke mindst Microsoft, der holder deres systemstandarder som "lukket" (proprietary) information, hvorved man søger at kunne kontrollere markedet selv. Vil konkurrenterne udvikle tilknyttede produkter, må de selv – ved "reverse engineering" mv. – regne ud, hvordan det skal gøres. Kildetekstlicenser gives kun til nære samarbejdsparter, som man selv udpeger efter eget skøn.

Open source

I tillæg til disse to principper for licensering af edb-programmel er der gennem de seneste år kommet et stigende marked for såkaldt *freeware*-programmel, dvs. programmel som udvikles af idealister, der efterfølgende opgiver enhver immateriel ret til det udviklede. Det såkaldte Linux-styresystem er et eksempel herpå, jf. nærmere i afsnit 3.2.e.

1.3. IT-rettens grænseflader

1.3.a. Problemet

Eksisterer der en "IT-ret", og hvor ligger i så fald dette fags grænseflader? Dette spørgsmål er talrige gange rejst i den IT-retlige teori. Se herved diskussionen i *E&A* s. 72 ff. med henvisninger samt mit indlæg i festskriftet Suum Cuique (1991), s. 110 ff.

Kært barn har mange navne. Selv om betegnelsen "IT-ret" synes at have vundet fodfæste herhjemme, dukker der i udlandet stadigt flere alternative betegnelser frem. Bortset fra det norske "informations-

ret", jf. nedenfor, anvender engelsk sprogbrug bl.a. ord som "IT-law" ("Information technology law") og "I&C-law" ("Informations and communications law"). Se også *Bing m.fl.* (2001), s. 54 ff.

Beklageligvis rejses disse spørgsmål typisk af forfattere, der – som jeg selv – allerede har placeret sig i IT-retten, f.eks. ved at skrive "edb-retlige" eller "IT-retlige" afhandlinger, monografier mv. Den, der deltager i debatten fra denne position, er almindeligvis forhåndspåvirket i sin holdning.

Ikke overraskende kan jeg da også tilslutte mig valget af IT-retten som juridisk ramme for en fremstilling af de problemer, der kort er skitseret i dette kapitel. Men når dette er sagt, ligger det også klart, at IT-rettens afgrænsning ikke er uproblematisk. Skal IT-retten omfatte samtlige juridiske problemer, der blot har en eller anden – nær eller fjern – tilknytning til IT-teknologien, frembyder der sig et uoverskueligt emneområde. En række af disse emner har enten allerede vundet indpas i eksisterende fagområder (f.eks. immaterialretten eller strafferetten), eller også angår de regler, der er så specielle, at de alligevel næppe kan bære en selvstændig disciplin.

Problemerne forstærkes af, at IT-teknologien end ikke på det faktiske plan har nogen naturlig afgrænsning. Som tidligere fremhævet er det evnen til at behandle *information*, der står bag IT-teknologiens fremmarch i det moderne samfund – ikke dens fysiske udslag. For så vidt kan det siges at være mere hensigtsmæssigt at bruge betegnelsen informationsret, således som der efterhånden synes at være tradition for i Norge.

1.3.b. IT-ret som teknologiret

Vælger man blot at betragte IT som kompliceret teknologi, vil IT-retten falde sammen med andre retsområder, der befatter sig med kompliceret teknik. Man kan for så vidt overveje, om ikke IT-retten er en del af en generel teknologiret, som også vil omfatte f.eks. entrepriseretten, patentretten, visse dele af miljøretten, retsreglerne vedrørende særlige bygningsskader mv.

Teknologibegrebet

Det centrale i teknologibegrebet er anvendelsen af kompleks viden (information) til industriel frembringelse af nyttige ting (produkter). En håndværker kan beherske en særlig teknik, men først, når han sætter sin viden om denne teknik i system, forvandler den sig til en teknologi, hvis ellers der er tale om en tilstrækkeligt "kompleks" viden. En gravemaskines princip er kun "teknologisk", for så vidt det repræsenterer en informationsanvendel-

se, der kan karakteriseres som "avanceret" sammenlignet med brugen af skovle mv.

Det ligger imidlertid klart, at det område, der kan afgrænses på denne måde, bliver for bredt og uhåndterligt til også at kunne danne rammerne for et *retsområde*. Reglerne er for forskelligartede, og de håndhæves tilmed ved forskelligartede prøvelsesinstanser, der ikke kan forventes at forme deres praksis ud fra et erfaringsmateriale, som er mere "fælles" end det, der kendetegner det omkringliggende retssystem (formueretsreglerne, immaterialretsreglerne, ansvarsreglerne etc.). Medvirkende hertil er, at det sjældent er samme aktører, der bevæger sig indenfor de forskellige retsområder – hverken når det gælder praktiserende advokater eller retsvidenskabelige forfattere.

Alligevel kan der være mening i at tale om en teknologi*ret* i en overordnet metodisk betydning. En række af de problemer, der opstår ved mødet mellem teknologien og den juridiske regulering, er nemlig identiske. Dette gælder for det første hele beskrivelsesproblematikken, der ud over dens teoretiske implikationer rummer en række helt konkrete problemer, f.eks. omkring kontraktskoncipering, håndhævelse mv. Dernæst gælder det de regulatoriske problemer, der udspringer af teknologirettens informationsafhængighed, f.eks. om eneretsbeskyttelse af teknologi, finansiering, overdragelse og beskatning. At IT-retten alligevel har udviklet sig i et særskilt forløb skyldes dels det egenartede beskrivelsesproblem, hvor informationsaspektet spiller en central rolle, dels den kolossale mængde af retskilder, der specifikt tager sigte på IT.

1.3.c. IT-ret som informationsret

Den historiske redegørelse viste, hvorledes den digitale teknik er blevet et værktøj for behandling, brug og distribution af enhver form for information, hvad enten der er tale om tekniske data, informationer, nyheder, underholdning, kunst og kultur eller andet. Det forhold, at den digitale teknik derfor i stigende grad bliver ramt af regler, der tager sigte på anvendelse og distribution af information i disse forskellige henseender kunne tale for, at man opgav den anden halvdel af IT-begrebet (teknologibegrebet) og i stedet anerkendte, at IT-retten falder sammen med den almindelige informationsret og medieret.

Således afgrænset ville IT-retten ikke alene komme til at omfatte reglerne om udvikling (herunder retsbeskyttelse og finansiering), anvendelse og overdragelse af IT-systemer, men også reg-

lerne om brugen af offentlige og private informationsmedier (herunder radiotransmissions- og telekommunikationsudstyr mv.). Herudover ville disciplinen omfatte den privat- og offentligretlige regulering af ytringsfrihed og offentlighed, for ikke at tale om reglerne om omsætning, sikring og hemmeligholdelse af information.

Det skal bemærkes, at ikke alle disse retsområder har været fremstillet i afgrænsede discipliner. Det medieretlige område har primært været behandlet i sagkyndige udredninger, der har fundet sted i to forløb. Et første forløb, der udfoldede sig i begyndelsen af 1980'erne inden for rammerne af *Mediekommissionen* og udmøntede sig i fem betænkninger om henholdsvis Nordsat-projektet (1. betænkning 936/1981), Video (2. betænkning 954/1982), De trykte mediers økonomi og beskæftigelse (3. betænkning 972/1983), Fremførelse af udenlandsk fjernsyn (4. betænkning 974/1983) og Øget dansk tv-udbud (5. betænkning, 986/1983).

I 1994 nedsatte statsministeren et *Medieudvalg*, der har afgivet en række betænkninger, henholdsvis igangsat diverse udredninger vedrørende en fremtidig mediepolitik, se herved den afsluttende betænkning om medierne i demokratiet, nr. 1320/1996. Det område, man herhjemme har betegnet som informationsret, angår reglerne for informationsmedierne. I *Knud Aage Frøbert*: Dansk Informationsret (bd. 1 – 5, 1975 -1977 og 1979), der tog sigte på journalistuddannelsen, behandles foruden disse spørgsmål grundlovens regler om ytringsfrihed, reglerne om tavshedspligt og offentlighed samt ophavs- og fotografiretten.

Det må erkendes, at informationsretten – således afgrænset – har tydelige fællestræk med IT-retten. Skal man finde en forskel mellem de to discipliner ligger den i, at den information, der formidles på radio eller i tv, ikke adskiller sig fra den information, der f.eks. formidles ved samtale eller på papir. Til sammenligning er den information, som indgår i en IT-baseret kommunikationsproces, langt mere kompleks end den, som eksempelvis skrives i en avis. På grund af den konvergens, der præger de informationsrelaterede retsområder, kan dette kriterium imidlertid ikke opretholdes i det uendelige. Når udviklingen er nået dertil, at der ingen funktionel forskel er mellem brugerens håndtering af tv, radio, aviser, computer, databaser mv., må sondringen tages op til revision. Det er efterhånden dertil, vi nu er nået. Og i takt hermed opstår spørgsmålet, om IT-retten fortsat kan opretholde sin egen identitet, eller om dens problemer da gradvis vil falde sammen med retssystemets øvrige.

Supplerende litteratur

Samspillet mellem IT og samfund har givet anledning til en stor og uoverskuelig litteratur, der spænder over de fleste samfundsvidenskabelige discipliner. I et længere tidsperspektiv kan der være grund til særligt at fremhæve *Alvin Toffler*s tre hovedværker: Future shock fra 1970 (dansk udg. 1972: Fremtidschok) The third wave fra 1980 (dansk udg. 1981: Den tredje bølge) og Powershift fra 1990 (dansk udgave 1991: Magtskifte). I den økonomiske teori er det navnlig *John Kenneth Galbraith*, der har behandlet samspillet mellem teknologi og økonomi, se: The new industrial state (4th edition 1985). Herudover kan henvises til de sagkyndige udredninger om "Info-samfundet", der er omtalt ovenfor i teksten.

En god og anbefalelsesværdig *teknologihistorisk* fremstilling findes på dansk med *Keld Nielsen*, *Henry Nielsen & Hans Siggaard Jensen*: Skruen uden ende – den vestlige teknologis historie (1990), se bl.a. kapitlerne 7 og 16-19. En god (til dels selvbiografisk) fremstilling af den historie, der ligger bag udviklingen af the World Wide Web foreligger med *Tim Berners-Lee*: Weaving the web (1999). Herudover er teknologiens historie bl.a. fortalt af *Joel Shurkin*: Engines of the mind (2nd ed., 1985), der anlægger et biografisk udgangspunkt omkring teknologiens pionerer bag de første regnemaskiner og frem til PC-revolutionen. I dette værk findes en god IT-historisk bibliografi (s. 313 ff.), hvortil henvises. Se ligeledes *Douglas K. Smith & Robert C. Alexander*: Fumbling the future – how Xerox first invented, then ignored the first personal computer (New York, 1988) og *Charles H. Ferguson & Charles H. Morris*: Computer wars – the fall of IBM and the future of global technology. (1993, 1994). Hos *Tracy Kidder*: The soul of a new machine (London, 1981) finder man en personligt præget beretning om et projekt om udviklingen af en computer.

Den almindelige IT-tekniske og IT-retlige litteratur vrimler i øvrigt med fremstillinger af enkelte teknologiers historie. I afhandlingen Five generations of computers, 52 Harvard Business Review 99 ff. (July-August 1974) gennemgår *Frederick G. Withington* de forskellige stadier af IT-systemets organisatoriske og teknologiske rolle, navnlig for private virksomheder. Afhandlingens konklusioner er fulgt op af *John T. Soma & Stephen D. Shirey* i 1 Software L.J. 123 ff. (1986).

IT-rettens – og retsinformatikkens – *metodeproblemer* er første gang analyseret i *Peter Seipel*s disputats Computing Law (1977), hvor fagets problemer, grænseflader og relevans behandles. Se også samme forfatters Juridik og IT (2001), der har undertitlen "Introduktion till rättsinformatiken", navnlig s. 161 ff. De faglige og terminologiske afgrænsninger er dernæst behandlet i *Jon Bing*s instruktive afhandling: A background analysis of information law i 1 ICLA (September 1987), s. 12 ff. Herudover henvises til *E&A* kapitel 1 – 4, der navnlig behandler de metodiske

problemer, der udspringer af beskrivelsesproblematikken. I NÅR 1990.116 har jeg endelig opstillet nogle forslag til, hvordan juristen kan gøre sig fortrolig med IT-teknologien. I denne årbog ser man i øvrigt ofte metodiske og grænsedragende spørgsmål rejst. Nordisk Årbog for Retsinformatik 2000 (*Peter Wahlberg, red.*) sætter f.eks. fokus på IT og jurauddannelserne.

Overvejelserne om nytten af en "analytisk" IT-ret overfor den eksisterende "empiriske" er først og fremmest lagt frem i *E&A*, jf. i det hele kapitel 1 – 4. Synspunkterne heri drøftes bl.a. af *Koktvedgaard* i U1989B.268, navnlig s. 271, *Ole Bruun Nielsen* i J1989.302, af *Blume* sst. s. 294 f. og af *Nørager-Nielsen* i forhandlingerne ved det 32. nordiske juristmøde i Reykjavik, august 1990, bd. I, s. 285 ff.

Birgitte Kofod Olsen har i sin licentiatafhandling: Identifikationsteknologi og individbeskyttelse (1998), beskæftiget sig med teknologivurdering i relation til disse særlige spørgsmål. En kort, men god, indføring i *teknologivurdering* findes i *Anne Lykkeskov Andersen og Bo Carstens*: "Teknologivurdering – en orientering" (Teknologinævnet, 1989). Se i øvrigt *E&A*, s. 220 ff. med henvisninger.

Kapitel 2. ALMENE TEORIDANNELSER

2.1. Beskrivelsesproblematikken

2.1.a. Retsteoretisk baggrund

Problemet

Man kan kun forholde sig til et juridisk problem, hvis man forstår den relevante *jus* (altså retsreglens retsfaktum og retsfølgen) såvel som det *faktum*, der ligger til grund for, at problemet er opstået. Ser man bort fra konkrete *bevistekniske* spørgsmål, volder forståelsen af faktum sjældent vanskeligheder på dagligdagens almindelige retsområder. For den teoretiske jurist er det den juridiske beskrivelse, der tiltrækker sig opmærksomhed. Praktikerens virkelighed er en anden. Talrige sager afgøres reelt på bevisvurderinger over det konkrete tilfælde uden teoretiske overvejelser om gældende ret.

Når der opstår særlige – men principielle – problemer med at beskrive en retsregel eller det faktum, der indgår i retsanvendelsen, kan man tale om, at den pågældende retsregel eller det pågældende faktum giver anledning til et *beskrivelsesproblem*.

Jus-siden

Beskrivelsesproblematikkens *juridiske* side angår selve retsreglen og knytter sig – som anført – til fortolknings- eller subsumptionsproblemer, der har mere principiel karakter. Grænsen mellem sådanne beskrivelsesproblemer og de mere almindelige tilfælde af tvivl, der opstår, når en retsregel viser sig selvmodsigende eller upræcis, er dog ikke skarp. Men når det giver mening at udskille visse problemer vedrørende fortolkning og udfyldning mv. fra andre, skyldes det, at sædvanlig juridisk metode ikke altid gør fyldest. Når man f.eks. skal forholde sig til, om begrebet "produkt" i produktansvarsloven også omfatter ren information, er det nødvendigt at inddrage en række principielle konsekvenser af at træffe dette valg. Og det er disse principielle spørgsmål, der gør det rimeligt at placere denne juridiske drøftelse som en del af en IT-retlig beskrivelsesproblematik. Foretog man ikke en sådan udskillelse, ville IT-retten falde sammen med en hvilken som helst anden fremstilling af det pågældende juridiske spørgsmål. Hvorfor operere med en IT-retlig ophavsret, kontraktsret, erstat-

ningsret etc., hvis den blot gentager, hvad man kan udlede af den almindelige ophavsret, kontraktsret og erstatningsret?

Faktumsiden

Beskrivelsesproblematikkens faktiske side er mere iøjnefaldende. I enhver sag skal der ske en sagsfremstilling og bevisførelse. Den kan være mere eller mindre kompliceret. Hvor dommeren i en færdselssag ved, hvad en fodgænger, et trafikfyr og et motorkøretøj er, kan det kræve en særlig indsats fra den procederende advokat at forklare, hvad et osmose-angreb i en glasfiberbåd er. Endnu mere kompliceret kan det blive, hvis opgaven består i at forklare, hvordan en hacker kan have skaffet sig adgang til et IT-system. I forhold til andre komplekse indretninger kan det være særligt vanskeligt ikke bare at opnå den fornødne forståelse af det problem, der konkret præsenteres af de procederende advokater, men navnlig at opnå sikkerhed for, at den indfaldsvinkel, der er valgt til faktumbeskrivelsen, er relevant.

Til disse to problemer kommer det paradoks, som undertiden omtales som *Vico*-paradokset, se nærmere *E&A* s. 145 ff., nemlig at IT kan være vanskelig, for ikke at sige umulig, at forstå for mennesker, selv om der er tale om en teknologi, som er skabt af mennesker. Paradokset præger behandlingen af en række specifikke IT-retlige problemstillinger: Kan en computer, der "træffer beslutninger" tænkes at besidde en særlig form for retssubjektivitet, som f.eks. skal begrunde, at den betragtes som "fuldmægtig" for sin ejer? Hvem har ophavsretten til værker, som frembringes under en vis "kreativ" medvirken af et IT-system ("computer-generated works")? Hvilke erstatningsretlige spørgsmål rejser det, at et IT-system overtager en del af de beslutninger, der udfolder sig i et skadesforløb?

Indfaldsvinkler

Ser man bort fra bevisretten og enkelte – og specialiserede – teknisk prægede discipliner (f.eks. patentretten, entrepriseretten, lægebehandlingsretten o.m.a., se nærmere *E&A* kapitel 3) indgår sådanne faktiske beskrivelsesproblemer sjældent i retsvidenskabelige fremstillinger. Litteraturen fokuserer primært på den sproglige beskrivelse af retsfaktum og retsfølge, uanset denne beskrivelse kan blive ganske upræcis, hvis reglen er formuleret generelt. Indfaldsvinklen forsvares ved, at det jo alligevel ikke lader sig gøre at foregribe tilfældets enkeltheder.

Denne indfaldsvinkel er praktikabel, fordi man enten kan bruge *common sense* eller har fundet håndgribelige løsninger på de beskrivelsesproblemer, der opstår i den konkrete sagsførelse (syn og skøn, sagkyndige vidner el.lign.). I en sag om ansvaret for en forgiftningsskade er det tekniske overblik over sagen enkelt at få pga. vort basale kendskab til fordøjelsessystemet. Selv i sager om lægers erstatningsansvar er juristens kendskab til organers virke-

måde, suppleret med udtalelser fra kompetente myndigheder om almindelig praksis mv., tilstrækkelig. Det er sjældent nødvendigt, at den procederende advokat tager den tekniske ekspertise med sig i retten.

Behovet

For at løse beskrivelsesproblemet er det hverken nødvendigt – eller realistisk – at forestille sig, at IT-juristerne skulle gennemgå en teknisk uddannelse. Noget sådant ville stride mod danske juridiske traditioner og ville i givet fald kunne risikere at føre til, at IT-juristerne kom til at forpuppe sig på et lille, indelukket domæne uden nogen ydre kontakt med de juridiske deldiscipliner. Beskrivelsesproblemet må løses af IT-retten selv. Der må findes et niveau for beskrivelsen, der ligger mellem det generaliserende lægmandsplan og ekspertplanet.

For at undgå, at denne mellemløsning ender med hverken at blive fugl eller fisk, nødsages faget til at befatte sig med en række basale metodiske problemer i tilknytning til den juridiske og faktiske beskrivelse. Det er disse principielle indfaldsvinkler, der løfter IT-rettens beskrivelsesproblematik fra at være en tilfældig overbygning til de retlige og bevismæssige problemer, der opstår i retsanvendelsen, og til at blive en del af disciplinens metodik.

Teknisk niveau

Et af beskrivelsesproblematikkens mest basale problemer er vurderingen af, hvor konkret og "teknisk" man tør og bør gå til værks. På den ene side kan man sige, at dette bl.a. beror på en personlig interesse og mentalitet. Men problemet er mere principielt, da valget af teknisk niveau og kompleksitet har en afsmittende betydning for kvaliteten af den retsvidenskabelige analyse. Betragter man teknikken som noget ukompliceret, vil man umærkeligt rette blikket mod generelle problemer og henskyde de mere komplicerede tekniske spørgsmål som noget, der kan tages konkret stilling til i den enkelte sagsførelse, hvor juristen kan hente bistand af eksterne sagkyndige. Med den hastige teknologiske udvikling vil en sådan fremstilling på grundlag af "sædvanlige" retskilder (lovgivning og domspraksis) føre til, at den retsvidenskabelige fremstilling kommer til at halte efter. Ofte når lovgivningsmagten ikke at give regler for påtrængende IT-spørgsmål. Går parterne domstolsvejen, tager det typisk 3 – 5 år, før en opstået retstvist er trykt som lands- eller højesteretspræjudikat. På dette tidspunkt vil det system, der var årsag til tvisten, ofte være forældet.

Som en generel tommelfingerregel kan man sige, at den faktiske beskrivelse bør søge imod et kompleksitetsniveau, der gør det muligt at anlægge relevante retlige sondringer. I relation til en konkurrenceretlig eller aftaleretlig problemstilling kan det f.eks.

være relevant at sondre mellem et styresystem og et applikationsprogram. En sådan sondring har dog mindre relevans i relation til den ophavsretlige vurdering af, om programmet har værkshøjde. I relation til ejendoms- og panteretlige regler kan det have betydning, om et program – eller et andet informationsprodukt – er integreret i et medium eller ikke. Denne sondring har derimod mindre betydning i relation til erstatningsretlige vurderinger.

At man derfor ofte er nødt til at vælge et detaljeringsniveau, der passer med den konkrete retlige problematik nødvendiggør derfor, at det tekniske beskrivelsesproblem på det almene plan er parat til at kunne sætte ind med et relevant abstraktionsniveau og et rammende teknisk detaljeringsniveau. Denne ambition søger denne bogs første del at løse ved *dels* – i nærværende kapitel – at introducere nogle metodiske værktøjer, der tjener til at karakterisere nogle helt basale aspekter af IT-anvendelsen, *dels* – i kapitel 3 – at introducere IT i en kaleidoskopisk præsentation af IT-systemets komponenter og af en række af de begreber, der indgår i forbindelse med IT-udvikling og anvendelse.

2.I.b. Beskrivelsesproblemets udspring

Fremtrædelsesform

At IT-retten står foran et særligt beskrivelsesproblem, skyldes først og fremmest, at en væsentlig del af IT-anvendelsen er immateriel: Information som sådan kan man ikke tage og føle på. Kun når informationen *manifesteres* i et medium eller i en beslutning, kommer den til syne; men denne manifestation er ikke nødvendigvis den relevante.

Terminologi

En anden faktor kan ligge i IT-terminologien, der selv blandt fagfolk er usikker. Nye IT-applikationer udvikles så hastigt, at introducerede begreber hurtigt mister deres betydning. En væsentlig årsag hertil er teknologiens generalitet. En teknologi, der kan anvendes til al form for informationshåndtering, vil få betegnelse efter sine fremtrædelsesformer. Da man anvendte teknologien til beregninger, talte man om "computere". Da den enkelte brugers databehandlingsopgaver kom i fokus, introduceredes den "personlige computer" eller PC'en. Efter at forskellige typer af information (der tidligere var knyttet til forskellige typer af medier) kan håndteres på samme udstyr, taler man om "multimedia". Men den fundamentale teknologi er i bund og grund den samme.

Tænkemåde

En tredje årsag til forståelsesproblemet ligger i den anderledes form for tænkning, der præger IT-folk og andre faggrupper. Psykologer har peget på, at den procedureorienterede IT-tænkning

adskiller sig fra den almenmenneskelige associationsorienterede tænkning, jf. nærmere mit indlæg i FSR's årsskrift, 1990, s. 15.

2.1.c. Konvergensproblemet

Den grænseoverskridende dimension

Fordi al information – tekst, grafik, musik og video – kan repræsenteres digitalt (som en lang række punktvise felter bestående af lys/ikke-lys, lyd/ikke-lyd etc.), er IT en uendeligt grænseoverskridende teknologi. I takt med, at det er blevet stadigt billigere at behandle information digitalt (dvs. repræsenteret gennem ettaller og nuller), er der sket en sammensmeltning mellem forskellige informationsteknologier. Som eksempler på sådanne *konvergensprodukter* kan nævnes telefoner, der ikke længere "bare" overfører mundtlig samtale, men også fungerer som medium for lagring af data med større eller mindre relation til klassisk telefoni. Kendt er det f.eks., at digitale telefoner også kan indeholde adresseoplysninger. Men navnlig mobiltelefonien har trukket helt nye typer af data ind i telefon-terminalen, ikke bare kalenderoplysninger, men også data og programmel til brug for elektroniske betalinger og – i moderne mobiltelefoni – musikfiler til afspilning hentet fra nettet. Et andet konvergensprodukt er PC'en. Den blev oprindelig primært anvendt som en avanceret skrivemaskine, men anvendes i dag til så forskellige opgaver som afsendelse og modtagelse af post, afspilning af levende billeder og lyd, telefoni foruden administrative "tillægsfunktioner" som f.eks. arkivering og databasehåndtering.

Denne sammensmeltning mellem typer af informationsteknologiske applikationer kan ses som en væsentlig årsag til de fusioner, man ser i disse år mellem den elektroniske industri (edb-siden) og nyheds- og underholdningsindustrien (informationssiden). Idéen bag disse og lignende fusioner må bl.a. ligge i muligheden for at producere de værker, der hidtil er gjort tilgængelige gennem klassiske informationstyper (aviser, bøger og film), billigere, mere effektivt og til et større publikum gennem elektroniske medier.

Konvergensproblemet opstår, når et lovreguleret forhold, der falder inden for et givet lovgivningsområde, *skifter medium* og nu udfolder sig ved brug af et andet medium, der er underkastet andre regler: Skal reklamereglerne for radio og tv f.eks. *reguleres ned* på niveau med reklamereglerne for den trykte presse, når "skreven" digital information udsendes til en brugerskare via Internet på en måde, som kan minde om en radio- og tv-udsendelse? Eller skal denne form for Internet-distribution *reguleres op* på niveau med radio- og tv-reglerne? Se herved *Søren Sandfeld Ja-*

cobsen i U 2003B.399 ff. og samme forfatters ph.d.-afhandling: Medieret i Informationssamfundet – en retlig analyse af sammensmeltningen mellem telekommunikation, Internet og radio/tv (2004). Der kan ikke gives generelle retspolitiske svar herpå; men problemstillingen synes præget af "læren om forbundne kar": De begrænsninger, der traditionelt har været gældende på et område (f.eks. om retten til at reklamere), må ofte begrænses, når mediet smelter sammen med andre medier uden sådanne begrænsninger.

Beskrivelsesproblemer

Konvergensproblemet giver anledning til særlige beskrivelsesproblemer, der må løses såvel i den retsdogmatiske analyse som ved den retspolitiske håndtering af en række af informationssamfundets spørgsmål. Det retspolitiske problem udspringer af, at man traditionelt har valgt at regulere informationsbehandling, -spredning og -anvendelse med udgangspunkt i det *medium*, der *typisk* anvendes hertil: Grundlovens regler om ytringsfrihed tager udgangspunkt i det talte og skrevne ord, se for svensk ret udredningen i SOU 1997:49: Grundlagsskydd för nya medier. Reglerne om radio- og tv-spredning tog i sin tid udgangspunkt i radiotransmission via radiobølger. Med den stigende anvendelse af IT er det imidlertid blevet de digitale medier, der for alvor repræsenterer informationsspredningen. Men da disse medier optræder i vekslende miljøer og anvendes ud fra varierende forudsætninger, er det vanskeligt at opretholde en enstrenget regulering, der ikke tager højde for forskellighederne i disse miljøer.

På en række områder har lovgivningen søgt at forholde sig til nogle af konvergensproblemets konsekvenser. For det første søger man i stigende grad at lovgive gennem regler, der sigter mod en *teknologineutral* regulering, jf. nærmere afsnit 5.I.d. I lov om behandling af personoplysninger (LBP), der har rod i direktiv 95/46/EF, har man forladt det teknologi-fikserede registerbegreb for i stedet at tale om *behandling* af personoplysninger. Men der findes talrige konvergensproblemer, hvis afklaring er overladt til den praktiske retsanvendelse og – ofte tilfældige – politiske kompromiser. Hvornår skal visse former for masseudsendelse af e-post mv. f.eks. betragtes som radio-/tv-spredning, sml. diskussionen i SOU 1997:49? Det anførte sted antager den svenske mediekomité, at sådanne transmissionsformer falder inden for dette begreb.

Konvergensproblemet er størst i relation til spredning af information til almenheden – navnlig accentueret med den eksplosive udbredelse af Internettet i løbet af 1990'erne. Vælger man at betragte Internettet som et "stærkt" medium som f.eks. radio- og

tv-mediet, taler dette for indførelsen af censurlignende kontrolforanstaltninger for bl.a. at beskytte "svage" brugere (børn mv.) mod anstødelig kommerciel eller anden information. Anskuer man derimod Internettet på samme måde som presse og bogudgivelse, taler dette for at lade informationsstrømmen være helt fri. Disse spørgsmål er genstand for fundamentale retspolitiske overvejelser i disse år. Herom henvises i det hele til fremstillingen hos *Sandfeld Jacobsen* a.st.

2.1.d. Empirisk og analytisk beskrivelse

IT-fænomener præsenterer ikke altid sig selv på en sådan måde, at det giver sig selv, hvilke aspekter af faktum, der skal beskrives og hvordan. En computer kan være monteret i et armbåndsur, dens data kan dukke op som undertekster på et TV-billede, styre en kassetransaktion eller generere "levende" billeder i et underholdningsspil. Derfor kan man opleve at være IT-bruger, hvor man mindst venter det. Dette kan betyde, at man ikke har et begrebsapparat i beredskab til at beskrive teknologien korrekt for den relevante sammenhæng.

Aspektet

Når man skal beskrive et fænomen, vil man altid – bevidst eller ubevidst – gå ud fra et *aspekt*. Aspektet vælges efter beskriverens viden om og hensigt med beskrivelsen. Alt efter omstændighederne kan en ituslået vinflaske f.eks. beskrives som: 1) et materiale, hvorigennem lys kan passere, 2) en stenart, 3) et potentielt våben eller en potentiel skadesårsag, 4) et farvet materiale, 5) en forhenværende flaske, 6) et efterforskningsmæssigt bevismiddel, 7) et udtryk for manglende omsorg for skrøbelige værdier, eller 8) et symptom på samfundets smid-væk kultur. Hvad der er det relevante aspekt, beror på vidt forskellige omstændigheder, f.eks. formål, tradition eller funktion. Står man foran en kriminel efterforskning (3), har det under 7 anførte aspekt eksempelvis ingen selvstændig betydning. For den, der foretager en geologisk undersøgelse, er det ligegyldigt, at skåret tidligere indgik i en flaske etc.

Associationsaspekter

Ofte knytter beskrivelsen af noget nyt sig til noget, der "ligner". Som nærmere udviklet hos *Edward de Bono*: The mechanism of mind (Penguin Books, 1990) er det en velkendt psykologisk kendsgerning, at vi i vor opfattelse af omverdenen forsøger at få det, vi oplever, til at harmonere med, hvad vi forventer at opleve. Denne effekt viser sig dels i forståelsen af nye fænomener, dels i den måde vi navngiver dem på. Oprindeligt betegnede man de IT-baserede underholdningsspil, man møder i spillearka-

der mv., som "videospil" – associationen var TV-apparatet. I dag taler man om "computerspil", hvor den hjemlige parallel findes i hjemmecomputeren.

Når man ikke ved, hvordan man skal beskrive en kompliceret sammenhæng, er det nyttigt at tænke i aspekter. Man kan som regel ikke blot begynde at beskrive, det man ser: En stor, grå kasse med en skærm i midten, et tastatur og en masse ledninger! Interessen samler sig om, hvorledes man da finder de relevante aspekter. Dette kan ske på to måder: empirisk og analytisk.

Empirisk valgte aspekter

En empirisk beskrivelse forudsætter fuld klarhed og enighed om, hvilke aspekter der har relevans. Med denne enighed fremstår objektet som noget umiddelbart – intersubjektivt – genkendeligt. Inden for byggeretten er en skovl så at sige en skovl. Inden for IT-retten har begrebet "program" talrige begrebsindhold. Anvender man dette begreb ureflekteret, rammer man ikke nødvendigvis præcist i retsanvendelsen.

Analytisk valgte aspekter

Analytisk valgte aspekter er herefter dem, der fremtræder som resultatet af en selvstændig begrebsovervejelse. Ved salg af "et program" giver det ikke sig selv, hvad det er for fænomener eller funktioner, der overdrages, hvilke rettigheder der skal følge med, og hvordan opfyldelsen skal finde sted. For i givet fald at kunne anvende købeloven på en sådan aftale, forudsættes en nærmere analyse. Afhængigt af, hvor alment det pågældende beskrivelsesproblem er, vil denne analyse kunne føre til en selvstændig referenceramme eller et præliminært begrebsapparat. Det afgørende i begge tilfælde er, at de relevante aspekter er afgrænset korrekt.

Som allerede nævnt rækker empiriske beskrivelser på de fleste retsområder, hvad enten de har teknisk eller almen karakter. Ved salg af "fast ejendom" behøver man i almindelighed ingen forudgående diskussion om, hvad der forstås ved f.eks. "bygning" og "grund". Når stærkstrøms- og bygningsreglementerne fastlægger de tolerancer, der skal gælde for fremførelse af elektriske kabler mv., volder dette sjældent heller beskrivelsesmæssige problemer. Man kan gå lige til retsfølgen, hvad enten denne består af straf eller erstatning.

Behovet for en analytisk beskrivelse opstår, hvor der ingen intersubjektive fornemmelser hersker omkring normen, og hvor *common sense* derfor ikke strækker til. Dette kan skyldes, at normen er upræcis, og at der hverken findes praksis eller sædvane til at udfylde den. Her vil retsudviklingen ofte ske i trin gennem konkrete afgørelser, der tager højde for den enkelte sags særpræg. Sagens faktum og reglens retsfaktum kommer dermed ind i en vekselvirkning, hvor retsanvenderens forståelse af fak-

tum virker tilbage på hans forståelse af jus etc. – en vekselvirkning, man f.eks. kender fra proces- og forvaltningsretten, jf. nærmere *E&A* s. 30 f. med henvisninger.

2.2. Informationsteori

2.2.a. Information som retsgode

En processor – en "edb-maskine", en "datamat", en "computer", et "IT-system" – er i bund og grund et værktøj, der er konstrueret til at gøre noget (*in casu*: modtage kommunikative instruktioner), som mennesket principielt godt kan, men som det helst vil undgå, enten pga. magelighed, styrkemæssig begrænsning eller af en anden grund. Alligevel adskiller IT sig fra megen anden teknik. Hvor f.eks. gravemaskiner og symaskiner understøtter rent manuelle og dermed i hovedsagen "stoflige" funktioner, udfører computere noget immaterielt: bearbejdning, lagring og formidling af *data* og *information*.

Ordene computer og datamat betyder det samme. Det engelske "computer" har dog vundet indpas frem for det tyske "datamat", fordi hovedparten af IT-terminologien er engelsksproget. Ordet IT-system betegner en totalitet bestående af komponenter sammensat i overensstemmelse med visse tekniske (herunder sproglige) og organisatoriske lovmæssigheder og forudsætninger, og som ved hjælp af digital teknik er i stand til at behandle information.

Universelt begreb

Kommunikation indgår i alle livets forhold. Den menneskelige hjerne bearbejder information ved hjælp af nerve- og hjerneceller. Ved mikrobiologiske celledelinger overføres genetisk information med DNA-molekylet som væsentligste medium. I social omgang udveksles en bred mangfoldighed af information, både direkte (skrift og tale) og indirekte (påklædning og manerer). Retlig regulering sker gennem formidling af information om normer og sanktioner.

Som andre af dagligsprogets basale termer har informations- og kommunikationsbegreberne et diffust indhold, som ikke desto mindre rummer et veldefineret kerneområde: Al IT-anvendelse – ikke blot i forbindelse med velkendte administrative funktioner og beregninger mv., men også i mere skjult form (f.eks. analysatorer, servomekanismer og udlæsningsenheder) – opfylder nogle helt ensartede funktioner, som kan forklares med udgangspunkt i informationsbegrebet.

Information og data

Begreberne information (som i IT, *Informations*Teknologi) og data (som i edb, Elektronisk *Data* Behandling) hænger nøje sammen. Data (af latin: "dare", at give) betegner noget, der er givet, men som ikke nødvendigvis er meningsfuldt for den iagttagende. En datamængde er en manifestation, som kan være bærer af et informationsindhold – en "mening" – men som i sin foreliggende form ikke tilkendegiver denne mening. Hvor en mængde tegn i sig selv udgør data, kan den mening, tegnet bærer, beskrives som information. En forkortelse, der dækker over en ordsammensætning, læseren ikke kender, fremstår umiddelbart som data. Men når ordsammensætningen går op for læseren, forandrer disse data sig til information (og når iagttageren tænker længe nok over dem – til visdom!). Den omkodningsproces, der transformerer data til information, behøver dog ikke have en sådan indforstået karakter. Før man læser en tekst, fremstår den som data (tegn); men gennem læsningen udleder man de informationer, bogstaverne bærer. Tallet 31 fremtræder isoleret set som data. I en sammenhæng, hvor det angiver antallet af dage i en måned eller kursen på en aktie, vil det derimod repræsentere information.

I talrige tilfælde fremtræder information som et selvstændigt og afgrænseligt fænomen, der kan gøres til genstand for bl.a. overdragelse og finansiering. Både de analoge informationer, der f.eks. fremtræder i bøger, aviser, radio/TV, videofilm etc., og de digitale informationer, der erhverves i CD'er, edb-programmer og databaser, udgør dele af et samlet marked for information. Se ligeledes SOU 1992:110: Information och den nya Informations-Teknologin, s. 155 ff., der diskuterer spørgsmålet, "om information är egendom". Som her nævnt har dette navnlig været aktualiseret i relation til straffelovens regler om tyveri mv., se herom i afsnit 17.2.a. og 17.2.b., hvor det konkluderes, at "tyveri" af information herhjemme vil blive behandlet som en kombination af tyveri/brugstyveri (i relation til mediet) og som krænkelse af erhvervshemmeligheder mv. (informationsindholdet).

For en ydre betragtning minder sådanne overdragelser om salg af andre formuegoder. Men når informationen er dominerende i en ydelse, er det ikke altid muligt at anvende retssystemets almindelige regler på den. Dette skyldes en række karaktertræk, der gør sig gældende ved enhver type information – karaktertræk, som træder mærkbart frem, når informationselementet dominerer en ydelse, og/eller når informationen på grund af mediets karakter kan adskilles fra ydelsens materielle fremtrædelse.

1. Information og medium

Først og fremmest fremtræder information i en kombination mellem noget materielt og immaterielt. Information er altid le-

gemliggjort i et medium. Ordet står på papiret, billedet er trykt på lærredet, og det mundtlige råd manifesterer sig i den fysiske tale (lydbølger). Selv den ikke-udtalte idé manifesteres i hjernens impulser. Sondringen mellem information og medium har betydning, når man disponerer over information. Et informations*medium* kan berøres med hænderne eller i det mindste mærkes med sanserne; men det giver ingen mening at tale om "berøring" og "sansning" mv. af information som sådan. Den ydelse, der består af mundtlig rådgivning, f.eks. i forbindelse med en advokatkonsultation, manifesteres vel i det talte ord eller den nedfældede juridiske redegørelse; men værdien af det pågældende råd vil helt bero på en kommunikativ sammenhæng, klientens konkrete situation.

2. Information og kommunikation

For det andet optræder information altid i en proces. Denne proces, hvor mindst to aktører eller enheder *kommunikerer*, resulterer i, at informationen – med større eller mindre præcision – genskabes. Når processen er afsluttet, befinder informationen sig på mindst ét yderligere medium. Dette forhold, at information altid "bruges" ved at blive "kopieret", giver anledning til problemer ved aftaler om overdragelse eller finansiering af information. Betaler "informationskøberen" ikke for sin ydelse, har leverandøren ofte ingen interesse i at få den tilbage igen; der var jo kun tale om en kopi. Ønsker sælgeren omvendt at afskære køberen fra at gøre brug af informationen, kan dette kun ske, hvis alle de medier, hvorpå informationen har nået at fæstne sig, enten bringes tilbage til deres oprindelige tilstand eller destrueres. Dette rejser en række problemer, hvis informationen uden vanskelighed kan springe fra medium til medium, eller hvis den kan fæstnes i modtagerens hjerne! Uden for kriminalromanernes verden må man i samme omfang acceptere, at den overdragne information må anses for utilbagegivelig.

3. Kommunikation og reproduktion

Hermed er også den tredje egenskab antydet, nemlig at information udfolder sig i en proces, hvor den *reproduceres*. Når jeg fortæller dig vejen til banegården, kommer du i besiddelse af denne information, men dermed slipper den jo ikke mig! Denne egenskab betyder dels, at samme information kan overdrages et uendeligt antal gange, dels at information ikke er udsat for de risici, der truer ting. For "køberen" af en oplysning er det underordnet, om det papir, oplysningen stod på, er gået til grunde, hvis blot informationen kan reproduceres, f.eks. fra hukommelsen.

4. Kommunikation og sprog

For det fjerde er det karakteristisk, at en kommunikationsproces kun kan gennemføres, hvis dens parter betjener sig af et identisk sæt af regler for, hvordan data fæstnes til et medium

henholdsvis transformeres til information – et såkaldt sprog. Jo mere præcist dette sprog er, og jo mere håndfast det efterleves, des mere effektivt forløber processen. Når processen anvender et såkaldt formalsprog, jf. nærmere nedenfor, vil kopieringen være perfekt. Det gælder navnlig for kopier af edb-data og -programmer.

Disse fire egenskaber gælder for al information – hvad enten den fremtræder som digitale bits i en computer eller som skrifttyper i en avis eller en bog. Men egenskaberne træder mærkbart frem og får selvstændig betydning, når man har at gøre med et medium, der besidder en effektivitet og præcision som edb-mediets. Når IT har fået så stor anvendelse, skyldes det netop – som vi så i forrige afsnit – dens kapacitet i henseende til hurtig og præcis *behandling* af information. Navnlig den heraf følgende løse tilknytning mellem information og edb-medium har fået en række af informationens grundlæggende egenskaber op til overfladen.

Pris og kvalitet

En væsentlig markedsmæssig konsekvens af denne mekanisme ligger i, at der ofte ikke er sammenhæng mellem pris og kvalitet af informationsydelser. Dette betyder f.eks., at den, der kan levere information, har en stor frihed i prissætningen. Han behøver alene tænke på markedets købekraft og -vilje. Denne faktor virker dog også i modsat retning. Brugerens bevidsthed om, at hver transaktion isoleret set kun "koster" leverandøren mediets pris, har dels været medvirkende til den forholdsvis ringe respekt, der beklageligvis hersker om de immaterielle rettigheder, dels fører den erfaringsmæssigt til, at brugere ofte "venter og ser", om ikke produktet bliver billigere – en praksis, der på kontraktsområdet dels fører til en jungle af rabatter mv., dels en heraf følgende kontraktspraksis om "most favoured customer"-klausuler, der garanterer den køber, der træder til, en kompensation svarende til den, som vil følge af efterfølgende prisnedsættelser. Se f.eks. pkt. 8.2, stk. 2, i henholdsvis K18 og K33.

Oversigt

I det følgende afsnit skal vi se nærmere på teorien bag begreberne kommunikation, information, medium og sprog. Teorierne har central betydning ikke blot for al IT-anvendelse, men for alle kommunikationsforløb. Analysen er vigtig for den senere forståelse af, hvordan retssystemets almindelige regler skal bruges på informationsrelaterede produkter og ydelser, og hvorfor det kan være nødvendigt at tilpasse retsgrundlaget.

2.2.b. Den matematiske kommunikationsteori

Ordet "computer" er udledt af det engelske "to compute", at beregne. Selv om den egentlige talbehandling kun fremtræder overfor brugeren som en begrænset del af IT-anvendelsen, ligger grundlaget for al moderne IT i tal, lagret i form af éttaller og nuller. Når et skærmbillede – tilsyneladende – står stille og viser en tekst eller en grafisk tegning, udføres der titusinder af instruktioner. Skærmen modtager disse løbende instruktioner fra en processor og instrueres dermed om at se ud, som den gør.

Kvantitativ definition

At det lader sig gøre at omskrive fænomener, der fremtræder så forskelligt som billeder, lyd, tekst osv., til tal, bygger på en teori, der forklarer informationsbegrebet som noget kvantitativt, altså i tal. Teorien, der er blevet betegnet den matematiske kommunikationsteori, har grundlag i nogle afhandlinger, der blev publiceret i slutningen af 1940'erne af *Claude Shannon*, *Warren Weaver* og *Norbert Wiener*, se nærmere henvisningerne i *E&A*, s. 268. Teorien er siden blevet en teoretisk "grundlov" for nutidens digitale computer.

Binær information

Informationsbegrebets kvantitative karakter fremtræder mest tydeligt, når man ser på, hvordan en meddelelse bliver til. Meddelelsen består af ord, tegn, bits, der hver for sig, eller gruppevis, udvælges inden for en sproglig (syntaktisk, semantisk, grammatisk) ramme. Afgives informationen via et tastatur, fremstår valgene ved hvert eneste tastetryk. Da man kan sætte tal på antallet af valgmuligheder, kan en informationsmængde altid omskrives til en *talværdi*. I et tegnsystem med 256 tegn kan tekstens samlede kvantum af information udmåles til antallet af tegn opløftet i 256. potens. Som vi så det i den historiske gennemgang, anvender nutidens computere et instruktionssæt opbygget efter et totalssystem. Den mindste informationsmængde repræsenteres derfor i valget mellem to muligheder. Som betegnelse herfor anvender man ordet bit (af engelsk: *bi*nary digi*t* – binært tal).

Parallelle sprog

Det kan måske forekomme mærkværdigt, at man ved hjælp af to tilstande kan repræsentere så megen information som den, der indlæses, behandles og udlæses under anvendelse af moderne IT. Når der til et sprog definitorisk hører et sæt af ord, jf. nedenfor, hvorledes kan man da "tale" ved kun at sige "1" og "0" i vekslende kombinationer? Forklaringen er, at IT-kommunikation anvender flere sprog samtidig, ganske som samtalepartnere foruden det talte sprog anvender kropssprog mv. På et basalt plan er der defineret en kode, der fastlægger informationsindholdet af hvert enkelt tegn (bogstaver mv.). Med udgangspunkt i mængden af til-

ladte tegn kan man definere ord, ordklasser og sætninger. Disse informationsmængder fortolkes derpå af de styresystemer, programoversættere og applikationer, som informationssystemet er programmeret med, og som med hver deres programmeringsmæssige ramme definerer en mangfoldighed af "sprogregler", ofte udtrykt gennem begreber som *kompatibilitet* og *interoperabilitet*.

Byte

Den grundlæggende kode bestemmer, hvor megen information (hvor mange bits), der skal kunne rummes i ét tegn. Sætter man denne kode til én bit, kan maskinen kun sige 1 eller 0. Anvender man to bits, bliver det muligt at fremkalde fire mulige instruktioner: 11, 00, 10 og 01. Anvender man tre bits, bliver det muligt at frembringe hele otte instruktioner (beregnet som 2 opløftet til tredje potens): 000, 001, 010, 011, 100, 101, 110 og 111. Ved hjælp af 8 bits kan man frembringe hele 256 instruktioner (dvs. 256 tegn), hvilket almindeligvis er rigeligt til de fleste formål. Da dette anses for at være en passende enhed, har man valgt at kalde 8 bits for en byte (*by* eigh*t*).

Typisk anvender man en ekstra bit som en såkaldt kontrolbit. Formålet hermed er at undgå fejl (hvorved et 0 sendes som et 1 eller omvendt), når data transmitteres som en binær kode. Kontrolbitten markerer, om tværsummen af de øvrige bits er lige eller ulige, hvorved man under kommunikationen kan afsløre enkeltbitfejl.

Kompatibilitet

Den, der udvikler et IT-system, kan principielt frit afgøre, hvad disse forskellige binære tegn skal betyde. Tillader han sig denne frihed, vil det færdige system imidlertid lide af *inkompatibilitet*, jf. om dette begreb nedenfor. Dette ville betyde, at den enkelte IT-leverandør så at sige måtte "genopfinde hjulet". Derfor har man på et tidligt tidspunkt udviklet standarder herfor. Den mest udbredte standard for en 7-bit kode er den såkaldte ASCII-kode. Udviklingen af en sådan kode er udtryk for de bestræbelser på standardisering, som omtales i afsnit 5.3. ASCII-koden er offentliggjort i forskellige standarder, se bl.a. ISO 646 og 8859, og som Dansk Standard 2089. Et andet eksempel er de standarder, der generelt definerer kommunikation på Internet (TCP/IP).

Høj informationsværdi = lav sandsynlighed

At informationsbegrebet kan defineres kvantitativt, kan også udtrykkes således, at en informationsmængde altid står i forhold til den *sandsynlighed*, hvormed dens indhold (dvs. resultatet af afsenderens valg) kan forudsiges. Består informationen af én bit, er der stor sandsynlighed (50%) for, at man kan gætte dens indhold. Informationsværdien er altså lav. Omvendt er det praktisk utænkeligt, at nogen kan gætte indholdet af en omfattende tekstmængde repræsenteret ved et stort tal. Sandsynligheden herfor er

ringe, og tekstmængdens informationsværdi tilsvarende høj. Dette forhold mellem information og sandsynlighed harmonerer for så vidt med dagliglivets erfaring. En nok så tyk bog er ikke informativ, hvis der står det samme ord side op og side ned fra ende til anden. En person, der altid gentager sig selv (og hvis tale dermed kan forudsiges med høj sandsynlighed), er som bekendt heller ikke udpræget informativ!

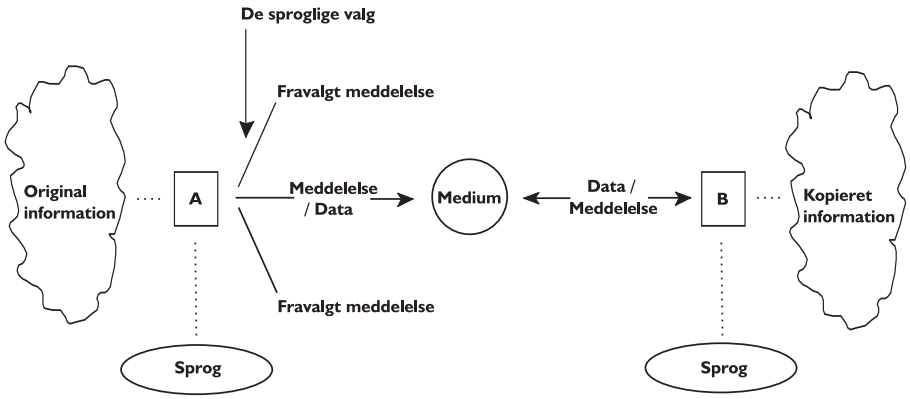
Information som påvirkningsfaktor

Kommunikationsteorien karakteriserer kommunikation som en proces, hvor én aktør søger at påvirke en anden ved hjælp af information. Kommunikationsprocessen sættes i gang ved, at afsenderen vælger et antal tegn inden for et sprog og fæstner dem til et medium. Afsenderens frihed til at vælge tegn begrænses af flere faktorer, sml. ovenfor om koden for tegnsæt. For det første ved reglerne i det sprog, han vil betjene sig af. For det andet ved de fysiske egenskaber og begrænsninger, som behersker det medium, tegnene fæstnes på. Og for det tredje ved selve formålet med kommunikationen – et formål, som ofte vil indebære begrænsninger af tids- og ressourcemæssig karakter.

Teorien er universel. Det er underordnet, om processen – og dermed påvirkningen – sker i forholdet mellem en kunstner og hans publikum, en cellekerne og et ribosom eller mellem forskellige styrende dele i en computer eller for den sags skyld en hvilken som helst anden maskine. *Shannon & Weaver* indleder deres fremstilling med at fremhæve, at information også indgår i "music, the pictorial arts, the theatre, the ballet ...". Tanken kan dog sagtens strækkes videre. Hvis en mekanisme til trykudligning virker ved, at en ventil holdes tilbage af en fjeder, indtil der opstår en given kraft, kan det vel forekomme aparte at tale om, at der tilgår ventilen "information" om trykkets kraft mv. Men sådan må forholdet rettelig rubriceres. Styres ventilen af en anordning, der registrerer trykket, konverterer det til digitale signaler og derefter – maskinelt – enten åbner eller lukker et spjæld, ligger det lettere for tungen at tale om en kommunikativ funktion. Set fra en kommunikationssynsvinkel sker der det samme. Fjederen i første eksempel er med sine særlige dimensioner et egnet medium til at overføre informationer om styrken af et vist tryk.

Sprogets funktion

Som før nævnt kan information kun overføres, hvis afsender og modtager anvender samme sprog. Skal radiotelegrafisten og flaggasten udnytte deres respektive færdigheder, må de kommunikere med fagfæller. Ethvert sprog – såvel edb-sprog som det talte sprog – består af et antal ord eller ordklasser (ofte suppleret med et alfabet), en syntaks (dvs. regler for brugen af forskellige ord-



De forskellige aktører i en kommunikationsproces kan illustreres i denne figur. A vælger inden for en sproglig ramme, som han har fælles med B, en besked, som han knytter til et medium. Når B sætter sig i fysisk forbindelse med mediet, får han med sit kendskab til sproget mulighed for at reproducere informationen. Kommunikationsprocessen er dermed tilendebragt, og informationen reproduceret.

kombinationer mv.) og en semantik (dvs. regler for betydningsindholdet af de enkelte ord og instruktioner).

Formalsprog

Man sondrer ofte mellem to typer af sprog, beroende på den stringens, hvormed syntaks og semantik defineres. Formalsprog – hvortil f.eks. programmeringssprog hører – er sprog, som ikke tolererer tvetydigheder. Deres syntaks og semantik kan fastlægges med matematisk præcision. Derfor må de tegn, afsenderen vælger i et formalsprog, nøje følge sprogets regler, hvis kommunikationsprocessen skal overføre information.

Naturlige sprog

Naturlige sprog – f.eks. dansk og engelsk – er omvendt præget af en løs struktur og en uprækcis semantik. Som man vil kunne erfare ved at tale med småbørn, er det muligt at overføre ganske præcis information trods tilsidesættelse af næsten enhver grammatisk forskrift. Forskningen i såkaldt kunstig intelligens arbejder bl.a. på at opbløde sondringen mellem naturlige og formelle sprog. I det omfang dette lykkes, vil man kunne tale med sin computer i et naturligt sprog (f.eks. engelsk). Udviklingen af sådanne systemer står overfor en række grundlæggende problemer. Maskinen arbejder stadig i tal og er derfor nødt til at håndtere den uskarpe menneskelige logik i en kompleks mangfoldighed af valgmuligheder.

Kompatibilitet

Reglen om, at en kommunikationsproces kun kan gennemføres (dvs. informationen dupliceres eller genskabes), hvis afsender og modtager har kendskab til et identisk sprog, kan formuleres som en betingelse om dobbelt regeloverholdelse. Når afsen-

der og modtager kan tale samme sprog og udveksle det medium, hvorpå tegnene er nedfældet, på en måde, der gør det muligt at udlede information af data, taler man om kompatibilitet.

På grund af de forskelligartede samtidige kommunikationsprocesser, der foregår under IT-anvendelsen, kan der bestå kompatibilitet på vidt forskelligartede niveauer. To kommunikerende enheder er kompatible, hvis de er i stand til at afgive og modtage information fra hinanden. Er der tale om den form for teknisk information, der udveksles inden for rammerne af et IT-system, betyder kompatibiliteten, at de to enheder kan arbejde sammen eller indtræde som erstatning for hinanden. Et program kan f.eks. være kompatibelt med en given program- eller maskintype og en printer til en given teksttype. En stor del af arbejdet med at udvikle moderne software består i at hidføre den fornødne kompatibilitet, internt (mellem programmets delmoduler mv.) såvel som eksternt. En utilsigtet ombytning af et I-tal med et O kan afskære hele systemets funktion. En enhed vil f.eks. være kompatibel i én henseende (f.eks. under afviklingen af en særlig form for databehandling), men ikke i en anden. En fejl vil kun vise sig under særlige kombinationer mellem programmer, data og maskinel.

Mediets funktion

Ganske som man kan tænke sig en uendelig mængde af sprog, er der ingen begrænsninger i, hvilke fysiske indretninger der kan anvendes som medium for information. Fjerner man blikket fra IT-området, har samfundet gennem tiderne anvendt så vidt forskellige medier som træ (med indhuggede markeringer), sten (runeskrift), røgsignaler, fagter (døvesprog), lydsignaler (kirkeklokker, sirener), papir og radiobølger.

Som fremhævet af *Fred I. Dretske* i hans indgående analyse af kommunikationsteorien (1981), kan et hvilket som helst materielt fænomen anskues som medium for en informationsmængde. "Any situation may be taken, in isolation, as a generator of information" (s. 14). Denne pointe er helt central for analysen af, hvornår et informationsrelateret produkt eller fænomen skal placeres inden for rammerne af de regler, der gælder for fysiske fænomener, f.eks. for reglerne om ejendomsrettens overgang eller i relation til produktansvaret. Det forhold, at enhver materie i den ydre verden kan tolkes som information, er imidlertid ikke ensbetydende med, at den nødvendigvis er bærer af information.

Praktiske aspekter

Når en retsregel anvender et begreb, der involverer information eller en kommunikationsproces, må man indledningsvis tage stilling til, om reglen herved tager sigte på et *informationsind-*

hold (f.eks. en injurie), på et *medium* (f.eks. et læserbrev) eller på den *påvirkning*, der indtræder ved kommunikationsprocessen (f.eks. følelsen af at blive injurieret). En sådan inddeling kan kaste lys over en bestemmelses generelle funktion. Når ophl. § 1 f.eks. taler om "værk", henviser dette til et informationsindhold (resultatet af ophavsmandens kunstneriske eller litterære indsats), hvorimod lovens anvendelse af ordet "originalværk" og "eksemplar" henviser til det medium, hvori værket er manifesteret, henholdsvis ved dets frembringelse, og når senere eksemplarer af det frembringes. Påvirkningen udgør i dette eksempel den kunstneriske oplevelse, som er hele formålet med at frembringe værket, og som efter omstændighederne indgår i vurderingen af, om der foreligger ophavsretlig værkshøjde eller originalitet, jf. herom afsnit 6.2.c. Tilsvarende væsentligt er det, om en panteret i et "program" omfatter ophavsretten hertil, et antal ophavsretlige beføjelser, eller blot et medium (en "programpakke"), hvori programmet er manifesteret.

Relation mellem information og medium

For en række praktiske formål kan det være nødvendigt at udsondre forskellige typer af medier fra hinanden ud fra deres vekslende evne til at integrere information i sig.

Integreret information

I en første kategori kan man udskille den information, der for de relevante praktiske forhold er *integreret i* og for praktiske tvangsfuldbyrdelsesformål dermed uadskillelig fra sit medium. I IT-sammenhæng gælder dette en stor del af systemets hardware (f.eks. halvlederkomponenter). Uden for IT-retten omfatter begrebet også materielle brugsgenstande mv., der i sig selv manifesterer en information, der kan have en funktionel karakter ved at meddele brugeren, hvordan produktet skal håndteres, som eksempelvis skruelågets oplysning til brugeren om, hvordan flasken åbnes. Ligeledes kan den æstetiske information, som en brugskunstner lægger i et værk af brugskunst, betragtes som sådan. Her ses informations-egenskaben netop ved den risiko for plagiering, der består for sådanne frembringelser: Selvom den for definitionsbegrebet definitorisk nødvendige mulighed for kopiering altså består, er denne mulighed for de fleste formål forbundet med så stort et besvær, at muligheden ikke har betydning ved den praktiske håndtering af genstanden, f.eks. ved stiftelse af ejendomsret eller pant.

Mediekompatibel information

I en anden kategori finder vi den information, der efter sin karakter og sit formål nødvendigvis må være knyttet til en *bestemt type* medium, som det til gengæld har en forholdsvis løs tilknytning til. Informationen kan altså ubesværet flyttes fra et eksemplar af mediet til et andet; den kan blot ikke flyttes til et

medium af en anden type. I denne kategori finder man den digitale information, der er indlæst på et magnetisk eller optisk medium (f.eks. harddisk, diskette eller CD-ROM). Muligheden for at flytte disse informationsmængder til medier af samme art indebærer ligeledes en mulighed for at optimere selve kopieringshandlingen. I ophavsretlig sammenhæng har dette givet grundlag for ophavsretslovens særlige regler om kopiering af værker i digital form.

Fleksibel information

En tredje kategori er den information, der ubesværet kan springe fra en type medium til et hvilken som helst andet medium. På grund af denne informations fleksibilitet, opleves informationen som et aktiv, der eksisterer uafhængigt af noget medium. Til denne gruppe hører generelle idégrundlag, slogans, forretningskoncepter, der på få sider kan nedfældes på papir, hvorfra det kan kopieres, men som også umiddelbart kan videregives mundtligt eller på anden måde, når de er sagt eller skrevet. Sådanne former for information har utvivlsomt den største betydning for den menneskelige omgang og giver ligeledes anledning til retlige problemer af forskellig art – f.eks. ved reglerne om ærekrænkelser, fortrolighedsbrud, nedsættende omtale etc. I pante- og ejendomsretlig henseende opstår der særlige problemer med hensyn til, om sådanne informationsmængder – når ikke de er omfattet af immaterialretlige retspositioner – kan rubriceres som "formuegoder", se hertil afsnit 12.1.c.

2.2.c. Foreløbig sammenfatning

Det ovenfor sagte kan sammenfattes som følger:

Sammenfatning

En kommunikationsproces udspiller sig mellem en afsender og en modtager under omstændigheder, hvor afsenderen ønsker at *påvirke* modtageren. Påvirkningen forudsætter, at afsenderen forandrer et fysisk medium, som såvel afsenderen som modtageren er i fysisk kontakt med. Forandringen sker inden for rammerne af et regelsæt, som både afsenderen og modtageren kender, et såkaldt *sprog*.

Begrebet information

Begrebet information kan herefter defineres som *manifestationen* af de *valg*, som nogen (afsenderen) har truffet i overensstemmelse med et *sprog*. Anskuer man de enkelte elementer i denne definition, fremtræder der en sondring, der er velkendt for al menneskelig tænkning, og som kan føres tilbage til klassiske filosoffers (Platon m.fl.) sondring mellem Ånd og Materie: På den ene side står nemlig den *materielle manifestation* (som vi i køberetten ser som "salgsgenstanden" og i ophavsretten som "ek-

semplaret" eller "originalværket"). Heroverfor står informationens *immaterielle side*, nemlig de valg, som afsenderen traf ved hjælp af sit sprog.

I kommunikationsteorien defineres begrebet *kommunikation* som den handling, hvorved information overføres mellem afsender og modtager. Rent praktisk realiseres overførelsen ved, at mediet bringes i fysisk kontakt med en modtager, som med sit kendskab til det anvendte sprog reproducerer de valg, afsenderen foretog, da han manifesterede informationen i mediet. Også her træder en sondring frem mellem noget materielt og immaterielt. Det materielle aspekt ligger i de fysisk-faktiske handlinger og mekanismer, hvorved henholdsvis afsenderen og modtageren kommer i fysisk kontakt med mediet. Det immaterielle i forudsætningen om, at såvel afsender som modtager gør brug af et sprog. Når modtageren konstaterer, hvilke tegn og signaler der er valgt, kan han *genskabe* den situation, afsenderen befandt sig i, hvorved han vil kunne reproducere den afgivne information. Den heraf følgende erkendelse giver grundlag for den *påvirkning*, afsenderen tilsigtede.

Atomer og bits

Den toneangivende amerikanske professor *Nicholas Negroponte* anvender i sin bog, "Det digitale liv" (1997, oversat fra engelsk: Being Digital), en sprogbrug om kommunikationsprocessens materielle og immaterielle side, der fokuserer på det mindste element i henholdsvis information og medium. Hvor den materielle side, mediet, repræsenteres ved *atomer*, repræsenteres selve informationsindholdet ved *bits*. Når boghandleren sælger en bog, sælger han atomer, hvorpå der er materialiseret bits. Køber man bogen ved at *downloade* den fra Internet, køber man kun bits, der ikke er "flyttet", men derimod "kopieret" til et medium, køberen i forvejen rådede over: Den ophavsretlige tilladelse (licens) til at foretage denne kopiering får dermed central betydning. Den transformation, som en række virksomheder i disse år undergår for at kunne omstille sig til det digitale samfund, indebærer netop, at man fremover skal sælge bits i stedet for atomer og i den forbindelse forholde sig til de ophavsretlige problemer, sådanne transaktioner rejser. Transformationsprocessen præger ikke alene de typiske informationsindustrier som forlags-, underholdnings- og nyhedsindustrien, men også klassiske "hardware"-industrier.

Praktisk terminologi

Selv om kommunikationsteorien fremstår som en abstrakt teori, der i kraft af abstraktionsniveauet kan forekomme verdensfjern, tilbyder den en god forklaring på nogle af de egenskaber, der præger enhver kommunikationsproces, hvad enten den udføres ved hjælp af digitale medier eller andre medier. Dernæst kommer dens principper til udtryk i den terminologi, man anvender i IT-praksis.

Den, der vil *udvikle* et nyt program, må – som vi senere skal se – anvende de programinstruktioner ("ord"), der anerkendes af det programmeringssprog, han gør brug af, og overholde sprogets syntaks og grammatik. Gør han ikke det, kan programmet ikke køre, når det "oversættes" til maskinens sprog.

Også *brugerens* betjening af et IT-system forudsætter, at der anvendes et sprog. Ønsker han f.eks., at maskinen skal finde frem til en information, han har lagret et bestemt sted, er det ikke tilstrækkeligt at skrive på tastaturet: "Vær så venlig at finde frem til de filer, hvor der står noget om ophavsret" eller "find det, der står om ophavsret, og vis det på skærmen". Denne ramme for forståelsen af systemet betegnes som systemets brugergrænseflade. Derimod taler man om "kommando-sprog" i forbindelse med brugen af databasesystemer. Kommandosproget knytter til hver kommando et ganske præcist sæt konsekvenser. Kommandoen "find" kan f.eks. betyde noget andet end "vis" og er kun aktiverbar under ganske specifikke omstændigheder.

2.2.d. Juridiske aspekter

Den digitale teknologi har frembragt en helt ny form for informationsbehandling. Hvor analog informationsbehandling almindeligvis knytter sig til en tilstand i den ydre verden, der kan være mere eller mindre veldefineret (f.eks. termometerets søjle, der følger molekylærhastigheden), beror indholdet af digital data altid på en værdi, der kan opgøres numerisk eksakt. Indholdet af den digitale datamængde y kan altid entydigt bestemmes på grundlag af indholdet af den forudgående datamængde x. Dette indebærer for det første, at sammenhængen mellem de enkelte digitale datamængder er mere kompleks (fordi der er denne logiske forbindelse), for det andet, at digital information altid må frembringes, henholdsvis læses, ved hjælp af et "teknisk" (formelt) sprog. Omvendt indebærer det digitale sprog for det tredje muligheden for at lagre, overføre og transmittere digital information med ekstrem effektivitet, idet muligheden alene beror på, hvor hurtigt og effektivt de pågældende tal kan frembringes, repræsenteres og overføres.

Mangelproblemer

Disse forskelle kommer til praktisk udtryk i relation til mangelsproblemerne i IT-overdragelse. IT-systemer vil ofte være fejlbehæftede i situationer, hvor man ikke ville vente fejl af et analogt system, og diskrepansen mellem fejl og fejlfrihed vil typisk være langt større. Programmøren er underlagt et komplekst sæt af regler, der stiller krav til de valg, der træffes under processen.

Dermed består der en latent risiko for fejl i programmeringen, der enten fører til mangler eller – under en udviklingsproces – til forsinkelser i aftalte afleveringsterminer.

Tidsdimensionen

Nutidens kraftfulde teknikker til behandling og transmission af information har på fundamental vis ændret *tidsdimensionen* i talrige kommunikationsprocesser. Ved hjælp af IT kan brugeren på kort tid fremskaffe og sammenstille information, som ellers ikke ville være tilgængelig inden for den for beslutningstageren relevante tidshorisont. Dermed er tidligere gældende barrierer for, hvilke informationer man kunne lagre eller registrere, forsvundet. Informationer, som før ville være hensunket i glemslen, vil de fleste brugere "for en sikkerheds skyld" gemme, og bliver der brug for dem, kan de i løbet af sekunder hentes frem uden besvær. Hvis man antager, at den enkelte har en ret til at blive glemt, rejser disse nye muligheder et problem. Dette problem er i dag reguleret ganske intenst ved reglerne om persondatabeskyttelse, jf. i det hele kapitel 13. Tidsdimensionen indebærer ligeledes, at der er opstået nye muligheder for hurtig og effektiv koordination af krav og ønsker, der foreligger maskinlæsbart, hvilket udnyttes bl.a. i det såkaldte "*just-in-time*" koncept, der går ud på at reducere produktionsomkostningerne ved målrettet kontrol med samtlige produktionselementer (f.eks. indkøb og lagerføring).

Grænseoverskridelse

Samtidig er den rumlige dimension gået i opløsning. Hvor der i tidligere tider gjaldt visse geografiske grænser for, hvilke påvirkningsmuligheder den enkelte aktør eller organisation kunne betjene sig af, transmitteres information i dag samtidigt og effektivt fra og til fjerne afkroge af kloden. Fænomenet kendes fra massemedieområdet. Minutter efter, at en dramatisk begivenhed har fundet sted, kan TV-modtagere over hele kloden følge med i forløbet.

"Digital fartbegrænsning"

På grund af disse forskelle mellem den moderne digitale informationsteknologi på den ene side og klassiske informationsteknologier som f.eks. papir og kartotekskort på den anden, kan man ikke altid fastholde, at det, der er lovligt i papirets verden også skal være det i den digitale. På visse områder af lovgivningen har man allerede taget konsekvensen heraf. Når ophl. § 12, stk. 2, nr. 3-5, f.eks. forbyder enhver kopiering til privat brug af edb-programmer, databaser og andre værker i digital form, men opretholder kopieringsadgangen for f.eks. manualer til edb-programmer, hænger dette sammen med det besvær, papirkopiering er forbundet med sammenlignet med den lethed, hvormed edb-programmer kan kopieres. De trykte programmer sidder så at sige

bedre fast på papirmediet, dels fordi de er besværlige at kopiere, dels fordi (foto-)kopiering fører til et kvalitetstab. På andre lovgivningsområder er det op til praksis at tage stilling til, om reglerne om fysiske fænomener uden videre skal overføres til IT-området, sml. f.eks. senere i denne bog om spørgsmålet om anvendelsen af reglerne i købeloven, produktansvarsloven og produktsikkerhedsloven på edb-programmel.

Immateriel fremtrædelse

Væsentlige dele af en digital kommunikationsproces kan ikke konstateres af brugeren. Kun dens resultat i form af f.eks. et skærmbillede, en lydimpuls eller en udskrift er måleligt. Programmets kildetekstversion, som er "menneskelæsbar", vil typisk udgøre leverandørens erhvervshemmelighed, som brugeren ikke kan få andel i. Derfor må IT-systemers funktioner altid være "forklaret" for brugeren eller efterfølgende systemudviklere, henholdsvis ved brugermanualer og systemdokumentation. Samtidig består der en latent risiko for, at systemerne rummer funktioner, der er skjulte over for brugeren, f.eks. en programvirus.

Original og kopi

Den flygtige forbindelse mellem IT-baseret information og medium gør det vanskeligt at anvende de regler, der knytter sig til papirmediet – f.eks. gennem krav om underskrift, skriftlig påførelse eller udsletning mv. Når reglerne om negotiable dokumenter går ud fra, at der er en *original* udgave af det pågældende dokument, som bærer den pågældende rettighed, støder man på problemer, når der er tale om digital information på diskette mv.: Informationen kan nemlig uden vanskelighed flyttes til en anden diskette, uden at hverken den første eller den anden diskette (modsat det underskrevne papir) bærer varigt præg af, at den har været det. Vil man definere et "originalt" digitalt dokument som et digitalt medium, hvor en information varigt har fæstnet sig, må betegnelsen reserveres til særlige indretninger, som er i stand til at holde fast på bestemte typer information og samtidig tjene som bevis for, at der ikke foreligger en kopi, som rettighedshaveren ikke har ønsket. Dette formål kan f.eks. opnås ved brug af visse "intelligente" chip-kort. Derimod må man opgive forestillingen om, at det medium, hvorpå de pågældende data *første gang* blev fæstnet, er det originale. Dette måtte i givet fald indebære, at det eneste originale medium var den hukommelsesenhed (RAM), hvortil informationen blev skrevet første gang, og som forlængst er anvendt til anden information. Efterfølgende lagring på lagermedier (f.eks. en diskette) er ikke længere "originale".

Dette problem har rejst et behov for teknikker, der skal ækvivalere med papirmediets "originale" karakter. Sådanne teknikker er allerede indbygget i værdipapirhandelsloven, der nu udgør de retlige rammer for Værdipapircentralers virksomhed. Lovens § 59, stk. 1, giver hjemmel til, at værdipapirer kan udstedes og overdrages i papirløs form (dematerialiseret) som fondsaktiver, der er registreret i en værdipapircentral. Problemernebehandles i betænkning 1394/2000 fra Justitsministeriets udvalg om papirløs tinglysning. En væsentlig ingrediens i disse løsninger vil være brugen af *digital signatur*, jf. herom nedenfor i afsnit 4.2.d., 16.2.c. og 16.5.

"Ret" til information

Den omstændighed, at information overdrages ved at blive kopieret, indebærer, at information, der lader sig kopiere ubesværet og uden omkostninger, isoleret set kun kan udnyttes kommercielt ved én overdragelse. Uden særlig retsbeskyttelse vil informationskøberen nemlig kunne reproducere den overdragne information ubesværet og dermed konkurrere direkte med informationssælgeren, se nærmere *Thomas Riis*: Ophavsret og retsøkonomi (1996), s. 58 ff. Dette problem kan i et vist omfang løses af parter, der forudsættes at fastlægge deres relation gennem aftaler om hemmeligholdelse mv. Men overfor tredjeparter, der ikke er bundet af sådanne aftalevilkår, er informationssælgeren (-udvikleren) prisgivet. Ønsker man fortsat at bevare hans incitament til at udvikle ny information, må der sikres en retsbeskyttelse, der afskærer køberen eller tredjeparter fra at kopiere uden samtykke. Dette behov er det retspolitiske grundlag for den immaterialretlige beskyttelse.

"Besiddelse" af information

Som foran antydet kan digital information ikke "besiddes" på samme måde som information, der materialiseres i medier, som der er en fast tilknytning til. Hvis A via Internet afsender en tekstfil til B, vil denne handling medføre, at såvel A som B er i besiddelse af denne fil, når transmissionen er gennemført. Dermed forsvinder muligheden for at fremkalde retsvirkninger mod denne information, der bygger på besiddelseskrav. For at udøve sådanne retsvirkninger måtte det i givet fald kræves, at informationen var eksklusivt og uløseligt manifesteret i et medium (f.eks. et intelligent chipkort), som man herefter gør til genstand for besiddelse.

De særlige omstændigheder, hvorunder digital information "besiddes", giver navnlig vanskeligheder ved finansiering af digitale informationsprodukter. Disse vanskeligheder imødegås kun delvis af immaterialrettens regler. I de tilfælde, hvor informations-"ejeren" ikke kan gøre en immaterialretlig retsposition gældende, må man i praksis konstatere, at information ikke er egnet som finansieringsgrundlag. Med et slagord kan man sige, at

når information ikke kan ejes, kan den heller ikke sælges, stjæles eller finansieres.

Disse – og andre – indvendinger mod at anvende de almindelige regler om overdragelse og finansiering på information fejes ofte væk under henvisning til, at informationsprodukter jo i praksis omsættes og finansieres som andre retsgoder (bøger, fonogrammer etc.). Se f.eks. *Ellen-Katrine Thrap-Meyer* i Complex 5/89 og *Ellen-Katrine & Robin Thrap-Meyer* i Complex 1/90, s. 26 ff. Se ligeledes den indgående analyse hos *Kim Frost*: Informationsydelsen (2002), kapitel II. Ser man nærmere på de nævnte eksempler, kan den praktiserede omsætning imidlertid *enten* forklares med, at det praktiske retsliv – de facto eller de jure – har måttet prisgive en effektiv informationsbeskyttelse, således at overdragelsen hovedsagelig kommer til at knytte sig til mediet (det gælder således for fonogrammer, der ofte kopieres), *eller* med, at information og medium i disse tilfælde er praktisk uadskillelige (det gælder f.eks. for bøger, som de færreste orker at kopiere). Spørgsmålet drøftes nærmere i afsnit 12.1. og 20.2.

2.3. Systemteori

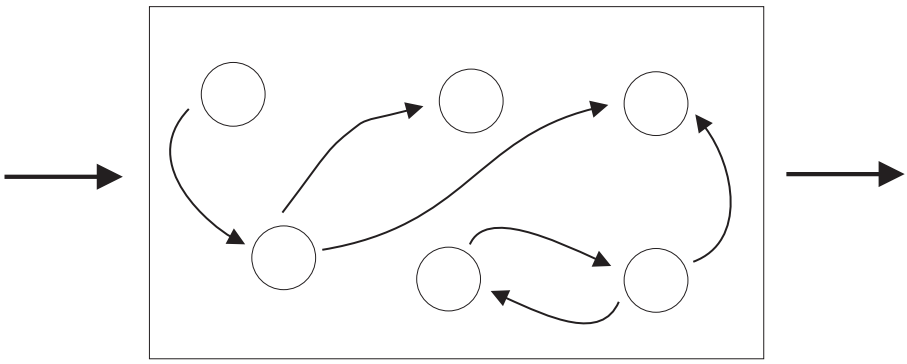
2.3.a. Generelt om systemteorien

Problemet

Skal informationsbegrebet være fællesnævner for alle de forskelligartede situationer, hvor IT kan anvendes, kan det være vanskeligt at fastholde overblikket. Derfor må der anlægges en synsvinkel, der kan opretholdes på tværs af fænomenernes faktiske og terminologiske fremtræden. En sådan tværgående metode findes i den såkaldte systemteori. Systemteorien er et metateoretisk tankeværktøj, der er udviklet af visse videnskabsteoretikere til at beskrive fænomener, der fremstår uhåndterligt eller med en usikker terminologi. Der er således tale om en *terminologi*, som er specielt velegnet til tværfaglige dialoger og om en *metode* til strukturering af fænomener.

Terminologi

Systembegreber indgår talrige steder i dagligsproget med identiske – omend ofte ubevidste – sproglige funktioner. Når vi kalder noget for "systemer", er det ofte, fordi vi mangler andre og bedre betegnelser. Vi ved, at der er en mekanisme, og at den virker på en bestemt måde. Vi kan også udpege de bestanddele og lovmæssigheder, der får den til at virke. Men selve mekanismen som sådan har vi svært ved at give navn. Tænk f.eks. på begrebets betydning i ord som immunsystem, politisk system, fordøjelsessystem og retssystem.



Det er almindeligt at skematisere systemtankegange i denne grafiske afbildning: Systemet er den firkantede kasse med de enkelte komponenter. Det træder i funktion, når det udsættes for en stimulus (pilen på venstre side) og ved hjælp af et sæt lovmæssigheder (de buede pile i kassen). Denne funktion (symboliseret ved pilen mod højre) udmønter sig herefter på systemets omgivelser, der igen kan give anledning til nye stimuli (ofte kaldet "feed back").

Begrebselementer

Som denne illustration viser kan ethvert system defineres ud fra følgende kriterier:

- afgrænselighed

Systemer er for det første fænomener, der kan adskilles fra noget andet. Fordøjelsessystemet er noget andet end respirationssystemet; det danske retssystem noget andet end det japanske. Kun når man kan lægge en sådan grænseflade mellem det, man vil beskrive systemteoretisk, og noget andet, er der plads for tankegangen.

- opdelelighed

For at noget skal kunne kaldes et system, må det for det andet kunne opdeles i bestanddele. I systemteorien taler man almindeligvis om, at systemer rummer komponenter eller elementer. Retssystemet består f.eks. af regelgivere, regel-adressater og håndhævende myndigheder. Fordøjelsessystemet bl.a. af tyggeorganer, spiserør, mavesæk og tarme. Systemer kan som regel opdeles i delsystemer. Et delsystem af retssystemet er domstolssystemet; et delsystem af fordøjelsessystemet er tarmsystemet. Også disse delsystemer kan opdeles i yderligere delsystemer og bestanddele – eventuelt ved at andre kriterier lægges til grund. For at bevare overblikket i en systembeskrivelse må man derfor anvende klare og stringente kriterier for afgrænsning og opdeling.

- lovmæssighed

Den tredje betingelse knytter sig til de lovmæssigheder, der gælder for systemets komponenter. Systemkomponenterne forudsættes at følge et mønster. I retssystemet fremgår disse lovmæssigheder af retsreglerne; for fordøjelsessystemet følger de af de fysiologiske og mikrobiologiske love, der gælder for vore organer og for de mikroorganismer, vi har i os. Kravet er så

centralt, at man kun meningsfuldt kan anlægge systembetragtninger for fænomener, der er genstand for lovmæssigheder. Også dette harmonerer med dagligdagens terminologi. En adfærd, der skifter, som vinden blæser, betegnes f.eks. som usystematisk. Kun når spilleren snyder, følger terningens udvisende et "system".

- funktion

Den fjerde egenskab – der sammenfatter de forudgående tre – indebærer, at man ved at kombinere betingelserne om adskillelse, inddeling og lovmæssigheder kan konstatere, at systemet udfører en *funktion*. Ofte er det netop funktionen, der giver systemet navn. Retssystemets funktion er at opfylde visse givne idealer om lighed, ressourcefordeling, konsekvens etc. og at skabe forudsigelighed om, hvorledes vore medmennesker vil reagere. Fordøjelsessystemets funktion består i at fordøje, dvs. omdanne føde til energi.

2.3.b. Anvendelse

System*terminologien* er velegnet som en slags "metaterminologi" til at understøtte en tværfaglig dialog mellem fagfolk, der ud fra forskellige forudsætninger befatter sig med disse aspekter. Dermed kan en person uden teknisk ekspertise stille de kvalificerede spørgsmål, der vil bibringe ham den nødvendige indsigt.

Eksempel 1

Den, der f.eks. vil vide mere om, hvad et "public key" krypteringssystem er, kan således spørge, hvilken *funktion* et sådant system tjener, og hvorledes denne funktion *adskiller* sig fra andre krypteringssystemer. Svaret herpå vil pege på *komponenterne* i et asymmetrisk krypteringssystem; den særlige anvendelse af flere nøgler samt sammenhængen mellem den ene og den anden nøgle. Et næste spørgsmål vil fokusere på brugen af nøglerne: Hvilke systemkomponenter materialiserer de sig i, og hvilke *regler* af teknisk og normativ karakter bestemmer deres anvendelse? Dette vil fokusere beskrivelsen på de forskellige måder, hvorpå et sådant system kan implementeres etc.

Eksempel 2

Et tekstbehandlingssystem rummer en række *komponenter* (f.eks. moduler til orddeling, stavekontrol, beregninger mv.) og hertil hørende *lovmæssigheder*, der i sidste ende sætter en slutbruger i stand til at opfylde disse respektive *funktioner* til indskrivning, revision, beregning, stavekontrol mv. Som helhed kan tekstbehandlingssystemet *afgrænses* over for f.eks. databasesystemet, regnearkssystemet etc.

Eksempel 3

Styresystemets *funktion* er at styre andre dele af IT-systemet, f.eks. tekstbehandlingssystemet. Styresystemet *afgrænses* dels i

relation til en mængde hardware (i PC-sammenhænge f.eks. maskinens "bus"), dels i relation til de brugersystemer, der forudsættes afviklet under det pågældende styresystem. Dets *komponenter* findes dels i maskinens hardware (BIOS), dels i den del af systemet, der indlæses fra disk. De *lovmæssigheder*, der ligger til grund for styresystemets funktioner mv., er nedfældet i dets programkode.

2.3.c. Juridiske aspekter

System*teorien* tjener primært som terminologisk grundlag og til at skabe overblik for en juridisk analyse. Som de netop skitserede eksempler viser, kan man med system*terminologi* anvende ensartede begreber på fænomener, der ikke "definerer sig selv". For den juridiske forfatter giver dette mulighed for at tale abstrakt (altså uden at referere til konkrete systemtyper mv.) og alligevel præcist (idet man gennem tjenlige systemafgrænsninger kan referere til den relevante tekniske problemkreds). For den praktiserende IT-jurist indebærer systemtænkningen, at man uden at kende en konkret teknisk terminologi kan stille kvalificerede spørgsmål og på grundlag heraf indhente yderligere viden.

Systembegrebet kan også afspejle konkrete juridiske problemstillinger.

I *ophavsretten* finder vi en kombination af kommunikations- og systemteoriernes grundlæggende tankegange i læren om ophavsretten til programudvikling. Ophavsmanden til et værk vil altid handle indenfor den systematiske ramme, der sættes af valget af sprog og medium, og de heraf flydende begrænsninger kan efter omstændighederne lægge så stærke bånd på hans udtryksmuligheder, at der ikke opnås nogen ophavsret til den færdige manifestation.

I *aftaleretten* har systemteorien først og fremmest betydning for forståelsen af, hvilke egenskaber ("funktioner") der skal hidføres ved en IT-installation. F.eks. har det stor betydning, om en IT-ydelse er defineret som en forpligtelse til at hidføre en funktion (i hvilket tilfælde udstyrets nærmere beskaffenhed har mindre betydning) eller som en række nærmere angivne komponenter mv. Se hertil *E&A* s. 363 ff., *PA* s. 210 ff. og nedenfor i kapitel 21.

Endelig er systemteoretiske analyser velegnede til at understøtte det retsskabende arbejde med at formulere IT-retlige regelsæt. Dette har f.eks. betydning, når man skal planlægge systemer, f.eks. til aftale- eller bevishåndtering. I talrige tilfælde må et bevis føres som systembevis, jf. nærmere nedenfor i afsnit 4.3.d.,

hvorved der fokuseres på de sandsynlige kausalfølger inden for rammerne af det pågældende system.

Supplerende litteratur

Den *matematiske kommunikationsteori* er bedst og klarest præsenteret af dens egne ophavsmænd (*Claude Shannon & Warren Weaver*) i 1949-optrykket af deres oprindelige afhandling: "Recent contributions to the mathematical theory on communication" (University of Illinois Press, Urbane, Ill.). Teorien er uddybet i talrige sammenhænge, jf. henvisningerne i *E&A*, s. 268, hvoraf navnlig fremhæves *Fred I. Dretske*: Knowledge and the flow of information (Oxford, 1981). Herudover kan henvises til *Arno Penzia*: Ideas and information (New York, 1989). I IT-juridisk litteratur er teorien bl.a. introduceret af *Jon Bing m.fl.* i Complex 12/1987 og i *E&A* s. 265 ff., hvor grundlaget for den her præsenterede version af teorien er lagt. Den har siden været anvendt i forskellige – andre – retsvidenskabelige sammenhænge, herunder af *Jesper Lau Hansen*: Informationsmisbrug (2001), s. 5 ff og af *Kim Frost*: Informationsydelsen (2002).

Studier af *systemteorien* vanskeliggøres af, at denne teori optræder i vidt forskellige faglige sammenhænge, såvel i juraen, indenfor andre tekniske og samfundsvidenskabelige fagområder som i videnskabsteorien. For en nærmere indføring i dette område henvises til *E&A*, s. 248 ff. En juridisk indføring til systemteorien findes hos *Eckhoff & Sundby*: Rettssystemer (1982). IT-tekniske indføringer i problemet finder man i hele litteraturen omkring IT-systemanalyse.

Kapitel 3. PRAKTISK IT

3.1. IT-systemets funktioner og komponenter

3.1.a. Funktioner

Beregninger

Dens øvrige kvaliteter ufortalt kommer menneskets hjerne til kort i relation til præcis og hurtig behandling af omfattende datamængder. De fleste trættes ved arbejdet med at addere lange talrækker, uanset hvor simpel den enkelte addition er. Udover det psykiske ubehag ved den slags tankeaktivitet opnår man hyppigt upræcise og dermed uanvendelige resultater. På dette punkt vinder den elektroniske computer ved sin hurtige og pålidelige funktionalitet. En af de første – og helt åbenbare – anvendelser for elektroniske computere er til komplicerede beregninger; en anvendelsesform, der – som vi så det i den historiske gennemgang – netop var formålet med udviklingen af de første computere.

Matematik

I et historisk perspektiv har IT på et tidligt tidspunkt været anvendt til matematisk problemløsning. I tekniske miljøer er dette f.eks. sket i forbindelse med teknisk konstruktion og byggeri (statik-systemer). Og i administrative miljøer som beregningsfunktioner integreret med tekstbehandlings- og konteringsfunktioner. En anden matematisk opgave af stor vigtighed har haft at gøre med *kryptering* og navnlig *dekryptering* (afkodning). Historisk var det den efterretningsmæssige opgave med at afkode fjentlig kommunikation – såvel under anden verdenskrig som under den kolde krig – der lå bag den intensive forskning i udvikling af ny computerteknologi. I fredstid indgår matematiske krypteringsfunktioner også til varetagelse af sikkerhedsmæssige formål (hemmeligholdelse af erhvervshemmeligheder og afgivelse af digital signatur).

ERP

At administrere en virksomhed (erhvervsmæssig eller af anden art) kræver nøje styring af den information, der ligger til grund for virksomhedens aktiviteter. Der er brug for koordinering af arbejdsopgaver, planlægning af økonomiske dispositioner, registrering af økonomiske transaktioner, udskrivning af breve, betaling af beløb etc. Til at styre disse kommunikative processer er der et evident anvendelsesområde for IT. Tidligere talte

man om administrativ databehandling, men den moderne betegnelse for sådanne systemer er ERP, Enterprise Resource Planning.

Simulation

Ved at føde et IT-system med data om, hvorledes et komplekst, skrøbeligt eller utilnærmeligt fænomen fungerer, kan man undersøge det uden risiko for skade eller tab. Dette udnyttes bl.a. til indlæringsprocesser som f.eks. uddannelse (pilottræning på flysimulatorer) eller som led i forskning (simulation af sammensætningen af en kemisk substans). Med IT kan man beregne forskelligartede stimulus/respons-sammenhænge hurtigt og uden materialeforbrug mv.

Visse IT-simulationer tager udgangspunkt i fysikkens love (som f.eks. organisk analyse); andre simulerer menneskeskabte situationer (f.eks. beslutningsstøttesystemer mv.). Endnu andre knytter an til teoretiske – f.eks. økonomiske – hypoteser. Det økonomiske Sekretariat under Økonomiministeriet anvender et IT-baseret beregningssystem, kaldet "lovmodellen", der til brug for den politiske beslutningsproces siges at kunne give hurtige, pålidelige og dækkende talmæssige oplysninger om konsekvenserne af at gøre brug af forskellige virkemidler i den økonomiske politik.

IT-simulationer rummer ingen garanti for, at virkeligheden vil opføre sig på samme måde som systemet. Tværtimod er der talrige – og tragiske – eksempler på, at man er nået til forskellige resultater gennem simulation og realanvendelse af forskellige løsninger. Problemet behandles nærmere i kapitel 18 i forbindelse med erstatningsansvaret.

Grafik

Grafisk databehandling er i dag en integreret del af al moderne IT-anvendelse. Hvad enten formålet er administrativ databehandling eller underholdning, indgår grafiske figurer i form af faste og levende billeder i enhver moderne IT-grænseflade og med en opløsning (præcision), som ofte langt overgår TV-billedet. Traditionelt er grafisk databehandling udviklet med sigte på helt andre formål. Ved at kombinere grafisk simulation og beregning mv. kan konstruktion og byggeri effektiviseres på væsentlige punkter. Det slidsomme arbejde med rentegning af konstruktionstegninger mv. er i dag stort set erstattet af computere, navnlig i systemer til såkaldt CAD/CAM = Computer Aided Design/Computer Aided Manufactoring. Herudover anvendes grafisk IT til fremstilling af trykte udgivelser. Gennem såkaldt desk-top publishing (direkte oversat: skrivebordstrykning, ofte fordansket: datatryk), der involverer brug af en PC eller en workstation med tilhørende laserprinter, kan man fremstille professionelt udseende dokumenter uden brug af kostbare fagspecialister som typografer og litogra-

fer. Udover de beskæftigelsesproblemer, teknologien implicerer for den branche, der beskæftiger sig med typografi og lay out, rummer teknikken et oplagt redskab for forfalskning af f.eks. offentlige dokumenter og bevismidler.

Videns-modellering

Systemer, der effektiviserer vor måde at tænke på, kender man strengt taget allerede fra og med antikkens kuglerammer. Med IT-udviklingen er der opstået et stort forskningsområde indenfor avanceret vidensmodellering. Forskningsfeltet fremkom i slutningen af 1950-erne, da edb-teknologiens strengt matematiske grænseflade blev fortrængt. I 1964-66 konstruerede MIT-professoren *Joseph Weizenbaum* – efter eget udsagn (jf. bogen Computer Power and Human Reason, 1976) som en provokation – en "elektronisk psykiater", som indgik i en dialog med brugeren, hvor brugerens meddelelser til systemet om sine problemer reflekteredes i systemets gensvar. Sådanne systemer kan også anvendes i den offentlige forvaltning. Således har Toldvæsenet taget et videnbaseret system – det såkaldte Escort-system – i brug til udgående stikprøvekontrol af regnskaber. Udover de budget- og personalemæssige aspekter i denne debat står diskussionen om, hvorvidt – og navnlig hvordan – man kan og vil leve med den ene eller anden type fejl. Ingen i debatten vil hævde, at hverken systemer eller personer er fejlfri.

Problematikkens forvaltningsretlige sider er behandlet af *Jon Bing* i NAT 1986.9 ff. En case-study vedrørende implementering af ekspertsystemer i norsk forvaltning findes med *Dag Wiese Schartum*: En rettslig undersøkelse av tre edb-systemer i offentlig forvaltning. CompLex 1/89. Se ligeledes *Conny Johanesson* i NAT 1990.153 ff.

3.1.b. Processoren

Databehandling består af serier af processer, der på det mest basale, numeriske, plan involverer *sammenligning* af data (hvorved der knyttes værdier til data), *flytning* af data (f.eks. kopiering fra én hukommelsesenhed til en anden) og *additioner*, der matematisk kan udtrykke alle fire regnearter. De pågældende processer finder sted på data, der repræsenteres som nuller og ét-taller. Disse funktioner udgør selve databehandlingen og styres af edb-programmer, der på forhånd slår fast, hvilke processer der skal udføres, hvornår, med hvilket indhold og under hvilke omstændigheder.

Terminologi

Digitale beregningsfunktioner foregår i *beregningsenheder*, der nu om dage er bygget ind i sådanne halvlederchips, der betegnes *processorer* eller *mikroprocessorer*. Der findes andre halvle-

derchips end disse, f.eks. til lagring af data (såkaldte RAM-chips). Terminologien omkring selve beregningsenheden har ændret sig gennem teknologiens udviklingsforløb. I tidligere terminologi talte man om "computere", af det engelske ord "to compute", at "beregne". Men fordi selve beregningsenheden ofte fortoner sig mellem andre komponenter i det system, brugeren anvender, er "computer"-terminologien i dag mindre hyppigt anvendt. Man taler oftest om "computer" for at betegne en større indretning, der udelukkende benyttes til bestemte databehandlingsformål, f.eks. til udførelse af omfattende beregningsopgaver. Den enhed, hvori den centrale mikroprocessor er placeret, omtales ofte som CPU (CPU = Central Processing Unit). Ved siden af denne kan systemet indeholde talrige decentrale mikroprocessorer, f.eks. til styring af skærm eller kommunikation.

Clock-frekvens

Som hermed antydet er processoren (eller processorerne) hjertet i ethvert databehandlingssystem. Det er her, alle programinstruktioner udføres i form af rækker af hver for sig simple instruktioner med de to talværdier 0 og 1. Processorens beregninger foretages i takt med en såkaldt klokke, der ved hjælp af et lille krystal "tikker" med en fast frekvens. Denne tikken frembringer en impuls med to tilstande, 0 og 1, eller i maskinens "sprog" høj henholdsvis lav spænding. For hvert trin i denne langstrakte proces (som dog ikke opleves som sådan pga. den ekstreme hurtighed, hvormed den udføres) afvikler processoren den enkelte operation, der hentes fra et register, hvortil processoren afleverer dataene igen, når beregningen er afsluttet. Hver clock-cyklus gennemfører således en enkelt simpel operation af typen "læg indholdet af register 1 sammen med indholdet af register 2". Den hurtighed, hvormed brugeren oplever processorens funktion, er dog ikke alene en funktion af denne clock-frekvens, men også af den måde, hvorpå dataene præsenteres for processorens enkelte beregninger: Jo enklere og logiske instruktioner, processoren udsættes for, desto hurtigere vil brugeren opleve, at systemet arbejder.

I en moderne PC måles clock-frekvensen i milliarder pr. sekund (gigahertz), f.eks. 6 gigahertz. Et andet mål for denne egenskab er antallet af beregninger pr. sekund. Denne egenskab måles ofte i MIPS = Million Instructions Per Second. En PC med en 100 megahertz processor har måske en gennemsnitlig udførelseshastighed på ca. 10 MIPS. Til sammenligning formår de nyeste supercomputere at arbejde med så høje kapaciteter, at man taler om Megaflops: Millions Floating Point Instructions Per Second.

Andre forhold

Blandt de andre faktorer, der kan influere på computerens hastighed, spiller det en rolle, hvor mange bits de enkelte instruktioner består af – en faktor, der bestemmes af *styresystemet*. Jo flere bits, der kan indgå i den enkelte beregning, desto mere kompliceret kan denne beregning være. Systemets hastighed beror dernæst på, hvordan de data, der indgår i eller udvirkes ved beregningen, håndteres. Forskellige former for system-arkitektur har flyttet systemets flaskehalse mellem de forskellige komponenter. I den tidlige stand alone PC-arkitektur var flaskehalsen RAM-hukommelsen og processorhastigheden. Med fremkomsten af den netbaserede PC er det i stigende grad blevet teleforbindelserne, der med deres begrænsede båndbredde er blevet flaskehalse.

Processorens kapacitet kan bl.a. få retlig betydning som kvalitetskrav for et IT-system, der overdrages ved aftale, eftersom kapaciteten udmønter sig i systemets svartider, men også andre forhold kan spille en rolle. Ved opdatering af et kundekartotek er flaskehalsen *lagermedierne*. Her spiller det ind, hvor hurtigt lagerenhederne arbejder, se herom straks nedenfor.

Chip-kort

Processorteknologi anvendes ikke kun i større IT-systemer. I den helt lave ende af prisskalaen anvendes mikroprocessorer som grundlag for såkaldt "intelligente" betalingskort mv., dvs. kort, der ikke blot lagrer data, men som også er i stand til at foretage forandringer i, eller ligefrem gennemføre beregninger på, disse data. Der findes to former for chip-kort; et hukommelseskort, der kun kan oplades med værdi én gang, og som derefter løbende kan holde rede på forbruget af denne værdi, og et processorkort, som kan genoplades, og som dernæst kan forsynes med andre funktioner (f.eks. digital signatur el.lign.). Princippet i moderne mobiltelefoni er, at den enkelte abonnent identificerer sig ved hjælp af et såkaldt SIM-kort (SIM = Subscriber Identity Module), der placeres i terminalen (dvs. mobiltelefonen), hvorefter denne aktiveres. Det *borgerkort*-projekt, som blev fremlagt i 1994, men som – indtil videre – blev lagt på hylden i 1996, var ligeledes baseret på et mikroprocessor-baseret kort.

3.1.c. Lagerenheder

Fordi en processor altid vil skulle modtage og afgive sine data i digital form, er det nødvendigt at disse data er til stede og parate i denne form straks før og efter beregningsprocessen igangsættes. For de fleste praktiske formål nødvendiggør dette tilstedeværelsen af et eller flere datalagre, der kan operere i tilknytning til processoren.

RAM-lageret

Systemets *interne lager* vil typisk være baseret på en halvlederchip. I denne halvlederchip vil der være en række lagerceller, der fungerer som *adresser* for givne datamængder. Hver celle er igen underinddelt i pladser, som hver kan opbevare en bit. Lagercellerne nummereres fra 0 og op til en øvre grænse, der bestemmes af konstruktionen. I de første PC'er var den del af lageret, der står til rådighed for brugeren, på 640 kilo-bytes (svarende til 655.360 tegn). Denne øvre grænse var en af grundene til, at IBM i midten af 1980'erne og Microsoft i midten af 1990'erne udsendte helt nye styresystemer (IBM's OS/2 og Microsofts Windows 95). Det interne datalager betegnes som RAM – en forkortelse for Random Access Memory. "Random" (vilkårlig) indicerer, at tilgangen til en tilfældigt udvalgt dataplads forløber uafhængigt af, hvornår eller hvor sidste tilgang til lageret fandt sted. Skal man sammenligne med hjernens tilsvarende data-adresseringer, svarer de telefonnumre, man kan huske i hovedet, til RAM, modsat dem, man skal slå op i en telefonbog. I princippet skal man læse forfra i telefonbogen, indtil man finder det telefonnummer, man søger.

ROM-lagre

I tilknytning til RAM-lageret er computeren udstyret med visse specielle lagre, der kun kan lagre informationer én gang. Disse lagre betegnes som ROM (Read Only Memory, dvs. "kun læse"-lager). ROM anvendes typisk til lagring af computerens styresystem, jf. herom nedenfor. ROM-lagre er permanente og mister altså ikke deres data, når strømmen afbrydes. Visse halvlederchips er dog indrettet således, at man kan ændre ROM-lagre ved at "brænde" informationer i form af programmer eller data ind i halvlederproduktet. I praksis er det derfor kun fagfolk, der kan lagre informationer i sådanne PROM's og EPROM's (Programmable ROM, hhv. Erasable and Programmable ROM).

Magnetiske medier

Den mest effektive lagring af mange data sker i dag på magnetiske medier, f.eks. disketter, magnetstriber på betalingskort, harddisks og USB-enheder af forskellig slag. Se nærmere herom s. 88 f. En magnetisk lagerenhed må være klargjort til data i det pågældende format. Denne klargøring betegnes som *formatering*. Ved formateringen sker der en magnetisk opdeling af lagermediet i en række koncentriske spor, der kan minde om rillen på en grammofonplade. Ved formateringen indlæses der ikke noget program på disken, og formateringen rummer derfor ikke i sig selv ophavsretlige problemer. De magnetiske spor kan herved bedst sammenlignes med de fortrykte linier på et stykke papir. Først, når der skrives på linierne, fremtræder de egentlige instruktioner. I modsætning til grammofonpladen har en diskette flere koncentriske spor (en LP-plade har som bekendt kun én rille

pr. side). Da et spor kan indeholde flere tusinde bytes, opdeles det af praktiske grunde i sektorer, der fremtræder som stykker af en lagkage. Filer lagres og genfindes via et index (i PC-sprogbrug kaldet *directory*). Når en fil slettes, markeres dette blot i indexet. De magnetiske impulser bliver derimod liggende, indtil de overskrives af nye data på samme måde som en båndoptagelse overspilles på en anden. Dette forhold har stor betydning, bl.a. for afgørelsen af, om der består et "register", for beskyttelsen af data som erhvervshemmeligheder og for, om der foreligger et ophavsretligt eksemplar.

WORM-medier

Magnetiske datamedier rummer den fordel, at de indlagrede data senere kan ændres. Dermed kan dette medium ikke blot lagre de programmer, der indlæses i færdig form, men også brugerens redigeringer heri samt egne data. Til forskel herfra kan de fleste optiske medier alene anvendes til lagring én gang (WORM – Write Once, Read Many). Sådanne medier kan til gengæld benyttes til opbevaring af langt større mængder af data på fysisk samme plads og egner sig derfor til omfattende databaser, som brugeren ikke forudsættes at skulle ændre. Gennem de seneste år er der dog også fremkommet en række optiske medier, der fungerer i R/W-mode ("read/write").

CD-teknologi

Med det stigende behov for at behandle omfattende mængder af data i nutidens IT-systemer, er der opstået et stort behov for billige medier til store datamængder. Frem mod slutningen af 1990'erne opfyldes dette behov ved brugen af *compact disc-teknologi*. Her er data lagret ved strukturer i et materiale, der herefter reflekterer en laserlysstråle. Når laserlysstrålen rammer skiven, reflekteres den på forskellig vis i overensstemmelse med de strukturer, der er lagt ned i den på forhånd. CD-teknologien fik sit første gennembrud på lydområdet, hvor mediet nu er trådt i stedet for vinyl-pladen ved distribution af fonogrammer. I løbet af 1990'erne er det også anvendt som grundlag for distribution af data, f.eks. i form af *CD-ROM* (Compact Disc Read Only Memory). Et eksempel herpå er de databaseprodukter, der gjorde deres indtog på det danske juridiske marked, se f.eks. om UfR på CD-ROM min præsentation i U1992B.385 ff.

Palmtops

I de seneste år er der set et støt stigende marked for håndholdte computere, der kan varetage de databehandlingsopgaver, det travle nutidsmenneske har i de daglige arbejdsrutiner, herunder notat-, kalender- og telefonbogsfunktion. Styrken ved disse såkaldte *palmtops* eller *PDAer* (Personal Digital Assistant) ligger i muligheden for at udveksle data fra og til den stationære maskine ved brug af infrarød dataoverførelse. I disse år er palmtop-com-

puteren ved at smelte sammen med andet elektronisk udstyr, der anvender infrarød teknologi og radiobølger, f.eks. fjernbetjeningsenheder og mobiltelefoni. Denne sammensmeltning understøttes bl.a. af den såkaldte *bluetooth-standard*, der fastslår, hvordan trådløse data, der transmitteres i luftrummet over korte afstande, skal struktureres.

Når computeren har behandlet en datamængde, må resultatet heraf – hvis det da skal have nogen funktion – nødvendigvis formidles til andre komponenter. Internt i systemet sker dette via en såkaldt *bus*. Bussen er en elektrisk forbindelse, der fungerer som systemets rygrad. Ligesom den menneskelige rygrad transmitterer nervesystemets informationer, virker en databus som hovedfærdselsåre for alle de data, der udveksles mellem systemets komponenter. Hver systemkomponent – f.eks. skærm, diskettestation, tastatur, skriveenhed og modem – er tilsluttet bussen, enten ved direkte opkobling eller ved en anordning, der er koblet op til bussen. For at bussen kan opfylde sin funktion som mellemled for kommunikationen mellem CPU og tilsluttede enheder, må den overholde krav om kompatibilitet. Bl.a. er det afgørende, hvor mange databits der kan transmitteres parallelt (f.eks. 8, 16 eller 32). Bussens standarder for kompatibilitet er afgørende for, hvilke tilslutningskort der kan tilsluttes computeren, og der findes i dag et stort sæt bus-standards.

Effektivitetsspørgsmål

Som nævnt etablerer databussen bl.a. forbindelse med systemets *eksterne* lagermedier. Disse medier kan betragtes som logiske udvidelser af det interne lager (RAM-lageret), fordi de fungerer på samme måde: Data kan lægges på mediet, uanset hvor på mediet der sidst har været lagret eller hentet data – man behøver altså ikke løbe hele mediet igennem for at lagre eller hente data på det. I praksis fremtræder de eksterne lagermedier dog anderledes end RAM-lageret. De er for det første langsommere, for det andet er de typisk billigere, og for det tredje bevarer de deres data, selv om strømmen afbrydes.

3.1.d. Indlæsning og udskrivning

Datafangst

Processoren udfolder sine funktioner i et samspil med andre enheder, der modtager og afgiver information, hvad enten denne information findes i forvejen på et lagermedium eller den bliver til under brugerens anvendelse, f.eks. i forbindelse med indtastninger mv. Begrebet datafangst betegner den situation, hvor et IT-system modtager data, hvad enten disse data hidrører fra et lagermedium f.eks. en diskettestation eller et modem, eller fra

indtastninger eller andre registreringer af forandringer i et ydre miljø. Allerede tilbage i 1960'erne ansås omkostningerne ved datafangst at repræsentere henimod halvdelen af de samlede omkostninger ved en databehandling. I erkendelse heraf er der gennem tiderne gjort en stor indsats for at finde billigere metoder til datafangst.

For hvert nyt princip for datafangst, som udviklingen har skabt, har teknologien åbnet sig for nye anvendelsesformer, en mekanisme, der senest har manifesteret sig med anvendelsen af Internet som medium for udveksling af data. I et system til styring af en automatisk produktionsproces vil en stregkodelæser egne sig bedre end et tastatur, medens det forholder sig omvendt i relation til f.eks. tekstbehandling. Den enhed, der konverterer den slags data til informationer, må blot være kompatibel med maskinen såvel som med datamaterialet. Gennem tiderne og i forskellige systemer har man betjent sig af vidt forskellige teknikker hertil.

Sådanne indlæsningsenheder kan i øvrigt anvendes til at genskabe en persons bevægelser, f.eks. bevægelser af kunstnerisk art. I forbindelse hermed kan der opstå særlige rettighedsspørgsmål: Kan en balletdanser f.eks. modsætte sig, at hans eller hendes fremførelse af et balletværk genskabes som en computer-genereret tegnefilmsanimation? Se herom i afsnit 9.2.a. om den ophavsretlige behandling af beskyttede præstationer, herunder såkaldt Visual Acting. Data i form af fuglesang, snorken eller nedbør kan med det rette udstyr omsættes til maskin-læsbare informationer og behandles derefter som sådanne i computeren, men gennem de seneste år er en række andre principper for datafangst kommet til, f.eks. systemer der ved hjælp af sensorer placeret på kroppen opfanger dennes bevægelser med henblik på undervisning (f.eks. i golfslag), forskning eller diagnostik. Som eksemplet viser – og som også anskueliggjort ved den udbredte anvendelse af bærbar teknologi – er computeren i stigende grad blevet "wearable".

Optiske medier

Visse indlæsningsenheder registrerer lysimpulser som data. I en scanner omsættes data fra en papirflade til digitale impulser, der som sådanne kan lagres, bearbejdes og udskrives påny. Princippet kendes f.eks. fra telefax-teknologien. Data i form af *stregkoder* – f.eks. på emballage – indlæses i elektroniske kasseapparater eller i lagerstyringssystemer. Indlæsningsenheden er her en lyspen. Endelig anvendes optisk datafangst i systemer, der registrerer faktiske fænomener f.eks. i en industriel produktionsproces. Som medium herfor anvendes fotoceller eller lysfølsomme dioder.

Magnetstribekort

Indlæsning af data i IT-systemer, der retter sig mod forbrugere mv. (f.eks. POS og ATM-terminaler), sker ofte ved hjælp af *magnetbærende kort* i "credit card"-format, som brugeren bærer på sig. Fordelen ved disse kort ligger i deres evne til entydigt at identificere kortindehaveren. Dette har bl.a. betydning ved elektroniske betalinger. For at undgå misbrug kan kortet dog kun aktiveres, hvis der samtidig indlæses en personlig identifikationskode. Udstedelse, opbevaring og anvendelse af PIN-koder giver anledning til vanskelige bevismæssige, sikkerhedsmæssige og erstatningsretlige spørgsmål.

Audiotex

I takt med, at telefoncentralerne er blevet digitaliserede og trykknaptelefonen udbredt som den typiske terminal, er der kommet et righoldigt udbud af såkaldte audiotex-tjenester (tast selvtjeneste). En audiotex-tjeneste er tilgængelig fra en trykknaptelefon med talsystemet og # og *-knapperne som kommandoer. Den modtager data fra telefonens taster og formidler sine data gennem digitaliseret tale – såkaldt voice response. Dermed udgør audiotex en slags hybrid mellem edb- og telefonteknologi. Audiotex-tjenester anvendes bl.a. til bestilling, booking og pengeoverførelser.

Mus

Hovedparten af nutidens grafiske brugergrænseflader anvender "point and click"-teknologi, hvor brugeren ved hjælp af en *mus* flytter cursoren rundt på skærmen og med et tast på musen "klikker" på de ikoner mv., der modsvarer hans instruktioner. Der foregår hermed en *interaktiv* dialog mellem system og bruger, hvor brugeren umiddelbart ser resultatet af sin datafangst på skærmen. Muse-teknologien har på den ene side sænket vidensbarrieren overfor megen IT, men har samtidig ført til en øget risiko for arbejdsmiljøbetingede "museskader", idet de hyppige, intense muskelbevægelser i håndleddet kan frembringe invaliderende lidelser hos brugeren, jf. *U 2005.1363 V*.

Dataskærmen

Det mest udbredte medium for læsning af information fra computere er dataskærmen. Det er denne komponent, der anvendes, når man surfer på www, forsøger at sætte sig ind i, hvorfor den avancerede kopimaskine ikke vil hæfte kopierne, eller læser en SMS-besked fra en mobiltelefon. Der findes to forskellige typer af skærme til *skrivebordsbrug* ("desk top").

- billedrør

*Billedrørs-skærmen*s princip der kendes fra TV. Skærmen fungerer ved, at stråler fra et katodestrålerør (en "elektron-kanon") brydes mod en fluorescerende overflade, enten i farve eller sort/hvid (mono-chrome). Da dette nødvendiggør en vis afstand mellem lys-kanon og skærm, er sådanne skærme store og uhandy. Dernæst nødvendiggør de et relativt stort strømforbrug. Som

en yderligere ulempe ved katodestråle-skærmen kan føjes risikoen ved dens elektromagnetiske udstråling.

- LCD

Med henblik på de pladskrav, man stiller til bærbare computere, har man udviklet en fladere skærmteknologi. Den såkaldte *LCD-skærm* (Liquid Crystal Display) danner billedet gennem flydende krystaller. Disse krystaller opbygges over en væske, der er indkapslet mellem to plader: den ene gennemsigtig, den anden af et reflekterende metal. Det er denne skærmteknologi, der anvendes i mobiltelefoner og i megen husholdningselektronik.

Forskellen mellem de to skærmtyper kan bl.a. have betydning for afgørelsen af, om et ophavsretligt beskyttet værk, der vises på skærmen, betragtes som et "eksemplar" af værket eller som en "visning" af det: Det ligger lettere for at tale om, at der foreligger et "eksemplar" af det viste billede, når skærmen bærer billedet i kraft af små lys-celler, end når billedet fremtræder i kraft af en lysstråle, der med stor hastighed bevæger sig ned over skærmens mange linjer.

Udprintning

Brugeren vil ofte have brug for, at systemets data er udskrevet på papir. Til dette brug anvendes en *printer*. De første printere byggede på bogtrykkerprincippet. Til hvert tegn hørte en spejlvendt trykflade i printeren. Tegnene var enten monteret på en type-arm af den slags, der kendes fra gammeldags skrivemaskiner, på et skrive-hoved eller på et skrivehjul (også kaldet "Daisy wheel"), og printeren skrev herefter tekst og billede tegn for tegn. Gennem 1960'erne anvendte man linjeskrivere, hvor typerne fremkom ved, at et printbælte kørte vandret forbi et antal hamre (80-150 stk.), der sad ud for bogstavernes plads på papiret. Når den rigtige type var ud for den rigtige hammer, slog hammeren på bæltet og frembragte tegnet. En linjeskriver kan skrive op til et par tusinde linjer pr. minut.

I 1970'erne fik vi (punkt-)matrix-printeren. Her påføres tekst eller grafik af et skrivehoved udstyret med et antal nåle, der ved at blive skudt frem og tilbage mod papiret danner de enkelte tegn. Under udskriften passerer dette skrivehoved herefter frem og tilbage over papiret. En udbygning af matrix-printeren findes i den såkaldte blæk-skriver (ofte betegnet som ink-jet printer). Her fremkommer skriften ved, at blækket skydes mod papiret i små dråber. I forhold til matrix-teknologien er denne printertype først og fremmest lydsvag. Siden slutningen af 1980'erne er laserprinteren blevet den almindelige printerteknologi. Hvor de hidtil omtalte printere frembringer tekst og grafik linie for linie, opererer laserprintere med hele udskriftssider. Informationen om sidens data genereres i en buffer, der bl.a. styres af programmer med information om skrifttyper mv., såkaldte fonte. Skriftbille-

det dannes af en laserstråle, der bevæger sig hen over en elektrostatisk opladet tromle.

Periferiudstyr

Indlæsnings- og udskrivningsenheder rubriceres ofte som "periferiudstyr". I en opfyldelsessituation giver disse enheder typisk anledning til færre installationsvanskeligheder end de maskin- og programkomponenter, hvori systemets funktionalitet defineres: Når periferiudstyret skal træde i funktion har selve databehandlingen fundet sted, og resultatet heraf vil – typisk – foreligge i en form, der følger den samme standard som udstyret.

Indretningsudstyr

Derudover suppleres et IT-system med udstyr som f.eks. ventilatorer, klimaanlæg, strømforsyningsanlæg samt visse rent kontormæssige indretninger. Selv om periferiudstyr typisk er mere komplekst end dette indretningsudstyr og dermed f.eks. giver anledning til andre kontraktsretlige typeforudsætninger mv., opfylder indretningsudstyret en række funktioner, der har afgørende betydning for databehandlingen. Fejl i strømforsyningen er ensbetydende med fejl i selve det medium, der bærer databehandlingen, og vil enten føre til afbrydelse af databehandlingsprocessen eller fejl heri. Uhensigtsmæssige klimaforhold kan f.eks. føre til statisk elektricitet med heraf følgende tilsvarende fejl eller føre til sammenbrud af computerens komponenter som følge af overophedning.

3.I.e. Telekommunikation

I takt med at den enkelte computer i stigende omfang modtager og afgiver data til andre computere, er der opstået et behov for effektiv understøttelse af denne eksterne kommunikation. Den kommunikation, en computer udfører med andre computere *inden for* en virksomhed, vil typisk foregå via et *lokalt netværk*, et såkaldt LAN (*Local Area Network*, sml. med *Wide Area Network*) Kommunikationen til computere *uden for* virksomheden kan *enten* foregå i et særligt konstrueret datanet (WAN, Wide Area Network), hvorved den enkelte bruger oplever disse eksterne computere som del af hans eget system (f.eks. en virksomheds "system" eller "intranet") *eller* ved at computeren kalder op til en ekstern computer, principielt på samme måde som man får en ekstern telefonabonnent i tale gennem et telefonopkald.

Sprog

Uanset hvilken kommunikationsform der er tale om, kan den enkelte computer kun udveksle data med andre computere, hvis disse data overføres og struktureres i overensstemmelse med et klart regelsæt, i kommunikationsteorien kaldet et *sprog*, se hertil afsnit 2.2.b. Inden for læren om telekommunikation foreligger

disse sprog i form af såkaldte *protokoller*, der foreligger i form af vedtagne *standarder* for udveksling af meddelelser samt anvendelse af digitalt udstyr hos sender og modtager.

Ved opbygningen af disse standarder anvendes almindeligvis en opdeling baseret på en referencemodel, "Open Systems Interconnection" (eller blot OSI-referencemodellen), der er vedtaget af ISO. Referencemodellen specificerer de kommunikative processer mellem forskellige IT-systemer i syv forskellige lag: anvendelseslaget, præsentationslaget, sessionslaget, transportlaget, netværkslaget, dataoverførelseslaget og det fysiske lag. OSI er oprindeligt udviklet af ISO, men siden varetaget i samarbejde med CCITT. Modellen anvendes som grundlag for udvikling af standarder inden for de forskellige lag, f.eks. til brug for elektronisk post (e-mail), EDI mv.

De fysiske lag

Medierne for denne kommunikation – de "fysiske lag" – kan være af vidt forskellig slags. Fra gammel tid er tele-infrastruktur (herhjemme såvel som i de fleste andre lande) opbygget på grundlag af en række fysiske netforbindelser bestående af kobber-kabler. Disse forbindelser udgør *rygraden* i vort telefonisystem. Gennem de seneste årtier er en række fiberoptiske kabler kommet til, ligesom infrastrukturen er blevet suppleret af et stort antal trådløse kommunikationsfaciliteter (satellit, GSM- og UTMS-telefoni mv.), ikke mindst for at kunne understøtte den stadigt stigende mobiltelefoni.

Brugeren af et kommunikationsnet vil typisk kun kende beskaffenheden af den del af nettet, hvorpå han tilslutter sit udstyr (det såkaldte net-terminalpunkt). Teleoperatørens valg af fysiske netforbindelser mellem to net-terminalpunkter vil afhænge af, hvilken kommunikationsvej der på transmissionstidspunktet er mest effektiv. Prisen for det udstyr, der er nødvendigt for at anvende disse forbindelser, bestemmes bl.a. af, hvilken grad af standardisering der anvendes på markedet.

I takt med denne udvikling er den klassiske telefoni i stigende grad smeltet sammen (*konvergeret*) med avancerede IT-funktioner. Her nævnes nogle af de mere vigtige:

GSM

GSM er en europæisk standard for digital mobiltelefoni, der er udviklet af ETSI. Forkortelsen stod oprindelig for Groupe Spéciale Mobile; men da man i takt med systemets udbredelse i resten af verden fandt den europæiske henvisning mindre adækvat, har man i nyere tid ladet forkortelsen referere til Général Système Mobile eller "Global System for Mobile (communication)". Udover at give abonnenten mulighed for uhindret at benytte sin mobiltelefon på tværs af landegrænserne, understøtter GSM-telefonien en række digitale tjenester, der fusionerer klassisk telefoni og IT, herunder overførelse af telefax og data, automatiserede

viderestillelsesfunktioner og andre funktioner, der nu også tilbydes af de "klassiske" telefonselskaber i det omfang, disse betjener sig af digitale centraler.

I løbet af de seneste år har GSM-teknologien udviklet sig til nye generationer af telefoni, herunder den senest udbudte UMTS-telefoni, der kan understøtte bredbåndstjenester (herunder transmission af levende billeder) til hastigheder op til 2 megabit/sekund.

ADSL

Også på området for telekommunikation via fastnet har der udviklet sig nye og kraftfulde teknikker til telekommunikation. Mest benyttet i dag er den såkaldte ADSL-teknologi, der understøtter overførelse af digital kommunikation med stor båndbredde via eksisterende kobberlinjer. Hastigheden på en ADSL-forbindelse afhænger af, om der sendes eller modtages data. ADSL-standarderne giver mulighed for at modtage mellem 1,5-9 mbit/s (såkaldt *downstream*), medens der kan overføres mellem 16 og 640 kbit/s (*upstream*). Computeren tilsluttes et særligt ADSL-modem, der i modsætning til tidligere telefon- og ISDN-modems ikke betjener sig af telefonnettet. ADSL-teknologiens store udbredelse skyldes bl.a., at kunden i modsætning til såvel telefoni som ISDN betaler et fast beløb for sin ADSL-opkobling, uanset brug. Dermed er det blevet muligt at modtage store informationsmængder (herunder levende billeder), samtidig med at computeren er tilsluttet nettet døgnet rundt.

EDI og e-handel

Med den moderne infrastruktur til telekommunikation benytter forretningslivet i stigende omfang elektronisk kommunikation. Denne elektroniske handel (eller e-handel) har såvel udviklet sig i forholdet mellem de handlende (*business-to-business*) som over for forbrugere (*business-to-consumer*). Man taler undertiden, men stadig sjældnere, om EDI (*Electronic Data Interchange*) som betegnelse for den *automatiserede* e-handel, der sker i forholdet mellem handlende på grundlag af formater, der er fastsat i forvejen ved aftale med de pågældende. Gennem et automatiseret EDI-system kan man f.eks. nøjes med at føde systemet med data én gang, hvorefter den videre ekspedition (fra ordre, via produktion og til den endelige fakturering) sker uden menneskelig indblanding. En international standard herfor, kaldet EDIFACT, er under opbygning i regi af FN under CEFACT (Centre for Facilitation of Procedures and Practices for Administration, Commerce and Transport). EDIFACT-standarden har til formål at skabe en fælles reference i måden at kommunikere på, virksomhederne imellem, imellem virksomhederne og det offentlige, og indbyrdes imellem de offentlige administrationer.

3.2. Programmering

3.2.a. Programbegrebet

Den tekniske ramme

Edb-programmer kendetegnes ved at kontrollere forløb i edb-systemer, dvs. systemer der har til formål at behandle data eller information, og som baseres på en dertil rettet teknisk indretning – en såkaldt processor. Hjertet i ethvert IT-system er netop denne processor. Det er mod dennes instruktionssæt (processorens "sprog"), programmets instruktioner retter sig, og som sætter processoren i stand til at udføre den pågældende funktion.

Alt efter det anvendte programmeringssprog har instruktionerne form af programkommandoer af typen "go to", "next", "if ... then". For at disse instruktioner skal kunne eksekveres i en computer (og kommunikationsprocessen lykkes), må de overholde reglerne i et særligt formalsprog – et programmeringssprog. Talrige andre maskiner og indretninger virker dermed i overensstemmelse med brugerens instruktioner: En bil kan tage sin fører til et hvilket som helst sted, hvor der er vejforbindelse. Men hvor instruktioner af denne karakter tilføjes udefra, evner IT-systemer at rumme en omfattende instruktionsmængde *i sig*. I denne henseende er computeren kun i familie med et fåtal af andre indretninger: En vaskemaskine kan vaske tøjet på grundlag af forskellige vaskeprogrammer og en symaskine kan sy forskellige typer af sting efter et på forhånd fastsat program. Men ser man bort fra disse eksempler var der – inden computerens indtog – ikke mange andre programmerbare indretninger.

Teknisk terminologi

Der findes mange definitioner af, hvad et edb-program er, og de kan efter omstændighederne have betydning for forståelsen af lovbestemmelser, der henviser til programbegrebet.

Se f.eks. *Troels Andreasen m.fl.* IT-lex – det store informatik-leksikon, 2. udg. (2001), s. 501: "Et fuldstændigt kompleks af sætninger, udformet i overensstemmelse med den gældende syntaks for det anvendte programmeringssprog, med det formål at få en datamat til at udføre en på forhånd fastlagt, afrundet opgave" og forarbejderne til 1989-ændringen af ophavsretsloven (FT 1988-89, till. A, sp. 3210): "en række instruktioner eller oplysninger, fikseret i en hvilken som helst form eller på et hvilket som helst medium, som tilsigter direkte eller indirekte at bringe en datamat til at angive, udføre eller opnå en bestemt funktion, opgave eller et bestemt resultat".

Sprogligt udspring

I sin sproglige form er ordet sammensat af de græske ord "pro", der betyder forud, og "grafein", der betyder at skrive. I daglig tale anvendes det om enhver systematiseret regel, der bestemmer et

forløb. Ord som politiske programmer, motionsprogrammer og teaterprogrammer angiver således, hvorledes politiske handlingsstrategier, motionsforløb eller teaterforestillinger intenderes udført. En del tekniske indretninger besidder samme egenskab (og anvender derfor også i stigende grad edb-styring). Et edb-program er for en computer, hvad et vaskeprogram er for en vaskemaskine. Det sørger for, at der bliver ind- og udlæst tal på en måde, der fører til et brugbart resultat for brugeren, ganske som vaskeprogrammet sørger for, at der kommer sæbe og vand ind og ud på de rigtige tidspunkter af vaskeprocessen.

Definition

Vi kan herefter definere et edb-program som *en serie instruktioner ("koder"), der er affattet efter forskrifterne i et formalsprog med henblik på afvikling i en processor, og som under forudsætning af et korrekt samspil mellem processoren, andre maskinelle enheder og andre programmer sætter processoren i stand til at behandle data af en given karakter.*

Mediet

Efter definitionen er det underordnet, på hvilket *medium* edb-programmer lagres, samt i hvilket nærmere *format* de fremtræder. Er programmet skrevet på papir med henblik på senere at blive "kodet", er papir-udgaven også et program. Derimod falder det forberedende *designmateriale* (f.eks. flowcharts og dataflow-diagrammer), der skrives under planlægningen af et edb-program, uden for begrebet. At art. 1, stk. 1, 2. pkt., i Rådsdirektivet om retlig beskyttelse af edb-programmer lader udtrykket "edb-program" omfatte også "forberedende designmateriale hertil" skyldes ønsket om at udvide den retlige beskyttelse af et program mod plagieringer, jf. herom i afsnit 7.2.b. Derimod er det ikke afgørende, om instruktionerne fremtræder som kildetekst eller objektkode. En halvlederchip, der gennem såkaldt mikrokodning har et sæt programinstruktioner manifesteret i sig, er i sig selv medium for det program, som disse instruktioner rummer. Som nævnt i afsnit 3.2.e. anvendes betegnelsen "firmware" undertiden herfor.

Dette spørgsmål blev på et meget tidligt tidspunkt afklaret i amerikansk ophavsretlig praksis. Se herom *Tandy Corporation v. Personal Micro Computers, Inc.*, 524 F.Supp. 171 (1979) om et program lagret på en halvlederchip (der omgør afgørelsen i *Data Cash Systems, Inc. v. JS&A Group, Inc.*, 480 F.Supp. 1063 (1979)), og den ledende afgørelse i *Apple Computer, Inc. v. Franklin Computer Corp.*, 545 F.Supp. 812 (1982), 714 F.2d 1240 (1983). Spørgsmålet om forberedende designmateriale med rimelighed kan anses for omfattet af programbegrebet, drøftes i øvrigt af *Thomas Riis* (2002), s. 20 f.

Det er allerede nævnt ovenfor, at IT-systemets funktioner ikke kun skyldes programmerne. Systemets hardware bestemmer f.eks., hvor hurtigt de elektriske signaler kan forløbe, uden at der derfor er tale om instruktioner skrevet i et sprog. Det er heller ikke enhver "instruktion", der er en programinstruktion. Ved formatering af et lagermedium udføres der vel en kommunikativ funktion, der bestemmer rammerne for den fremtidige informationshåndtering, men selve formateringen retter sig ikke mod systemets processor.

Afledte begreber

Fra programbegrebet kan man mere eller mindre klart udskille en række nabo-begreber. Betegnelsen *software* anvendes ofte om totaliteten af kommunikative aspekter af et IT-system, altså foruden selve programmængden *skærmtekster*, *dokumentation* mv. samt *data* – enten i ustruktureret form eller som større systematiserede samlinger (såkaldte *databaser*). Betegnelsen *kode* fremhæver navnlig programmets instruktionskarakter. Ordet *programmel* er blot en ubestemt form for programdelen, ligesom *maskinel* er en ubestemt betegnelse for maskindelen. Det er derfor ikke sprogligt korrekt – som det ofte ses – at tale om "ét" programmel.

3.2.b. De tekniske rammer

Omfanget af et edb-program veksler helt efter dets nærmere formål og karakter. Udviklingen af teknologien for lagermedier har betydet, at programmerne er kommet til at fylde mere og mere. Det har bidraget til denne udvikling, at man i stigende grad indbygger pladskrævende information i form af grafiske billeder, stereolyd og undertiden også levende billeder i applikationerne.
En processor kan ikke tænke. Den kan kun reagere på instruktioner, der kan omskrives til ét-taller og nuller. Det lægger nogle tekniske rammer for, hvordan man kan "tale med" og dermed programmere en computer. Signalerne skal under alle omstændigheder angives i talform. Fra leverandørens side er processoren bygget til at kunne modtage et givet sæt af sådanne instruktioner. Dette ordresæt udgør processorens såkaldte *maskinsprog*. Maskinsprog er populært sagt nuller og et-taller, der umiddelbart kan konverteres til elektromagnetiske impulser.

Lavniveau-sprog

At programmere i et maskinsprog stiller store krav til programmøren. I et program af en vis størrelse vil han hurtigt miste overblikket. Instruktionerne må nøje afpasses maskinfabrikatet, da hver computer (processor) taler sit maskinsprog. Dernæst er den, der programmerer i maskinsprog, nødt til at foretage en

række trivielle gentagelser af enkelte kommandoer. Maskinprogrammering er derfor forbundet med en betydelig fejlrisiko. Samme egenskaber præger de såkaldte *assembler-sprog*, også kaldet "symbolske maskinsprog". Assembler-sprog rummer samme ordrer som maskinsprog, men lader dem fremtræde som mnemo-tekniske kommandoer, f.eks. "add" for addér og "sto" for gem. Programmering i maskin- og assembler-sprog anvendes primært til funktioner, der skal udføres hyppigt, og hvor der derfor spares megen tid og/eller lagerkapacitet ved at optimere databehandlingsforløbet.

Højniveau-sprog

I teknologiens barndom foregik al programmering i maskin- eller assemblersprog. Dette var en teknisk nødvendighed, primært fordi man med den daværende hardwareteknologi måtte spare på processor-ressourcerne. Med maskinprogrammer kunne den forhåndenværende processorkraft udnyttes effektivt. Da hardwareteknologien blev stærkere og billigere, opstod behovet for de *højniveau-sprog*, der er omtalt i den historiske gennemgang, f.eks. "ADA", "C", "BASIC", "Pascal", "APL", "PROLOG" og "PL I". Med sådanne sprog kan programmøren skrive sine instruktioner i noget, der ligger tættere på hans naturlige sprog (i praksis engelsk), og dermed bevare et mere sikkert overblik over sin programmering.

3.2.c. Kilde- og objektkode

Begreberne

Når et program skrives i et højniveau-sprog, findes det altid i to udgaver: I en menneske-læsbar udgave, der fremtræder med de førnævnte engelske instruktioner i en slags telegram-stil. Og i en maskin-læsbar udgave, der er oversat til maskinsprog, og som – hvis man forsøger at læse den fra det maskin-læsbare medium, hvorpå den er lagret – fremtræder som en usystematisk række af tilsyneladende tilfældige tegn. I sin menneske-læsbare fremtrædelse betegnes programmet som kildekode. Ofte bruges i stedet ordet "kildetekst" eller "source", da der er tale om noget, der fremstår som skreven tekst. I sin oversatte tilstand betegnes programmet som objektkode eller maskinkode.

Oversættelse

Oversættelsen fra kildetekst til objektkode foregår ved hjælp af et program, der kaldes en "oversætter", og som er beregnet til det pågældende programmeringssprog. Danske programmører har været dygtige til at udvikle programoversættere til nogle af tidens førende højniveau-sprog, f.eks. C++ (*Bjarne Stroustrup*) og Turbo Pascal (*Anders Hejlsberg*). Oversættelsen initieres fra en kommando i oversætterprogrammet (som regel "compile" el-

ler "c"). Når denne kommando er gennemført, foreligger et eksekverbart edb-program, som (i denne udformning) til gengæld er praktisk taget umuligt at forstå for mennesker. En (oversat) objektkode ækvivalerer helt med den kildetekst, hvorpå oversættelsen bygger. Der frembringes intet nyt i den proces, der realiserer oversættelsen, ganske som der intet nyt tilføjes ved oversættelsen af ordene "luk venligst døren op" til "please open the door". Det er imidlertid væsentligt at pege på, at man ikke uden videre kan "oversætte tilbage" fra kildetekst til objektkode. Ligeså let det er at sende kødet gennem kødhakkemaskinen og frembringe hakket kød, lige vanskeligt er det at gøre det modsatte.

Hvis ikke man har rådighed over kildeteksten til et program – eller i det mindste er i besiddelse af viden om, hvordan man uden kildeteksten er i stand til at ændre på de parametre, der f.eks. kræver vedligeholdelse i en applikation – er man henvist til enten at skifte programmet ud med et andet eller – i det omfang det er muligt – at forsøge at ændre programmet på anden måde. Gennem såkaldt *patching* kan man f.eks. rette fejl i programmel gennem rettelser i selve den binære kode. Patching er dog vanskelig at gennemføre og anvendes primært ved brugerens egen fejlretning i styresystemer. Behovet for at kende programmets tekniske grænseflader kan undertiden løses ved undersøgelseshandlinger, der har karakter af *reverse engineering*, se herom afsnit 7.4.g.

Fordi kildeteksten typisk holdes hemmelig, jf. herom straks nedenfor, har tilhængere af "åbne systemer" presset kraftigt på for at opnå ret til såkaldt dekompilering, altså at kunne anvende applikationen således, at de nødvendige specifikationer kan hentes frem. Dette spørgsmål var genstand for voldsom debat i årene 1989-90 forud for vedtagelsen af Rådsdirektivet om retlig beskyttelse af edb-programmer.

Kildetekstens betydning

Derfor er adgangen til programmets kildetekst central for brugeren. Med kildeteksten til program X vil en tredjepart kunne udvikle et "nyt" program, Y, der i sin objektkode fremtræder som noget helt andet end program X's objektkode, men som ikke desto mindre indeholder betydelige dele af program X's kildetekst. Men af samme grund bevarer de fleste leverandører kildeteksten som en dyb forretningshemmelighed – en praksis, der også kan begrundes rent praktisk med, at objektkoden jo er beregnet for slutbrugerens computer og kildeteksten for programmøren. Da brugeren omvendt har en åbenbar interesse i at få adgang til kildeteksten, når der er behov for at ændre programmets funktioner (f.eks. for at få rettet en fejl eller at få programmet ajourført til de nye krav, brugeren har), og når leverandøren

enten ikke kan eller ikke vil foretage disse ændringer, er der behov for ordninger, der tilgodeser begge, berettigede interesser. Den slags ordninger gennemføres ofte ved, at man lader kildeteksten deponere hos en uafhængig tredjepart, jf. nærmere i afsnit 8.6.d.

Fortolkning

Visse højniveau-sprog anvender i stedet for oversættelse såkaldt "fortolkning". I en fortolker sker der samtidig oversættelse og eksekvering af programinstruktionerne, således at den første sætning er udført, før den anden oversættes osv. Det tager længere tid, men til gengæld er arbejdet med at kontrollere programforløbet og at ændre det lettere. Et eksempel på et sprog, som typisk fortolkes, er det dansk udviklede COMAL (COMmon Algorithmic Language).

Syntaks mv.

Som andre sprog består programmeringssprog (højniveausprog) af et antal ord eller ordklasser, en syntaks og en semantik. Når programmøren skriver sit kildeprogram, må han overholde syntaks og semantik og kun anvende de ord og instruktioner, sproget anerkender. Det oversætterprogram, der hører til sproget, virker nemlig kun, hvis programmøren har overholdt disse regler – og uden en oversættelse af kildeteksten er programmørens arbejde værdiløst. Ønsker han f.eks., at computeren under tekstbehandling skal give en lyd fra sig, når brugeren nærmer sig sidste linje på en side, er det ikke tilstrækkeligt, at han skriver: "sig dut, når brugeren nærmer sig sidste linje". I stedet må han i kildeprogrammet skrive et antal instruktioner, der svarer hertil. I programmeringssproget BASIC vil dette f.eks. kunne se sådan ud:

```
300 If lines => 70 then beep
```

Instruktioner, syntaks og grammatik varierer fra det ene programmeringssprog til det andet. Derfor er sprogene netop tilpasset de behov, programmørerne har. Udvikling af et tekstbehandlingsprogram, der ikke kræver den helt avancerede matematik, kan ske ved én type sprog; komplicerede beregninger over bygningskonstruktioners bæreevner kræver en anden.

3.2.d. Udviklingsprocessen

Problemet

Enhver med kendskab til et programmeringssprog, kan frembringe et edb-program. Selv mere komplekse programmer kan udvikles af enkeltpersoner. Arbejdet med at udvikle et edb-program af blot nogenlunde størrelse må dog planlægges. Skal mere end én programmør medvirke, må de enkelte opgaver afgrænses overfor hinanden. Man må være sikker på, at de enkelte progra-

melementer til slut kan indgå i en helhed. Dernæst må det sikres, at andre programmører kan træde til, hvis én forlader projektet. Udvikling af edb-programmer, hvori der medvirker mere end få programmører, må derfor styres. Denne styring indebærer først og fremmest, at alle inddata og uddata på forhånd er fastlagt. Gennem hele udviklingsforløbet må den udviklingsansvarlige vide, hvilke data systemet eller dets delmoduler vil modtage og afgive.

En oversigt over programudviklingsprocessen foreligger hos *Wagle & Ødegaard* (1997), s. 536 ff. Der findes en lang række fremgangsmåder, betegnelser og "skoler", der foreslår retningslinier for strukturering af dette forløb, f.eks. den danske SYSKON-model og de svenske RAS- og ISAC-modeller. *Egebjerg Johansen m.fl.* (1986) anbefaler s. 160 ff. en fasemodel med det mnemotekniske navn FAKIR: *F*orundersøgelse, *A*nalyse, *K*onstruktion, *I*gangsætning og *R*evision. Se i øvrigt Andersen, *Grude & Haug*: Målrettet projektstyring (dansk udg., 1989).

Analysearbejdet

Det første trin vil typisk rumme en analyse af den pågældende opgave. Denne analyse tager ofte udgangspunkt i den arbejdsgang, programmet skal fungere i, idet man hermed ser på, hvorledes de pågældende informationer behandles efter eksisterende manuelle eller IT-understøttede procedurer. Hvis programmet skrives på grundlag af en aftale, vil resultatet af analysen udmønte sig i en kravsspecifikation, der angiver, hvilke krav brugeren forventer til systemet.

Programspecifikation

Når analysen (kravsspecifikationen) ligger fast, går man videre med at analysere opgavens del-elementer. I tidligere tider gjorde man herved brug af rute-, proces- eller blokdiagrammer, dvs. grafiske afbildninger af forskellige typer af data, tilstande og processer mv. Fordelen ved at anvende et sådant arbejdsredskab er at skabe overblik over de forskellige samspillende funktioner. Diagrammet kan dernæst anvendes som grundlag for beskrivelser af andre processer mv. I dag er rutediagrammet i vid udstrækning erstattet af andre metoder til oversigtsmæssig repræsentation af en databehandlingsproces, f.eks. dialogdiagrammer og data flow-diagrammer.

Algoritme

På grundlag af programspecifikationen kan programmets enkelte dele planlægges. Hvor detaljeret denne planlægning skal være, beror på en række valg, der bl.a. må træffes efter, hvor kompliceret den samlede programmeringsopgave er, hvor mange personer der forudsættes at skulle medvirke, hvilken koordinering der ønskes her imellem, og hvilke programværktøjer der står til rådighed. Som betegnelse for beskrivelsen af en sådan frem-

gangsmåde, angivet ved et endeligt antal trin og med vished for, at et givet resultat opnås, anvendes ofte ordet algoritme.

Begrebet algoritme anvendes i flere betydninger. Sprogligt hidrører det fra en omskrivning af efternavnet på en arabisk matematiker, Mohammed Ibn-Musa *al-Khowarizmi*, der i et af sine værker lagde grundlaget for den moderne algebra (dvs. bogstavregning). I matematikken anvendes ordet algoritme om en regneforskrift eller metode til løsning af et matematisk eller logisk problem. Udover den betydning, der er angivet i teksten ovenfor, anvendes ordet også om visse færdige programmer, f.eks. krypterings-, sorterings- eller søgealgoritmer.

Kodning

Algoritmen angiver, hvordan programmøren kommer fra en startbetingelse til en sluttilstand. De mellemliggende led markeres ved de operationer, der skal foretages på inddata, og den rækkefølge, hvori dette skal ske. Algoritmen er derfor typisk det sidste arbejdspapir, der foreligger, inden den egentlige programmering påbegyndes i form af kodning (dvs. valget af de enkelte programkommandoer), se dog nedenfor om struktureret programudvikling. Sideløbende med kodningen dokumenteres systemet ved, at programmøren, den udviklingsansvarlige eller andre udarbejder en teknisk beskrivelse – en *dokumentation* – der gør det muligt for andre, f.eks. efterfølgende programudviklere, at få kendskab til de funktioner og principper, der finder udtryk i programmet.

Implementering

Det sidste element i konstruktionsfasen er *implementeringen* af det færdige program i en systemsammenhæng. Man taler om "implementering" på vidt forskellige niveauer og tidspunkter af et udviklings- eller anvendelsesforløb. Består systemet af forskellige del-moduler, vil man typisk implementere hver enkelt modul i dets forudsatte sammenhæng, inden hele systemet implementeres. Parallelt med implementeringsarbejdet *aftestes* programmet, bl.a. for at afklare, om det fungerer som forudsat under atypiske omstændigheder. Er systemet udviklet i medfør af aftale, vil der ofte være aftalt et endeligt slutprodukt for implementeringen i form af en afleveringsprøve, jf. herom nedenfor i kapitel 21.

Ingeniørvidenskab eller kunst?

Traditionelt – og til dels stadig – er programmering blevet opfattet som en kunst, hvor den enkelte programmør kunne manifestere og realisere sig. Denne opfattelse, der vel nok hidrører fra en tid, hvor programmer i højere grad var resultatet af en enkelt programmørs præstation, har efterhånden fået en anden karakter. I dag betragtes programudvikling på mange måder som byggeri. Der er i hovedsagen tale om en ingeniørmæssig disciplin ("software engineering"), der opstiller metoder og regler for hele

programudviklingsprocessen. Men samtidig er der opstået et betydeligt vidensområde vedrørende den måde, hvorpå systemerne implementeres i brugerens miljø og ikke mindst kommunikerer med denne (brugergrænseflader). Disse mere æstetisk betonede elementer af systemudviklingen kan derimod i højere grad siges at have kunstnerisk karakter.

SPU

Et af de principper, man finder inden for læren om programudvikling, er den såkaldt strukturerede programudvikling (i det flg.: SPU). SPU tager navnlig sigte på udvikling af systemer, hvor der er behov for en høj grad af fejlfrihed og gennemsigtighed. Behovet herfor kan f.eks. udspringe af, *at* mange programudviklere skal deltage i udviklingsprocessen, *at* databehandlingen angår kritiske data, eller *at* der må forventes en udskiftning af programmører. For at opfylde dette mål foreskriver SPU intens planlægning inden påbegyndelsen af den egentlige programmering, opdeling af opgaven i små moduler ("trinvis forfining") og løbende kritisk gennemgang af afsluttede del-opgaver.

Pseudokode

Til at understøtte en struktureret programmering anvender man ofte "pseudokode" ("pseudo", fordi det ikke er egentlig kode, selv om det udtrykker indholdet af en kode) som et mellemprodukt, inden kildekoden skrives. Pseudokode minder i det ydre om kildetekst og fremstår i et "næsten" naturligt sprog. Koden er opbygget over præcise notationer for de tre basiselementer, der indgår i enhver programmering (sekvens, valg og gentagelse), men kan hverken læses af computeren eller oversættes maskinelt til kildetekst. Der skal m.a.o. en programmør til at frembringe kildekoden. Jo mere detaljeret pseudokoden er affattet, jo færre valgmuligheder er der da overladt til programmøren, og i tilsvarende omfang kontrollerer pseudokodeforfatteren kildetekstens endelige udseende og dermed også det færdige program.

Walk through

En central bestanddel i SPU-princippet er den løbende evaluering af programmeringen. En sådan evaluering kan f.eks. ske ved, at den enkelte programmør lader andre gennemgå hans program, såkaldt *review* eller *walk through*, typisk under et uformelt møde. Formålet er at finde fejl, mangler eller kvaliteter. Herigennem sikres det bl.a., at koden overholder gældende kodestandarder, og – ikke mindst – at den er letforståelig for andre. Når andre end forfatteren selv kan læse programteksten, sikrer man, at en anden kan træde ind, hvis den oprindelige forfatter f.eks. skifter job. Dernæst sikrer en walk through, at grundlaget for at gå videre til en efterfølgende aktivitet er i orden. Som en sidegevinst ved teknikken kan nævnes den rent uddannelsesmæssige funktion.

Hvor de ovennævnte teknikker til programudvikling alle har det til fælles, at de bygger på en intens planlægning, såvel forudgående som undervejs i udviklingsprocessen, findes der en række nyere programudviklingsteknikker, der bygger på en udviklingsfilosofi, som set oppefra (med blik på hele projektet) kan forekomme mere kaotisk, men som i et perspektiv, der tager udgangspunkt i det enkelte modul, er mere overskuelig og dermed også lettere at kvalitetssikre. Til denne gruppe hører såkaldt *extreme programming*. Her begynder man ofte med små og simple dele af det færdige program, som man derefter aftester og vurderer sammen med brugerne, uden på forhånd at føle sig bundet af en fast plan for udviklingsprocessen. Gradvis vokser projektet sig større og større, idet såvel udvikleren som brugeren bevarer kontrollen med det. Metoden blev i sin tid foreslået af Kent Beck, Ward Cunningham og Ron Jeffries i en bog (med samme titel) fra 1999 (2. udg., 2005). Blandt de grundlæggende værdier, forfatterne fremlagde som bærende for denne form for programmering, er kommunikation, simpelhed, feedback, mod og respekt. Extreme programming kan anskues som et eksempel på *agil programudvikling*, der koncentrerer udviklingsindsatsen om små forløb (kaldet iterationer) typisk af mellem 2 og 4 ugers varighed.

Bonnerup-udvalget

Medvirkende til udbredelsen af sådanne alternative metoder til programudvikling har også været de uheldige erfaringer, man i det offentlige har haft med enkelte større IT-udviklingsprojekter, som har været planlagt efter de klassiske principper for rollefordelingen mellem kunde og programudvikler. I den rapport med titlen "Erfaringer fra statslige IT-projekter – hvordan gør man det bedre", som en arbejdsgruppe under Teknologirådet afgav i marts 2001 med forhenværende departementschef *Erik Bonnerup* som formand, opstilles et antal gode råd til den praktiske gennemførelse af IT-projekter. Heri anbefales det bl.a., at man splitter det samlede projekt op i delprojekter, med løbende leverancer (Appendiks 1, pkt. 11). Rapporten antager i øvrigt (pkt. 4.2), at den klassiske samarbejdsmodel for IT-udvikling bygger på en fejlagtig antagelse om, at det fra projektets start er muligt at lave en detaljeret og bindende aftale om hele projektforløbet. Dernæst påpeges det som et problem i mange statslige IT-projekter, at parterne ikke har haft den fornødne indsigt i hinandens faglige områder og har manglet forståelse for projektets fælles vision.

3.2.e. Programmel og maskinel

Grænsen mellem programsiden og maskinsiden er ikke skarp. Det er allerede nævnt, at enhver hardware-del gennem ledningsføringer mv. markerer, hvordan computeren kan fungere. Men herudover har enhver computer en mængde programmer indbygget i sig fra producentens side: Den må så at sige være programmeret til at kunne blive programmeret. I stedet for at stirre sig blind på sondringen mellem hardware og software, bør man afklare de forskellige typer af programmer og sondringsgrundlag.

Software og firmware

På grundlag af den forbindelse, der kan bestå mellem programmet og maskindelen, sondrer man undertiden mellem to former for IT-information: Den egentlige *software*, som brugeren selv kan flytte fra det ene medium til det andet, og den såkaldte *firmware*, der er manifesteret i mediet i en form, der for brugeren fremstår som uløselig. Sondringen korresponderer med den sondring mellem *mediekompatibel* og *integreret* information, der er præsenteret i afsnit 2.2.b.

Applikationsprogrammel

En anden sondring knytter sig til, hvordan programmet fremtræder overfor operatøren. Man sondrer her mellem anvendelsesprogrammel (også kaldet brugerprogrammel, på engelsk: *application software*) og systemprogrammel. Brugerprogrammerne (i det følgende kaldet applikationsprogrammellet eller blot "applikation") er de programmer, der opfylder brugerens umiddelbare behov for databehandling (regneark, tekstbehandling, bogføring og skatteberegning).

Systemprogrammel

Systemprogrammel varetager systemfunktioner, der som sådanne knytter sig til systemets "indmad" og altså ikke fremtræder for brugeren – f.eks. kommunikation mellem systemets elementer eller definition af tegnsæt. En væsentlig del af systemprogrammellet er *styresystemet* (operativsystemet), der sørger for at fordele og kontrollere computerens ressourcer. Styresystemet leveres ofte sammen med computeren og består af en maskinbaseret del, der er indbygget af producenten, og en disk-baseret del, der indlæses ved opstart. Maskindelen (der i PC'er kaldes *BIOS* = Basic Input/Output System) sørger for, at computeren kender de enkelte komponenter i systemet. Den disk-baserede del rummer dels nogle utilities, dels styrer den afviklingen af brugerprogrammellet.

Windows

Valget af styresystem er vigtigt, da det sætter rammerne for, hvilke brugerprogrammer computeren kan afvikle. Det mest udbredte styresystem til PC'er var oprindelig Microsofts "Disk Operating System" (DOS), som blev introduceret af IBM sammen med

de første PC'er. I 1987 introducerede IBM sammen med Microsoft et nyt og kraftigere styresystem – OS/2, der umiddelbart stod til at blive markedsførende. Ved indgangen til det nye årtusinde er det mest udbredte styresystem til PC'er stadig Windows-systemet fra Microsoft. Windows blev oprindeligt udviklet som en grafisk grænseflade til DOS-styresystemet, der på samme måde som tidligere set i den populære Macintosh-computer fra Apple Computer anvendte "point and click"-teknikker baseret på mus. I senere versioner, fra og med Windows 95, er Windows blevet et selvstændigt styresystem, hvis grænseflader bl.a. har sat standarden for, hvorledes applikationsprogrammel fra andre programleverandører fremtræder overfor brugeren. Vil man udvikle et e-mail program eller et tekstbehandlingssystem, der skal afvikles under Windows, kan man således knytte sit programs funktioner (f.eks. ved åbning og lukning af programmer, udprint af data og sletning mv.) til de funktioner, Windows allerede har indbygget i sig.

Den kraftige udbredelse af Windows-styresystemet har gjort Windows-grænsefladerne til en af de vigtigste tekniske *de facto standarder* på pc-området og har medvirket til at give Microsoft den før omtalte dominans på pc-markedet, der i samspil med beskyldninger mod selskabet for misbrug af denne dominerende stilling i forskelligartede sammenhænge har ført til konkurrenceretlige søgsmål mod virksomheden i en række amerikanske delstater og ved konkurrencemyndigheder i en række lande. De PC'er, der markedsføres af Apple Computer, opererer med egne styresystemer, der dog i senere versioner også har grænseflader svarende til Windows. På grund af den heraf følgende kraftige markedsdominans har Microsoft gennem de seneste mange år været i konkurrencemyndighedernes søgelys, såvel i USA som i EU, hvor virksomheden gentagne gange er blevet dømt for overtrædelser af konkurrencereglerne.

UNIX

På lidt større maskiner er det almindeligt at anvende styresystemet UNIX. UNIX kan også afvikles på IBM-PC'er. De standarder, der gælder for UNIX-systemet, kan beskrives som "åbne": Den oprindelige UNIX-kildetekst har været alment tilgængelig og alle centrale specifikationer (der bl.a. også følger af den såkaldte POSIX-standard) offentliggjorte. Dette har på den ene side ført til UNIX's store udbredelse, men også til, at der er opstået et stort antal versioner af UNIX, idet leverandørerne hver for sig har udformet deres egen UNIX-version. Man har dermed – paradoksalt nok – opnået det modsatte af den oprindelige intention, nemlig en manglende standardisering, der i de senere år har taget kraften ud af UNIX.

Undertiden ser man de programoversættere og -fortolkere, der er omtalt i afsnit 3.2.c., betegnet som systemprogrammel. Dette er kun delvis betegnende. For den, der udvikler et program – og som i denne egenskab utvivlsomt er "bruger" af computerens funktioner – er programoversætteren en applikation.

LINUX

I de seneste år har et nyt styresystem set dagens lys, primært til brug i pc-miljøer, der er baseret på principper hentet fra UNIX-styresystemet. Det drejer sig om styresystemet LINUX, der i 1991 blev udviklet af den finske studerende *Linus Torvalds*. Via Internet inviterede Torvalds hele verden til at være med i udviklingen af LINUX, og i dag er der tale om et fuldt brugbart styresystem, som bl.a. er indbygget i en række pc-producenters udstyr. Da såvel Torvalds' oprindelige version af systemet som de efterfølgende forbedringer af det er udviklet efter freeware-principper, er dette system som udgangspunkt gratis at erhverve, ligesom kildeteksten er alment tilgængelig.

Den amerikanske virksomhed SCO Group Inc., som har overtaget rettighederne til det oprindelige UNIX-operativsystem fra AT&T Bell Laboratories, har i 2004 rejst sag mod IBM med påstand om, at IBM's anvendelse af Linux-styresystemet indebærer en krænkelse af rettighederne til UNIX-systemet. Sagen, der endnu ikke er afgjort, er blandt andet omtalt af *David Bender* i 20 CLAB 2005, s. 18 ff.

Specialprogrammel og standardprogrammel

Programmer kan være særligt udviklet til en konkret bruger (typisk en konkret virksomhed). I så fald taler man om *specialprogrammel* eller "skræddersyet programmel". Eller det kan være udviklet med henblik på massedistribution til vidt forskellige brugere med samme databehandlingsbehov. Her bruges betegnelsen *standardprogrammel*. Da specialprogrammel – ligesom skræddersyet tøj – er dyrt at anskaffe, bruges det kun til særlige opgaver. Viser der sig et marked for den pågældende funktion, vil specialprogrammel ofte senere blive til standardprogrammel.

Utilities

Et utility-program er et mindre programværktøj, der typisk knytter sig til et eksisterende system, og som på forskellig vis nyttiggør eller supplerer funktioner, dette system i forvejen har. Funktionen kan f.eks. gå ud på at øge hastigheden af visse processer mv. eller at genskabe slettede datamængder. Det er kun delvis korrekt at henregne utilities til systemprogrammel, for så vidt der tænkes på funktioner som f.eks. at øge systemets hastighed, at tillade afvikling af flere programmer samtidig el.lign. Andre utility-funktioner fremtræder som applikationsprogrammel. Det gælder f.eks. de, der tager sigte på funktioner, der i forvejen udføres af andre applikationer, f.eks. sletning, flytning

og redigering af filer. De supplerende funktioner som f.eks. at genskabe slettede filer falder nærmest i en mellemgruppe.

3.2.f. Programmel og data

Definitionen af programbegrebet forudsætter herudover en sondring mellem programmel og data. Som nærmere udviklet i afsnit 2.2.a. betegner begrebet "data" noget givet; noget, man i givet fald må forholde sig til. I relation til programbegrebet kan man sige, at programmet beskriver den *proces* (eller lovmæssighed), som programmeringen resulterer i, medens dataene er de *objekter*, der indgår i processen. Sætter man sig f.eks. for at beskrive den proces, hvorved to tal divideres med hinanden, vil denne beskrivelse være programmet, hvorimod det tal, der efterfølgende divideres, udgør data. Sondringen kan også udtrykkes således, at programmet ved én gang for alle (indtil programmet ændres) at fastsætte de lovmæssigheder, der skal bestemme forløbet af en efterfølgende procedure, udgør en *statisk* komponent i databehandlingen, hvorimod de data, der indgår i behandlingen, har mere *dynamisk* eller tilfældig karakter, idet dette bl.a. bestemmes af, hvilke "inddata" brugeren vælger at udsætte programmet for.

Sondringen mellem programmel og data har retlig betydning bl.a. i ophavsretten, hvor der sondres mellem programmel (instruktioner til processoren), der beskyttes efter et regelsæt, se hertil ophl. § 1, stk. 3, og data, der beskyttes efter et andet (som databaser), jf. ophl. § 71. Selv om den i udgangspunktet er klar, må det erkendes, at der i den praktiske anvendelse af sondringen peges på tilfælde, som det kan forekomme vanskeligt at placere. Disse grænsetilfælde behandles i relation til de relevante retlige problemer.

Et par eksempler: *1.* Under programudviklingen har programmørens instruktioner ud fra en strengt logisk betragtning karakter af "data", eftersom de i denne kildetekstversion ikke udgør instruktioner til processoren. Først når kildeteksten konverteres til objektkode, kommer programmet rigtigt til at leve op til det definitoriske krav. I ophavsretlig henseende spiller dette forhold dog ingen betydning, idet kildeteksten i alle tilfælde betragtes som et eksemplar af programmet, jf. ophl. § 2, stk. 2. *2.* Når et program afvikles, vil det indeholde en række udsagn (*"statements"*), der slet ikke retter sig til processoren, men som f.eks. tjener til at informere senere programudviklere om rent tekniske forhold. Disse statements må strengt taget udgå af programbegrebet. *3.* Som led i programanvendelsen er programmet nødt til at trække på en række data, der ofte inkorporeres i den proces, der realiserer den ønskede IT-funktion. Disse data kan

for så vidt også siges at indeholde instruktioner til processoren. Men da de hentes ind af programmet – og kun påvirker databehandlingsprocessen i det omfang dette tillades af processoren – holdes de udenfor programbegrebet.

Databaser

Med den stigende lagerkapacitet i moderne IT er det blevet mere almindeligt at indlægge omfattende datamængder i IT-systemerne. Man anvender udtrykket database om en sådan samling af data, der er struktureret (dvs. ordnet) i overensstemmelse med en række veldefinerede regler og på en måde, der gør det muligt effektivt at lagre og hente data. I praksis anvendes ordet i flere betydninger. For det første indgår der databasefunktioner i systemets interne komponenter, f.eks. ved den interne registrering af data til tekniske formål. En anden type database opbygges af brugeren selv som samlinger af information (f.eks. telefonnumre), der mest af alt minder om kort i et kartotek. Endelig kan man se på de databaser, der produceres af en leverandør med henblik på levering til forbrugere på samme måde som bøger og aviser. Sådanne applikationer kan enten baseres på medier, der overdrages til brugeren, eller på online-opkobling.

Hypertekst

For at lette brugerens søgning i databaser med information, der tager sigte på brugeren, er det blevet almindeligt at anvende *hypertekst-teknologi* som den f.eks. kendes ved surfing på www. På grundlag af et antal koder, der er lagt ind i teksten på forhånd efter *redaktionelle* overvejelser, kan brugeren springe rundt i teksten som han vil (alt efter, hvad koderne tillader). Han kan f.eks. beslutte sig til at "folde teksten ud" på forskellige niveauer. Hypertekst-applikationer har tidligst været anvendt som grundlag for digitale ordbøger og leksika: Når brugeren befinder sig i et ordbogsopslag på en digital ordbog og ser en henvisning til et andet ord, "klikker" han med sin mus på dette ord, hvorefter den bagved liggende kode bringer ham hen til det sted i ordbogen, hvor det er forklaret. Ordbøger læses netop ikke-lineært (modsat skønlitterære værker); men gennem hypertekst-teknologien er der stadigt flere fagbøger og databaser, der også med fordel kan læses således.

Offentlige databaser

I en særlig kategori finder man den offentlige database, der rummer information af almen interesse, f.eks. nyheder, statistik, lovgivning og retsafgørelser. I modsætning til den trykte samling af informationer kan publikationstiden i en online-database minimeres så kraftigt, at databasen til enhver tid indeholder den nyeste information. Dermed er et nyt elektronisk informationsmarked opstået. En del af dette marked baseres på et indtægtsgrundlag, der ikke kendes fra den klassiske økonomi, hvor realydelser

udveksles mod pengeydelser. Nogle databaser er etableret og finansieret ved offentlige midler – andre finansieres ved bannerannoncering, og endnu andre baseres på betaling via abonnementsordninger eller pr. forbrug.

Multimedia

Betegnelsen multimedia (efter det engelske udtryk, tidligere talte man om "multimedier") dækker over den integrerede anvendelse af forskellige typer af information på samme medie. Da begrebet opstod i begyndelsen af 1990'erne tog det sigte på visse bestemte typer af applikationer inden for navnlig underholdnings- og undervisningsområder, hvor man i samme produkt kunne søge og læse i omfattende tekstmængder, se teksten illustreret med levende fotografier, billeder, filmsekvenser, lydimpulser, musik, grafer etc. etc. Betegnelsen er imidlertid på retur. For det første er den ikke logisk, eftersom der netop er tale om ét medium, der håndterer en flerhed af informationstyper. Men dernæst er den integrerede anvendelse af talrige informationstyper i dag en helt sædvanlig ingrediens i IT-anvendelsen og en væsentlig forklaring på, at systemerne i dag er blevet så brugervenlige. Udviklingen af sådanne systemer rummer i øvrigt ophavsretlige problemer, der kan forekomme ligeså komplekse som dem, der præger lignende ophavsretlige produktioner som f.eks. filmproduktioner. Et retsgrundlag til beskyttelse af multimedia-udvikleren er nu skabt ved EU-direktivet om retlig beskyttelse af databaser.

3.3. Internet

3.3.a. Teknisk princip

Ved at koble en computer op til det globale net af kommunikationsledninger (telefoni mv.), der i dag er forbundet i Internet, kan brugeren forvandle sin computer til en *klient* for det gigantiske informationsudbud, der befinder sig på nettet, og dermed til et kraftfuldt instrument til indsamling og distribuering af information.

Packet-switching

Kommunikation på Internet benytter sig af princippet for "pakke-kobling" ("*packet-switching*"): Hver meddelelse ("brev") deles op i et antal mindre meddelelser (pakker eller "postkort"), der herefter sendes afsted som sådanne. I mange tilfælde kan det tænkes, at disse mange postkort passerer samme routere på vej fra afsender til modtagere, men hvis et antal af disse routere er optaget eller ude af drift, kan det tænkes, at nogle postkort må

komme frem via andre routere. Først når postkortene er ved modtageren, samles de, så det oprindelige brev igen dannes.

De færdselslove, der styrer denne vildtvoksende globale kommunikation, er indeholdt i TCP/IP-protokollerne, der oprindelig blev udviklet til *ARPA-net*. Disse protokoller fungerer i dag som en *de facto-standard* for datakommunikation udenfor den enkelte virksomheds lokalnet. Dette betyder bl.a., at protokollerne er indbygget i den software, der i dag anvendes af Internet-brugere, f.eks. e-post-programmer og web-browsere. Et centralt element i denne funktion er, at informationsudvekslingen sendes afsted i pakker ("postkort"). Et andet centralt element går ud på, at hver tilsluttet computer har et nummer (IP-nummer, jf. nedenfor). Den information, der er i disse pakker, fortolkes altså ikke, men hver af dem er udstyret med en adresse på den computer, hvor pakkerne siden skal samles til den oprindelige meddelelse.

Gennem denne kommunikationsform undgår man en *central styring*, f.eks. udført via en central computer, der løbende har styr på, hvad der afsendes og modtages: Ved hjælp af routerne finder de enkelte pakker selv frem til deres bestemmelsessted, hvor de stykkes sammen med de andre pakker og gendanner den oprindelige meddelelse.

TCP/IP er ikke "en" protokol, men en serie bestående af en række hjælpeprotokoller med forkortelser som RIP, ICMP, ARP, RARP m.fl. Hertil hører en lang række applikationsprotokoller, som understøtter de tjenester, der kan anvendes på Internet, herunder *telnet, ftp, smtp, nntp, http* etc. En ny version 6 af Internet-protokollen (i daglig tale kaldet IPv6) blev vedtaget af IANA den 14. juli 1999, men har næppe udsigt til at blive indført fuldt ud før tidligst om 5-10 år. En sådan indførelse kræver nemlig, at alle de DNS-servere, der p.t. fungerer ved hjælp af den eksisterende version 4, skal skiftes ud og opsættes på ny. Det driftsmæssige behov herfor er beskedent, eftersom det nuværende adresserum (dvs. antallet af potentielle adresser på nettet) fortsat må betragtes som ganske rummeligt for de næste mange år. IPv6's væsentligste egenskab er et gigantisk adresserum. En anden, ikke længere så udbredt, standard for overførelse af information er X.400-standarden, der tidligere har været udbredt som grundlag for kommunikation mellem statslige myndigheder.

3.3.b. Internet-leverandøren

En central komponent i informationsudvekslingen på Internet er de virksomheder, der fungerer som mellemled mellem de kommunikerende brugere, de såkaldte Internet-leverandører. I kraft af bilaterale aftaler mellem de enkelte leverandørvirksomheder og/eller via nationale Internet-udvekslingspunkter (bl.a. her-

hjemme den såkaldte DIX: "Danish Internet Exchange point") sørger de for kommunikationen mellem de tilsluttede Internet-brugere.

Man kan sondre mellem tre typer af leverandørfunktioner. I praksis vil den enkelte Internet-leverandørvirksomhed tilbyde sine kunder flere af disse funktioner.

IAP

I en første gruppe kan man udpege leverandører af *Internet-adgang* (også kaldet IAP, Internet Access Providers). IAP'en har betydelige lighedspunkter med den rene netværksleverandør (f.eks. et teleselskab), idet hans tjeneste dog er begrænset til Internet-kommunikation. Selv om en IAP begrebsmæssigt ikke leverer andet og mere end adgangen til nettet, er det dog nødvendigt at stille visse programfunktioner til rådighed. En IAP, der leverer faciliteter til e-post kommunikation, er nødt til at programmere sin postserver således, at modtagerne kan betjene den. Derimod er han ikke nødt til også at forsyne sine kunder med et e-postprogram. Et andet eksempel er en *host-provider*, der udlejer plads på sin server til kunder eller stiller nyhedsgrupper til rådighed fra newsservere.

ISP

Den anden leverandørfunktion, som spiller den største rolle i praksis, går ud på at levere *Internet-tjenester*. En sådan leverandør betegnes ofte som ISP, Internet Service Provider. Denne leverandør kendetegnes ved – i forskellige afskygninger – at gøre andet og mere end at stille kommunikationsfaciliteter til rådighed. Der kan f.eks. være tale om programleverancer eller om at give adgang til nyhedsgrupper, "chat-kanaler", databaser el.lign.

Hvor netværksoperatøren som før nævnt ikke øver nogen indflydelse på indholdet af den kommunikation, der transmitteres på nettet, kendetegnes IAP'en og ISP'en ved i højere grad at spille en rolle for informationsstrømmens forløb. Særlig tydeligt er dette for ISP'en, der i hvert fald vil kende navnet på de forskellige nyhedsgrupper, der udveksler information; men i princippet gælder det samme for den virksomhed, der alene optræder som *host*, altså som vært for en kommunikationsfacilitet, hvis beskaffenhed han i øvrigt ikke har indflydelse på. Også han kan jo – på lige fod med alle andre – blot vælge at koble sig op på de hjemmesider mv., hans kunder udbyder fra nettet. Sondringen kan have juridisk betydning, f.eks. i relation til spørgsmålet om medvirkensansvar. Skal IAP'en og ISP'en f.eks. have pligt til at foretage sådanne undersøgelser, eller kan forholdet snarere sammenlignes med postudbringning, hvor postbudet jo heller ikke har pligt til at læse indholdet af de (åbne) postkort, han putter i brevsprækkerne? Dette spørgsmål behandles i afsnit 17.1.d. og 17.1.e.

En tredje leverandørfunktion angår *Internet-informationsindhold* (i det følgende kaldet ICP, Internet Content Provider). Denne gruppe omfatter ret beset enhver, der vælger at stille information til rådighed for omverdenen via Internet, hvad enten der er tale om kommercielle virksomheder, offentlige myndigheder, institutioner eller privatpersoner. Informationen kan enten være offentlig eller lukket, den kan ligge på en hjemmeside eller være transmitteret til en nyhedsgruppe (dvs. en afgrænset kreds af modtagere), eller den kan indgå som en del af Internet-ydelser af andet indhold. ICP

Det gælder for alle de nævnte ansvarskategorier, at de både kan tænkes præsteret i et aftaleforhold eller uafhængigt af aftale. At der f.eks. ofte ikke foreligger noget aftaleforhold mellem brugeren af en hjemmeside og dennes udbyder er åbenbart for enhver, der har "surfet" på nettet. Men det samme gælder for levering af selve Internet-adgangen (som ofte er mulig gennem faktisk brug af udstyr opstillet på offentlige steder, som f.eks. biblioteker el.lign.) samt for forskellige Internet-tjenester. Et eksempel på sidstnævnte er faciliteter til e-post kommunikation, som i stigende omfang tilbydes vederlagsfrit (reklamefinansieret gennem såkaldte banner-annoncer på hjemmesider) fra the World Wide Web (www).

3.3.c. IP-adressering

Hvor mennesker foretrækker at give hinanden navne, har computere lettest ved at identificere hinanden ved hjælp af numre. Derfor har hver eneste computer, der er sluttet til Internet, et nummer, der kan læses af den protokol-standard, der anvendes i Internet-kommunikationen. Dette nummer kaldes en IP-adresse. IP-adressen identificerer den enkelte computer unikt, eftersom den angiver computerens placering i nettets forgrening. Det er et grundlæggende teknisk krav, at hver computer, som der kommunikeres fra og til, har en entydig adresseidentifikation: Hvis flere personer, intetanende, har samme telefonnummer, kan opkaldet jo heller ikke føres entydigt frem! Opgaven med at fordele disse IP-adresser er fordelt globalt mellem forskellige registreringsenheder, jf. nedenfor.

Pga. sin størrelse egner IP-numre sig primært til maskinel læsning. Der er dog intet til hinder for, at man kan adressere en computer via sin Internet-browser ved blot at indtaste IP-nummeret for den computer (f.eks. den hjemmeside), man ønsker at kontakte. En sådan indtastning har i øvrigt nyttige anvendelsesområder til brug for målrettet levering af information til en bestemt bruger: Når betalingen er erlagt, udstyres brugeren med

IP-nummeret for den hjemmeside, hvor informationen er tilgængelig – typisk kun i en bestemt periode. Samme teknik kan omvendt anvendes til at formidle information af retsstridigt indhold, som – af samme grund – ønskes skærmet fra den overvågning, visse retshåndhævende myndigheder foretager ved "surfing" på hjemmesider.

Som nævnt har man for at lette den praktiske brug af Internetadresseringen indført et særligt navnesystem, hvorefter IP-adresserne "oversættes" til let genkendelige domænenavne (undertiden også kaldet hostnavne). Et sådant domænenavn kan enten understøtte web-applikationer, hvorved det optræder som <www.isoc.org>, eller elektronisk post, hvorved det optræder som en e-post-adresse af typen navn@isoc.org. I en adresse, der understøtter World Wide Web-kommunikation, betragtes alle navnene, herunder forkortelsen "www" (der angiver, fra hvilken server der præsteres web-service) som domænenavnene. I en e-post-adresse baseret på Internet-kommunikation er det de elementer, der følger efter @-tegnet, der er domænenavne.

Navnehierarkiet

Afhængig af, hvor mange punktummer ("dots"), der optræder i domænenavnet, taler man om topdomæner eller (synonymt) topleveldomæner (f.eks. .dk) eller andenordensdomænet (f.eks. ku.dk). Synonymt hermed tales om root, sub-root eller sub-sub-root domænenavne. Feltet umiddelbart til venstre for topleveldomænenavnet angiver andet niveau af domænenavnet og bestemmes af indehaveren. De fleste topleveldomæner er landeforkortelser, f.eks. .dk for Danmark, .no for Norge og .uk for Storbritannien. Fordelingen af domænenavne bærer dog fortsat præg af, at Internet er en amerikansk opfindelse med stærke rødder i den amerikanske universitetsverden og kontrolleret og støttet af den amerikanske regering. Således var .com-domænet oprindelig tiltænkt amerikanske virksomheder, ligesom der optræder en række topleveldomæner, der primært tager sigte på amerikanske brugere, herunder .gov-domænet. Se nærmere hertil dokumentet *RFC 1591* af marts 1994.

Da mange af disse domænenavne vil være sammenfaldende med betegnelser for personer, virksomheder, myndigheder eller andre enheder, som betjener sig af særlige kendetegn, har fordelingen af disse navne givet anledning til en række juridiske problemer, jf. nærmere herom i afsnit 11.4. Som nærmere udredet her, knytter der sig forskellige typer af juridiske problemer til de forskellige niveauer af domænenavne.

Domain name service

For at oversætte en maskines IP-nummer til et hostnavn benyttes en såkaldt DNS-tjeneste (Domain Name System). Der er tale

om en databasetjeneste, der registrerer, hvilke computere der står bag hvilke domænenavne på Internet. Domænenavne er hierarkisk opbygget, og DNS-tjenesten udføres på forskellige niveauer i Internet-hierarkiet og knytter sig til forskellige typer af adresser (kaldet zoner). På øverste, internationale niveau findes der 13 DNS-rodservere, hvoraf den nærmeste er placeret i Stockholm. De pågældende servere repræsenterer altså ikke nogen navnezone. Deres eneste formål er at holde styr på de navne, der er registreret under Internet-roden, altså samtlige landedomæner (ccTLD) og generiske topleveldomæner (gTLD).

På trinnet lavere – dvs. topleveldomæneniveauet (f.eks. .dk) – findes der et antal DNS-servere, for dk-domænets vedkommende i alt 6. Disse DNS-servere peger videre på de enkelte Internet-leverandørers DNS-servere under .dk-domænet. Hver DNS-server afgiver enten de pågældende oplysninger selv eller foranstalter kontakt med de DNS-servere, der tilhører den pågældende Internet-leverandør.

I praksis fungerer dette system som følger: Hvis en seer ønsker at kontakte en hjemmeside – f.eks. den, der drives af tv2 – skriver han "www.tv2.dk" i sin browser. Ved angivelsen "www" signalerer brugeren, at han kun ønsker at kommunikere med domænenavne til www-browsing, jf. om dette begreb nedenfor. Var formålet med at kontakte tv2 derimod at sende en e-post meddelelse til en bestemt medarbejder, skulle han i stedet anvende et program til e-post kommunikation og f.eks. adressere domænet som følger "per.hansen@tv2.dk".

Når domænenavnet kaldes af en bruger, f.eks. med henblik på www-browsing, vil hans Internet-browser udvirke en række opslag i forskellige DNS-databaser med det formål at lokalisere det IP-nummer, der hører til den maskine, brugeren ønsker at kontakte. For at gennemføre disse opslag må brugeren have hjælp fra en Internet-udbyder, der på forhånd har sat sit udstyr op, således at opslaget – hvis ikke IP-adressen er kendt – rettes mod en navneserver, der kan løse denne opgave. Kendes adressen ikke, vil opslaget gå til en af de 13 rodservere på Internet, der vil indeholde den autoritative information om, hvor databaserne for de enkelte topleveldomæner findes. Når adressen herpå er kendt, vil forespørgslen gå videre til de servere, der ligger under dette toplevel-niveau. Resultatet af denne søgning vil – i eksemplet – være, at www.tv2.dk har IP-nummeret 195.249.225.28.

Den nærmere opbygning af denne DNS-tjeneste skal ikke uddybes her. Nærmere oplysninger herom kan hentes fra <www.dk-hostmaster.dk>. For at sikre driftsstabiliteten (ved dels at fordele belastnin-

gen, dels at sikre mod følgerne af enkeltstående nedbrud) er systemet opbygget således, at der altid er to navneservere for et domæne, en primær og en sekundær. De sekundære (og i givet fald tertiære) navneservere foretager med jævne mellemrum opkald til den primære navneserver for at få oplyst, om deres oplysninger om domænenavne er fuldt opdaterede. Den overførsel af opdaterede oplysninger, der i givet fald finder sted, betegnes som en *zoneoverførsel*.

ccTLD

Som grundlag for forkortelsen af de enkelte landebetegnelser anvendes ISO 3166-standarden, f.eks. .dk for Danmark. Man sondrer mellem ccTLD-domæner og gTLD (Generic Top Level Domain), hvor sidstnævnte defineres efter generiske – modsat nationale – betegnelser. Det væsentligste eksempel herpå er .com, der oprindeligt alene tog sigte på kommercielle brugere, men som i dag også er navnerum for en række private brugere. Der findes i dag ca. 250 ccTLDer og 7 (snart 14) gTLDer. Nærmere herom i afsnit 11.1.c.

gTLD

Særlige problemer knytter sig i den forbindelse til administrationen af de såkaldt generiske topleveldomænenavne, f.eks. "edu" for uddannelsesinstitutioner og "com" for kommercielle virksomheder. Denne del af nettets navnestruktur har rod i nogle af de beslutninger, der blev truffet, da den amerikanske del af nettet blev løsrevet fra kontrollen fra U.S. Department of Commerce. I 1999 har Department of Commerce indgået aftale med ICANN og den private virksomhed Network Solutions, Inc. (NSI), som hostmaster for .com, .net og .org-domænerne, der bl.a. giver NSI ret til indtil videre at videreføre denne service. I samme forbindelse fastsættes en pris pr. registrering på 6 USD fra og med 15. januar 2000. Ligeledes forpligter NSI sig til at yde visse økonomiske tilskud til ICANN.

3.3.d. Internet-styring

Fra en juridisk synsvinkel er det nærliggende at stille spørgsmålet, hvem der "ejer" eller i det mindste "styrer" Internet. Svaret på dette spørgsmål beror på, hvilke *aspekter* af nettet man anskuer. Når det gælder de *fysiske netforbindelser* er det på den ene side enkelt at konstatere ejerskabet (hvad enten der er tale om private net-installationer, særligt nedgravede kabler eller det "rå kobber", der fra gammel tid har været i de statskoncessionerede selskabers eje). Men på den anden side er Internet ikke synonymt med disse netforbindelser, da disse jo også anvendes til anden telekommunikation, f.eks. telefonforbindelser eller fremførelse af kabel-tv. Ser man dernæst på de *standarder*, der ligger til grund for al kommunikation på nettet, er det kendetegnende, at

disse er *åbne* og ikke genstand for ejerskab, jf. herom straks nedenfor. For så vidt er der heller ikke her noget egentligt ejerskab i juridisk forstand.

Organisationerne

Det nærmeste man kommer en juridisk beskrivelse af ejerforholdene bag Internet er en beskrivelse af de *organisationer*, der styrer de kommunikationsformer, der udfolder sig på nettet.

- ISOC

Central er her *Internet Society* (ISOC), der har ansvaret for vedligeholdelse af de standarder, der definerer kommunikation på Internet. Internet Society opererer via en række nationale afdelinger, herunder – siden 1999 – også en dansk. En del af det praktiske arbejde er dog henskudt til forskellige organisationer (herunder IANA), der igen har delegeret sit arbejde videre til andre.

- ICANN

En anden central instans i den internationale Internet-styring er The Internet Corporation for Assigned Names and Numbers, se <www.icann.org>. Der er tale om en amerikansk (i Californien) baseret juridisk person, der bl.a. styrer fordelingen af topleveldomænenavne på Internet (forkortet TLDs) samt uddeling af IP-numre, men som også har et vist ansvar for standardisering mv. på nettet.

ICANN's arbejde vedrørende domænenavne har grundlag i de anbefalinger, der har fundet udtryk i dokumentet *RFC 1591*. Hovedprincipperne heri er, at den virksomhed, der administrerer et topleveldomæne, der dækker over en landebetegnelse, udfører en tjeneste i den lokale almenheds interesse, og at virksomheden derfor har en særlig forpligtelse til at tjene denne almenhed.

Vanskelighederne ved at styre kommunikation og domænenavnstildeling på Internet har fra tid til anden givet anledning til politiske overvejelser, i USA i forbindelse med de aftaler, U.S. Department of Commerce har indgået med ICANN og NSI, herhjemme ved Kommissionens initiativer vedrørende "Internet Governance", se således KOM(1998) 111, endelig udg. af 20. februar 1998. En fuldt opdateret oversigt over de seneste politiske initiativer kan findes fra ICANN's hjemmeside, <www.icann.org>. Den form for demokratisk kontrol, der udøves i ICANN-systemet, har undertiden givet anledning til kritik, herunder også fra retsvidenskaben. Se f.eks. den veldokumenterede redegørelse hos *John Palfrey* i 17 Harvard Journal of Law & Technology (2004) 409 ff., der konkluderer at organisationens forsøg med at indføre et globalt Internet-demokrati er forfejlet.

3.3.e. Internet-applikationer

En-til-en

Da Internet fik sit første kommercielle gennembrud, var det som understøttelse af bruger-til-bruger-kommunikation ("one-to-one communication"). I en sådan kommunikation mellem parter, der i forvejen kender hinanden, spiller nettet samme rolle som teleselskabet gør ved telefoni og postvæsenet ved postbesørgelsen. Bruger-til-bruger-kommunikation kan enten ske ved, at parterne udveksler tekstmeddelelser med hinanden som i en telefon (såkaldt "chat", altså "snak"), ved at der overføres elektroniske meddelelser i særskilte pakker (elektronisk post eller filudveksling) eller som isolerede tekstmængder (særskilt fil- eller pakkeoverførelse). Undertiden finder grupper af brugere sammen for at kommunikere fra *en til mange* ("one-to-many").

Kommunikation i lukkede brugergrupper har været kendt længe før Internet kom til, nemlig ved de såkaldte *bulletin board systems*, også kaldet BBS eller "elektroniske opslagstavler". I et BBS stiller en enkelt person, en organisation eller en virksomhed sit edb-system – der måske blot består af en hjemmecomputer, der er forbundet med et modem – til rådighed via telefonnettet, idet almenheden, eller en lukket skare, herefter inviteres til at hente og afgive information, ligesom på en fysisk opslagstavle. Et andet eksempel på kommunikation i en lukket brugergruppe, som har været kendt længe før Internet, er at et hovedkontor kommunikerer med sine afdelingskontorer via modemforbindelser eller med teleforbindelser, der har været lejet til formålet.

- e-post

Den mest udbredte en-til-en kommunikation på nettet er elektronisk post, også kaldet *e-mail*. Brugen af elektronisk post giver navnlig anledning til juridiske problemstillinger i relation til de handlinger, hvorved denne kommunikation overvåges, hvad enten dette sker i et ansættelsesforhold (se hertil i afsnit 14.1.d. og 17.4.) eller som led i en strafferetlig efterforskning, jf. herom betænkning 1377/1999, s. 63 ff.

En-til-mange

En Internet-tjeneste kan dernæst præsteres ved kommunikation fra en person og til en flerhed af modtagere. Det første udslag af denne tanke var de såkaldte *nyhedsgrupper*, som man fortsat kan abonnere på via en Internet-leverandør: I kraft af abonnementet modtager de tilsluttede brugere de oplysninger, der udsendes centralt (fra en informationsleverandør) eller fra andre brugere.

Man kan sondre mellem de nyhedsgrupper, der baseres på envejskommunikation (f.eks. ved løbende oplysninger om kursudvikling eller meddelelser om børsnoterede selskaber) og de, der indebærer en

tovejs-diskussion mellem de tilknyttede brugere. Begge former for informationsudveksling kan tjene åbenbart nyttige formål (f.eks. udveksling af erfaringer vedrørende bestemte sygdomme, politisk meningsudveksling og faglig dialog); men teknologien kan i sagens natur også anvendes til retsstridige formål, f.eks. distribution af ulovlig børnepornografi eller piratkopier af ophavsretligt beskyttede værker.

- www

Gennem de senere år forekommer det stadigt mere hyppigt, at Internet-brugere betjener sig af *databaser* eller andet informationsudbud tilsluttet nettet. Et afgørende gennembrud i udviklingen af sådanne applikationer kom i 1992, hvor *Tim Bernes-Lee* foreslog en ny teknik til kommunikation til og fra Internet-databaser ved brug af hypertekst-links. Det var indtil da velkendt, at man kunne forvandle en database til en hypertekst-applikation, således at brugeren *inden for en tekst* kan "klikke" på bestemte ord for herved at bevæge sig ind i underniveauer af den. Det nye var at anvende denne teknik til at sætte brugeren i forbindelse med *andre tekster* (andre databaser, hjemmesider mv.), som der ved den forudgående kodning skabes en umiddelbar netforbindelse (såkaldt hypertekst-link) til. Når man anvender hypertekst på Internet mærker brugeren ikke, hvorfra han henter sin information. De interaktive valg, han foretager ved sine "klik" på fremhævede punkter på den enkelte hjemmeside, giver brugeren en følelse af at "surfe" på nettet. Hvad der derimod sker er, at brugeren springer fra database til database i en glidende bevægelse, hvorfra han på grund af sine indtastede kommandoer ("museklik") modtager serier af information svarende til den tekst mv., der kan læses på, eller som ligger gemt bag hjemmesiden.

- Mosaic

Denne teknik blev i sin første udformning indbygget i et program, kaldet *Mosaic*. En første version af dette program blev stillet til almenhedens rådighed som såkaldt "freeware" (dvs. uden ophavsretlige betalingskrav). Produktet nød hurtigt udbredelse, idet det viste sig at have overkommet to barrierer, der hidtil har hindret en udstrakt brug af databaser blandt private brugere: Det var nu blevet lettere at *identificere* databaser (adressen behøver ikke nødvendigvis at være kendt, eftersom man springer fra sted til sted). Og ikke mindst gjorde programmet det lettere at *bruge* de identificerede databaser.

- Standarder

Www understøttes af en standard for, hvorledes teksten præsenteres af de forskellige informationsudbyderes databaser ("Homepages" eller på dansk: hjemmesider). Denne standard er HTML (HyperText Mark-up Language). En anden standard, HTTP (HyperText Transfer Protokol), definerer den måde, hvorpå information formidles via hypertekst-links. Det er således HTTP-marke-

ringerne, der indeholder den information, der sender brugeren fra en hjemmeside videre til en anden.

Kombinationen af hypertekst-teknikken og Internet-mediet gav grundlaget for opbygningen af the "World Wide Web" (også kaldet www). Betegnelsen illustrerer, at de mange computere på nettet udgør et verdensomspændende "spindelvæv". Når man taler om www sigtes altså til de computere, der via Internet stiller information til rådighed (som servere) over hele verden. Brugerens adgang til www er hans browser-program. Siden Mosaic blev udsendt i sin første version i 1992 er der kommet mange flere browserprogrammer til. Flere centrale udbydere har siden konkurreret om, at deres teknologi skulle sætte standarden for kommunikation på nettet, ganske som DOS satte standarden for 1980'ernes PC-teknologi og Windows for 90'ernes. I håbet om også at komme til at dominere denne del af IT-anvendelsen har verdens to største udbydere af browsere, Microsoft Inc. og Netscape Communications, stillet deres netbrowsere – Internet Explorer og Netscape Navigator – til fri afbenyttelse.

Det er navnlig udviklingen af www, der har fået Internet til at eksplodere. Den første web-server blev forbundet til nettet i 1990. Ved årtusindskiftet var tallet steget til 9.950.491 servere og med udgangen af 2004 var der registreret 56.923.737 web-servere.De seneste statistiske oplysninger findes på <http://www.zakon.org/robert/internet/timeline>. Det var i øvrigt "browserkrigen" mellem Netscape og Microsoft, der i sin tid gav anledning til konkurrenceretlig indgriben mod Microsoft, der i slagets første bølge, efter at være blevet overhalet af Netscape, valgte at indbygge sin browser "gratis" i sit Windows-styresystem.

Hjemmesider

De punkter, hvorfra og hvortil man kommunikerer på www, benævnes ofte *sites*, henholdsvis *hjemmesider*. Begge begreber beskriver informationsmængder på nettet, som præsenterer sig i grafisk form i overensstemmelse med en af de standarder, der er vedtaget for Internet, f.eks. i form af tekst, grafik og anden information, så man med det rette udstyr (grafikkort og højopløselig farveskærm) får hjemmesiden til at tage sig ud som en avanceret elektronisk opslagstavle. Inden for en given *site* (der f.eks. indehaves af et supermarked under adressen "www.supermarked.dk") kan brugeren herefter finde frem til et antal *hjemmesider* (homepages), der f.eks. repræsenterer de enkelte afdelinger. I det følgende benyttes ordet hjemmesider – for nemhed skyld – for såvel sites som hjemmesider.

Hjemmesider er typisk forsynet med *links*, hvorved brugeren fra enkelte punkter (fremhævet skrift) kan springe hen til andre

hjemmesider. Der er ingen grænser for, hvilken type information der kan holdes tilgængelig fra en hjemmeside eller for, hvordan denne kan stilles til rådighed for almenheden. Visse hjemmesider tjener rent markedsføringsmæssige formål (reklamer for produkter, omtale af virksomheden mv.). Andre virker som fora for personer med fælles interesser. Og endnu andre, f.eks. hjemmesider, der drives af akademiske institutioner eller offentlige myndigheder, tjener almennyttige formål. Ofte vil en virksomhed anvende sin hjemmeside til at varetage en flerhed af kommunikationsformål, f.eks. markedsføring, brugsanvisning, afhjælpning af fejl, kundesupport, opretholdelse af "brugerklubber" etc.

Der er ingen retlige begrænsninger i adgangen til at oprette hjemmesider på Internet og ej heller nævneværdige praktiske vanskeligheder herved. Derfor er det en enkel sag for selv mindre virksomheder eller enkeltpersoner at optræde "på nettet" med egen hjemmeside. Ved hjælp af standardprogrammel kan man i løbet af få timer klargøre en hjemmeside til offentliggørelse på Internet. En erhvervsvirksomhed, som ikke selv ønsker at stå for dette arbejde, kan i stedet henvende sig til en leverandørvirksomhed, der yder denne service som såkaldt "web-hotel".

Kommunikation til og fra en hjemmeside foregår delvis automatisk. Der er i sagens natur ikke tale om, at indehaveren af hjemmesiden "kigger med", når brugeren kalder op. Kommunikationen sker i overensstemmelse med, hvad hjemmesiden er programmeret til. I de programmer, der styrer hjemmesiden, er der typisk indbygget funktioner, der registrerer, hvilke brugere der kontakter hjemmesiden, og hvilke informationer der hentes derfra. En sådan registrering vil ofte være nødvendig for virksomhedens vurdering af, hvilke dele af hjemmesiden der er mest interesse for. Hvis hjemmesiden danner grundlag for kommunikation, som kan give anledning til retskrav (f.eks. betalingskrav), kan informationen dernæst tjene som bevisunderlag. Medaljens bagside er, at denne registrering af nogle opleves som en trussel mod forbrugerens integritet – navnlig, hvis oplysninger om, hvad, hvornår og hvordan forbrugeren har efterspurgt bestemte produkter, kompromitteres.

Supplerende litteratur

IT-litteraturen er beriget med mange gode og pædagogiske indføringer i teoretiske IT-principper og praktiske anvendelsesformer mv., som læseren bedst selv kan skaffe sig overblik over ved at besøge et velassorteret folkebibliotek. I det følgende omtales kun de værker, der særligt fokuserer på nogle af de emner, der er omtalt i teksten.

De grundlæggende principper bag *edb-programmering* findes beskrevet i de introducerende IT-værker, hvis antal er så overvældende, at det er muligt her at give nogen oversigt. Herudover henvises til ordforklaringerne i det meget værdifulde IT-leksikon, IT-lex (2001), forfattet af et bredt forfatterkollegium under faglig redaktion af Klaus Hansen.

Udviklingen indenfor de såkaldte kognitive videnskaber rummer en række særlige samfundspolitiske og etiske aspekter af teknologiens historie. Se herom bl.a. *Hubert Dreyfus*: What computers can't do (2nd ed., 1980) og af *Howard Gardner*: The mind's new science (2nd ed. 1987). Læren om struktureret programudvikling er bl.a. præsenteret hos *Stephen Biering-Sørensen m.fl.*: Struktureret program-udvikling (1988), s. 19. Se også *Beck, Monrad & Salomon* (1990), s. 12 ff.

Der findes en overvældende litteratur om de forskellige styresystemer, der gennem tiderne er udviklet. Historien om LINUX-styresystemets fødsel og udvikling er bl.a. fortalt i PC World 1/2000, s. 88 ff. Yderligere oplysninger herom kan hentes fra <www.kernel.org> og <www.linuxhq.com>.

Den, der ønsker at være nogenlunde jævnt holdt ajour med den teknologiske udvikling på IT-området, kan det anbefales at læse ugeavisen Computerworld, der giver den bredeste og samtidig bedst opdaterede information herom. I en lang række lande udgives tilsvarende (men ikke identiske) aviser med samme navn. Herudover kan man i tidsskrifter som Alt om Data og PC World læse mere specifikt, men dog forståeligt for lægmand, om enkelte IT-tekniske spørgsmål.

Der findes en lang række udmærkede redegørelser for den tekniske opbygning og udvikling af det Internet, vi kender i dag. Se f.eks. redegørelsen hos *John Palfrey* i 17 Harvard Journal of Law & Technology (2004) 418 ff.

Fra den amerikanske debat om edb-teknologiens sociale og filosofiske dimensioner kan navnlig fremhæves *Joseph Weizenbaum*'s klassiker: Computer power and human reason (1976), der rummer et stærkt og følelsesfuldt etisk angreb mod den teknologi-optimisme, der navnlig prægede 1960'ernes diskussion omkring disse kognitive systemer. Litteraturen herhjemme er navnlig kommet frem gennem 1980'erne, se bl.a. *Ole Fogh Kirkeby*: Etik, planlægning og videnbaserede edb-systemer (1988). Fra den filosofisk orienterede litteratur mærkes antologien

Kognition og sprog, redigeret af *Niels Ole Finnemann & Frederik Stjernfelt* (1992) med indlæg af bl.a. Claus Emmeche, samt temanummeret "Kognition og ånd" af tidsskriftet Litteratur & Samfund, 47-48 (november 1992) med indlæg af bl.a. Ib Ravn og Andreas Rischel.

Kapitel 4. SIKKERHED OG BEVISHÅNDTERING

4.1. Introduktion

4.1.a. Problemstillingen

Den foregående redegørelse tegner så småt billedet af de særlige problemer, den digitale teknologi giver anledning til, og som for en stor dels vedkommende reflekteres i denne fremstilling af dansk IT-ret. Inden denne fremstilling er det imidlertid hensigtsmæssigt at se på nogle af disse retsspørgsmål fra den *tekniske* side. I den tekniske emneverden er der for det første opbygget en terminologi og metode for behandlingen af centrale sikkerhedsspørgsmål, som også får betydning, når disse spørgsmål præsenterer sig i den juridiske fremstilling, jf. herom straks i det følgende. For det andet giver nogle af de tekniske løsningsprincipper anledning til retlige – og retspolitiske – problemstillinger.

4.1.b. De generelle temaer

IT-sikkerhed

I dagligsprogets betydning betegner ordet sikkerhed visheden for, at en ønsket tilstand vil blive opretholdt. Når den pågældende tilstand har relation til IT taler man om IT-sikkerhed. Dermed kommer IT-sikkerhed – også kaldet "datasikkerhed" og "edb-sikkerhed" – til at betegne den kvalitet, at et IT-system fungerer som forventet. Gør det ikke det, foreligger en såkaldt IT-sikkerhedsbrist. Sådanne brister vil ofte medføre skuffelser, økonomiske tab og besværligheder af forskellig art: Information fra systemet er f.eks. fejlbehæftet, utilgængelig eller skadevoldende (som ved flyovervågningssystemer, lukkeanordninger, signalsystemer mv.).

IT-sikkerhedsproblemer præsenteres ofte i fire kategorier.

Tilgængelighed

Den første kategori angår sikkerheden for, at data er tilgængelige for rette vedkommende. Sikkerhed er her synonymt med driftsmæssig stabilitet. I henseende til denne del af sikkerhedsbegrebet er der ikke den store forskel mellem IT og anden teknologi. At man alligevel ofte fremstiller IT-sikkerhedsrisici som noget

særligt, skyldes skrøbeligheden af det digitale medium. Der er flere faremuligheder og et større spring mellem den tilsyneladende lille tue (f.eks. berøring af en følsom elektronisk komponent med en hånd, ladet med statisk elektricitet) og det store læs (komponentens ødelæggelse og heraf følgende flaskehalsvirkninger for hele systemet). Da systemernes hardware bl.a. bygger på finmekanik, kan også utilsigtede fugt- og varmepåvirkninger true IT-sikkerheden. De menneskelige trusler kan enten skyldes uforsigtighed (fejlagtig indtastning af data eller kommandoer) eller forsætlige handlinger (uautoriseret indtrængen i et system med påfølgende fjernelse, ændring, ødelæggelse, anvendelse eller offentliggørelse af data).

- retlige problemer

Angreb mod et IT-systems funktionalitet vil i almindelighed kunne straffes efter de almindelige regler om hærværk, jf. strfl. § 291, eller efter de skærpede regler om forstyrrelse af kommunikations- og samfærdselsmidler mv., jf. § 193.

- forebyggelse

I relation til de *utilsigtede* nedbrud mv. kan sikkerhedsmålsætningen tilgodeses gennem løbende forebyggende og afhjælpende *fejlretning* og anden *vedligeholdelse* samt ved at sikre en løbende fyldig *dokumentation*. Dernæst kan systemet sikres mod kriminelle angreb gennem fysisk eller logisk afskærmning, jf. herom straks nedenfor. En sådan afskærmning kan ligeledes imødegå risikoen for oversvømmelse og lynnedslag. Ligeledes kan der være behov for at sikre systemets forsyning med elektricitet (f.eks. gennem nødstrømsanlæg) og vand (til brug for afkøling).

- afhjælpning

Hvis nedbruddet er en kendsgerning, må en sikkerhedspolitik søge at afhjælpe de opståede problemer bedst muligt. Man må her sondre mellem genskabelse af systemet (hardware såvel som software) og dets data. Sikkerheden for, at systemets *hardware* kan genskabes, kan opnås ved aftale med leverandøren om garanterede erstatningsleverancer og med tredjeparter om ret til at drive systemerne fra en anden installation under en genopbygningsfase, jf. om disse såkaldte backup-aftaler i afsnit 4.4.d. Når det gælder genskabelse af *data* og *programmel* er den typiske modforanstaltning løbende *backup*-kopiering (også kaldet sikkerhedskopiering). Ved backup-kopiering af data med *personoplysninger* må de almindelige regler i lov om behandling af personoplysninger (LBP) iagttages, herunder sikkerhedskravene i § 41. Backup-kopiering af programmel kan altid finde sted, jf. den præceptive hjemmel hertil i ophl. § 36, stk. 1, nr. 2. For virksomheder, der er afhængige af deres IT-baserede informationer, er daglig backup-kopiering sædvanlig, typisk udført i nattetimerne, hvor systemerne ikke er i hyppig anvendelse. I særligt kritiske

systemer sker der en løbende backup-kopiering ved, at hele systemet (dvs. såvel programmer som data) "spejles" (dvs. løbende kopieres) over til andet medium.

Fortrolighed

I en anden kategori falder tilfælde, hvor data uberettiget er kommet uvedkommende i hænde således, at der altså sker brud på fortroligheden af de data, der behandles i systemet (også kaldet *konfidentialitet*). Vel kendes dette sikkerhedstema også uden for IT-området (f.eks. i form af brud på en almindelig tavshedsforpligtelse eller særlig hemmeligholdelsespligt), men pga. det digitale mediums kompleksitet har temaet en særlig betydning på IT-området: Ikke alene er der blevet flere muligheder for den, der uberettiget ønsker at "lytte med"; det er også blevet vanskeligere at kontrollere, om en aflytning har fundet sted.

En detaljeret oversigt over sådanne risici findes hos *Grabosky & Smith* (1998), s. 19 ff. om retsstridige aflytningsteknikker. Foruden de mere iøjnefaldende veje til en sådan aflytning, der f.eks. består i afluring af passwords eller franarring af samme ved såkaldt "social engineering", omtaler forfatteren de – for mange sikkert overraskende – muligheder, der består for med simpelt og prisbilligt udstyr at aflæse information ved hjælp af de elektromagnetiske bølger, der udsendes fra en edb-skærm (s. 38). Denne form for aflytning har en parallel ved almindelig telefoni, der udføres ved håndholdte trådløse telefoner i hjemmet. De ældre – men fortsat meget udbredte – modeller af denne art betjener sig af analoge radiobølger, der uden videre kan aflyttes af skanningsudstyr, der kan erhverves lovligt i handelen. De strafferetlige problemer, der er forbundet med sådanne handlinger, omtales i afsnit 17.4.a.

- retlige problemer

Angreb, der realiserer denne type risici vil, ofte – men ikke altid – forekomme i forbindelse med et egentligt retsbrud. To væsentlige eksempler herpå er overtrædelser af straffelovens regler om fredskrænkelser (og herunder navnlig den såkaldte hackerparagraf i straffelovens § 263, stk. 2) og tilsidesættelse af regler om beskyttelse af personoplysninger, jf. LBP. Til samme kategori henregner man typisk også krænkelser af immaterielle rettigheder (f.eks. bestående af ulovlig kopiering af software), ud fra den betragtning, at der også her sker en utilsigtet (uhjemlet) tilegnelse af information (f.eks. i form af en retsstridig eksemplarfremstilling eller spredning).

- forebyggelse

Når det gælder de midler, der kan tages i brug mod sådanne risici, sondrer man mellem logiske og fysiske sikkerhedstiltag. Et praktisk eksempel på et *fysisk* sikkerhedstiltag er fysisk sikring af bygninger, adgangskontrol og elektromagnetisk afskærmning. Et eksempel på *logiske* sikkerhedsforanstaltninger er brug af logisk adgangskontrol, hvorved brugeren afkræves et password bestå-

ende af et antal tal og/eller bogstaver for at få adgang til systemet. Passwordet kan eventuelt være indlæst på et magnetisk medium, f.eks. et magnetstribekort, som kendes fra de fleste kreditkort. Password-sikring er derimod mindre velegnet til at sikre mod uberettiget adgang til data, der transmitteres over en teleforbindelse. Sikkerheden ved password-beskyttelsen står og falder med passwordets styrke (fornavnet på brugeren selv eller et nært familiemedlem anses på forhånd som et usikkert password!) og med hvordan man omgås det. En anden hyppigt anvendt sikkerhedstjeneste er her brugen af kryptering.

Se nærmere om begrebet kryptering afsnit 4.2. Som her anført kan man betragte kommunikation, der baseres på kryptering, således, at de kommunikerende parter indfører et særligt *sprog*, der har den anvendte krypteringsalgoritme og de hertil hørende unikke krypteringsnøgler som fællesnævner. Kryptering kan ikke alene finde sted på kommunikationsprocessens applikationsniveau (dvs. i det niveau, som de kommunikerende parter er sig direkte bevidst, som f.eks. når en statshemmelighed transmitteres til en fjern ambassade), men også i relation til de enheder, der benyttes i kommunikationsprocessen (som f.eks. når de servere, der styrer kommunikation via Internet-hjemmesider, foretager kryptering ved brug af SSL-protokollen).

- kopibeskyttelse

Risikoen for uønsket kopiering af digital information (data såvel som programmel) kan imødegås ved *kopibeskyttelse* (*copy protection*) eller ved tiltag, der pga. de besværligheder, man påfører brugeren ved en uautoriseret kopiering (f.eks. anmodning om indtastning af et ord, der står på et nærmere angivet sted i en omfattende manual!), nedsætter incitamentet hertil (*copy discouragement*). Begge teknikker bygger på et princip om logisk adgangskontrol. Leverandøren indbygger en logisk betingelse i sit program, der skal være opfyldt for, at programmet kan anvendes. I visse tilfælde skal betingelsen opfyldes af brugeren i form af et password. I andre kan den knytte sig til et medium, der fungerer brugeruafhængigt, f.eks. en magnetstribe på et kreditkort.

Ægthed

Et tredje sikkerhedstema angår sikkerheden for, at data hidrører fra den angivne kilde, også kaldet originalitet, autenticitet eller ægthed. Når data overføres under en kommunikationsproces, ønsker de kommunikerende parter typisk sikkerhed for, hvem den anden part er.

Når man bruger ordet originalitet om denne egenskab, bør man være opmærksom på, at sprogbrugen her er anderledes end i juridisk terminologi. Hvor det retlige originalitetsbegreb (således som dette f.eks. anvendes, når man i ophavsretten taler om originalværket og i gældsbrevsretten om det originale pantebrev) knytter sig til tilstedeværelsen af en bestemt informationsmængde (bits) på et bestemt

medium (atomer), er det originalitetsbegreb, der anvendes inden for læren om IT-sikkerhed, knyttet til rent kommunikative aspekter:

Data er originale, hvis de stammer fra den angivne kilde, uanset om de pågældende data er fuldstændigt identiske med andre data.

Integritet

Sikkerheden for, at en meddelelse i sin nu foreliggende form svarer til det indhold, den havde på afsendelsestidspunktet, benævnes almindeligvis som sikkerheden for integritet. Dette sikkerhedstema er langt større ved brug af digitale medier end inden for traditionelle medier som f.eks. papir. Hvor det ofte er let at konstatere, om et dokument er blevet forfalsket, kan en digital meddelelse på et magnetisk medium som udgangspunkt forfalskes til perfektion, eftersom det ene eksemplar af meddelelsen er fuldstændigt identisk med det andet.

Opdelingen er ikke udtryk for nogen absolut oversigt over IT-risikobilledet. Bl.a. kan det altid diskuteres, hvor grænsen går mellem IT-sikkerhed og anden sikkerhed (f.eks. mod brand, vandskade el.lign.). Problemerne tangeres lejlighedsvis i den IT-retlige litteratur, se f.eks. *Seipel* (2001), s. 237 ff. For en kort indføring i sikkerhedsproblematikken henvises til *IT-sikkerhedsrådet*: Danmarks IT-sikkerhedspolitik, et baggrundspapir (1996), navnlig s. 16 f.

4.1.c. Aktualitet

Interessen for IT-sikkerhedsproblemerne er vokset i takt med den teknologiske udvikling. Udviklingen har for det første medført, at IT kontrollerer stadigt mere vitale og kostbare processer end tidligere. Dernæst har sammensmeltningen af IT og telekommunikation ført til, at IT-systemer, hvis komponenter knyttes sammen over afstande, ikke udelukkende kan sikres gennem individuelle foranstaltninger. Interessen for IT-sikkerhedsanliggender er dermed blevet et lovgivningsanliggende, der berøres såvel nationalt som internationalt.

IT-sikkerhedsrådet

I 1995 nedsatte regeringen et IT-sikkerhedsråd, der bl.a. fik til opgave at bidrage til at formulere en overordnet dansk sikkerhedspolitik for anvendelsen af IT og telekommunikation. Rådet fungerede gennem to treårsperioder frem til 2002, hvor det formelt blev nedlagt. Foruden en række konkrete udtalelser har IT-Sikkerhedsrådet i november 1996 udsendt et Oplæg til en dansk it-sikkerhedspolitik, i 1998 en vejledning om privatliv på Internet, i 1999 en Vejledning om digitale dokumenters bevisværdi og i 2000 en vejledning om praktisk brug af kryptering af digital signatur. I 2002 nedsatte regeringen et Råd for IT-sikkerhed, som fik til opgave at varetage nogenlunde samme opgaver som det tidligere IT-sikkerhedsråd. Dette råd har blandt andet udsendt et

antal vejledninger, for eksempel om trådløse netværk, om spyware, om firewall-teknologi og om brug af e-post og Internet på arbejdspladsen. Derudover har rådet videreført det statistiske undersøgelsesarbejde om datasikkerheden i Danmark, der blev igangsat af det tidligere IT-sikkerhedsråd. Se i det hele <www.rfits.dk>.

EU

EU-kommissionen har i flere sammenhænge forsøgt at understøtte arbejdet med IT-sikkerhed. Den 7. april 1995 afgav rådet en henstilling om ensartede kriterier for vurdering af informationsteknologisk sikkerhed (95/144/EF), EFT 1995 L 93/27. Henstillingen går ud på, at der i en foreløbig periode på to år vedtages kriterier for vurdering af sådan sikkerhed som led i "visse vurderings- og certificeringsordninger", således at de øjeblikkelige vurderingsbehov i forbindelse med handel og brug af IT-produkter og -tjenester kan dækkes. Samtidig anbefales det, at den særlige arbejdsgruppe vedrørende IT-sikkerhed, SOG-IS, søger at tilstræbe en international harmonisering og standardisering for kriterier til IT-sikkerhed. Indtil dette ønske om harmonisering er opnået henstilles det, at der træffes bilateral aftale mellem medlemsstaterne om anerkendelse af sikkerhedsvurderingscertifikater. Som et markant udtryk for EU's IT-sikkerhedspolitiske arbejde kan nævnes direktiverne om persondatabeskyttelse (95/46/EF) og om elektronisk signatur (99/93/EF).

Allerede i dag findes der talrige regler, der kan anskues som udtryk for ønsket om at tilvejebringe en given grad af IT-sikkerhed. Som følge af navnlig EU-myndighedernes bevågenhed kan der fremover ventes mange flere regler af denne karakter. Der er imidlertid ingen juridisk tradition, hverken i IT-retten eller på andre retsområder, for at systematisere regler om sikkerhed under ét. Visse sikkerheds-relaterede regler (de erstatningsretlige regler, betalingsmiddelloven, produktsikkerhedslovgivningen, EMC-lovgivningen) har en *præventiv* funktion med det primære formål at tilskynde til "sikker" adfærd. Andre (lovgivningen om persondatabeskyttelse) har i højere grad *regulerende* karakter ved at afklare parternes retsforhold, når forventningerne til en IT-funktion ikke er indfriet. Visse regler (de immaterialretlige) sikrer *indehaveren* af et produkt eller et system mod skader forvoldt på eller angreb forvoldt mod dette. Andre – og primært de førnævnte offentligretlige regler af præventiv art – søger navnlig at sikre mod skader mv. på *tredjemand*.

Enkelte forsøg er dog gjort på at systematisere reglerne om IT-sikkerhed, se f.eks. *Robert Bigelow* i 12 CLSR 361 ff. (1996) og 13 CLSR 87 ff. (1997).

4.1.d. Faktisk IT-sikkerhed

Oversigt

IT-sikkerhed kan opnås gennem faktiske foranstaltninger, der enten udfolder sig *omkring* det pågældende system eller i kraft af funktioner *i* det. Sådanne foranstaltninger kan hindre forskellige sikkerhedstrusler i at blive aktuelle eller minimere resultatet af utilsigtede følger. Sikkerhed for tilgængelighed kan f.eks. opnås ved at etablere driftssikre systemer (evt. suppleret med nødstrømsanlæg, erstatningssystemer mv.). Hertil må føjes brug af hensigtsmæssige procedurer for backup-kopiering (evt. suppleret med pengeskabe, eksterne deponeringsordninger mv.). Sikkerheden mod indtrængen i IT-systemer kan tilvejebringes gennem fysisk adgangskontrol, personalekontrol eller logisk adgangskontrol som f.eks. kryptering, jf. nærmere herom i afsnit 4.2. Sikkerheden mod udefra kommende naturkræfter kan f.eks. bestå i installering af lynafledere, brandsikringer samt forskellige former for magnetiske indkapslinger.

Afvejningen

Inden for forskellige IT-discipliner har man forsøgt at anvende muligheden for hurtig og præcis behandling af data til at imødegå dens risici. For mange af de særlige sikkerhedsproblemer, som den digitale teknologi giver anledning til, gælder det, at "The answer to the machine is the machine": at evnen til at foretage beregninger effektivt og hurtigt, som moderne IT giver mulighed for, også rummer muligheden for at foretage sådanne beregninger med rent sikkerhedsmæssige formål, uden at dette "koster" brugeren nævneværdige ressourcer. Gennem automatisk sikkerhedskopiering, "spejling" af datalagre, paritetskontrol af filer (dvs. løbende kontrol med disses størrelser), skjult digital signering og heraf følgende kontrol med de tabeller, der styrer datahåndteringen, kan man løse en ganske stor del af de sikkerhedsmæssige behov, der gør sig gældende.

Den egentlige barriere, og det væsentligste modhensyn, der indgår i en sådan afvejning, er imidlertid ofte bekvemmelighedshensynet: Et "godt" password er nærmest pr. definition svært at huske og kræver derfor andre foranstaltninger (f.eks. nedskrivning under sikrede former eller teknikker til passwordgenkendelse). De procedurer, man skal gennemgå i forbindelse med adgangskontrol, vil ofte føles som bureaukratiske i en organisation, hvor man efterhånden kender vagten.

Sårbarheds-analyse

Et sikkerheds-koncept må tilpasses de risici, der er aktuelle for den pågældende bruger, hvilket afdækkes gennem en såkaldt sårbarhedsanalyse. Hvor omfattende og følelige, IT-sikkerhedsbrister kan blive, beror bl.a. på, hvor vitale de pågældende data er. Meget informationsafhængige virksomheder, f.eks. inden for den finansielle sektor står og falder med deres IT-systemer. Bl.a. derfor er det navnlig her, man finder de mest veludviklede metoder til IT-sikkerhed. For andre virksomheder kan det derimod være relevant at foretage en nøje afvejning af de tekniske løsninger, der ligger for, overfor de omkostninger af økonomisk og/eller administrativ karakter, som sikkerhedsforanstaltningen vil koste (*cost/benefit-analyse*). For en lang række trusler vælger man – ofte ubevidst, men sjældent helt uberettiget – at tage risikoen for, at truslen realiseres, frem for at investere de store beløb, der vil være forbundet med at etablere total sikkerhed.

Der findes ingen absolutte "løsninger" på et sikkerhedsproblem. De forholdsregler, virksomheden vælger, kan aldrig stå alene. Derfor er det vigtigt, at beslutningstageren har et klart overblik over, hvilke funktioner konceptets enkeltbestanddele tjener. En brandalarm forhindrer f.eks. ikke brande i at opstå, men kan formidle information om en opstået brand så hurtigt og effektivt, at branden kan bekæmpes i tide.

En væsentlig del af sikkerhedsarbejdet går ud på at analysere forskellige systemers sårbarhed. Til brug for dette arbejde er der udviklet forskellige teknikker, f.eks. den svenske SårBarheds Analyse (SBA) og den engelske Security Risk Analysis and Management Methodology. Tidsskrifter om IT-sikkerhed beretter undertiden om, hvordan en tilsyneladende formfuldendt overholdelse af sikkerhedsforskrifter helt har mistet sin værdi pga. manglende forståelse for de kritiske aspekter. Som et grotesk eksempel kan nævnes et tilfælde, hvor den backup ansvarlige udførte sit arbejde ved dagligt at klæbe disketterne fast i pengeskabet ved hjælp af magneter!

Arbejdet med IT-sikkerhed er en løbende proces, der på den ene side søger at udnytte kendskab til aktuelle sikkerhedsrisici, samtidig med at den på den anden side søger at foregribe fremtidige risici. I mange tilfælde vil sikkerhedsarbejdet basere sig på ukendte formodninger om sandsynligheden af en risiko. F.eks. har usikkerheden om risikoen for elektromagnetisk stråling på den ene side ført til EU-regler vedrørende elektromagnetisk kompatibilitet, men derimod ikke til regler om stråling fra skærmterminalerne.

Certificering

I takt med den stigende interesse for kvalitetssikring gennem certificering er det blevet stadigt mere almindeligt, at virksomheder indhenter udtalelser fra tredjemand om det IT-sikkerhedsniveau, der er gældende. Et eksempel herpå er de erklæringer, som statsautoriserede revisorer afgiver i henhold til FSR's revisionsvejledninger. I USA, hvor mange virksomheder tillægger værdien af immaterielle rettigheder større betydning end herhjemme, er det ikke ualmindeligt, at advokatfirmaer gennemfører såkaldt "intellectual property audits" eller ved at gennemføre såkaldte *compliance*-undersøgelser, der fokuserer på virksomhedens licensforhold. Som grundlag for en sådan udtalelse gennemgår advokatfirmaet virksomhedens produktsortiment med henblik på at undersøge, om immaterielle rettigheder i nødvendigt omfang er sikret. Herudover gennemgås licens- og vedligeholdelsesaftaler, salgsmateriale samt aftaler med uafhængige konsulenter mv., idet det bl.a. kontrolleres, om vital kildetekst til programmel leveret af tredjemand er behørigt deponeret. Endelig gennemgås forholdet til medarbejdere i henseende til afståelse af immaterielle rettigheder og ret til konkurrerende virksomhed efter ansættelsen. I samme forbindelse gennemgås medarbejdermanualer og interne sikkerhedsforskrifter.

4.1.e. Særlige regler

Afvejningsproblemet

Lovgivningen, navnlig om persondatabeskyttelse, indebærer ofte begrænsninger i friheden til at vælge et sikkerhedskoncept. F.eks. afskærer LBP muligheden for at registrere visse sikkerhedsrelevante personoplysninger om personalet (f.eks. telefonsamtaler, tidligere kriminelle forhold mv.). Ligeledes kan anvendelsen af biometriske systemer til adgangskontrol indebære en registrering af følsomme helbredsoplysninger, som er afskåret. Det er tankevækkende, at et forslag om at etablere et såkaldt borgerkort som løsning på en række centrale sikkerhedsmæssige problemer ved digital kommunikation med det offentlige og mellem borgerne måtte opgives på grund af bekymringer om en heraf følgende overvågning mv. Men det må ventes, at der i fremtiden vil opstå et stort antal situationer, hvor sådanne interesser må afvejes mod hinanden.

I sit oplæg fra november 1996 påpeger IT-sikkerhedsrådet den væsentlige IT-sikkerhedspolitiske opgave, der ligger i at foretage sådanne afvejninger, se herved oplægspapiret, s. 15 f. og mere udtømmende baggrundspapiret s. 29 ff., om de enkelte IT-sikkerhedspolitiske hensyn, og s. 35 ff. om afvejningsproblemet.

I det følgende omtales nogle regler, der i forskellige henseender regulerer – og i den forbindelse understøtter – sikkerhedsmæssige løsninger.

Erstatningsregler

De regler, der sikrer tredjemand mod følgerne af en IT-sikkerhedsbrist, må først og fremmest udledes af den almindelige erstatningsret, jf. kapitel 18. I praksis udgør de erstatningsretlige regler formentlig en af de væsentligste motivationsfaktorer på IT-området. Hvor der typisk gælder en øvre grænse for omfanget af de fiskale eller strafferetlige retsfølger, gælder dette principielt ikke for de erstatningsretlige, sml. dog EAL § 24. Alene tanken om de vidtrækkende beløb, der kan blive følgen af en IT-fejl, vækker med god grund bekymring. Ingen IT-systemer er fejlfri (endsige kan være det), og de fejl, der kan opstå, kan som følge af kopieringsmuligheden reproduceres i det uendelige. Navnlig har leverandørerne – af forståelige grunde – været bekymrede for, om salg af standardprogrammel på det åbne marked er undergivet et objektivt produktansvar. I givet fald vil dette uden tvivl indgå som en væsentlig faktor såvel ved valget af de produkter, producenten sender på markedet, som ved tilrettelæggelsen af selve produktionsprocessen.

Mere detaljerede regler om IT-sikkerhed kender IT-retten kun på ganske enkelte områder.

LBP

LBP kapitel 11 indeholder en generel regulering af kravene til behandlingssikkerhed ved behandling af personoplysninger. Ifølge § 41 skal den dataansvarlige og/eller databehandleren træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. For oplysninger, som behandles for den offentlige forvaltning, og som er af interesse for fremmede magter (f.eks. CPR-registeret), skal der træffes foranstaltninger, der muliggør bortskaffelse og tilintetgørelse i tilfælde af krig el.lign.

Ved bekendtgørelse nr. 528 og 535 af 15. juni 2000 har Justitsministeriet fastsat nærmere regler om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for henholdsvis den offentlige forvaltning og domstolene. Der er tale om rammebestemmelser, der bl.a. pålægger den dataansvarlige at fastsætte nærmere interne sikkerhedsbestemmelser, herunder om organisatoriske forhold (hvem har sikkerhedsansvaret for hvad), fysisk sikring, adgangskontrol og autorisationsordninger. For behandling af personoplysninger i den private sektor samt for den

offentlige forvaltnings behandling af personoplysninger i manuelle register gælder lovens regler om sikkerhed umiddelbart.

Som nævnt gælder de nævnte forpligtelser såvel for databehandlere som for dataansvarlige. For at sikre, at databehandleren rent faktisk efterlever disse lovkrav, foreskriver § 42, at den dataansvarlige ved overladelsen af databehandlingsopgaven til databehandleren skal sikre sig, at vedkommende *kan* træffe de nævnte sikkerhedsforanstaltninger. Ligeledes foreskriver bestemmelsens stk. 2, at der skal foreligge en *skriftlig aftale* mellem parterne herom. Ifølge § 41 må personer og virksomheder, der udfører arbejde under den dataansvarlige eller databehandleren (jf. om disse begreber LBP § 3, nr. 4-5), og som får adgang til oplysninger, kun behandle disse efter instruks fra den dataansvarlige. Bestemmelsen modvirker, at personer, der udfører opgaver med persondatabehandling på den dataansvarliges eller databehandlerens vegne (som altså ikke selv formodes at have ret til at behandle de pågældende oplysninger), ikke disponerer på egen hånd, og i konsekvens heraf, at ansvaret for denne databehandling kan rettes mod den dataansvarlige eller databehandleren.

Visse betalingsmidler

Efter § 4, stk. 2, i lov om visse betalingsmidler skal et betalingssystem indrettes og virke således, at der sikres brugerne gennemsigtighed, frivillighed, beskyttelse mod misbrug samt fortrolighed om brugerens anvendelse af betalingsmidlet. Bestemmelsen fastslår i tillæg hertil, at der løbende skal træffes de juridiske, organisatoriske, driftsmæssige, tekniske og sikkerhedsmæssige foranstaltninger, som er nødvendige for, at der er tale om et sikkert og velfungerende betalingssystem. Forbrugerombudsmanden påser, at betalingskortsystemer indrettes og virker således, at der sikres brugerne overskuelighed, frivillighed og beskyttelse mod misbrug og at fornødne kontrol-, sikkerheds- og korrektionsprocedurer er etableret og skal – om muligt ved forhandling – søge eventuelt kritisable forhold bragt til ophør. Se i det hele hertil *Susanne Karstoft*: Lov om visse betalingsmidler med kommentarer (2001), s. 57 ff.

Telebekendtgørelsen

Ifølge § 28 i bekendtgørelse nr. 638 af 20. juni 2005 om udbud af elektroniske kommunikationsnet og tjenester (*telebekendtgørelsen*) skal udbydere af offentlige telenet eller teletjenester sikre, at trafikdata vedrørende slutbrugere slettes eller anonymiseres efter samtalens afslutning, jf. dog stk. 2-5. Ligeledes fastslår bekendtgørelsens § 31, at udbyderne med henblik på sikring af netsikkerheden skal træffe passende tekniske og organisationsmæssige foranstaltninger for at beskytte de udbudte tjenester.

Dette skal om nødvendigt ske i samarbejde med ejeren eller udbyderen af det anvendte telenet.

Nøglecentre

Ved bekendtgørelse nr. 923 af 5. oktober 2000 er der givet regler om sikkerhedskrav til nøglecentre (dvs. certificeringscentre, jf. herom i afsnit 4.2). Bekendtgørelsen indeholder en i det væsentligste formel regulering af sikkerhedsprocedurerne i et nøglecenter. Således pålægges nøglecentret at udarbejde en *certificeringspolitik* (CP), som angiver det sikkerhedsniveau, nøglecentret anvender i forbindelse med udstedelse og administration af kvalificerede certifikater, § 2, stk. 1. Dernæst skal nøglecentret i en *certificeringspraksis* (CPS – "Certification Practice Statement") beskrive de procedurer, som nøglecentret og de virksomheder og myndigheder, som nøglecentret har outsourcet opgaver til, anvender i forbindelse med udstedelse og administration af kvalificerede certifikater, § 2, stk. 2. Begge dokumenter skal godkendes af nøglecentrets daglige ledelse. De materielle krav til nøglecentrets sikkerhedsniveau er angivet i en retlig standard, jf. § 3. Således skal nøglecentret "træffe passende foranstaltninger for at sikre, at nøglecentrets drift hurtigst muligt kan genoptages i tilfælde af systemnedbrud, såfremt nøglecentrets private nøgle er blevet kompromitteret, eller der er mistanke herom".

Bogføring

I tilknytning til den bogføringsretlige generalklausul, jf. § 6, stk. 1, 1. pkt., i lov nr. 1006 af 23. december 1998 om bogføring, foreskriver bestemmelsens andet pkt., at bogføringen skal tilrettelægges og udføres således, at regnskabsmaterialet ikke ødelægges, bortskaffes eller forvanskes, ligesom det skal sikres mod fejl og misbrug.

NATO

I Statsministeriets cirkulære nr. 204 af 7. december 2001 er der givet detaljerede regler om, hvorledes oplysninger, der er af fælles interesse for NATO-landene, som er klassificerede eller i øvrigt af sikkerhedsmæssig betydning, sikres. Cirkulæret, der finder anvendelse inden for forsvaret, fastslår en række klassifikationsgrader og hertil hørende regler om, hvem der kan få adgang til informationer inden for de enkelte klassifikationsgrader, og hvordan de skal sikres. Hvad angår de NATO-relaterede oplysninger, er Danmark forpligtet til at yde sådanne oplysninger en særlig beskyttelse i henhold til en aftale mellem NATO-landene. Denne pligt er præciseret i et NATO-dokument. Reglerne er for så vidt obligatoriske, men kan finde anvendelse vedrørende oplysninger, hvor der i øvrigt består en offentlig beskyttelsesinteresse.

DS 484-1

I forbindelse med de retsregler, der på disse forskellige områder regulerer IT-sikkerheden, er det relevant at nævne den Norm for edb-sikkerhed, som Dansk Standard har udstedt den 21. janu-

ar 2000. Normen er udarbejdet med udgangspunkt i de krav, der er defineret i den britiske standard BS 7799, Code of Practice for Information Security Management, men indeholder en række sikringsforanstaltninger, der ikke er indeholdt i dette dokument. Formålet med normen er at skabe et grundlag for virksomhedens sikkerhedsmæssige målsætning, der bl.a. kan fungere som referenceramme i beslutninger om anskaffelse og implementering af IT-løsninger. Det er en gennemgående tanke i denne og andre normer om IT-sikkerhed, at det er *ledelsen* i den pågældende virksomhed (og altså ikke driftsfunktionen), der har ansvaret for disse beslutninger. Ved denne angivelse af en ansvarlig personkreds adskiller denne norm sig fra andre *tekniske standarder*, der almindeligvis blot beskriver kravene til en funktion eller procedure.

Systemrevision

Talrige lovregler, bl.a. inden for det finansielle område, indeholder regler om gennemførelse af såkaldt systemrevision. Eksempler herpå er bekendtgørelse nr. 254 af 10. april 2005 om systemrevisionens gennemførelse i fælles datacentraler og bekendtgørelse nr. 1001 af 7. decemer 2001 om systemrevisionens gennemførelse i værdipapircentraler samt § 5, stk. 2, i lov om elektroniske signaturer (LES), der foreskriver systemrevision gennemført i nøglecentre (CA'er), der udsteder kvalificerede certifikater.

En systemrevision indebærer, at der udpeges en udefra kommende troværdig tredjepart – typisk en statsautoriseret revisor med særlig uddannelse – som gennemgår de IT-systemer, der er afgørende for troværdigheden af de data, der anses for kritiske i det pågældende system. Denne gennemgang sker på grundlag af en særlig systemrevisionsinstruks og i samarbejde med en systemrevisionsafdeling, der er funktionelt adskilt fra drifts- og regnskabsfunktionerne i den pågældende organisation. I erklæringen udtaler den udpegede systemrevisor sig om, hvorvidt den samlede data-, system- og driftssikkerhed efter systemrevisors opfattelse må anses for betryggende og i overensstemmelse med de regler, der gælder i medfør af det pågældende lovgrundlag. Anmærkninger i denne erklæring vil i almindelighed resultere i en pligt for den daglige ledelse og bestyrelsen til at reagere. Tilsidesættes denne pligt kan der tænkes at indtræde såvel strafsom erstatningsansvar.

4.2. Kryptering og digital signatur

4.2.a. Det tekniske problem

Når digital information fremstår med sin karakteristiske løse tilknytning til et medium, opstår risikoen for, at disse data tilegnes af uvedkommende (tab af fortrolighed) eller at data ændres uautoriseret på en måde, som den rette bruger ikke kan konstatere. Sådanne risici kan både aktualisere sig under *kommunikation*, og når data foreligger *lagret* på mediet. Angreb på lagrede data kendes bl.a. fra den form for kriminalitet, der almindeligvis benævnes *hacking*. Ved digital kommunikation, hvad enten der er tale om digital telefoni (GSM-telefoni), e-post, web-surfing, EDI eller andet, sker der en udveksling af bitstrenge, der i kraft af de anvendte protokoller og sprog sammensætter sig som menneskelæsbar tekst, grafik, billeder, lyd etc. Hvis sådanne bitstrenge sendes gennem ubeskyttede netværk (f.eks. som radiosignaler gennem luft eller som TCP/IP-segmenter via Internet), opstår en række særlige sikkerhedsproblemer. Der er almindelig enighed om, at måden til at beskytte sådanne data på er ved brug af kryptografiske funktioner.

Fortrolighed

Som allerede nævnt kan sikkerheden mod tab af fortrolighed tilvejebringes gennem teknikker, der enten afskærer den fysiske *adgang* til det system, der indeholder data (f.eks. gennem adgangskontrol mv.), lægger logiske begrænsninger på muligheden for at komme ind i systemet (gennem brug af passwords mv.) eller som *modificerer* de pågældende data, således at de kun er forståelige for brugere, der kender den procedure, hvorigennem denne modifikation har fundet sted (kryptering).

I tillæg til disse førnævnte sikkerhedsmål (tilgængelighed, fortrolighed, ægthed og integritet) opstår der to yderligere sikkerhedsspørgsmål, når man vil anvende digital kommunikation som grundlag for aftalestiftelse mv.

Uafviselighed

For det første vil der ofte være behov for at skulle bevise, at meddelelsen er afsendt henholdsvis modtaget. I papirets verden kan behovet for denne uafviselighed løses ved udstedelse af kvitteringer eller brug af anbefalede breve. I papirets verden markeres meddelelses-uafviselighed, dvs. sikkerheden for, at indholdet ikke har ændret sig siden afgivelsen, ofte ved en *underskrift*, der typisk placeres på sidste side, eller ved initialisering af hver side af dokumentet.

Til sammenligning opfylder skriftlige signaturer (under*skrifter*) langt fra altid behovet for at fastslå afgiverens *identitet* og

meddelelsens *integritet*. At en underskrift er ulæselig fratager den dog ikke sin gyldighed, jf. *U 1978.856 Ø*, hvor der kunne iværksættes vekselsag, selv om underskriften var ulæselig, idet vekselunderskriverens identitet kunne fastslås. Tinglysningspraksis går i samme retning, jf. *U 2000.1635 ØLK*, hvor en underskrift på et pantebrev fandtes behørig, selv om den ikke indeholdt underskriverens fulde navn (som derimod var angivet ved maskinskrift).

Tinglysningssystemet bygger på et princip, hvorefter underskriverens identitet sikres gennem vitterlighedsvidner. Da et vitterlighedsvidne kan substitueres (hvad underskriveren i sagens natur ikke kan), og da vidnet forventes at indtage rollen som troværdig tredjepart, stiller tinglysningspraksis i visse henseender strengere krav til vitterlighedsvidnet end til dokumentets udsteder. Således forlanges det normalt, at vitterlighedsvidner underskriver skøder og pantebreve med deres almindelige personlige underskrift, se *U 2001.1947 ØLK*. Samme krav behøver man derimod ikke stille til udstederen, når dennes underskrift netop er bevidnet af to vitterlighedsvidner, se *U 2000.1635 Ø* (hvor debitors underskrift på pantebrev var behørig, selvom den ikke indeholdt fulde navn) og *U 2002.635 VLK* (hvor debitor havde underskrevet et pantebrev med blokbogstaver, "men dog med et vist personligt præg").

I praksis påføres mange underskrifter ved rent formelle handlinger (f.eks. til opfyldelse af regler om prokura i en virksomhed). Dette har formentlig været medvirkende til en stigende anerkendelse af automatiske underskrifter, f.eks. med et faksimile-stempel, jf. f.eks. om checks *U 1992.753 Ø* og *Søren Theilgaard*: Checkret (1998), s. 34 med note 14.

Som det fremgår indebærer flere af disse fremgangsmåder begrænsninger. Beviset for, at en skriftlig meddelelse er *afsendt* via det almindelige postvæsen på et bestemt tidspunkt, sikres forskelligt af henholdsvis afsender og modtager. Afsenderen kan udbede sig en kvittering, der sammen med en genpart af den afsendte meddelelse kan indicere, hvad han sendte, og hvornår. Omvendt kan modtageren fremvise en kuvert med en påstemplet tidsangivelse (medmindre dokumentet er frankeret med en hjemmefrankeringsmaskine). Begge disse bevismidler lider imidlertid under den svaghed, at de alene knytter sig til kuverten. Kvitteringen/stemplet indebærer principielt intet bevis for, hvilken meddelelse kuverten indeholdt. Til at belyse dette er det i almindelighed nødvendigt at føre et *sammenhængsbevis* (jf. om dette begreb afsnit 4.3.d.), hvorved det f.eks. må komme modtageren af et tomt anbefalet brev til skade, at han ikke reagerer overfor afsenderen. Det indgår i vurderingen af, hvilken type meddelelse der er tale om.

I den digitale verden løses dette problem gennem flere metoder. Sikkerheden for, at en meddelelse havde et bestemt indhold, kan

opnås gennem *kryptering* eller *digital signatur*, jf. herom nedenfor. Sikkerheden for, at den er kommet frem til modtageren, kan opnås gennem brug af *troværdige tredjeparter*, der registrerer parternes kommunikation.

Tidsmæssighed

Herudover kan der opstå spørgsmål om sikkerheden for, at en informationsmængde er født henholdsvis transmitteret på et bestemt tidspunkt (tidsmæssighed). Også her kræver sådanne teknikker brug af troværdige tredjeparter. Nutidens IT-systemer er alle forsynet med et ur, der knytter tidsangivelse til den enkelte datalagring, men tidsangivelsen herpå sættes af den enkelte bruger. Sikkerhed for, hvornår en meddelelse er lagret, sendt eller modtaget, kræver igen brug af en troværdig tredjepart og et hertil hørende regelsæt, således som det f.eks. kendes fra værdipapir- og tinglysningsområdet.

4.2.b. Kryptografi

Kryptografi betyder kodelære. Når informationer lagres i et sprog, der ikke kan læses af udenforstående, taler man om, at de er *krypterede* (af græsk: kryptos = skjult, grafein = skrive). Meddelelsen er dermed *lukket* for omverdenen, dvs. billedligt talt "låst af" for andre end dem, der råder over den anvendte nøgle. Når man krypterer, tager man udgangspunkt i et "åbent" dokument ("klartekst"), som krypteringen "låser" ("kryptotekst"). Ligesom der må en nøgle til at åbne en dør, kan kun den, der kontrollerer krypteringsalgoritmen, dekryptere kryptoteksten, medmindre låsen er så svag, at den kan brydes af en indtrænger.

Teoretisk ramme

I kommunikationsteoriens termer kan krypteringsnøglen betragtes som et særligt meta-sprog, der befinder sig bag det sprog, som klarteksten er formuleret i (f.eks. et naturligt sprog som dansk). Den proces, der definerer nøglen, må derfor overholde et forud fastsat regelsæt; krypterings*algoritmen*. En simpel krypteringsalgoritme kan f.eks. skrives som x = x+1, hvor x er meddelelsen i klartekst og det valgte tal "1" den nøgle, der aktiverer krypteringsalgoritmen. En sådan simpel algoritme indebærer, at hvert bogstav erstattes med (i eksemplet) det næste bogstav i alfabetet, f.eks. således at "HAL" – navnet på den magtfulde computer i Kubricks science fiction film "Rumrejsen år 2001" – bliver til "IBM". Når dokumentet låses, lægges et bogstav til. Det åbnes igen, ved at bogstavet trækkes fra.

Den netop nævnte algoritme er forholdsvis enkel at bryde, men den kan udbygges og suppleres – f.eks. ved, at man efter et fast system lægger forskellige talstørrelser til x, se hertil *Peter Landrock*

& Knud Nissen: Kryptologi (1990), s. 9 f. Gennem de sidste mange hundrede år har man forsøgt at skabe stadigt mere avancerede krypteringsalgoritmer. En af de hyppigst anvendte binære krypteringsalgoritmer er den amerikanske DES-algoritme (DES = Data Encryption Standard), der arbejder med en klartekst opdelt i blokke på 64 bit. DES blev offentliggjort i 1975 af NBS (nu NIST), se NIST Notices, vol. 56, no. 169 af 30. august 1991. NIST garanterede oprindeligt for algoritmens sikkerhed – men garantien blev senere trukket tilbage. Se hertil *Lars Frank* (1987), s. 99 ff., *Borking* (1985), s. 90 ff. og *R. A. Franks* i 72 Iowa L.R. 1015 (1987), s. 1016. DES anvendes bl.a. til transmission af betalingstransaktioner i Dankort-systemet. Ifølge artikel 3, stk. 5, i direktivet om elektroniske signaturer kan Kommissionen efter en særlig procedure offentliggøre referencenumre på almindeligt anerkendte standarder for elektroniske signatur-produkter. Der skal herefter gælde en formodningsregel, hvorefter et elektronisk signatur-produkt, der opfylder sådanne standarder skal formodes at overholde kravene i bekendtgørelsens bilag II, litra f, og bilag III (de kvalificerede krav). Efter at dette arbejde i en periode har været henlagt til en særlig arbejdsgruppe, The European Electronic Signature Standardization Initiative (EESSI), er arbejdet med den videre standardisering henlagt til ETSI.

Funktioner

Ved brug af kryptering kan man løse en væsentlig del af informationssamfundets sikkerhedsproblemer: Findes nøglen til et låst dokument med sikkerhed kun to steder – hos afsenderen og modtageren – og anvender man i øvrigt en sikker algoritme, der er implementeret korrekt, kan modtageren opnå en høj grad af sikkerhed for dokumentets *ægthed*. Herudover kan kryptering sikre meddelelsens *fortrolighed*: for at kunne låse den pågældende meddelelse op, må en udefra kommende være i besiddelse af den anvendte nøgle. Selve brugen af matematiske algoritmer til kryptering og dekryptering sikrer endvidere meddelelsens *integritet*, altså for, at meddelelsen ikke er ændret i perioden efter krypteringen: Ændres meddelelsen i sin krypterede form med blot en enkelt bit, lader den sig slet ikke dekryptere (hvis den er krypteret) eller verificere (hvis der er anvendt andre matematiske sikkerhedsteknikker). Kryptering kan dermed bruges til at etablere sikkerhed i persondatabehandling, se *RÅB 1984.25*.

4.2.c. Asymmetrisk kryptering

Den form for kryptering, der er nævnt i eksemplet ovenfor, kendetegnes ved, at samme nøgle anvendes ved kryptering og dekryptering. Da kryptering og dekryptering dermed følger samme mekanisme, taler man om *symmetrisk* kryptering eller single key-kryptering. Svagheden ved et sådant system er, at bruger og af-

sender da også må være i besiddelse af samme nøgle. For brugere, der har mulighed for at mødes med hinanden ansigt til ansigt, inden de giver sig til at kryptere deres meddelelser, rejser dette vel ingen vanskeligheder. Sådan vil forholdene ofte være i såkaldt "lukkede net", f.eks. mellem filialerne i en international organisation. Men for at kunne kryptere i "åbne net", hvor parterne ikke nødvendigvis har været i kontakt med hinanden forinden, må den anvendte nøgle udveksles på anden vis, f.eks. ved post- eller kurerforsendelse.

Af praktiske grunde kan der imidlertid være behov for også at bruge nettet til at udveksle nøglen. På Internet rejser dette det problem, at nøglen da kan tænkes at falde i de forkerte hænder og efterfølgende skabe risiko for, at personer uberettiget optræder "autentisk" under nøglen. Dermed er opstået et behov for såkaldt asymmetriske krypto-systemer, hvor der ikke bruges én nøgle, men et nøgle*par*.

Nøglepar

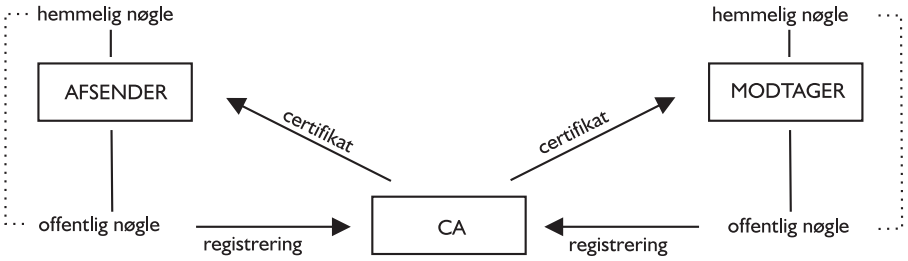
Et nøglepar fungerer således, at den ene nøgle aldrig kan bruges til både kryptering og dekryptering af samme meddelelse. Er meddelelsen først krypteret med den ene nøgle, kan den betragtes på samme måde som hakket kød, der har været turen igennem en kødhakkemaskine: Man kan ikke genskabe udgangspunktet ved at gøre det omvendte. Det kan man derimod ved at anvende den anden nøgle, der hænger uløseligt sammen med den, der blev brugt ved krypteringen. Har man krypteret en tekst ved hjælp af den ene nøgle i parret, kan samme tekst kun dekrypteres ved hjælp af den anden. Dermed kan nøgleparret anvendes således, at den ene nøgle holdes hemmelig, medens den anden offentliggøres. Asymmetrisk kryptering giver dermed grundlag for såkaldt *public key-kryptering*.

Anvendelsen

Public key-krypteringssystemer går altså ud fra, at hver af de kommunikerende parter råder over et nøglepar, hvoraf den ene nøgle – den *private* – holdes hemmelig, og den anden – den *offentlige* – offentliggøres overfor omverdenen af en part, der står inde for nøgleindehaverens identitet, en såkaldt certificeringsinstans eller Certification Authority (CA). Af sikkerhedsmæssige grunde tilvejebringes nøgleparret af nøgleindehaveren, f.eks. ved hjælp af særligt udstyr eller programmel. Systemets troværdighed forudsætter nemlig, at den hemmelige nøgle aldrig vises til tredjemand; derfor bør tredjemand heller ikke frembringe nøglen!

Den logiske – og efter sigende uafviselige – sammenhæng mellem de to nøgler i et nøglepar tilvejebringes ved, at nøglerne opbygges på grundlag af primtal. Princippet bygger på, at det er

relativt nemt at fastslå, om et tal er et primtal eller ej, medens det, i fald tallet er et produkt af to primtal, er vanskeligt at udfinde de divisorer, der kan frembringe tallet (primtalsdivisorerne). Vanskeligheden ved at finde frem til et tals primtalsdivisorer stiger eksponentielt med tallets størrelse. I praksis anvendes primtal på flere hundrede cifre. Sandsynligheden for, at en person "tilfældigt" skulle udfinde lige netop det primtal, der svarer til den offentlige nøgles hemmelige modstykke, siges at svare til sandsynligheden for netop at finde ét bestemt atom ud af samtlige universets atomer!



Eksempler

Systemet i asymmetrisk kryptering kan anskueliggøres med ovenstående figur. Med udgangspunkt i den kendsgerning, at en tekst krypteret med den ene nøgle kun kan dekrypteres med den anden, kan man nu opnå følgende forskelligartede bevissituationer:

Fortrolighed

A krypterer en tekst med B's offentlige nøgle, som han f.eks. henter fra en CA: Teksten kan alene dekrypteres af B med B's hemmelige nøgle. Når B kan gennemføre en sådan dekryptering, ved han, at ingen andre end han selv og A kender den pågældende meddelelse, hvis ellers B har holdt sin hemmelige nøgle hemmelig og den anvendte krypteringsalgoritme er tilstrækkeligt sikker. Hermed opnås sikkerhed for meddelelsens fortrolighed i forholdet mellem A og B. Hvis ellers A har sikkerhed for, at CA'en har ført korrekt regnskab med, hvem der gemmer sig bag de registrerede offentlige nøgler, kan A også være sikker på, at meddelelsen ikke læses af andre end B.

Ægthed og integritet

A krypterer en tekst med sin egen hemmelige nøgle. Teksten kan nu kun dekrypteres med A's offentlige nøgle. Når B (eller en anden) har dekrypteret med denne offentlige nøgle, ved han, at teksten virkelig kommer fra A, for kun A's offentlige nøgle kan dekryptere en meddelelse krypteret med A's private nøgle. Både i denne situation og i den forrige ved den, der dekrypterer meddelelsen, tillige, at meddelelsen ikke er blevet udsat for ændrin-

ger undervejs. Var den det, var det ikke muligt at dekryptere den. Dermed opnås både sikkerhed for ægthed og integritet.

Forudsætninger

Der er flere kritiske punkter i et sådant nøglesystem. Dels må der herske sikkerhed for, at A, henholdsvis B, virkelig er de personer, der fremtræder i det register, som CA'en fører, dels må det kunne klarlægges, at de anvendte algoritmer besidder den fornødne sikkerhed. Dette rejser dels et retspolitisk problem, dels – og i forlængelse heraf – et erstatningsretligt, som løbende er genstand for intense drøftelser i forbindelse med den retlige regulering af digital (elektronisk) signatur.

Lovgivnings-opgaven

Gennem de årtier, hvor man har diskuteret behovet for en lovgivning om elektronisk signatur, har vekslende retspolitiske strømninger gjort sig gældende. For nogen opleves foranstaltninger til opbygning af en digital infrastruktur som udtryk for "*Big Brother*"-tanken. Dette sås bl.a. i debatten om det forslag om indførelse af et digitalt *borgerkort* baseret på public key-teknologi, som Indenrigsministeriets CPR-kontor fremlagde i 1994, og som – indtil videre – blev afsluttet, da den daværende indenrigsminister valgte at opgive borgerkortprojektet i efteråret 1996. Andre ser derimod en public key infrastruktur som en nødvendig mulighed for at sikre den information, der passerer på den stadigt mere uoverskuelige digitale informationsmotorvej. Hertil kommer de endnu uafklarede retspolitiske forhold vedrørende brug af teknikker til stærk kryptering: Myndighedernes adgang til "aflytning" af krypteret information, valget af standarder, forbrugerbeskyttelse, erstatningsretlige spørgsmål o.m.m. En række af disse spørgsmål forfølges på internationalt plan, jf. afsnit 4.2.e. om OECD's retningslinjer for krypteringspolitik.

4.2.d. Digital signatur

At en meddelelse er krypteret eller digitalt signeret af sin ophavsmand ved brug af stærk (dvs. ubrydelig) kryptering, kan i sig selv – omend alt efter omstændighederne – være et tegn på, at ophavsmanden står ved den. Derfor er krypteringsteknikker i stigende grad taget i brug som surrogat for den skrevne signatur på et dokument. Som bredt udtryk for den kryptering, der anvendes til at give en digital meddelelse et særpræg, der bestemmes af afsenderen ved hjælp af en personlig krypteringsnøgle, taler man om *digital signatur*.

Signaturbegrebet

Signaturbegrebet er centralt i forpligtelseslæren. Det rummer tre elementer. For det første en objektiv information om den underskrivendes *identitet*, typisk et navn eller andet symbol. Der-

næst rummer den skrevne signatur et *personlighedspræg*, der afspejles i underskriftens konkrete udformning. Endelig indebærer den proces, hvorved signaturen *fikseres*, en manifestation af den forpligtedes vilje (viljeserklæring), jf. nærmere herom i afsnit 19.1.c.

Se nærmere om signaturbegrebet og dets funktion *Roger Henriksen* (1982), s. 39 ff. Signaturbegrebet (af lat.: *signum* = tegn) går videre end underskriftbegrebet ved også at medtage visse tegn, der bærer andre af erklæringsgiverens personlige præg, f.eks. fingeraftryk eller segl.

Digital signatur

I teknisk terminologi defineres begrebet *digital signatur* almindeligvis som en *talværdi*, der fastlægges på grundlag af en meddelelse i digital form og i overensstemmelse med en procedure (algoritme), som gør det muligt entydigt at *verificere*, at talværdien er udvirket på grundlag af den digitale meddelelse og med den private krypteringsnøgle i et nøglepar. Talværdien kan enten bestå i en fuldstændig kryptering af meddelelsen, den kan bestå i en hashværdi af meddelelsen, jf. herom straks nedenfor, eller den kan bestå i en kryptering af en hashværdi, der repræsenterer meddelelsen. For at opnå sikkerhed for, at den signerede meddelelse virkelig hidrører fra afsenderen, må modtageren kunne knytte tillid til den CA, der påtager sig at stå inde for afsenderens identitet. Grundlaget for denne tillid kan i rene partsrelationer tilvejebringes gennem treparts-aftaler mellem afgiveren af den signerede meddelelse, CA'en og modtageren. En vis regulering af den virksomhed, der udøves af sådanne troværdige tredjeparter i en infrastruktur til digital (eller elektronisk) signatur – en såkaldt public key infrastruktur (PKI) – findes i lov om elektroniske signaturer (LES).

Biometriske teknikker

En mindre udbredt metode til at signere en elektronisk meddelelse er gennem biometriske teknikker. Hermed menes metoder, hvorefter en unik egenskab ved den berettigede person (pupilbygning, fingeraftryk, stemme el.lign.) registreres og sammenholdes med de egenskaber, som den disponerende person fremviser. En biometrisk metode må imidlertid kombineres med en metode til kodning af den meddelelse, der ønskes sikret. Typisk vil dette ske ved, at den biometriske teknik anvendes som en adgangskontrol til det system, der kan udvirke en signering.

Navnlig registrering af fingeraftryk har været anvendt til disse formål, jf. *Galtung* (1989), s. 52 f. og *Birgitte Kofod Olsen*: Identifikationsteknologi og individbeskyttelse (1998), der drøfter de betænkeligheder, sådanne teknologier kan give anledning til ud fra synspunkter om databeskyttelse. Et eksempel herpå er den såkaldte *PENOP-*

løsning, se <www.penop.com>. Løsningen bygger på såkaldt signatur-dynamisk genkendelse: Underskriveren frembringer sin underskrift ved hjælp af en pen på en elektronisk skriveplade. Skrivepladen registrerer herefter en række egenskaber ved underskriften, herunder hvilke vinkler der indgår, hvor hurtigt forskellige dele frembringes, grafisk fremtrædelse etc. Det er imidlertid væsentligt at fremhæve, at løsninger som denne ikke kan stå alene i åbne netværk, hvor der altid vil være behov for en kryptering og verificering af de data, der således frembringes. Se for en nærmere gennemgang af de biometriske metoder til afgivelse af digital signatur, *R.R. Jueneman & R.J. Robertson, Jr.*: Biometrics and Digital Signatures in Electronic Commerce, 38 Jurimetrics J.427-457 (1998).

Brugen af biometriske teknikker til at identificere kommunikerende parter har endnu ikke vundet indpas. Den standardisering, som normalt vil være forudsætningen for, at man kan gennemføre en sådan personidentifikation over en brev kam, har ladet vente på sig, selvom der er flere brugbare applikationer på markedet, som uden vanskelighed kan implementeres på pc-terminaler til en udgift på få hundrede kroner. Over for den vanskelighed, der ligger i at skulle gennemføre den nødvendige *standardisering*, står den enkelhed, hvormed man ad "biometrisk" vej kan identificere en kommunikerende part med eksisterende udstyr, f.eks. ved brug af det web-kamera, der er monteret på computeren, eller ved en telefonsamtale med den part, man kommunikerer med og hvis stemme man med sikkerhed kan genkende.

Hashing

En række af de funktioner, der kan opnås ved brug af kryptering, kræver ikke, at det er meddelelsen i sin fulde udstrækning, der krypteres. Hvis formålet f.eks. er at opnå sikkerhed for, hvem afsenderen er (ægthed) eller at meddelelsen ikke er forvansket undervejs (integritet), er det tilstrækkeligt at kryptere et "fingeraftryk" af meddelelsen, hvis blot dette fingeraftryk er skabt på en måde, der vil afsløre, hvis meddelelsen siden ændres. Ressourcemæssige hensyn vil ofte tale for at kryptere sådanne *hashværdier* frem for at kryptere hele meddelelsen. Man taler da om, at meddelelsen "*hashes*". Selv med nutidens hurtige IT-systemer tager det lang tid at gennemføre de beregninger, der er forbundet med krypteringen. Hashingen foretages da på grundlag af en særskilt algoritme, der ligeledes anviser en fremgangsmåde for, hvordan man efterfølgende kan verificere, hvem meddelelsen kom fra.

Bevisførelse

Den digitale signatur kan ikke – som den skrevne – fremvises i retten. Bevisførelser vedrørende de omstændigheder, der ledsager signaturens afgivelse og verifikation forudsætter et indgående kendskab til kryptografiske principper og teknikker. Der må derfor føres et indgående systembevis med brug af sagkyndige

erklæringer om det anvendte system og om den sikkerhed, de anvendte krypteringsalgoritmer kan leve op til. Almindeligvis vil de CA-virksomheder, der understøtter systemer til digital signatur, også tilbyde de tjenesteydelser, der vil kunne understøtte en sådan bevisførelse, herunder ved at afgive udtalelser om, at bestemte nøgler på bestemte tidspunkter var i stand til at verificere bestemte digitale meddelelser.

4.2.e. Almindelig regulering

Den retlige regulering af teknikker til kryptering og digital signatur knytter sig til tre forskellige aspekter af denne sikkerhedsteknologi.

Aftalevirkning

Et første aspekt angår den *aftaleretlige* gyldighed af viljeserklæringer, der er forsynet med en digital signatur. Da dansk aftaleret som udgangspunkt udfolder sig under et princip om formfrihed gælder her de almindelige aftaleretlige regler, jf. nærmere herom afsnit 19.1, medmindre der i medfør af særlig hjemmel gælder særlige, formueretlige, formkrav, jf. herom afsnit 16.2.

Forvaltningsret

Et andet aspekt drejer sig om den *forvaltningsretlige* gyldighed af digitale dokumenter, der er sikret ved brug af digital signatur-teknologi. For en almindelig gennemgang af de retlige problemer, der er forbundet med brug af digitale meddelelser i den offentlige forvaltning henvises til afsnit 16.4. Reglerne om gyldigheden af elektroniske signaturer, særligt efter loven herom fra 2000, behandles i afsnit 16.5.

Særlige restriktioner

Tilbage står for det tredje spørgsmålet om, hvorvidt selve brug af teknikker til digital signatur og kryptering kan tænkes at stride mod særlige regler. Navnlig kan de *immaterialretlige regler* få betydning, jf. nærmere herom kapitlerne 7 og 10. Men herudover kan det tænkes, at der ud fra offentligretlige overvejelser, herunder navnlig ud fra *kontrol- og efterforskningsmæssige hensyn*, kan være en interesse i at begrænse brugen af disse teknikker.

For dansk rets vedkommende er svaret herpå klart. Der gælder ingen almindelige begrænsninger i adgangen til at anvende sikkerhedsteknologier (herunder teknikker til stærk kryptering), der har til følge, at det offentlige har vanskeligere ved at udføre kontrol- og efterforskningsarbejde. Det forhold, at man ved at kryptere datatransmission *de facto* afskærer politi- og efterforskningsmyndigheder fra at foretage indgreb i meddelelseshemmeligheden, indebærer ikke, at en sådan kryptering er ulovlig, ligeså lidt som det er ulovligt at tale et eksotisk/uforståeligt sprog med

hinanden i telefonen. Forholdet er anderledes i visse andre lande, der på forskellig vis begrænser denne adgang, f.eks. ved at stille krav om, at nøgler anvendt til kryptering deponeres hos troværdige tredjeparter, hvorfra de kan rekvireres af efterforskende myndigheder mod retskendelse.

Spørgsmålet har imidlertid fra tid til anden været søgt reguleret på internationalt plan efter pres fra lande med større efterretningsmæssige interesser end vore. Et foreløbigt resultat af disse drøftelser forelå, da OECD i marts 1997 vedtog et sæt retningslinjer om krypteringspolitik, der betoner, at brugeren (være sig privatpersoner eller virksomheder) som udgangspunkt har fri adgang til at anvende kryptologiske værktøjer, men at lovgivningen i enkelte lande kan fastsætte begrænsninger heri, se <www.oecd.org>. OECD-retningslinjerne hverken pålægger eller anbefaler medlemsstaterne at indføre sådanne regler.

Problemerne vedrørende aflytning ctr. hemmeligholdelse ved brug af kryptering er bl.a. behandlet i *Teknologirådet*s rapport: "En dansk krypto-politik – hvordan skal digitale informationer hemmeligholdes?", ved Steffen Stripp (red.) – Teknologirådets rapporter 1995/5 og af *Mads Bryde Andersen & Peter Landrock* i J1995.306 ff. Se ligeledes *Stewart A. Baker & Paul R. Hurst*: The Limits of Trust – Cryptography, Governments, and Electronic Commerce (Kluwer Law International, The Hague, 1998) og antologien Building in Big Brother – The Cryptographic Policy Debate, ved *Lance J. Hoffman* (ed.), New York 1995).

Selv om Danmark ikke har taget skridt til direkte at forbyde kryptering, indeholder vor lovgivning enkelte regler, der indirekte begrænser den frie anvendelse af sådanne teknologier.

Udførsel

I medfør af § 2 i lov om udførsel af varer, teknologier og knowhow med dobbelt anvendelse, jf. lovbekendtgørelse nr. 612 af 25. juni 2003, kan man straffes med bøde, hæfte eller fængsel i indtil 2 år (medmindre højere straf er forskyldt efter anden lovgivning) for at udføre (bl.a.) visse former for krypteringsprodukter uden tilladelse fra Erhvervsfremmestyrelsen. Reglerne herom udspringer af det såkaldte *Wassenaar-arrangement*, jf. nærmere i afsnit 12.2.e. Også såkaldte "hyldevarer" (hvortil f.eks. hører Internet-browsere og e-post-programmer), der indeholder faciliteter til stærk kryptering (hvilket i denne sammenhæng er afgrænset som en nøglelængde udover 64 bits), er underlagt eksportkontrol. Reglerne er transformeret til EU-ret i den "forbudsliste", der afgrænser pligten til at søge eksportgodkendelse, jf. nærmere afsnit 21.2.e.

I amerikansk ret har det været antaget, at sådanne eksportforbud strider mod den konstitutionelt sikrede ytringsfrihed, se senest sagen *Bernstein v. United States* (9th Cir. 6 May 1999), der bl.a. fremhævede den mangel på procesretlige garantier, som prægede eksportkontrolregimet. Se også *Bernstein v. U.S. Dept. of State*, 922 F.Supp. 1426 (1996) og *Junger v. Daley*, 209 F.3d 481 (6th Cir., 2000). Sagerne drejede sig om kildeteksten til et krypteringsprogram, der ansås for at udgøre en ytring, der var beskyttet som sådan under den forfatningsretlige ytringsfrihed. Derfor kunne spredning af denne kildetekst ikke lovligt begrænses ved reglerne om strategisk kontrol med eksport af våben.

Telekommunikation

En anden begrænsning i den frie ret til at kryptere gælder for udbydere af offentlige telenet og teletjenester. Ifølge § 15 i lov om konkurrence- og forbrugerforhold på telemarkedet, jf. lovbekendtgørelse nr. 679 af 23. juni 2004, skal udbydere af offentlige telenet eller teletjenester uden udgift for staten, herunder for politiet, sikre, at de centraler, udbyderen etablerer, er indrettet således, at politiet kan få adgang til at foretage indgreb i meddelelseshemmeligheden, jf. retsplejelovens kapitel 71. Heri ligger bl.a., at faciliteter til den kryptering, som sker på nettet, skal indrettes således, at der mod retskendelse uden videre kan frembringes klartekst. Forskningsministeren kan efter forhandling med justitsministeren fastsætte nærmere regler om de tekniske krav til sådanne centraler og om udbyderens bistand til politiet i forbindelse med indgreb i meddelelseshemmeligheden, jf. stk. 2-3.

4.2.f. Lov om elektroniske signaturer

Formål og funktion

Ved lov om elektroniske signaturer (LES), nr. 417 af 31. maj 2000 er der indført almindelige regler i dansk ret om visse elektroniske signaturer samt regler for de virksomheder mv., der udsteder certifikater til visse typer af elektroniske signaturer, de såkaldte *certificeringscentre* (i loven – med et misvisende udtryk kaldet "nøglecentre", i teknisk terminologi – og i det følgende – kaldet CA, Certification Authorities). Loven gennemfører Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer (EFT 2000 L 13/12).

Direktivet blev skabt på baggrund af den lovgivning, der var undervejs til at blive indført, herunder i Danmark – med et første lovudkast fra efteråret 1996 – og i Tyskland, der indførte sin første Signaturgesetz i 1997. Gennem sådanne nationale lovgivninger opstod flere EU-retligt kritiske risici, dels for en uensartet juridisk anerkendelse af den digitale signatur, dels for at de enkelte medlemsstater ville stil-

le forskellige, og indbyrdes diskriminerende, lovkrav til CA-virksomheder. En del af lovens ganske komplicerede terminologi har rod i det arbejde, der sideløbende har været gennemført i UNCITRAL, og som i sit seneste forløb har søgt at finde juridiske løsninger, der er robuste også overfor fremtidens signaturteknologier, jf. herom straks i det følgende. UNCITRALS arbejde har til dato manifesteret sig i tre instrumenter. I 1996 vedtoges en modellov om elektronisk handel (med en lille ændring i 1998), i 2001 en modellov om elektroniske signaturer og i 2005 en konvention om brug af elektronisk kommunikation i internationale aftaler (Convention on the Use of Electronic Communications in International Contracts). Alle tre instrumenter indeholder bestemmelser, der fastslår de generelle kriterier for at knytte retlig og bevismæssig gyldighed til elektroniske meddelelser og underskrifter af forskellig art. De fleste lande har i dag indført lovgivning om elektroniske signaturer mv. Der findes talrige Internet-sites, der angiver disse forskellige lovgivninger med tilhørende nøglecentre (CA'er) mv., se f.eks. <www.searchlaw.com/digital.htm> og <www.pki-page.org>.

Som hermed antydet har der allerede på nuværende tidspunkt vist sig mange forskellige måder, hvorpå der lovgives om digital signatur: Efter en *minimalistisk* model (som f.eks. er lagt til grund i UNCITRAL's hidtidige arbejde) lovgives der kun om de ydre rammer for brugen af e-signatur. Hovedformålet er at undgå regulatoriske barrierer og andre tekniske handelshindringer. En anden, *aktiv*, variant søger at sikre opbygningen af en PKI-infrastruktur ved at opstille særlige regler for dennes opbygning. Man forudsætter derfor, at der anvendes en bestemt teknologi (f.eks. public key-baseret kryptering), og lovgivningen går dermed foran i standardiseringsbestræbelserne. Herhjemme har vi ikke set egentlige eksempler herpå; men de bestræbelser, IT- og Forskningsministeriet har gjort for at udbrede standardiseringsarbejdet på området for digital signatur – f.eks. inden for rammerne af Forum for Digital Signatur – kan ses som udtryk for en sådan målsætning. En tredje variant (som er lagt til grund i EU-direktivet om elektroniske signaturer) søger at *kombinere* de to første ved dels at opstille nogle principper for anerkendelse af elektroniske signaturer, dels ved at tildele visse – avancerede – signaturer særlige lovgivningsmæssige fortrin.

Ifølge § 1 har loven til formål at fremme en sikker og effektiv anvendelse af elektronisk kommunikation gennem fastsættelse af de nævnte krav til visse (men ikke alle) elektroniske signaturer og til CA-virksomheder ("nøglecentre"). I praksis er lovreguleringen fokuseret omkring det, der i lovens terminologi betegnes som avancerede elektroniske signaturer, der baseres på kvalificerede certifikater, jf. nærmere afgrænsningen i § 2, stk. 1.

"Elektronisk signatur"

Ifølge § 3, nr. 1, defineres begrebet "elektronisk signatur" bredt som enhver form for data i elektronisk form, der knyttes til andre elektroniske data ved hjælp af et *signaturgenereringssystem*, og som anvendes til at *kontrollere*, at disse data stammer fra den person, der er angivet som underskriver, og at de ikke er blevet ændret. Som definitionen fremstår kræves det, at der anvendes et særligt "system" til generering af den elektroniske signatur. Det forhold, at man afslutter en e-mail med sit navn, vil ikke opfylde dette krav, hvorimod et særligt indføjet navnetræk (f.eks. en indskannet version af ens håndskrevne underskrift), der indplaceres på grundlag af en makro-rutine, formentlig vil. Kravet om, at den elektroniske signatur skal have til *formål* at give mulighed for at kontrollere underskriveren, indebærer isoleret set alene et subjektivt krav, der knytter an til omstændighederne ved signaturens afgivelse. Formålet med signaturgenereringssystemet må være at kunne identificere underskriveren, men ikke at blotlægge de nærmere formål, underskriveren har for at underskrive. Der ligger ikke heri nogen yderligere tekniske krav til det pågældende system.

"Underskriveren"

Loven forudsætter, at en signatur, og herunder en elektronisk signatur, afgives af en fysisk person. Dette fremgår direkte af § 3, nr. 8, hvor et "certifikat" defineres som en elektronisk attest, som knytter bestemte signaturverificeringsdata til "underskriveren", hvilket ifølge samme bestemmelses nr. 3 er en "fysisk person", der besidder et signaturgenereringssystem. Baggrunden herfor er, at en juridisk person, endsige et apparat, ikke antages at kunne signere noget: en juridisk person, fordi signaturen altid vil være afgivet af en fysisk person; apparatet, fordi det ikke kan besidde nogen "vilje" til at forpligte sig mv.

I direktivets art. 2, stk. 3, defineres "underskriveren" som "en person, der besidder et signaturgenereringssystem og handler på egne vegne eller på vegne af den *fysiske eller juridiske person* eller det organ, som vedkommende repræsenterer" [udhævet her]. Den danske lov har hermed valgt side i et principielt spørgsmål, der i direktivets formulering er efterladt åbent ved en bevidst tvetydighed.

I princippet er alle typer af elektroniske signaturer omfattet af loven. Loven sondrer imidlertid mellem forskellige typer af signaturer, idet den knytter forskellige typer af retsvirkninger hertil, jf. nærmere afsnit 16.4.c.

Avancerede eller ikke

For det første sondres mellem avancerede og ikke-avancerede elektroniske signaturer. Ifølge § 3, nr. 2, er en avanceret elektronisk signatur en elektronisk signatur, der opfylder fire krav. Den skal for det første være *entydigt knyttet* til underskriveren, a). For

det andet skal den gøre det muligt at *identificere* underskriveren, b). Den skal dernæst skabes med midler, som kun underskriveren har *kontrol* over, c), og som er knyttet til de data, den vedrører på en sådan måde, at enhver efterfølgende ændring af disse data kan *opdages*, d).

Kravene til en avanceret elektronisk signatur vil almindeligvis være opfyldt gennem en *digital signatur*, der er baseret på brugen af en *hemmelig nøgle* som underskriveren har eksklusiv råden over (sml. herved de under a) og c) anførte krav), og som indebærer en fuldstændig kryptering af den signerede meddelelse eller generering af en *hashværdi* af samme (sml. det under d) anførte krav). I tillæg hertil kræves det, at sådanne signaturer kan verificeres på en sådan måde, at underskriveren kan identificeres klart (sml. det under b) anførte krav). Dette kan enten ske gennem en troværdig tredjepart eller ved forudgående aftale mellem underskriveren og modtageren, der fastlægger en procedure herfor. Den troværdige tredjepart er inde i billedet i de tilfælde, hvor signaturen baseres på et certifikat, jf. herom i det følgende. I kraft af dennes rolle taler man om, at der opbygges en *public key infrastruktur*, også kaldet PKI.

Web of trust

Avancerede digitale signaturer kan dog også forekomme i tilfælde, hvor verifikationen af den afgivne signatur afgives af de involverede parter selv, evt. under bistand med "venner og venners venner": Man kan således opbygge en såkaldt *web of trust* ved at rekvirere certifikater vedrørende mulige samarbejdsparter gennem parter, der i forvejen kender de pågældende og dermed kan godtgøre deres identitet. Sådanne private systemer anvendes af mange private Internet-brugere til udveksling af krypterede meddelelser på grundlag af det meget udbredte krypteringsprogram PGP ("Pretty Good Privacy").

Certifikatets beskaffenhed

En anden sondring knytter sig til de tilfælde, hvor underskrivelsen af en meddelelse lader sig verificere gennem et certifikat udstedt af en tredjepart, altså gennem en PKI, som opfylder visse på forhånd angivne krav. Ifølge lovens § 3, nr. 8, defineres et certifikat som en elektronisk attest, som knytter bestemte signaturverificeringsdata (i praksis den *hashede* eller krypterede meddelelse) til underskriveren og bekræfter dennes identitet. Definitionen kan i princippet tænkes at omfatte en hvilken som helst erklæring, der udtaler sig om den tekniske forbindelse mellem signaturen på en meddelelse og identiteten af den part, der står bag den hemmelige nøgle, der er anvendt til at signere eller kryptere meddelelsen. For at indsnævre et område for særligt trovær-

dige certifikater sondrer loven mellem kvalificerede og ikke-kvalificerede certifikater.

- kvalificerede certifikater

Ifølge LES § 4 er et "kvalificeret certifikat" et certifikat, der opfylder de i stk. 2 og 3 nævnte krav, og som udstedes af en CA (et "nøglecenter"), der opfylder bestemmelserne i kapitel 4 samt regler fastsat i medfør heraf. Gennem de således opstillede krav til det kvalificerede certifikat defineres en række funktioner, der gør dette certifikat egnet til kommunikationsprocesser, hvor der kan være særligt behov for at identificere underskriveren og dennes formodede ønske om at forpligte sig ved underskrivelsen.

Et kvalificeret certifikat skal for det første indeholde en række oplysninger, der identificerer det som sådant, og som angiver CA'ens navn og hjemsted, underskriverens *navn eller pseudonym* med angivelse af, at der er tale om et pseudonym samt eventuelle *yderligere oplysninger* om underskriveren, for så vidt det er nødvendigt for anvendelsen af certifikatet. I den forbindelse skal certifikatet også indeholde oplysninger, der sikrer en *entydig identifikation* af underskriveren, jf. nærmere LES § 4, stk. 2, nr. 1-4.

Foruden disse identitetsoplysninger skal det kvalificerede certifikat indeholde angivelse af en gyldighedsperiode samt en tydelig angivelse af eventuelle begrænsninger i certifikatets anvendelsesområde (formålsbegrænsninger), se nr. 5-6. Vigtigt er det, at der herudover skal være tydelig angivelse af eventuelle begrænsninger med hensyn til de transaktionsbeløb, certifikatet kan anvendes til, jf. nr. 7. Gennem denne angivelse kan brugeren foretage en begrænsning i, hvilke forpligtelser – økonomiske eller af anden art – som kan tænkes påført ved brug af en signaturnøgle og et hertil hørende kvalificeret certifikat.

Det er dernæst foreskrevet, at det kvalificerede certifikat skal indeholde en identifikationskode samt de signaturverificeringsdata, der svarer til de signaturgenereringsdata, som var under underskriverens kontrol på udstedelsestidspunktet, nr. 8-9. Bestemmelsens stk. 3 foreskriver endelig, at et kvalificeret certifikat skal være underskrevet med nøglecentrets avancerede elektroniske signatur.

Sikre signaturgenereringssystemer

LES kapitel 8 opstiller en række særlige krav til såkaldt sikre signaturgenereringssystemer. Hermed forstås ifølge loven signaturgenereringssystemer, der ved hjælp af procedurer og tekniske midler sikrer, at signaturgenereringsdata, der anvendes til at skabe en elektronisk signatur, 1) i praksis kun kan fremtræde en gang, 2) med rimelig sikkerhed forbliver hemmelige og ikke kan udledes, 3) er beskyttet mod forfalskning og 4) på pålidelig vis

kan beskyttes af underskriveren mod andres uretmæssige brug, jf. nærmere § 14, stk. 1. Loven indfører et system, hvorefter en af Forskningsministeren udpeget prøveanstalt medvirker til at efterprøve, om signaturgenereringssystemer opfylder disse krav.

En væsentlig retsvirkning – og med den formodede retsudvikling, der vil komme: stadigt væsentligere – af at bruge et sikkert signaturgenereringssystem er ifølge LES § 13, at bestemmelser i lovgivningen, hvorefter elektroniske meddelelser skal være forsynet med signatur, dermed anses for opfyldt. Det kræves dog, at signaturen tillige er baseret på et *kvalificeret certifikat*, og at den er fremstillet ved brug af et *sikkert signaturgenereringssystem*. Ved elektroniske meddelelser til og fra en offentlig myndighed gælder dette dog kun, såfremt andet ikke følger af lov eller bestemmelser fastsat i medfør af lov. Gennem denne bestemmelse kombineres de optimale krav, loven opstiller i henseende til både certifikat, CA og det anvendte system.

Bestemmelsen gælder kun i det omfang lovgivningen henviser til brug af elektroniske signaturer. Der findes talrige eksempler herpå i nyere lovgivning, navnlig inden for uddannelses-, skatte- og afgiftsområdet og inden for det selskabsretlige og finansielle område. LES § 13 tager ikke ikke hermed taget stilling til, hvornår et lovkrav om "underskrift" kan opfyldes gennem brug af elektronisk eller digital signatur, jf. om dette spørgsmål i afsnit 16.4.c.

Algoritmekrav?

Loven indeholder heller ingen forskrifter om karakteren af den algoritme, der skal anvendes ved udstedelse af et certifikat. Når det gælder denne del af konceptet er der overladt CA'en en betydelig frihed. Der findes en række standarder herom, som CA'en ofte vil henvise til; men også disse standarder vil overlade et betydeligt spillerum. I IT-sikkerhedsrådets vejledning fra 2000 om Praktisk brug af Kryptering og Digital Signatur har rådet afgivet nogle mere specifikke anbefalinger herom, se herved s. 56 ff.

Identitetskontrol

Loven stiller heller ikke krav om, at den part, der identificerer sig til brug for udstedelsen af et certifikat til elektronisk signatur, skal legitimere sig ved personligt fremmøde mv., se derimod § 6, stk. 2-3, i bekendtgørelse nr. 923 af 5. oktober 2000 ("nøglecenterbekendtgørelsen"), der som udgangspunkt foreskriver, at underskriveren skal være fysisk tilstede i forbindelse med identitetskontrollen, medmindre nøglecentret på forhånd har kendskab til underskriverens person. Det certifikat, der udstedes i henhold til den danske OCES-standard, kræver ikke personligt fremmøde og udgør derfor ikke et kvalificeret certifikat i henholdt til LES.

I praksis vil man ofte placere ansvaret for identitetskontrollen hos andre virksomheder eller myndigheder, der da optræder som lokale registreringsenheder (LRA: Local Registration Authority), og som netop må formodes at besidde den nødvendige kendskab til underskriverens identitet. Denne fremgangsmåde har udtrykkelig hjemmel i nøglecenterbekendtgørelsens § 8. Alt efter karakteren af den pågældende PKI (offentligretlig eller privat mv.), kan LRA-funktionen tænkes henlagt til så forskellige enheder som det lokale folkeregister (som i det tidligere Borgerkort-projekt), en personaleafdeling (hvis signaturen forudsættes afgivet af en person i rollen som stillingsfuldmægtig) eller en bankfilial (hvis signaturen skal anvendes til at disponere over bankkonti mv.). At CA er underlagt et strikt præsumptionsansvar, kan muligvis incitere mange CA-virksomheder og lokale registreringsenheder til at kræve et sådant personligt fremmøde.

Krav til CA'ens virksomhed

Lovens kapitel 4 opstiller en række krav, der skal følges af CA'er, der udsteder kvalificerede certifikater. Disse virksomheder mv. skal træffe de foranstaltninger, som er nødvendige for et sikkert, pålideligt og velfungerende udbud af kvalificerede certifikater. Der skal anvendes *betryggende administrative og ledelsesmæssige procedurer*, som overholder anerkendte standarder (se § 5, stk. 1, nr. 1). Man må kun beskæftige *personale med den fornødne ekspertise*, erfaring og kvalifikationer, herunder personale med sagkundskab inden for elektronisk signaturteknologi og indgående kendskab til korrekte sikkerhedsprocedurer i forbindelse hermed (se § 5, stk. 1, nr. 2). Og der skal generelt anvendes *pålidelige systemer og produkter*, som er beskyttet imod uautoriserede ændringer, og som sikrer den tekniske og kryptografiske sikkerhed af de processer, som disse systemer og produkter understøtter (se § 5, stk. 1, nr. 3). Endelig skal CA'en *træffe foranstaltninger mod eventuelle muligheder for forfalskning* af certifikaterne (se § 5, stk. 1, nr. 4) og til stadighed have tilstrækkelige *økonomiske ressourcer* til at drive virksomhed i overensstemmelse med bestemmelserne i denne lov, herunder til at opfylde erstatningsforpligtelser i henhold til loven (§ 5, stk. 1, nr. 5).

Også de nærmere krav hertil er udmøntet i bekendtgørelse nr. 923 af 5. oktober 2000, der er udstedt med hjemmel i § 5, stk. 3.

I 2001 er tre danske virksomheder i funktion med udstedelse af kvalificerede certifikater: PBS/Post Danmark, Kommunedata (KMD-CA) og TDC Internet (TeleDanmark). De danske pengeinstitutter har besluttet at lade PBS fungere som CA for de certifikater, der inkluderes i de nye Dankort og Visa/Dankort, men det er endnu ikke afklaret, om der udbydes kvalificerede eller ikke-kvalificerede certifikater.

Procedurekrav til CA

Foruden disse almindelige krav til virksomheden er en CA undergivet visse krav til den procedure, der skal følges i dens virksomhed. Ifølge § 6 skal CA fastsætte og følge betryggende kontrolprocedurer. Sådanne procedurer nedfældes almindeligvis i en såkaldt *CPS*, Certification Practice Statement, som er almindeligt og let tilgængelig fra den site, hvorfra CA driver sin virksomhed.

Se ligeledes Finanstilsynets afgørelse af 9. november 2000 i en forespørgsel om, hvorvidt pengeinstitutter kan drive virksomhed i henhold til lov om elektroniske signaturer, sml. § 1 a, stk. 2, jf. § 1, stk. 3, i lov om banker og sparekasser, nu § 24 i lov om finansiel virksomhed. For at den her omhandlede virksomhed skal kunne anerkendes som "accessorisk" skal den ligge i naturlig forlængelse af pengeinstituttets hidtidige virksomhedsområde, idet der samtidig må foretages en vurdering af risikoen ved virksomheden. I sin afgørelse peger Finanstilsynet på den risiko for erstatningsansvar, der består i medfør af LES § 11. Finanstilsynet finder ikke, at dette ansvar adskiller sig markant fra det ansvar, pengeinstitutterne har i forvejen, f.eks. i henhold til lov om visse betalingsmidler. Derfor finder Finanstilsynet ikke, at risikoen ved drift af nøglecentervirksomhed vil være så stor, at et pengeinstitut ikke kan påtage sig risikoen. At der er tale om et produkt, der ikke nødvendigvis er relateret til den finansielle sektor, eller til pengeinstitutvirksomhed, gør ingen forskel heri. Ifølge Finanstilsynet er der tale om et virksomhedsområde, hvor det vil være naturligt at udnytte den viden og erfaring, som pengeinstitutterne har om registrering og behandling af følsomme data og data på edb-medier mv. Nøglecentervirksomhed vil derfor kunne betragtes som "accessorisk virksomhed" i henhold til den citerede bestemmelse. I overensstemmelse hermed har Finanstilsynet ved sin afgørelse af 9. februar 2004 godkendt Net-ID-løsningen.

I juridisk henseende befinder CPS'en sig i en særegen mellemstilling mellem offentlig ret og privatret og mellem kontrakt og delikt. På den ene side er der tale om en lovhjemlet konstaterende erklæring, som udstedes i almenhedens interesse. På den anden side er det klart, at en CPS afføder retsvirkninger af såvel erstatningsretlig art samt – alt efter sagens konkrete omstændigheder – som aftalegrundlag. Der er ikke nogen klar praksis for, hvordan disse dokumenter opbygges, og fordi der ofte indgår beskrivelser af, hvordan forskellige parter – i og uden for det enkelte kontraktsforhold – forventes at optræde, kan der være tvivl om, hvilke elementer af CPS'en der har aftalekarakter.

Territorial afgrænsning

LES finder anvendelse på nøglecentre etableret i Danmark, der udsteder kvalificerede certifikater til offentligheden. Derimod kan loven ikke udstrækkes til at gælde for udenlandsk virkende CA-virksomheder, hvis certifikater anvendes af danske brugere – et forhold, der bl.a. har betydning for den erstatningsretlige vur-

dering. Dette spørgsmål har størst betydning i relation til lande uden for EU og EØS-området. Gennem den EU-retlige harmonisering, som loven er udtryk for, kan danske virksomheder påregne, at tilsvarende regler, der nogenlunde svarer til de danske, vil være gældende i andre EU-lande, når direktivet foreligger implementeret (hvilket ifølge art. 13 skal være sket inden den 19. juli 2001), 19 måneder efter direktivets vedtagelse.

4.2.g. De danske løsninger

Gennem de seneste 10-15 år har danske regeringer forsøgt at skabe grundlag for, at danske borgere og virksomheder kunne gøre brug af løsninger til kryptering og digital signatur. Potentialet for en sådan PKI-infrastruktur er åbenbart. En ganske stor del af den danske befolkning benytter Internet-applikationer i det daglige. Kvaliteten af de data, der befinder sig i de offentlige systemer er, bl.a. pga. vor relativt tidlige indførelse af CPR-nummeret, høj. Og vi har tradition for at udvikle sikre kommunikations- og betalingsløsninger, som forholdsvis enkelt burde kunne tilpasses til også at gælde for en brug af kryptering og digital signatur.

Alligevel har det været vanskeligt at vænne danskerne til også at benytte sig af løsninger – eller rettere, af ensartede statslige løsninger – til at understøtte disse sikkerhedsteknikker.

OCES-løsningen

Gennem en årrække har VTU-ministeriet arbejdet på at udvikle en fælles standard for de softwarebaserede certifikater, der er rygraden i den infrastruktur, som skal bruges til digitale signaturer. Certifikat-standarden hedder OCES, og Datatilsynet har givet tilsagn om, at den opfylder kravene til sikker kommunikation mellem myndigheder og borgere. Til standarden hører tre OCES-certifikatpolitikker (CP) for person-, medarbejder- og virksomhedscertifikater. Disse CP'er udgør en fælles offentlig standard, der regulerer udstedelsen og anvendelsen af den digitale OCES-signatur. CP'erne fastsætter krav til nøgleinfrastrukturen og dermed sikkerhedsniveauet for OCES-signaturen. Såvel standard som certifikatpolitik er tilgængelig fra <www.signatursekretariatet.dk>. Projektet drives af IT- og Telestyrelsen, men det praktiske arbejde med udstedelse af certifikater forestås af et nøglecenter under TDC A/S, der har fået tildelt denne opgave efter et afholdt offentligt udbud.

Net-ID

I 2004 har danske pengeinstitutter – der også deltog i det udbud om driften af det centrale nøglecenter, der blev vundet af TDC – udviklet en alternativ sikkerhedsløsning til web-baseret

kommunikation. Ved hjælp af adgangskoden til en netbank-løsning får brugeren mulighed for at identificere sig over for en virksomhed via en web-kommunikation, der understøttes af samme sikkerhed som den, der gælder for brugerens netbank. Virksomheder, som ønsker at udbyde sikkerhedsløsninger via Net-ID, indgår aftale herom med PBS. Se nærmere <www.pbs.dk/it-services/net-id>.

4.3. Elektronisk bevishåndtering

4.3.a. Papirmediet og det digitale medium

Problemstillingen

På grund af sin fleksibilitet efterlader den digitale information, der manifesteres ved hjælp af elektromagnetisme, ikke noget "fingeraftryk" på sit medium. Data kan frit kopieres fra en diskette til en anden eller fra en server på Internet til en anden, og en sådan kopiering er ligefrem en nødvendig bestanddel af sådanne former for digital program- og dataanvendelse, informationsspredning mv. Udover at vanskeliggøre beviset for dokumenters ægthed og integritet har dette udvisket grænsen mellem original og kopi på det digitale område. Det har altid været vanskeligt at skelne den ene fotokopi fra den anden, men det er umuligt at skelne en datafil fra en "kopi" af den. Dette forhold, der har givet grundlag for frembringelsen af de sikkerhedsmæssige løsninger, der omtales i afsnit 4.2., kommer frem i den processuelle håndtering af digitale meddelelser i parternes Internet-aftaleforhold, ved sagsførelser ved domstole og i myndighedernes administrative arbejde.

Papirdokumentet

En række af disse problemstillinger tager udgangspunkt i de regler og den praksis, der er udviklet vedrørende papirmediet. Selv om det er muligt, ja ligefrem enkelt, at forfalske papirdokumenter, tillægger parter, myndigheder og domstole papiret en høj bevisværdi. Forklaringen herpå ligger delvis i vanens magt, dels i den lovregulering, der findes på en række områder om brug af dokumenter i papirform. Dertil kommer det strafferetlige værn mod indgreb i dokumenter ved reglerne om dokumentfalsk mv., jf. straffelovens kapitel 19. For underskrevne dokumenter antages det almindeligvis, at den part, der vil modbevise en underskrifts ægthed, må begrunde sin tvivl og føre det pågældende bevis, jf. generelt *Gomard*: Civilprocessen, 5. udg. (2000), s. 495 ff. med henvisninger. Papiret er først og fremmest velegnet til at bevise ægthed og integritet. I ældre tider var det almindeligt at

forsyne papirdokumenter med vandmærker eller at præge eller forsegle dem. Det papir, der anvendes til trykning af pengesedler, har en anden struktur end det, der anvendes i gængs kontorhold, hvilket vanskeliggør falskmøntneri. Også fortroligheden af papirbaserede informationer kan sikres, f.eks. gennem kuvertering og forsegling.

I takt med den teknologiske udvikling har papiret fået en mere tilbagetrukken rolle. I stigende grad må man nøjes med at lade informationen tale for sig selv. Talrige virksomheder og myndigheder anvender end ikke brevpapir, men påfører adresse og/eller bomærke under den almindelige udprintning. Denne udvikling, hvorefter mediet ikke udgør noget endegyldigt bevis for afsenderens autenticitet mv., mærkes også ved den stigende anvendelse af fotokopier. I talrige tilfælde tjener fotokopierede dokumenter (f.eks. tilladelser mv.) samme funktioner som originaleksemplaret. Retsplejelovens § 351, stk. 3, der pålægger procesparter at fremlægge sagens "dokumenter", håndteres i vid udstrækning således, at retterne tillader fremlæggelse af fotokopier. At der eksisterer en kopi indicerer, at der foreligger en tilsvarende original. Forfalskning i forbindelse med fotokopiering er ikke hyppigt forekommende, og den forvanskning, der kan indtræde under selve kopieringsprocessen, fremstår almindeligvis klart for omverdenen.

Det er altså ikke retlige krav, der tvinger retslivet til at gøre brug af papirmediet. Når handelspartnerne desuagtet ofte besegler rettigheder og forpligtelser med papir, skyldes det først og fremmest praktiske forhold af den art, der ligeledes har ført til papirets dominans som grundlag for etablering af aftaleretlige forpligtelser. Hvor digital information alene kan læses ved hjælp af udstyr, kan den skrevne tekst læses af enhver, der har kendskab til det pågældende sprog. Papiret er velkendt og let håndterbart for alle. De hændelser, hvorved information knyttes til papiret, har man typisk kontrol over.

4.3.b. Bevismulighederne

Mulighederne for at føre et elektronisk bevis beror først og fremmest på det anvendte medium. Herudover spiller det ind, hvorledes de agerende parter har optrådt i forbindelse med dette medium, jf. herom i afsnit 4.3.d.

Det første elektroniske medium, der vandt generel anvendelse som grundlag for aftaleindgåelse mv. var fjernskriverteknologien, også kaldet telex. Telex var en videreudvikling af telegrafi, Telex

hvorved data overførtes bogstav for bogstav i en kode (morsealfabetet), der repræsenterer hvert bogstav med lange og korte signaler. Til hvert tegn hørte en impuls (en elektrisk strøm), der transmitteredes på nettet fra en telex-maskine og til en anden, hvor den frembragte et tegn. I dag anvendes telex primært ved handelssamkvem med parter, der ikke har adgang til et effektivt telefonnet, f.eks. i den 3. verden.

Telefax

Telefax har gennem årtier udgjort den hyppigst anvendte teknologi til elektronisk transmission af tekst over afstande. I modsætning til telex overfører fax-transmissionen den information, der fremtræder visuelt på en papirflade, f.eks. som ord, billeder, håndskrift mv. Ved transmissionen skannes dette billede ind i afsender-faxen, hvor det konverteres til digitale signaler, der transmitteres via det offentlige telefoni-net for at blive modtaget i modtager-telefaxen. Her konverteres det til et tilsvarende billede, som enten udskrives på en ny side eller lagres i fax-maskinens hukommelse. Telefax kan dog også sendes rent digitalt fra computer til telefax-apparat, fra computer til computer eller fra telefax til computer. I relation til denne teknologi er der således indtrådt en betydelig grad af konvergens. Afgørende er, om den pågældende standard (telefaxens "sprog") er overholdt af afsender og modtager.

- sikkerhed

Telefax-transmission sker i overensstemmelse med standarder, der bl.a. sikrer, at afsender og modtager identificeres, og at transmissionen forløber som forventet. Efter hver side sender afsender-faxen et såkaldt MPS-signal (Multi Page Signal) til modtager-faxen, der bekræftes med modtager-faxens MCF-signal (Message ConFirmation). Først når MCF-signalet er modtaget, kan næste side sendes. Når sidste side sendes, sender afsendermaskinen et EOP-signal (End Of Procedure), der igen kvitteres med et MCF-signal. Modtagelsen af dette MCF-signal giver afsenderens maskine ordre til at skrive "OK", der markerer afslutningen på telefax-transmissionen. To parter kan også kommunikere via telefax efter særlige standarder, bl.a. for at hindre aflytning.

- bevisværdi

Som bevismiddel fungerer en telefax nogenlunde som en fotokopi af et brev, og det er i dag almindeligt anerkendt, at telefax-kopien af en underskrevet kontrakt udgør et bevis for aftaleindgåelse. Denne praksis kan dog ikke helt overføres til den rent digitale telefax, hvor teksten frembringes af afsenderens computer. Undertiden anerkendes telefax som bevis for, at en meddelelse er sendt til en given part. Dette skyldes, at telefax-transmissioner normalt afsluttes med, at afsender-maskinen udskriver en såkaldt transmissionsrapport (*activity report*).

Bevisværdien af denne rapport beror dog på de nærmere omstændigheder omkring afsendelsen og modtagelsen af det pågældende telefax-dokument, herunder ikke mindst *sammenhængsbeviset*. Det må antages, at beviskravene skærpes, hvis der er tale om et påkravsdokument, der tilsigter at udløse bestemte retsvirkninger, sml. således den utrykte ØLD, af 21. august 1998, der er omtalt i Advokaten 2/1999, s. 76. Dommen fandt det ikke bevist, at en telefax-transmitteret ophævelse i henhold til lejelovens regler, som ifølge lejeren var fremsendt til en defekt telefax-maskine, var kommet frem til lejeren. Udsættelse nægtedes derfor.

- tidsbeviset

Transmissionsrapporten angiver, hvor mange sider der er sendt og til hvilken abonnent. På visse fax-maskiner angives herudover tidspunktet for transmissionen. Ved siden af originaldokumentet, som dog almindeligvis vil være upåvirket af telefax-transmissionen, vil denne rapport være det eneste "bevis" for, at der er afsendt en fax. Bevisværdien af denne rapport er dog begrænset. Tidspunktet for afsendelsen bestemmes af det ur, der er placeret i afsenderapparatet, og dette ur indstilles af fax-operatøren. Rapportens angivelse af antal transmitterede sider siger dernæst intet om, hvilke sider der er tale om. Transmission af blanke sider vil figurere på linie med transmission af tekstfyldte sider. Blanke sider vil dog pga. den nødvendige skanningsproces blive transmitteret hurtigere end informationstunge sider. Men da transmissionstiden også påvirkes af andre faktorer – net-tilgængelighed, varighed af *handshake* procedure etc. – står tid og informationsmængde ikke i et så præcist forhold til hinanden, at man kan regne baglæns fra tidsforbruget og til informationsmængden. Dertil kommer, at modtagermaskinens anerkendelse af, at en telefax er modtaget, ikke indebærer bevis for, at det modtagne også er læsbart. Som nærmere udviklet i afsnit 19.1.e. må det ikke desto mindre antages, at telefaxen i sådanne tilfælde er "kommet frem".

Internet-kommunikation

Da Internet fik sit første kommercielle gennembrud, var det som understøttelse af *bruger-til-bruger*-kommunikation ("one-to-one communication"), hvor kommunikationsprocessen alene indbefatter en afsender og en modtager. I en sådan kommunikation mellem parter, der (typisk) i forvejen kender hinanden, spiller nettet samme rolle som teleselskabet gør ved telefoni og postvæsenet ved postbesørgelsen. Bruger-til-bruger-kommunikation kan enten ske ved, at parterne udveksler tekstmeddelelser med hinanden som i en telefon (såkaldt "chat", altså "snak"), ved at der overføres elektroniske meddelelser i særskilte pakker (elektronisk post) eller som isolerede tekstmængder (såkaldt filoverførelse). Uanset om digitale meddelelser overføres på denne måde eller ved kommunikation "*one to many*" (f.eks. via hjemmesider

eller nyhedsgrupper), kopieres den enkelte meddelelse fra et medium til et andet i en lang kæde, der ultimativt fører til, at meddelelsen til sidst genskabes på et medium, som den tilsigtede modtager har adgang til. Denne procedure forudsætter en protokol, der fastslår, hvilke dataelementer der flyttes hvorhen og i hvilken rækkefølge. De Internet-protokoller, der anvendes, indebærer, at man ikke på forhånd ved, hvilke *routere* og *hosts* meddelelsen lægger sig på undervejs fra afsender til bruger.

Elektronisk post

Når meddelelser udveksles som led i elektronisk post (e-post), går meddelelsen fra og til en e-postadresse på Internet. E-postadressen styres af en Internet-leverandør, der som led i sin tjeneste vil tilbyde funktioner, hvorefter pakken ligger klar til afhentning, når brugeren kobler sig op på systemet. Visse systemer vil tillige sende en kvittering til afsenderen, når en meddelelse er modtaget, henholdsvis læst af modtageren. Generelt vil systemet advare afsenderen inden et par dage eller timer, hvis en e-mail-meddelelse ikke kommer frem. Denne advarselsfunktion er dog ikke ganske sikker. Under et må det nok siges, at afsendelse og modtagelse af e-mail ikke foregår under særligt høje sikkerhedskrav. For det første kan der være usikkerhed om, hvorledes den person eller virksomhed, der *hoster* e-mail-serveren, sikrer modtagne mails. Navnlig ved brug af e-mail-adresser, der stilles til rådighed for brugeren som en gratisydelse (for eksempel den meget populære *hotmail.com*), har brugeren ingen garanti for, at modtagne e-mails opbevares sikkert. Hertil kommer – for alle typer af mails – den usikkerhed, der består for, at modtagne mails utilsigtet slettes som uønsket *spam*. Det antages i dag, at hovedparten af de e-mails, der transporteres på internettet, er spam. Derfor har såvel brugere som mailhosts set sig nødsaget til at etablere spam-filtre, der med større eller mindre præcision afviser indkomne mails. Usikkerheden om denne præcision er samtidig en usikkerhed om, hvorvidt *ønskede* e-mail modtages. Ligeledes må det antages, at de transaktionsoplysninger, der registreres i forbindelse med megen elektronisk kommunikation, *i sig selv* har en begrænset bevisværdi, bl.a. fordi det er forholdsvis enkelt at ændre disse oplysninger efterfølgende, uden at en sådan ændring kan eftervises.

Pdf-filer

Med udbredelsen af det meget benyttede pdf-format for lagring af elektroniske dokumenter har vi fået en kommunikationsform, der bevismæssigt befinder sig midt mellem e-mail og telefax. En pdf-fil bygger på et grafisk format, der sikrer en høj grad af lighed med et dokument af anden art. Pdf-filer kan enten frembringes ved, at dokumenter printes fra et tekstbehandlingssystem

til pdf-formatet, eller gennem indskanning. I begge tilfælde opnås en grafisk fremtrædelse, som efter udprint på en printer med højoplysning (f.eks. en laserprinter) fremstår med samme kvalitet som ethvert andet dokument, og navnlig med en bedre kvalitet end et dokument overført med telefax.

Ifølge § 4, stk. 3, 2. pkt., i bekendtgørelse nr. 1331 af 14. december 2004 om indsendelse og offentliggørelse af årsrapporter m.v. i Erhvervs- og Selskabsstyrelsen kan regnskaber i en forsøgsperiode indsendes i bl.a. et pdf-format, som indeholder den fuldstændige version af den reviderede og godkendte årsrapport.

4.3.c. Bevisreguleringen

Et bevis knytter altid an til et tema: den faktiske omstændighed, som beviset skal godtgøre eksistensen af, og som – direkte eller indirekte – er slået an i retsreglen. Temaets karakter vil bero på sagens problem.

Bevisbedømmelsens frihed

Dansk bevisret bygger på få og generelle principper, der dels fremgår af retsplejeloven, dels udledes af domstolenes praksis. Efter retsplejelovens § 344 afgør retten på grundlag af det, der er passeret under forhandlingerne og bevisførelsen, hvilke faktiske omstændigheder der skal lægges til grund for sagens pådømmelse. Lovens § 896, der gælder i straffeprocessen, fastslår udtrykkeligt, at bedømmelsen af bevisernes vægt ikke er bundet ved lovregler. Begge regler udtrykker en almindelig grundsætning om bevisbedømmelsens frihed, der ligeledes afspejles i en række af de materielle retsregler, jf. hertil i det hele *IT-sikkerhedsrådet*: Digitale dokumenters bevisværdi (1999).

Se ligeledes CISG artikel 11, hvorefter beviset for en aftale kan godtgøres på en hvilken som helst måde og nærmere *Gomard*: Civilprocessen, 5. udg. (2000), s. 495 ff., *Eva Smith*: Civilproces, 4.udg. (2000), s. 140 ff., *Zahle* U1978B.375 ff. og i det hele *Klaus Østergaard Jensen*: Elektronisk udveksling af informationer i juridisk belysning. EDB-gruppen Herning, Oktober 1996.

De fleste former for bevis kan derfor fremføres for en dansk domstol, sml. f.eks. *U 1984.40 H*, *U 1997.1290 ØLK* og *U 2000.2210 H*, der alle tillod afspilning af, henholdsvis fremlæggelse af udskrifter fra, en båndoptagelse, *U 1999.673 ØLK*, der tillod afspilning af en videofilm med henblik på spørgsmål til skønsmand, men derimod *U 2004.2863 ØLK*, der ikke ville lade videofilm og fotos danne grundlag for et syn og skøn i en sag mod en byggesagkyndig. Se også *TBB 2000.224 Ø*, der tillod

afspilning af videooptagelser i en lejesag til brug for rettens vurdering af sammenligningslejemål.

Der er således ingen tvivl om, at også digitale bevismidler kan føres og efter omstændighederne kan tillægges vægt ved danske domstole.

Det sidstnævnte resultat følger udtrykkeligt af art. 5 i direktivet om elektroniske signaturer (1999/93/EF), hvis stk. 2, litra b) fastslår, at medlemsstaterne skal sikre, at avancerede elektroniske signaturer, der er baseret på et kvalificeret certifikat, og som er genereret af et sikkert signaturgenereringssystem, kan godtages som bevismateriale under retssager. Bestemmelsen er ikke implementeret direkte i dansk ret, da dette så åbenbart følger af gældende bevisret. Digitale medier synes således første gang – omend forudsætningsvis – antaget ved *U 1978.652 HKK*, der fulgte en begæring fra anklagemyndigheden om udlevering af navne, CPR-numre og adresser fra et socialkontor's IT-system med henblik på en straffesag. Kendelsen tager dog ikke stilling til, hvorvidt – og i givet fald: hvordan – de pågældende edb-lister ville kunne anvendes som bevis under den senere sag. Se tilsvarende *U 1994.576 H*, hvor Værdipapircentralen blev pålagt pligt til at udlevere elektronisk lagrede oplysninger til brug for en straffesag, jf. retsplejeloven § 827. I henhold til strfl. § 263, stk. 1 nr. 1, er det alene strafbart at aflytte eller optage udtalelser fremsat i enrum, telefonsamtaler eller anden samtale mellem andre eller forhandlinger i lukket møde, som gerningsmanden ikke selv deltager i. Pkt. 5.4.4. i de advokatetiske regler, der er vedtaget af Det Danske Advokatsamfund, fastslår, at en advokat ikke må optage eller medvirke til optagelse af telefonsamtaler eller andre kommunikationer på lydbånd eller lignende, uden at den anden part eller de andre deltagere på forhånd har samtykket i optagelsen. Bestemmelsen er et udtryk for det princip om transparens, der gælder for danske advokater, se hertil *Bryde Andersen*: Advokatretten (2005), s. 482 f.

Hvorvidt det er nødvendigt at oplyse sagen på et givet punkt, beror på rettens skøn over, om belastningen ved at føre et bevis står i forhold til sagens genstand, og på mulighederne for, at beviset vil belyse relevante dele af sagsforløbet. Bevisadgangen vil ofte være større i sager, der udspringer af et kompliceret forløb, og som involverer store værdier. Tilsvarende vil man ofte give friere adgang til at føre bevis i voldgiftssager, hvor der ikke er mulighed for appel, end i byretssager.

Bevisvægt

At kunne føre et bevis er ikke ensbetydende med, at beviset tillægges vægt ved sagens pådømmelse. I denne vurdering vil dommeren sammenligne det pågældende forhold med sin egen fornemmelse af livets erfaringer. Dele af handlingsforløbet vil gradvist sammensætte sig til det billede, dommeren herefter lægger til grund. Dommerens bevisskøn må inddrage visse normati-

ve hensyn. Derfor opererer man i praksis med forskellige *bevisformodninger*. Ved afgørelsen af, om et bevis opfylder den *bevisbyrde*, der påhviler en procespart, må man inddrage de konsekvenser, der vil følge af at operere med et lavt eller strengt beviskrav. Strenge beviskrav vil alt andet lige tilskynde parterne til forudgående at sikre sig deres bevis. På den anden side kan de føre til en ubillig forskelsbehandling mellem dem, der er forudseende nok til at sikre deres beviser, og andre.

Risikoregler

Det kommer for det første den part, der er nærmest til at sikre sig et bevis, til skade, at han i det konkrete tilfælde ikke har sikret sig. Har man f.eks. teknisk mulighed for i sit IT-system at registrere tidspunktet for afsendelse og modtagelse af transmissioner (f.eks. gennem logning el.lign.), kan undladelse af at gøre brug af disse faciliteter efter omstændighederne komme den systemansvarlige til skade, når han skal føre sit bevis for, hvornår en meddelelse blev sendt. Synspunktet rummer et culpa-element i sig og forudsætter en kvalificeret vurdering af den almindeligt fulgte handlemåde. Er det f.eks. sædvanligt at anmode modtageren af en meddelelse om at kvittere herfor, og undlader man at anmode herom, har man i givet fald selv bevisbyrden for, at meddelelsen er sendt. Tilsvarende, hvis det i en given sammenhæng ikke forventes, at kommunikerende parter gør brug af log, vil en undladelse af at gøre dette næppe få negative bevisvirkninger.

Enhver form for bevissikring er ikke nødvendigvis til fordel for den bevissikrende. I *U 1985.877 H* havde en forbruger sikret sig et bevis for en prisangivelse i en forretning ved at fotografere dennes udstillingsvindue. Højesterets flertal anså dette som et indicium for ond tro om rigtigheden af den pågældende – fejlagtige – prismærkning.

Retlige hensyn

For det andet beror beviskravene på retsforholdets karakter. Er der store værdier på spil, vil man i almindelighed stille større krav til bevissikringen end ved mindre værdier. Således skal der i almindelighed meget til at fastslå, at endelig aftale om køb af fast ejendom er indgået mundtligt, om end et sådant bevis kan tænkes, jf. til illustration dommene i *U 1988.233 H* og *U 1988.522 H*. Ligeledes kan offentligretlige krav få betydning. *U 1989.1098 H* lod f.eks. bevisbyrden for, at en havelåge stod åben, falde på havelågens indehaver, da havelågen var indrettet i strid med en bygningsforskrift, der påbød lukkeanordning.

"Hearsay"

Dansk ret indeholder ikke – som visse udenlandske retssystemer – et forbud mod indirekte beviser (såkaldt *hearsay evidence*). Selv om vidne- og dokumentbeviserne dominerer i danske retssale, afskærer det forhold, at en hændelse hverken er bevidnet eller

beseglet, ikke parterne fra at bevise, at den fandt sted. Talrige masseforsendelser afsendes af offentlige myndigheder, banker, forsikringsselskaber og organisationer, uden at der ligger nogen specifik vilje bag hvert enkelt brev. I sådanne tilfælde, samt hvor hændelsen er initieret automatisk, må der føres bevis for systemets indhold eller egenskaber.

4.3.d. Bevisformer

1. Aftalt bevis

I dispositive sager kan parterne selv råde over processen og træffe aftaler om dens tilrettelæggelse og førelse. Denne frihed gælder imidlertid kun *under* processen, hvor rækkevidden af procesaftalen er til at overskue. Anderledes stiller det sig med bevisaftaler indgået *før* processen, hvor aftalefriheden dels kolliderer med reglerne om bevisbedømmelsens frihed, dels kan risikere at medføre uoverskuelige konsekvenser for parterne. Det antages derfor, at en aftale, der på forhånd afskærer en part fra at føre et bevis, ikke udelukker adgangen til at føre modbevis, jf. nærmere *Gomard* (2000), s. 472 f. I de kommunikationsaftaler, der ofte indgås mellem parter, der påtænker at anvende digital teknik som grundlag for deres samhandelsforhold, indtager den bevisretlige regulering en central placering.

- gyldighed

I konsekvens af dansk rets udgangspunkt om bevisbedømmelsens frihed er domstolene ikke bundet af forudgående aftaler mellem parterne om, hvorledes et bevis skal føres eller vægtes. En aftale, der fastslår, at en meddelelse skal anses som "afgivet", når modtageren kan bevise, at den må være krypteret efter en særlig algoritme eller ved brug af et magnetkort el.lign., afskærer derfor ikke domstolene fra – hvis der er grundlag herfor i den konkrete sag – at antage, at der foreligger et falsum. Sådanne aftaler er da heller ikke udbredte. Derimod må domstolene i højere grad formodes at ville acceptere aftaler, der omlægger bevisbyrden i den senere sag. Ligeledes vil en vedtagelse om, at der for bestemte, forpligtende meddelelser mv. anvendes særlige medier (f.eks. skriftlig opsigelse), ofte blive fortolket således, at der påhviler den part, der undlader at efterkomme dette krav, en særligt stor bevisbyrde, jf. *U 1998.1623 Ø*.

Den britiske EDIA-kontrakt bestemmer bl.a. i pkt. 5.2, at "[e]ach party accepts the integrity of all Messages and agrees to accord these the same status as would be applicable to a document or to information sent other than by electronic means, unless such Messages can be shown to have been corrupted as a result of technical failure on the part of machine, system or transmission line". En sådan bevis-

byrdeaftale vil navnlig have autoritet, hvis den følges op af foranstaltninger, der tjener til at skabe sikkerhed for troværdigheden af det pågældende bevis.

Faktum og hæftelse

Retsvirkningen af aftaler, der på forhånd slår fast, hvorledes et bestemt faktum skal anses for at være forløbet, har i hovedsagen samme virkning som aftaler, der på forhånd tager stilling til, hvem der hæfter økonomisk for et bestemt forhold. Forskellen mellem disse to måder at regulere en usikkerhed på kommer ofte frem i sager om regningsklager mod forbrugere. Her må der i givet fald anlægges to forskellige strategier af den part, der vil gøre indsigelse mod en sådan aftale. Hvor bevisaftaler kan blive underkendt af retten med henvisning til det *frie bevisskøn*, retsplejeloven overlader retten, må en aftale, der på forhånd pålægger forbrugeren en vidtgående hæftelse, i givet fald angribes efter aftaleretlige ugyldighedsregler som *urimelig* mv. Overfor en forbruger kan det således tænkes, at en sådan aftale vil "stride mod hæderlig forretningsskik og bevirke en betydelig skævhed i parternes rettigheder og forpligtelser til skade for forbrugeren", hvorved aftl. § 38c finder anvendelse, således at de i § 36, stk. 1, nævnte retsvirkninger også gælder. Forbrugeren kan i så fald kræve, at den øvrige del af aftalen skal gælde uden ændringer, hvis dette er muligt.

Bestemmelsen er f.eks. anvendt i *U 2003.1883 V* i en sag, hvor forbrugeren – og i et tilfælde også dennes søn – via et såkaldt opkaldsprogram havde udvirket, at der i tiden fra 14. til 27. juli 2000 var foretaget 74 udlandsopkald til St. Helena. TDC afkrævede forbrugeren et beløb på 30.969,26 kr. under henvisning til abonnementsvilkårene, der lod kunden hæfte for alle ydelser leveret i henhold til abonnementsaftalen. Landsretten fandt, at det for den almindelige bruger uden særlige forudsætninger kunne fremstå som ganske uklart, hvilke nærmere konsekvenser en accept af disse vilkår ville få. Navnlig havde risikoen for at kunne udvirke opkald til en anden og langt højere takst end den almindelige takst for internetforbindelsen ikke været betydet for kunden. TDC, der kendte til problemerne med de uønskede opkald til Skt. Helena, havde ikke taget skridt til at forhindre disse. På denne baggrund fandt retten det urimeligt at gøre det nævnte vilkår gældende mod forbrugeren, jf. aftl. § 38c, jf. § 36.

2. Systembevis

I tilfælde af tvivl om, hvorvidt en elektronisk meddelelse er afsendt eller modtaget, vil det almindeligvis være nødvendigt at føre bevis for systemets funktioner samt de arbejdsgange, der omgiver det – et såkaldt systembevis. Et sådant bevis vedrørende systemets *funktioner* må almindeligvis tilvejebringes gennem sagkyndige erklæringer og udtalelser om muligheden for at udskrive forskellige typer af informationer. Se til illustration *U*

1991.451 V, der på grundlag af diagramark fra fartskriveren i en lastvogn samt forklaringer fra tre sagkyndige vidner lagde til grund, at der var begået en hastighedsoverskridelse. Omvendt fandt landsretten i *U 1995.144 V* ikke, at de oplysninger om en kommunes udsendelse af årsopgørelser, der var lagt frem under sagen, indebar tilstrækkeligt bevis for, at en årsopgørelse var blevet sendt til og modtaget af tiltalte (som dermed blev frifundet for skatteunddragelse). I *U 2005.404 V* havde en udlejer heller ikke ført tilstrækkeligt bevis for, at et istandsættelsespåkrav var afsendt. Brevet var kun afsendt med almindelig post, udlejeren havde ikke sikret sig kvittering for indlevering af brevet til postbesørgelse, og det eneste bevis, der forelå for dets afsendelse, var en medarbejders forklaring om, at brevet var lagt i postrummet for udgående post. *U 2005.___ VLK* (13.5.05) fandt, at den historiske oversigt, der kunne uddrages af en banks IT-system, udgjorde tilstrækkeligt bevis for, at der var sendt et brev, der gyldigt opsagde et gældsbrev. Oversigten var bankens eneste bevismiddel, idet det ikke var muligt at udskrive en kopi af hver enkelt af de breve, der var udsendt. Brevene havde en standardtekst, der efter det oplyste ikke kunne ændres i det enkelte brev.

I sager om kompliceret teknik må beviset for sådanne tekniske forhold ofte føres med bistand af ekspertise udefra. Sådanne sagkyndige erklæringer og vidneudsagn er i almindelighed uproblematiske at have at gøre med, for så vidt de afklarer en teknisk kendsgerning, som retten ikke selv kan anskue eller forstå, men som den sagkyndige med sin ekspertise har fuldt overblik over. Den dømmende instans vil ikke altid – og bør ikke – uden videre lægge indholdet af en sagkyndig erklæring til grund, selv om det vidensspring, der består mellem den og sagkundskaben, ofte vil gøre dette nærliggende.

Særlige problemer opstår, hvis erklæringen alene udtaler sig om en sandsynlighed eller i øvrigt beror på et skøn. Efter det domstolssystem, der er gældende i Danmark, ligger kompetencen til at udøve sådanne skøn mv. som udgangspunkt hos domstolene, og det er da også fornemmelsen, at domstolene anser sig for bedst skikket hertil. Eksempelvis har domstolene udvist betydelig skepsis overfor grafologiske skøn, se nærmere *Palle H. Dige* (1945), s. 84 ff. med henvisning til praksis.

- arbejdsgange

For at supplere oplysningerne om systemfunktionerne er det ofte nødvendigt tillige at belyse de *manuelle arbejdsgange*, der f.eks. bringer systemets data ud på papir og derfra videre til forsendelse. Dette vil typisk ske gennem afhøringer af de personer, der er placeret ved systemets indlæsnings- og udskrivnings-

enheder. Se herved *U 1990.233 H*, der lagde til grund, at en skrivelse – om hvilken der alene forelå et elektronisk lagret bevis for afsendelsen – var afsendt. Der forelå forklaringer af de systemfolk, der stod for den tekniske effektuering af udsendelsen.

- masseudsendelser

En organisation, der beror på en stærkt styret og effektiv administration, og som fører en hårdhændet sikkerhedspolitik (forsikringsselskaber, banker m.fl.), har lettere ved at løfte en sådan bevisbyrde end en organisation, der anvender mere tilfældige rutiner for, hvordan data bringes fra udskrivningsenheder til adressat.

- U 1977.216 Ø

Illustrerende herfor er *U 1977.216 Ø*: Et forsikringsselskab havde opsagt sine forsikringer ved brev til samtlige kunder. Brevene var distribueret automatisk og sendt som masseforsendelser adskilt fra forsikringsselskabets anden post. En forsikringstager bestred at have modtaget den pågældende notits. Han forklarede i retten, at han vel havde modtaget anden post fra selskabet – blot ikke det pågældende brev. Der var under sagen ikke oplyst noget om irregulære omstændigheder ved postgangen. Østre Landsret lagde herefter til grund, at brevet var kommet frem til forsikringstageren.

- U 1995.144 V

Omvendt fandt Vestre Landsret ved dommen i *U 1995.144 V*, at en skatteyder ikke havde modtaget kommunens meddelelse om indkomstansættelsen, jf. skattekontrollovens § 16. Vel var tiltalte optaget på den liste, som Kommunedata for den pågældende kommune havde udarbejdet over skatteydere, der ikke havde indleveret selvangivelse; men det var ikke oplyst, hvilken kontrol kommunen havde gennemført samt de nærmere omstændigheder ved udsendelsen. Selv om landsretten fandt, at der var stor sandsynlighed for, at tiltalte havde modtaget denne meddelelse, var systembeviset med andre ord ikke ført. For rettens bevisafvejning har det formentlig spillet ind, at der var tale om en straffesag.

Se ligeledes Forbrugerklagenævnets afgørelse, der er gengivet i *FKNbrtn 1993-94, s. 245 f.* En benzinkunde afviste at være ansvarlig for nogle træk, der var foretaget på hans benzinkort i den periode, hvor kortene var under ombytning fra benzinselskabet. Trækkene var foretaget med det nye kort, som kunden afviste at have modtaget. Under sagen oplyste kortudsteder, at man ingen mulighed havde for at kontrollere, at brevet med det nye kort + kode var afleveret. I stedet kunne man føre systembevis vedrørende den svenske kortproducents sikkerhedsrutiner. Nævnet fandt, at benzinselskabet som kortudsteder bar risikoen for, at fremsendte betalingskort rent faktisk kommer frem. På baggrund af oplysningerne i sagen fandt nævnet ikke, at selskabet havde løftet bevisbyrden for, at kort nr. 2 med tilhørende pin-kode var

kommet frem til forbrugeren. Nævnet tilføjede, at benzinselskabet kunne have sikret sig et bevis herfor, f.eks. ved at fremsende kortet anbefalet.

Under procesordninger, der ikke anerkender sekundære beviser (hearsay), kan sådanne beviser ikke umiddelbart føres. Federal Rules of Evidence, Rule 803 (6), tillader som en undtagelse fra forbuddet mod hearsay-evidence bevisførelser af forretningsmæssige optegnelser mv. "... if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of the information or the method or circumstances of preparation indicate lack of trustworthiness."

- Digitale dokumenters bevisværdi

En part, der har makuleret et papirbilag, eller på anden måde skaffet det af vejen, står som udgangspunkt bevismæssigt svagt, hvis der efterfølgende opstår tvivl om dokumentets indhold. Denne tvivl kan ganske vist reduceres, hvis dokumentet forinden er blevet fotokopieret – hvis ellers fotokopien er god. Men der er i sagens natur intet fornuftigt formål med at makulere et dokument, hvis man i stedet opbevarer en fotokopi af det. Et sådant formål kan der derimod være, hvis man ønsker at erstatte dokumentet med en digital kopi af det i form af et *indskannet* dokument, som man herefter ønsker at anvende i den videre sagsbehandling. I sådanne tilfælde søges en eventuel bevisførelse løftet ved, at man lader en udprint af det indskannede dokument tjene som bevis for dets indhold. I disse tilfælde opstår spørgsmålet, om det er bevismæssigt forsvarligt generelt at indføre en procedure, hvorefter modtagne papirdokumenter makuleres, når de er indskannet.

- IT-sikkerhedsrådet

I *IT-sikkerhedsrådet*s vejledning: Digitale dokumenters bevisværdi, s. 13, udtales det, at en sådan procedure må anses for forsvarlig, hvis der gennemføres en række nærmere angivne foranstaltninger i forbindelse med dokumentets indskanning og efterfølgende lagring. Anbefalingen hviler på min juridiske redegørelse om den bevismæssige stilling, der er optrykt i bilagshæftet til vejledningen, s. 119 f. og 122 ff. Den understøttes i øvrigt af nyere bevisretlig praksis. Ved dommen i *U 1997.949 V* havde et forsikringsselskab, der havde makuleret en forsikringsbegæring, således løftet den – tunge – bevisbyrde, selskabet havde for, at begæringen på tidspunktet for forsikringstagerens underskrivelse indeholdt et selvrisikobeløb.

De procedurer, der således må gennemføres, må for det *første* sikre, at den information, der indskannes, informationsmæssigt kommer til at svare til originaldokumentet. Med nutidens tekno-

logi er der som regel ingen nævneværdige problemer herved. De fleste systemer til "bitmap"-skanning tilbyder en fasthed i så henseende, der mindst er på højde med den fotokopiering, som almindeligvis nyder anerkendelse ved domstolene. Men for det *andet* må det sikres, at der ikke sker efterfølgende manipulationer med den indskannede tekst. Navnlig dette krav giver anledning til en del særlige procedurer. Således kræver rådet, at der er gennemført en stram organisatorisk adskillelse af de forskellige funktioner, der spiller en rolle ved indskanningen og brugen af dokumentet.

På linje med de retningslinier, der følger af god skik for bogføring og regnskab, og som sikrer, at en enkelt person ikke har kontrol over alle funktioner i processen, udtaler rådet som nævnt, at arbejdsgangene omkring digital dokumentbehandling bør opbygges således, at der gennemføres en klar adskillelse mellem forskellige funktioner i forbindelse med dokumentbehandlingen. For dokumenter, som modtages på papir, bør der således være en organisatorisk adskillelse mellem: 1. Procedurer til modtagelse, skanning og lagring; 2. Kvalitetssikring af skanningen; 3. Sagsbehandlingsfunktioner og 4. IT-driftsfunktioner.

Det siger sig selv, at sådanne krav alene er praktikable, hvis man befinder sig inden for en organisation af en vis størrelse. Derfor forudsætter vejledningen, at den primært finder anvendelse i organisationer med mere end 30 ansatte.

- makulering?

Hvis de nævnte krav opfyldes, udtaler IT-sikkerhedsrådet, at det ikke vil være tilrådeligt at gemme de indskannede dokumenter for f.eks. at opbevare dem i en "dokumentsøjle". Der vil i sagens natur være dokumenter, der ikke bør makuleres, og det vil til enhver tid være op til organisationen at vurdere, hvilke typer af dokumenter som man – af juridiske grunde – vil bevare i original papirform (f.eks. organisationens eksemplar af en kontrakt eller et tilbud). Men ulempen ved at indføre en "dokumentsøjle" ligger i, at man herved etablerer to sideordnede arkiveringssystemer. For offentlige myndigheder kan dette være i strid med de regler, der er fastsat af Statens Arkiver, og som kræver, at elektroniske arkiver skal betragtes som det primære arkiv efter arkivlovens regler. Dertil kommer de særlige bevisproblemer, brugeren vil stille sig i, hvis det efterfølgende viser sig, at et dokument rent faktisk ikke lå i "dokumentsøjlen".

3. Sammenhængsbevis

En af de mest effektive metoder til at afsløre usande udsagn består i at konfrontere det enkelte udsagn med andre udsagn eller kendsgerninger. Har man sagt A, må man i mange tilfælde også sige B, C, D osv. Når præmisser udsættes for stringente logiske konsekvensfølger, får den, der ikke har sagligt grundlag for en

påstand, ofte vanskeligt ved at opretholde konsekvens og troværdighed. Man kan i disse tilfælde tale om, at der føres et bevis for sammenhængen i en faktuel påstand – et sammenhængsbevis.

I det praktiske retsliv tilgodeses muligheden for et efterfølgende sammenhængsbevis f.eks. ved, at vitale forpligtelseserklæringer, der ikke foreligger på tryk eller er manifesteret på anden vis, efterfølgende bekræftes på skrift. Ved at henvise til et afsendt brev i den senere korrespondance kan man på tilsvarende vis indicere, at brevet faktisk er afsendt og modtaget. Modpartens passivitet overfor sådanne tilkendegivelser vil – i hvert fald i forretningsmæssige mellemværender – kunne være bevis på, at brevet er modtaget, og at aftale svarende til bekræftelsen følgelig anses for indgået.

Sammenhængsbeviset indgår ofte som en rutinemæssig bestanddel i elektronisk kommunikation, fordi man i IT-systemet kan frembringe de ledsagende informationer automatisk, f.eks. i form af en "log", der angiver modtagen og afsendt elektronisk post. Herudover spiller det en stor rolle i praksis, at man kan fremkalde et sammenhængsbevis gennem sin optræden overfor den part, som bevistvivlen i givet fald vil rette sig imod.

- kvitteringskrav

Dette kan således ske, hvis afsenderen af en meddelelse stiller krav om, 1) at modtageren skal kvittere for meddelelsen, og 2) se bort fra meddelelsen, hvis ikke denne kvittering foreligger. En regel af dette indhold fandt allerede vej til de såkaldte UNCID-regler, som ICC vedtog så tidligt som i 1988, se art. 7, stk. 1. I artiklens andet stykke hedder det videre, at en afsender, der ikke har modtaget anerkendelsen inden for en rimelig eller aftalt tidsramme, skal tage initiativ til at fremskaffe den. Fører dette initiativ ikke til, at modtagelsen anerkendes inden for en yderligere rimelig tidsramme, skal der gives meddelelse herom. Afsenderen er herefter berettiget til at lægge til grund, at meddelelsen ikke er modtaget. Afkrævning af sådanne kvitteringer kan f.eks. meddeles automatisk i en EDI-løsning mellem parterne. En tilsvarende regel findes i art. 14, stk. 3-4, i UNCITRAL-modelloven om Electronic Commerce (1996). Artiklen giver ligeledes regler om retsstillingen mellem parterne, når et sådant krav er stillet: Modtages i så fald ikke en kvittering, kan afsenderen efterfølgende give meddelelse (reelt sætte en slags *Nachfrist*) om, at meddelelsen vil blive betragtet som ikke afsendt, hvis ikke kvittering modtages inden for "a reasonable time".

4.3.e. Særlige bevisregler

Betalingsmidler

Ved brug af betalingskort og andre betalingsmidler omfattet af LVB (lov om visse betalingsmidler) kan der opstå bevismæssig tvivl om, hvorvidt et betalingskort har været anvendt eller ikke. Denne bevissituation stiller sig forskelligt, alt efter om betalingsmidlet har været anvendt i den fysiske handel – under tilstedeværelse af i hvert fald en af parterne – eller i Internet-handel (hvor muligheden består for, at der kun er en part "tilstede", nemlig den gerningsmand, der retsstridigt anvender det pågældende betalingsmiddel).

- Internet-handel

Når der i forbindelse med Internet-handel opstår spørgsmål om, hvorvidt et betalingsmiddel er anvendt ved brug af betalingsmidlet *som sådant* (men uden tilhørende SET-signaturnøgle), må bevistvivl i almindelighed komme betalingsmodtageren (forretningsstedet) til skade. Kan betalingsmodtageren ikke bevise, at indehaveren af betalingsmidlet rent faktisk benyttede det, må der ikke debiteres fra betalingsmidlet.

I overensstemmelse med det bevisretlige udgangspunkt fastslår pkt. 5 i Forbrugerombudsmandens Retningslinjer vedrørende fjernsalg m.v. i betalingssystemer med betalingskort af december 1996, tilgængelig fra <www.fs.dk>, at en Internet-butik har pligt til at sætte debiteringen i bero – eller tilbageføre denne, hvis den er gennemført – hvis kunden gør gældende, at det enten ikke er kunden selv, der har foretaget eller givet tilladelse til betalingstransaktionen, at de bestilte varer ikke er blevet leveret, eller at kunden ønsker at udnytte en lovbestemt eller aftalt fortrydelsesret.

- fysisk handel

Situationen stiller sig noget anderledes, når betalingskort anvendes i den almindelige handel. En betalingskortindehaver, der gør gældende, at han på intet tidspunkt har sluppet hverken sit betalingskort eller dets kode, uanset der rent faktisk er sket træk herpå, står som udgangspunkt svagt, hvis der alligevel er sket træk på den pågældende konto. Betalingskortsystemerne er undergivet sikkerhedsmæssigt tilsyn af Forbrugerombudsmanden, jf. LVB § 4, og uden for tilfælde, hvor betalingskort og kode er blevet kopieret i forbindelse med brug af falske betalingskort-automater (i hvilke tilfælde der viser sig en flerhed af uberettigede hævninger, gerne udført uden for Danmark) vil det være vanskeligt at skabe en bevisformodning for, at hævningen *ikke* er autoriseret af kortindehaveren. Normalt anses kortindehaveren at have løftet sin bevisbyrde for, at han ikke har autoriseret brugen, ved at afgive en tro- og loveerklæring over for udstederen. Udste-

deren vil dernæst ofte stille som betingelse for at tilbageføre et debiteret beløb til kortindehaverens konto, at kortindehaveren politianmelder misbruget.

Talrige sager af denne art har været afgjort i byretspraksis. Se til eksempel dom afsagt af *Retten i Roskilde*, 15. oktober 1987 i SS nr. 140/1987 B, der afviste en forklaring afgivet af en Dankort-bruger om, at denne ikke havde udført et antal træk på sit kort. Dommen henviser til, at der i forbindelse med oprettelse af Dankort-systemet er truffet en række sikkerhedsforanstaltninger for at forhindre, at der sker misbrug af kortet, og at det er praktisk umuligt gentagne gange at hæve på kontoen uden kontohaverens medvirken. Begrundelsen er ikke uproblematisk, og dommens resultat kunne være nået ved hjælp af et sammenhængsbevis, sml. herom nedenfor, eller ved en troværdighedsvurdering af de afgivne forklaringer. Et tilsvarende bevis er i 1986 lagt til grund af Svea Hovrätt, se *Lindberg* (1987), s. 83 – ligeledes i en straffesag. Det norske Bankklagenemda har afvist lignende sager under henvisning til, at kundens oplysninger var så ekstraordinære, at sagen ikke egnede sig til skriftlig behandlingsform, se Complex 5/90, s. 98 (1989), sml. om dansk praksis *Møgelvang-Hansen* i Complex 5/91, s. 136 f., der bl.a. omtaler PIA 493/1989, hvor kortindehaverens manglende bidrag til sagens oplysning blev udslagsgivende.

Sager, hvor kortindehaveren bestrider, at kortet har været brugt til betaling af et så stort beløb som det bogførte (f.eks. pga. manglende omhu med at kontrollere det beløb, der angives, inden man taster "godkend" på salgsstedets terminal), må løses efter almindelige bevisretlige regler: Bevisbyrden for, at kortindehaveren har modtaget ydelser for et mindre beløb end det trukne, påhviler som udgangspunkt denne, hvis den gældende pinkode er indtastet. Men denne bevisformodning kan svækkes, hvis der er tale om et usædvanligt stort beløb og omstændighederne i øvrigt tyder på, at der har foreligget en fejl. Se i den forbindelse dommen i *U 2000.1853 V*, hvor det fandtes bevist, at et Dankort kun havde været anvendt til køb af drinks på en natklub for en værdi af 105 kr., uagtet kortindehaveren med sin pin-kode havde godkendt et træk på 10.500 kr.

Regningsklager

Et andet retsområde, hvor der hyppigt forekommer bevismæssig tvivl om, hvorvidt en digital transaktion har fundet sted, er klager over teleregninger. Også for disse tilfælde er det kendetegnende, at bevisførelsen knytter sig til et tema, som udspiller sig uden samtidig tilstedeværelse af parter og vidner. Sådanne regningsklager afgøres løbende af Telebrugernævnet, se <www.telestyrelsen.dk>, og ofte under inddragelse af sagkyndige erklæringer mv. Retsanvendelsen må her falde tilbage på *systembeviser*

kombineret med sandsynligheden for, at der foreligger retsstridigt misbrug fra anden side.

Se f.eks. Forbrugerklagenævnets afgørelser i *JÅF 1990.88* om bevisbyrden for, at det opkrævede beløb på en telefonregning ikke svarede til forbrugte telefonsamtaler. Teleselskabet fik her medhold under dissens og *JÅF 1997.97*, der fastslår, at teleleverandøren har bevisbyrden for, at sex-ydelser leveret pr. telefoni var bestilt af abonnenten. I Ballerup Rets dom af 16. december 2002 var spørgsmålet, hvem af parterne i en aftale om et telefonabonnement, der skulle bære bevisrisikoen for uberettiget brug af telelinjer, som kunne være foretaget af uvedkommende. Retten fandt, at teleselskabet var nærmest til at bære risikoen for uberettiget brug, der førte til et utilsigtet forbrug på godt 50.000 kr. Tvister vedrørende regningsklager mv. kan nu behandles af det private, godkendte klagenævn Teleankenævnet, der blev etableret i 2003 af telekommunikationsindustrien i Danmark og Forbrugerrådet til afløsning af det offentlige Telebrugernævn (der herefter er blevet nedlagt af VTU-ministeren i december 2004 på grundlag af bemyndigelsen i § 98, stk. 1, i telekonkurrenceloven). Se nærmere <www.teleanke.dk>.

4.4. Aftaler om IT-sikkerhed

4.4.a. Problemstilling

Aftaler om IT-sikkerhed indgås som regel kun for systemer af en vis størrelse og følsomhed. Spektret spænder fra den meget udbredte aftale om vedligeholdelse, som hyppigt forekommer i erhvervsmæssige driftsmiljøer af en vis størrelse, og til aftaler om mere særegne sikkerhedsløsninger – backup-centre, kildetekstdeponeringer og public key-infrastruktur.

4.4.b. Vedligeholdelse

En aftale om *vedligeholdelse* af et IT-system tilsigter at give brugeren en driftsmæssig stabilitet, der sikrer, at behov og funktion stedse svarer til hinanden. "Vedligeholdelse" af IT dækker dog ikke over helt det samme som vedligeholdelse af f.eks. biler og maskiner. Vel er visse aspekter ved IT-vedligeholdelse sammenfaldende med den vedligeholdelse af mekaniske dele, man kender i relation til andet teknisk udstyr – f.eks. justering af diskettestationer, rensning af magnethoveder og støvsugning af kabinetter. Men med nutidens modulært opbyggede systemer har dette arbejde undertiden håndværksmæssig karakter. I en række tilfæl-

de er det leverandøren af systemet, der yder denne vedligeholdelse, og overdragelse/implementering henholdsvis vedligeholdelse kan derfor være integrerede dele af samme kontrakt, jf. f.eks. modellen i K18, K33 og K01. Undertiden består der ligefrem en økonomisk sammenhæng mellem overdragelse og vedligeholdelse efter princippet om gyngerne og karrusellerne: Leverandøren prissætter sit system lavere mod til gengæld at få sin fortjeneste hjem i det lange løb gennem vedligeholdelsesafgifterne.

De større problemer omkring vedligeholdelse angår programmerne: dels den retning af småfejl og uhensigtsmæssigheder, der er en nødvendig følge af, at programmer aldrig er fejlfri, dels de ændringer, der er nødvendige for, at systemet kan modsvare de ydre forhold, det skal virke i (f.eks. rente- og afgiftssatser i et bogholderisystem). Var IT-systemerne 100% driftssikre og altid i harmoni med brugernes forudsætninger, ville der ikke være brug for vedligeholdelse. Et IT-system er imidlertid et fleksibelt værktøj, der stedse må tilpasses de gældende tekniske, regnskabsmæssige, juridiske og brugermæssige behov. Dernæst vil IT-systemer som regel være behæftet med fejl, der ofte optræder under uforudsete vilkår mv. Dette rejser et almindeligt behov for stedse at kunne ændre IT-systemets indmad – at vedligeholde det.

IT-vedligeholdelse har forskellig karakter, alt efter om der er tale om hardware eller software. For så vidt angår *hardware* (f.eks. printere, skærme, diskette- og båndstationer mv.) vil IT-brug og ydre påvirkninger være forbundet med slitage. Her indebærer vedligeholdelsen en teknisk pasning i form af f.eks. rengøring og udskiftning af bevægelige dele (forbrugsdele, f.eks. tonervæske, dog typisk undtaget). Et sådant slid opstår ikke på *softwaresiden*. Programvedligeholdelse afhjælper de uhensigtsmæssigheder og småfejl, som edb-programmer uundgåelig vil lide af, og sikrer den tilpasning, der er nødvendig, når brugerens organisatoriske miljø ændrer sig. En sådan vedligeholdelse vil enten ske i form af løbende fejlretning eller ved opdatering, hvorved brugeren modtager en ny udgave af programproduktet.

Uden særlig aftale kan køberen ikke forvente, at standardprogrammel vedligeholdes, ved at leverandøren efterfølgende tilbyder nye versioner af det. Det vil almindeligvis ligge klart, at leverandørens opdateringer hviler økonomisk i sig selv. Forholdet vil sjældent være således, at en del af købesummen dækker efterfølgende udvikling af nye versioner. Forsvinder markedet for disse nye versioner, forsvinder incitamentet ligeledes. En pligt til at forlange en økonomisk urentabel opdatering af et standardprogram må derfor have sikker aftalemæssig hjemmel. I

amerikansk retspraksis er man endog gået så vidt, at man har bortfortolket en kontraktsforpligtelse, hvorefter leverandøren skulle tilvejebringe "field installable model upgrades", se *Storage Technology Corp. v. Trust Company of New Jersey*, 842 F.2d 54 (1988).

Kildetekstadgang

Man kan kun vedligeholde et edb-program med adgang til dets kildetekst. Men da den, der har kildeteksten i hånden, forholdsvis enkelt kan frembringe lignende systemer, der i det ydre ingen lighed har med det eksisterende, er det almindeligt, at rettighedshaveren nægter at give kildetekst fra sig. Denne praksis er vel under opblødning i konsekvens af den såkaldte *open source*-bevægelse, der går ind for, at kildetekst skal være tilgængelig for brugeren, bl.a. med henblik på fejlrettelse og opdatering. Men holdes kildeteksten i *closed source* har brugeren et behov for at etablere ordninger, hvorved den kan skaffes til veje fra en uafhængig tredjepart hos hvem den er deponeret. Et program, som giver brugeren denne mulighed, er derfor mere "værdifuldt" for brugeren end ét, der i sin yderste konsekvens aldrig vil kunne opdateres.

Der er i øvrigt forskellige opfattelser af, om det generelt er en sikkerhedsmæssig fordel, at kildeteksten til et program er offentligt kendt. På den ene side giver det – alt andet lige – en højere sikkerhed, at brugeren kan konstatere, hvorfor programmet fungerer som det gør. Men på den anden side indebærer denne viden også, at en gerningsmand, der har i sinde at udnytte svagheder i programmet (f.eks. til at installere en virus eller skaffe sig adgang til hemmeligholdt information) har lettere herved. Her, som på andre områder af læren om IT-sikkerhed, kan der ikke gives generelle svar. Den enkelte bruger må ud fra en konkret risikovurdering bestemme sig for, hvad der passer bedst i hans situation.

Dokumentation

Selv om man råder over kildeteksten, kan vedligeholdelse være mere eller mindre kompliceret. Mulighederne for at ændre et program beror på, hvor godt programmet er dokumenteret, dvs. hvor klart og præcist de ledsagende beskrivelser er formuleret. Mange IT-systemer, der udvikles i småvirksomheders IT-afdelinger, udspringer af en enkelt programmørs arbejde. Denne person er måske tilmed overbelastet, og da han – subjektivt – godt kan huske, hvordan han skrev de enkelte programmer, får han aldrig skrevet dokumentationen ned. Problemet kommer da først op til overfladen, når medarbejderen forlader afdelingen – og en anden skal træde i hans sted – eller hvis virksomheden skulle finde på at sælge et eksemplar af sit system til en anden virksomhed, der herefter selv skal vedligeholde det.

Andre forhold

Endelig beror vedligeholdelsesmuligheden på en række forhold, der har at gøre med det enkelte programs karakter. Bl.a. spiller den *struktur*, der er lagt til grund i systemet, en stor rolle for muligheden for at vedligeholde. I et dårligt struktureret program, hvor en udenforstående hverken kan se hoved eller hale i mængden af programinstruktioner, er det selvsagt vanskeligere at finde den instruktion, der skal ændres, end i et klart struktureret program. Også dette udgør et væsentlig kvalitetsparameter.

På markedet for standardprogrammel indgås der sjældent aftaler om vedligeholdelse. Brugerens behov tilgodeses af markedsmekanismerne. Leverandører af standardløsninger giver ofte udtrykkeligt eller forudsat tilsagn om i fornødent omfang at udsende opdaterede versioner af programmet, når efterfølgende forhold (herunder nye tekniske eller markedsmæssige krav) gør dette nødvendigt. Se f.eks. K18, bilag 10, pkt. 3.1, hvorefter leverandøren "i overensstemmelse med god praksis inden for branchen" vil udarbejde nye udgaver af det leverede programmel. Sådanne nye versioner eller "releases" kan typisk købes af brugere af tidligere versioner for beløb, der ligger langt under startprisen, forudsat at de medier (diskette, tastatur-skabelon, manual mv.), der hører til den tidligere version, returneres til leverandøren.

For de skræddersyede edb-programmer er forholdene anderledes. Når systemet er udviklet og afleveret, vil leverandøren alt andet lige ikke længere være tilskyndet til at vedligeholde systemet. Principielt ville der intet være til hinder for, at brugeren herefter selv forestod vedligeholdelsen. En sådan vedligeholdelse forudsætter en rådighed over kildeteksten; men den vil leverandøren sjældent ønske at give fra sig, sml. dog pkt. 6 i K33, hvorefter dokumentation for specialprogrammel også omfatter "opdaterede kildetekster". Uden særlig aftale herom kan leverandøren nægte at udlevere kildeteksten under henvisning til de residuelle ophavsretlige beføjelser, han ifølge de deklaratoriske regler herom vil være rådig over. I denne interessemodsætning mødes parterne typisk i et kompromis, hvorefter der indgås en vedligeholdelsesaftale med leverandøren.

Aftalepraksis

Aftalepraksis om vedligeholdelse har endnu ikke udmøntet sig i en veldefineret kontraktspraksis endsige veldefinerede spilleregler. EDB-rådet og administrationsdepartementet udgav i sin tid en kontrakt om vedligeholdelse af databehandlingsudstyr sammen med deres øvrige kontrakter. Kontrakten er næppe anvendelig i dag. Et mere tjenligt forlæg findes i den Specifikation vedrørende vedligeholdelsesforpligtelse, der er optrykt som bilag 10 til K18. Her sondres der mellem vedligeholdelse af udstyr og pro-

grammel. For vedligeholdelse af udstyr sondres der herefter mellem forebyggende vedligeholdelse (der navnlig omfatter en pligt til at "efterse, justere, smøre, reparere og om fornødent udskifte dele og enheder, der vil kunne medføre fejl i systemet") og reparation efter tilkaldelse. På programmelsiden sondres mellem udsendelse af nye udgaver af leveret programmel (pkt. 3.1) og fejlrettelse (pkt. 3.2). En endnu mere indgående vedligeholdelsesregulering findes i bilag 7 til K01. Denne vedligeholdelsesaftale knytter sig til K01, pkt. 13, hvorefter leverandøren (som almindelig regel) påtager sig at forestå vedligeholdelse af alle dele af systemet med de undtagelser, der er specificeret i vedligeholdelsesaftalen. I modsætning til den vedligeholdelsesaftale, der hører til K18, pålægger dette bilag tillige leverandøren at vedligeholde tredjepartsprogrammel.

Baggrundsret

Vedligeholdelsesaftaler er ikke omfattet af købeloven. Ydelsen må rubriceres som andre tjenesteydelser, og kravene til dens indhold udledes af almindelige regler, se hertil afsnit 21.2. Ganske ofte må vedligeholdelsesaftalen forstås således, at vedligeholderen afgiver en form for tilsikring af, at det vedligeholdte system er tilgængeligt i en nærmere fastlagt "oppetid". Sådanne tilsikringer vil dog sjældent indebære nogen pligt for vedligeholderen til at betale kunden erstatning for det driftstab, der lides, hvis den tilsikrede oppetid ikke nås.

I vurderingen af, hvilke krav man kan stille til en enkeltstående *afhjælpningsydelse* (en "reparation") indgår bl.a. et subjektivt vurderingskriterium. Som antaget i betænkning 1133/1988 om forbrugeraftaler om arbejder på løsøre og fast ejendom (forbrugertjenester), s. 73, må et teknisk kompliceret arbejde, hvori der indgår en række usikkerhedsfaktorer (f.eks. at få en teknisk kompliceret genstand til at fungere igen), hvis andet ikke fremgår, ofte fortolkes således, at den erhvervsdrivende blot har påtaget sig at foretage en fagligt forsvarlig undersøgelse af genstanden med henblik på at finde fejlen og i den forbindelse udbedre de forefundne fejl på en fagligt forsvarlig måde. Se hertil afsnit 21.5.d.

Særlige problemer

Ved formuleringen af en vedligeholdelsesaftale må koncipisten tage aftalens overordnede formål om at sikre driften af det pågældende system i betragtning. Behovet for aftalemæssig sikring må afstemmes med, hvilken pris, kunden er parat til at betale for vedligeholdelsen. Denne afvejning beror dels på systemets funktion, dels på muligheden for at erstatte systemet med andre systemer, der kan opfylde samme funktioner.

Varighed

Parterne har typisk modsatte interesser i varigheden af en vedligeholdelsesaftale. For kunden er idealet, at systemet er undergivet vedligeholdelsespligt i hele dets forventede levetid, dvs. at

vedligeholdelsesaftalen er uopsigelig. Dette ideal vil imidlertid kollidere med leverandørens interesse i ikke at blive bundet til en måske mindre profitabel virksomhed med vedligeholdelse i en uoverskuelig fremtid. Leverandøren vil ikke ønske at vedligeholde en ældre version af et system. At bruge kostbar programmørtid på at korrigere fejl og uhensigtsmæssigheder, der er rettet i senere versioner, savner økonomisk mening. Omvendt vil brugeren ikke altid have interesse i at købe nye versioner. Udover den meromkostning, der vil være forbundet hermed, vil implementeringen af nye faciliteter mv. kunne indebære en belastning af virksomheden og dens medarbejdere, der ikke står i forhold til de mulige nyttevirkninger. Fastlæggelsen af dette forhold beror på talrige faktorer, f.eks. på systemets pris og udbredelse, samt på den pris, der betales for vedligeholdelsen. Ofte aftales en uopsigelighed på 5 år fra leveringstidspunktet, se f.eks. pkt. 1.13.6 i ESF's Totalkontrakt.

Hvis ikke leverandøren tilbyder vedligeholdelse efter udløbet af programmets økonomiske levetid og heller ikke tilbyder alternerende, funktionelt identiske, programmer til tilsvarende pris, bør han i almindelighed ikke modsætte sig, at kildeteksten stilles til rådighed for kunden eller for en af leverandøren udpeget virksomhed, der er parat til at videreføre denne opgave. Han har dog næppe pligt hertil uden særlig aftale.

Tilkaldetid

Et af de forhold, der ved afviklingen af en vedligeholdelsesaftale erfaringsmæssigt rejser problemer, er fastlæggelsen af tilkaldetiden. Brugeren, for hvem en forsinkelse kan være ensbetydende med et lammet produktionsapparat, vil typisk ønske omgående bistand ved nedbrud mv. Leverandøren, for hvem prisen herfor nødvendigvis må betales i form af en øget medarbejderstab, der i givet fald måske ikke vil blive udnyttet optimalt, vil trække i den modsatte retning. Nøglen til at løse denne konflikt ligger bl.a. i aftaler, der giver mulighed for at foretage fejlretning uden samtidigt besøg, f.eks. gennem telefonkonsultation eller med telematisk etableret fjernbetjening af det pågældende system.

Reservedele

For at kunne vedligeholde enhver form for teknisk udstyr er det nødvendigt at have adgang til de reservedele, der løbende skal udskiftes. Derfor pålægger de fleste aftaler om vedligeholdelse vedligeholderen en pligt til at opretholde et forsvarligt reservedelslager indenfor en afstand, der giver mulighed for at fremskaffe de nødvendige dele uden forsinkelse. Se f.eks. K18, pkt. 5 (7 år) og ESF's totalkontrakt pkt. 1.11 (5 år) og 6. Også på dette punkt vil parterne ofte have modsatte interesser. Et reservedelslager, der blot skal ligge parat med henblik på en uvis eventualitet,

vil for vedligeholderen repræsentere et likviditetsbelastende dødt aktiv. Kompromis'et vil her ofte ligge i en aftale, der sondrer mellem mere eller mindre vitale henholdsvis hyppigt anvendte reservedele.

Misligholdelse

Hvis ikke leverandøren har afgivet indeståelse for, at systemet i en nærmere fastsat periode (aftalt "oppetid") er i funktionsdygtig stand, er det udgangspunktet, at leverandøren alene har pligt til at præstere en fagligt forsvarlig ydelse. En sådan ydelsen kan godt være præsteret, selv om kunden ikke opnår en forventet funktion, sml. herved EDB-rådets udtalelse til Forbrugerklagenævnet af 26. august 1981 (*ERA 1.67*), der antager, at den omstændighed, at en periodisk fejl kræver flere teknikerbesøg, ikke i sig selv var udtryk for, at udbedringsforsøgene var mangelfulde. Det må i almindelighed bero på en samlet vurdering af aftaleforholdet, om misligholdelse af en pligt til at vedligeholde skal give brugeren ret til at hæve den samlede aftale om leveringen af dette system.

Naturalopfyldelse i kildetekst?

Foreligger der væsentlig misligholdelse (f.eks. i form af overskridelse af tilkaldetid, gentagne forgæves forsøg på fejlretning el.lign.), vil brugeren stå i valget mellem at ophæve aftalen eller at kræve naturalopfyldelse. I begge tilfælde vil der kunne påløbe krav om erstatning. Da (fortsat) vedligeholdelse af et edb-program forudsætter rådighed over dets kildetekst, opstår i begge tilfælde spørgsmålet om, hvorvidt brugeren kan forlange kildeteksten udleveret. Selv om brugeren herved kan reducere erstatningskravet, er spørgsmålet ikke ukompliceret. Almindeligvis bevares kildeteksten som leverandørens (vedligeholderens) eksklusive erhvervshemmelighed, og han – eller hans konkursbo – vil derfor sjældent ønske at give den fra sig. Spørgsmålet er derfor, om brugeren i disse tilfælde har et retskrav på at få adgang til kildeteksten.

Spørgsmålet er ikke afgjort i praksis. Sat på spidsen drejer det sig om, hvorvidt en kontraktsparts berettigede krav på at kunne redressere et retsbrud skal gå forud for modpartens ligeså berettigede interesse i at kunne bibeholde en erhvervshemmelighed. I denne afvejning er det nærliggende at anlægge en helhedsvurdering, der afvejer brugerens skadevirkninger ved ikke at kunne få adgang til den tilsagte funktionalitet, overfor leverandørens risiko for kompromittering af erhvervshemmeligheder mv. Da problemstillingen set i forhold til leverandøren er mindst ligeså indgribende som et krav om ophævelse, må der som minimum stilles krav om, at leverandøren skal have udvist væsentlig misligholdelse. Er dette tilfældet, må der herudover foretages en interesse-

afvejning. Falder denne ud til brugerens fordel, må dennes ret til at anvende kildeteksten dog i alle tilfælde begrænses til de dele af den, der er nødvendige for at kunne rette opståede fejl og kunne foretage nødvendige opdateringer. Dernæst bør adgangen kun bestå, så længe det er nødvendigt af hensyn til fejlretningen. Lignende begrænsninger ligger til grund for de regler om anvendelsen af dekompilerede programmer, der findes i ophl. § 37.

Misligholdelsens virkninger

Selv om kunden får medhold i et krav om udlevering af kildeteksten, er hans problemer ikke nødvendigvis løst hermed, da en kildetekst kan være vanskeligt forståelig for uindviede. Da der efter gældende ret ikke er mulighed for at tvangsfuldbyrde et krav om udførelse af personligt arbejde, må man i mange tilfælde indstille sig på, at retssystemet på dette punkt ikke tilbyder en fuldstændig sikring af brugerens interesser.

Udgør vedligeholdelsesforpligtelsen en integreret del af leverandørens samlede præstation, opstår spørgsmålet om, hvorvidt en misligholdelse af vedligeholdelsespligten får virkninger på overdragelsen. I K33, pkt. 5, sidste stk. (og tilsvarende K18, pkt. 4, sidste stk.), er det bestemt, at kunden ved væsentlig misligholdelse af vedligeholdelsesforpligtelser uden varsel kan hæve "vedligeholdelsesordningen". Om kunden herudover kan hæve hovedaftalen, beror på dennes indhold. K18 pkt. 4, sidste stk. henviser herom til aftalens almindelige misligholdelsesregler, herunder ophævelsesreglen i pkt. 14.4. Heraf følger, at misligholdelse af vedligeholdelsespligten skal betragtes på samme måde som misligholdelse af hovedaftalen – som om der var tale om ét og samme aftaleforhold.

I mangel af særskilt aftale kan en sådan ophævelse kun komme på tale, hvis leverandøren i henhold til hovedaftalen også er vedligeholdelsesleverandør, sml. dog *U 1984.1032 Ø* og *U 1985.334 H*, der begge lod en aftale borfalde ud fra forudsætningssynspunkter som følge af forhold hos en tredjepart, hvis forhold leverandøren var "nærmest til at bære risikoen" for. Er han det, og er overdragelsesaftalen indgået under en klar forudsætning om, at der skal leveres vedligeholdelsesydelser i en tilsvarende periode, må det også antages, at misligholdelse af vedligeholdelsesaftalen kan få retsvirkninger for overdragelsesaftalen. Det forhold, at de respektive forpligtelser er nedfældet i et eller flere aftaledokumenter, har ikke afgørende betydning for svaret.

4.4.c. Kildetekstdeponering

At gennemføre et krav om naturalopfyldelse efter de ovenfor angivne retningslinjer, kan være forbundet med betydelige praktiske vanskeligheder. For det første vil det ofte tage tid, inden der er taget stilling til berettigelsen af kundens krav. Dernæst kan leverandøren være gået konkurs – eller kildeteksen være fortabt – med den virkning, at et udleveringskrav er illusorisk.

IT-brugerens behov for at råde over kildeteksten er vel ikke principielt anderledes end den interesse i at kunne råde over nødvendige reservedele, som gør sig gældende ved vedligeholdelsen af andet teknisk udstyr, jf. ovenfor. Men hvor det ofte vil være teknisk overkommeligt at genskabe en reservedel, er det – med de nuværende teknikker – udenfor mulighedernes grænser at genskabe en kildetekst. Vel er det muligt at hidføre en række af de funktioner, kildeteksten indeholder, gennem *reverse engineering*; men da en række væsentlige informationer ofte vil gå tabt ved konverteringen fra objektkode til kildetekst (herunder f.eks. navne på variable samt bemærkninger i kildeteksten til brug for programmøren), er denne mulighed uden praktisk betydning. Har han ikke faktisk rådighed over kildeteksten til et program, mister brugeren derfor muligheden for at udføre de tekniske ændringer i programmaterialet, der er nødvendige for at overkomme opståede fejl og uhensigtsmæssigheder.

For at løse dette problem og i visse tilfælde for at opfylde lovkrav (herunder kontrolmæssige, jf. bogføringslovens § 14), indgår parterne undertiden en særlig deponeringsaftale vedrørende programkildetekst. En deponeringsaftale – eller med et ikke hensigtsmæssigt engelsk udtryk: en *escrow*-aftale (det uhensigtsmæssige består i, at begrebet "escrow" efter common law-terminologi betegner en håndpante-lignende situation) – involverer vedligeholdelsesaftalens to parter og en tredje part, der – typisk mod betaling eller som led i en service ydet på andet grundlag – påtager sig at opbevare en kildetekst.

Det er ikke ukompliceret at etablere en deponeringsordning. For det første involverer den en tredje part, der måske ikke uden videre vil være indstillet på at tiltræde de betingelser for deponeringen, der måtte være aftalt mellem leverandør og bruger. For det andet vil aftalen – såfremt den aktualiseres – kunne føre til en åbenbaring af leverandørens mest følsomme erhvervshemmeligheder. Beslutningen om at udlevere kildeteksten, eller beholde den i depotet, kan være tvivlsom, og – givet de involverede værdier – ubehagelig at skulle træffe. Når udlevering bliver aktuel,

vil parterne ofte true depositaren med erstatningsretlige krav for den standpunktsrisiko, der vil ligge i henholdsvis udlevering eller ikke-udlevering.

Derfor er det et centralt punkt i deponeringsaftalen, hvornår depositaren må henholdsvis skal udlevere kildeteksten. En stillingtagen til dette spørgsmål forudsætter en afklaring af, hvornår misligholdelse foreligger. Og da dette spørgsmål ofte vil give anledning til tvivl, vil det være hensigtsmæssigt at indføre en metode til hurtig konfliktløsning, hvorved der – i hvert fald med sigte på spørgsmålet om udlevering – kan træffes afgørelse om dette spørgsmål.

Både i ind- og udland er der etableret deponeringscentre for kildetekst. Herhjemme har Dansk Teknologisk Institut etableret et Dansk Deponerings Institut. Ifølge den standardaftale, der gælder herfor, skal instituttet frigive det deponerede til depositaren, hvis deponenten, eller den til sikkerhed for hvis forpligtelser depotet er oprettet, misligholder eller med overvejende grad af sandsynlighed må forventes at ville misligholde sine forpligtelser til at opfylde i henhold til den sikrede aftale, f.eks. på grund af konkurs, betalingsstandsning eller tvangsakkord. Ved uoverensstemmelser om, hvorvidt de materielle betingelser for frigivelse er opfyldte, træffes der afgørelse herom af en af DTI nedsat udleveringskomité.

På europæisk plan er etableret et deponeringsselskab ved navn Escrow Europe, der i partnerskab med den svenske virksomhed Deposit AB i august 2000 har etableret deponeringsinstituttet Escrow Europe Scandinavia, se <www.deposit.se>. Selskabet markedsfører sig ved at give mulighed for deponering ét sted til fordel for frigivelse i hvert af de lande, hvor deponentens kunder findes.

4.4.d. Backup-aftaler

I visse tilfælde kan det være hensigtsmæssigt, at flere brugere går sammen om at tilvejebringe et fælles grundlag for at sikre sig mod IT-nedbrud, således at A lover at stille sit system (og/eller sine lokaliteter) til rådighed for B, hvis B's system bliver uarbejdsdygtigt i kortere eller længere tid. Et sådant samarbejde kan organiseres på forskellig vis, f.eks. (hvis der er tale om systemer, der ikke er genstand for vid udbredelse) i klubber, som et løbende samarbejdsforhold af kommercielt tilsnit eller som mere eller mindre uforpligtende "gentlemen's agreements". Anskuet under ét – i formål og indhold – minder aftalerne forbløffende om de aftaler, der findes indenfor landbrugsområdet (brugsaftaler ve-

drørende maskiner, andelssamvirker mv., jf. til illustration dommen i *U 1975.969 V*).

Sådanne aftaler betegnes almindeligvis som backup aftaler, fordi de pålægger en forpligtelse til at tilvejebringe erstatningsfunktioner. Fra gammel tid har man sondret mellem to hovedtyper: Den *gensidige backup aftale* og *backup center aftalen*. Gennem de seneste år, og navnlig efter udviklingen af de åbne digitale netværk, er backup-tjenester blevet et supplement til andre kommercielle databehandlingstjenester, f.eks. i form af *online-backup*, hvor brugeren løbende overfører sit datamateriale til en leverandør til opbevaring her.

Gensidige

En gensidig backup aftale forpligter en eller flere brugere til at stille deres systemer til rådighed for hinanden i tilfælde af nedbrud. Aftalen indgås ofte helt uformelt. Dette kan indebære en vanskelighed ved den senere fortolkning og gennemtvingelse. Skriftlige aftaler må tilrådes, hvis der tilsigtes andet end uforpligtende tilkendegivelser.

En gensidig backup aftale må nødvendigvis knytte sig til en given systemtype. Systemets kompatibilitet er forudsætningen for at kunne udveksle de data, som det er aftalens formål at sikre behandling af. Heraf følger ligeledes, at parterne i aftalens løbetid må forpligte sig til ikke at udskifte dette udstyr. Da en sådan teknologibinding kan være uhensigtsmæssig over længere tidsrum, vil de bestemmelser, der regulerer længde og opsigelsesvarsel, få central betydning.

En principiel vanskelighed ved gensidige backup aftaler angår håndhævelsen. Uanset hvor utvetydigt en forpligtelse er formuleret, kan den forpligtede stille faktiske hindringer i vejen for opfyldelsen: Nægter han f.eks. medkontrahenten adgang til virksomheden og/eller IT-systemet, når uheldet er ude, vil der sjældent være tid eller ressourcer til at rekvirere fogedbistand mv. Dernæst kan en foged kun gennemtvinge aftalens forpligtelser ved at pålægge tvangsbøder.

Har den gensidige backup aftale mere end to parter, må aftalen tage stilling til, hvilke aftaleparter der skal have adgang til hvilke øvrige anlæg og – hvis flere systemer er nede samtidigt – i hvilken rækkefølge. En særlig vanskelighed angår her formuleringen af den tilstand, der giver adgang til backup systemet. Det må præciseres, hvor funktionelt omfattende et nedbrud er, f.eks. ved angivelse af antallet af funktionsudygtige terminaler. Ligeledes kan det være hensigtsmæssigt at sætte nedbruddet i forhold til den situation, virksomheden befinder sig i, når nedbruddet indtræffer, samt til årsagen til nedbruddet. En fejl, der kunne være

rettet under en afhjælpende vedligeholdelse, bør ikke give adgang til backup systemet. Endelig må der sættes en tidsramme. Kan et nedbrud forventes afhjulpet indenfor et døgn, bør dette ikke give ret til backup systemet.

Backup-center

En backup center aftale fungerer som en slags forsikring. Den indgås mellem en part, der driver en lokalitet (centret), og en række tilknyttede brugere, der gennem aftalen tilstås rådighed til centret i tilfælde af nedbrud.

Sådanne centrer findes i to hovedformer: Det "varme" center rummer såvel lokaliteter som maskinel. Det "kolde" center stiller derimod alene driftsklare lokaliteter til rådighed tillige med elforsyning, køleanlæg og transmissionslinjer. Brugeren af et koldt center må derfor sørge for at indgå udtrykkelige aftaler med sin system-leverandører om maksimale leveringstider med henblik på installeringen af det nødvendige udstyr.

Kolde centre

Et koldt backup center forudsættes at træde i funktion i tilfælde af en fysisk ødelæggelse af brugerens IT-system eller den lokalitet, der huser det (f.eks. ved brand, vandskade eller anden omfattende ødelæggelse). Den ydelse, det kolde center kan tilbyde, er – foruden husly – tilslutning af elektricitets- og kommunikationsledninger. Hvor husly undertiden kan tilvejebringes gennem midlertidige bygninger, telte mv., omend denne udvej efter omstændighederne kan være tidkrævende, kan det være forbundet med større problemer at skaffe reservesystemer til kommunikation. Et koldt backup center, der f.eks. skal kunne huse et større pengeinstitut, må typisk skulle tilbyde et par hundrede højhastigheds kommunikationslinier for at kunne tjene sit formål.

Værdien af et koldt backup center beror i vid udstrækning på, hvilke konkrete faciliteter der stilles til rådighed. Bortset fra de rent fysiske rammer må køle- og ventilationsforholdene f.eks. kunne opfylde de krav, det pågældende system stiller. Dertil må de sikkerhedsmæssige rammer omkring centret – f.eks. adgangsforhold og afskærmning – være tilfredsstillende.

Varme centre

Et varmt center har navnlig betydning for virksomheder, som er afhængige af hurtig databehandling. Dette er f.eks. tilfældet indenfor den finansielle sektor (banker, børsmæglerselskaber mv.).

Begge backup center modeller rummer det generelle problem, at samme center principielt kan være optaget af flere brugere på samme tid. Aftalen giver typisk ingen sikkerhed mod, at denne situation opstår. Derfor får det betydning, om centret prioriterer større brugere frem for mindre, eller om den, der kommer først til

mølle, først får malet. Antallet af øvrige brugere med adgang til centret må derfor tages i betragtning.

4.4.e. Aftaler om certificering og digital signatur

Forløbet omkring udstedelse af certifikater til elektronisk signatur indebærer en række retlige relationer, såvel i som uden for kontraktsforhold. For at få overblik over disse relationer er det nødvendigt at udskille de relevante partsforhold.

Underskriver-modtager

I forholdet mellem underskriver og modtager gælder enten den *aftale*, der foreligger mellem parterne om brug af digital signatur el.lign., eller en *retlig regulering* af anden art – f.eks. en lovhjemmel, forpligtende retssædvane eller andet retligt grundlag for at betjene sig af denne teknologi. For så vidt angår de aftaleretlige problemer henvises til gennemgangen i kapitel 19. Om retsforholdet til offentlige myndigheder – som undertiden også kan være aftalereguleret – henvises til kapitel 16.

Underskriver-CA

Forholdet mellem underskriveren og CA'en vil derimod typisk være løst gennem aftale: Der er jo tale om, at underskriveren ved at opnå certifikatet hos CA erhverver en *ydelse*, som underskriveren typisk vil betale for. Denne aftale vil ofte henvise til CA'ens egen beskrivelse af de procedurer, der gennemløbes i forbindelse med certifikatets udstedelse, herunder i forbindelse med kontrollen med certifikatindehaverens *nøglegenerering*, *identitet* og om certifikatets *offentliggørelse* og *tilbagekaldelse*.

LES indeholder visse regler til udfyldelse af dette aftaleforhold, jf. § 8, stk. 1. Ved indgåelse af en aftale om udstedelse af et kvalificeret certifikat skal nøglecentret skriftligt oplyse underskriveren om:
1) Vilkårene for anvendelsen af certifikatet, herunder eventuelle formåls- eller beløbsbegrænsninger.
2) Eventuelle krav til underskriverens opbevaring og beskyttelse af signaturgenereringsdataene.
3) Underskriverens omkostninger ved erhvervelse og anvendelse af certifikatet og brug af nøglecentrets øvrige tjenester.
4) Hvorvidt nøglecentret er tilknyttet en frivillig akkrediteringsordning.
5) Procedurer for behandling af klager og bilæggelse af tvister.
Det følger af bestemmelsens stk. 2, at kontraktsvilkårene kan afgives elektronisk, forudsat at det sker i en for modtageren umiddelbart læsbar form. De relevante dele af de i stk. 1 nævnte oplysninger skal på anmodning stilles til rådighed for tredjemand, der forlader sig på et kvalificeret certifikat, stk. 3.

CA-tredjepart

Retsforholdet mellem CA'en og tredjeparten er først og fremmest præget af risikoen for, at der kan blive påført tredjeparten et tab,

fordi certifikatet blev udstedt for en anden person end den angivne (med risiko for, at en gerningsmand herefter uberettiget tegner den berettigede).

- kvalificerede certifikater

For *kvalificerede certifikater* er dette forhold reguleret ved LES § 11. En CA, der udsteder sådanne certifikater til offentligheden, eller som overfor offentligheden indestår for sådanne certifikater udstedt af et andet nøglecenter, er ansvarlig for tab hos den, der med rimelighed forlader sig på certifikatet, såfremt tabet skyldes visse nærmere angivne forhold, se hertil afsnit 18.3.d., medmindre nøglecentret kan godtgøre, at nøglecentret ikke har handlet uagtsomt eller forsætligt. Der gælder med andre ord et *præsumptionsansvar* for sådanne skader.

Ansvaret tilpasses dog indholdet af det pågældende certifikat. Således er CA ikke ansvarlig for tab opstået som følge af anvendelse af et kvalificeret certifikat uden for de *formålsbegrænsninger*, som gælder for certifikatet, eller for tab opstået som følge af en overskridelse af de *beløbsbegrænsninger*, som gælder for certifikatet. For at undgå vidtgående retsfølger af småttrykte tilføjelser i et certifikat kræves dog, at de pågældende begrænsninger tydeligt fremgår af certifikatet, jf. § 4, stk. 2, nr. 6, og på forespørgsel oplyses, jf. § 9, stk. 1 og 3.

Præsumptionsansvaret i LES § 11 kan ikke ved forudgående aftale fraviges til skade for skadelidte, jf. § 11, stk. 4. Omvendt fortrænges præsumptionsansvaret af særlige regler, der måtte hjemle et videregående – objektivt – ansvar. Dette siges udtrykkeligt med en henvisning til erstatningsreglerne i LVB §§ 11-12, jf. LES § 11, stk. 5. Men det almindelige princip om *lex specialis*-fortolkning må føre til et tilsvarende resultat også for andre objektive erstatningsregler, således f.eks. værdipapirhandelslovens § 80.

- andre certifikater

For andre certifikater gælder de almindelige regler for erstatning uden for kontraktsforhold, dvs. en almindelig culparegel. Det hører til sjældenhederne, at der etableres formelle aftalerelationer mellem tredjepart og CA gennem underskrevne kontraktsvilkår mv. Visse CA-virksomheder søger at bringe sådanne kontraktsrelationer til eksistens ved i certifikaterne at angive, at brugen af certifikatet indebærer tiltrædelsen af en *"relying party agreement"*; men den aftaleretlige gyldighed af sådanne konstruktioner må betegnes som i høj grad diskutabel.

Se til eksempel den hos Verisign (<www.verisign.com>) angivne *Relying Party Agreement*. Det må i høj grad anses for tvivlsomt, om den blotte anvendelse af et certifikat, der jo i sig selv blot er en *konstaterende erklæring* (svarende til en revisionspåtegning) kan antages at etablere et sådant aftaleforhold.

Grænsen mellem kontrakt og delikt er dog ikke knivskarp på dette punkt. De fleste CA-virksomheder offentliggør deres praksis for udstedelse og tilbagekaldelse af certifikater i deres CP og CPS, og en sådan pligt gælder udtrykkeligt i medfør af § 2 i nøglecenterbekendtgørelsen for CA'er, der udsteder kvalificerede certifikater. En sådan erklæring giver almenheden (brugerne) en almindelig forventning om, at CA vil optræde som her anført: På den ene side kan brugeren ikke forlange "mere" sikkerhed end angivet i CPS'en, men på den anden side kan der opstå en culpaformodning, hvis CA ikke optræder som angivet i CPS. Spørgsmålet behandles af *Henrik Udsen*: Den digitale signatur – ansvarsspørgsmål (2002).

Supplerende litteratur

Litteraturen om IT-sikkerhed florerer i disse år. Hvor den ældre litteratur primært havde fokus på de fysiske rammer omkring systemerne – se herved *Lars Frank*: Edb-sikkerhed (1985), samt generelt den ovenfor i teksten omtalte Norm for edb-sikkerhed, som Dansk Standard har udstedt den 21. januar 2000 – har de senere års litteratur, forståeligt, fokuseret på de nye – og stadigt mere vanskelige – sikkerhedsproblemer, der opstår i og omkring telekommunikationssystemer. Se herved *Othmar Kyas*: Sikkerhed på Internet (Teknisk Forlag, 2000), *Warwick Ford og Michael S. Baum*: Secure Electronic Commerce (1997), og sidst, men ikke mindst, *Bruce Schneier*s både instruktive, let-læste og ikke mindst underholdende bog: Secrets and Lies, Digital Security in a Networked World (John Wiley & Sons, 2000). *CLSR*, der er et kombineret IT-juridisk/edb-sikkerheds-tidsskrift, publicerer løbende afhandlinger, der berører de centrale spændingsfelter mellem sikkerhed og jura. En god oversigt over IT-sikkerhedsspørgsmål og afledte juridiske spørgsmål findes i *Ronald G. Balding*: Computer breaking and entering: the anatomy of liability, 5 The Computer Lawyer (January 1988), s. 5 ff.

De særlige problemer omkring sikkerheden på Internet er bl.a. behandlet i *IT-sikkerhedsrådets* redegørelser Privatliv på Internet (1998), Digitale dokumenters bevisværdi (1999) og Praktisk brug af kryptering og digital signatur (2000). Ønskes en mere prosaisk indføring i emneområdet, anbefales *Cliff Stoll*: The cuckoo's egg – tracking a spy through the maze of computer espionage (Simon & Schuster, 1989, 1990), der handler om, hvordan forfatteren – dengang edb-chef på Lawrence Berkely Laboratories – identificerede og afslørede en omfattende hacking mod laboratorierne.

Den *almindelige bevisret* er bl.a. præsenteret hos *Gomard*: Civilprocessen, 5. udg. (2000) hos *Eva Smith*: Civilproces, 4.udg., (2000), s. 140 ff. og i *Henrik Zahle*: Det juridiske bevis (1976). Se også *Henrik Zahle*:

Om bevisbedømmelsen – kommentar til nogle aktuelle emner U1978B.375 ff. Bevisproblemerne vedrørende nye elektroniske *medier* er præsenteret af *Eivind Einersen*: Elektronisk aftale- og bevisret (1992), s. 18 ff. og *Klaus Østergaard Jensen*: Elektronisk udveksling af informationer i juridisk belysning. EDB-gruppen Herning, Oktober 1996.

Problemerne vedrørende *digital signatur* er bl.a. behandlet af *IT-sikkerhedsrådet* i flere rapporter, første gang i baggrundspapiret Danmarks IT-sikkerhedspolitik (november 1996) og senest i vejledningen Praktisk brug af kryptering og digital signatur (2000). Herudover behandles emnet i Forskningsministeriets udredning vedrørende digital signatur. Se også <http://www.mbc.com/ds_sum.html>. Herudover kan henvises til den af ICC udsendte vejledning *GUIDEC* – General Usage for International Digital Electronic Commerce, som blev vedtaget af ICC i 1997 og udsendt i en revideret udgave i 2001. Dokumentet er tilgængeligt fra adressen <www.iccwbo.org/home/guidec/guidec.asp>. For en mere teknisk indføring i emnet henvises til *Warwick Ford og Michael S. Baum*: Secure Electronic Commerce (1997) og *Stefan A. Brands*: Rethinking Public Key Infrastructures and Digital Certificates (2000).

De teknikker, der findes til sikring af uretmæssig kopiering mod eller adgang til IT-systemer, er beskrevet af *Lars Frank*: Edb-sikkerhed (1987), se navnlig s. 19 ff. (der beskriver truslerne) og kapitel 3 (s. 77 ff.), der angiver metoder til styring af sikkerheden. Det matematiske grundlag for nutidens teknikker til *asymmetrisk kryptering* og *digital signatur* er beskrevet af *Peter Landrock* i U1992B.176 ff. Herudover henvises til DS-publikationen Kryptografi og datasikkerhed (DS/INF 43, 1988). En god oversigt over de lovforslag, der foreligger verden over vedrørende digital signatur findes hos *Stewart A. Baker & Paul R. Hurst*: The Limits of Trust – Cryptography, Governments, and Electronic Commerce (Kluwer Law International, The Hague, 1998).

Vil man stifte bekendtskab med et vigtigt kapitel af kryptografiens historie, anbefales *Ole Immanuel Franksen*: Mr. Babbage's secret – the tale of a cypher (1984). De juridiske aspekter af disse teknikker behandles nedenfor i kapitel 9 om retlig disponeren med IT. Se i øvrigt *Roger Henriksen* (1982), s. 53 ff. og min artikel i R&R Februar 1991, s. 39 ff.

Fra den engelsksprogede litteratur om katastrofeplanlægning gennem *backup-aftaler* henvises til *David A. Feldheim*: Computer backup and disaster recovery agreements. 24 Jurimetrics Journal 210 ff. (1984) og til *Gemignani* (1985), s. 220 ff., der betegner disse aftaleforhold som "mutual aid agreements".

De juridiske problemer vedrørende *IT-vedligeholdelsesaftaler* er bl.a. omtalt hos Christophersen & Føyen (1981), s. 347 ff. og hos *Bender & Bruun Nielsen* (1989), s. 40 ff. Om vedligeholdelsesaftaler generelt henvises til *Bryde Andersen*: Enkelte transaktioner (2004), afsnit 5.5. (s. 313 ff.). En god oversigt over problemerne vedrørende *kildetekstdepo-*

nering findes hos *L. J. Kutten* (1989 med senere updates), chapter 9: Proprietary information deposit. Se ligeledes *Nørager-Nielsen*: Sikkerhedsordninger vedrørende kildeprogrammel, trykt i Beck & Bruun Nielsen (1987), s. 73 ff. og *Hanne Bender & Susanne Karstoft* i U1991B.81 ff.

Kapitel 5. RETSKILDER

5.1. Lovgivning og retsafgørelser

5.1.a. Regulatorisk lovgivning

Teleområdet

Den første lovgivning, der søgte at lægge retlige begrænsninger i anvendelsen af informationsteknologi, fik vi længe før den moderne IT, nemlig med reguleringen af *teleområdet*. Loven om telegrafer og telefoner fra 1897 har etableret et system af koncessioner med hertil hørende kontraktsbaserede kunderelationer, der den dag i dag udgør den retlige ramme for anvendelsen af medier til offentlig telekommunikation. I løbet af 1990'erne skete der en grundlæggende omstrukturering af det danske televæsen. Omstruktureringen tog oprindelig sigte på, at Danmark kunne leve op til den europæiske liberalisering af teleområdet. Siden er teleområdet blevet et fokusområde for landets seneste regeringer (bl.a. under mottoet "bedst og billigst"). Prisen for denne liberalisering har været, at teleområdet nu hører til et af de mest komplicerede IT-retlige lovgivningsområder.

Registerlove

Den første egentlige IT-lovgivning kom imidlertid først med *registerlovene* fra 1978. Til grund for denne lovgivning lå et omfattende betænkningsarbejde i form af del-betænkningerne om henholdsvis offentlige og private registre, nr. 687/1973 og 767/1976. 1978-lovene om henholdsvis private registre og om offentlige myndigheders registre blev efterfølgende ændret adskillige gange, inden man i 2000 fik lov nr. 429 af 31. maj om behandling af personoplysning (LBP). Loven, der indfører direktiv 95/46/EF i dansk ret, har rod i et forarbejde i betænkning 1345/1997 om behandling af personoplysninger. Ved siden af denne lov findes der imidlertid talrige særregler, der lægger begrænsninger i retten til at behandle personoplysninger ved hjælp af IT, jf. nærmere afsnit 13.1.c.

Strafferetten

I 1985 var det *strafferetten*, der stod for tur. Med lov nr. 229 af 6. juni 1985 indsattes en række regler i straffeloven om såkaldt datakriminalitet, der skabte klar hjemmel for at straffe visse former for berigelseskriminalitet begået ved hjælp af IT samt visse angreb mod IT-systemet og dets bestanddele. Ved lov nr. 352 af

19. maj 2004 blev straffeloven på ny tilpasset IT-udviklingen – denne gang på grundlag af betænkning 1417/2002 om IT-kriminalitet. Reglerne omtales i kapitel 17.

Betalingskort

Det næste – større – lovgivningsinitiativ på IT-rettens område blev indført med reguleringen af *betalingskort* og nu *visse betalingsmidler*. Startskuddet til denne lovgivning kom med 1984-loven om betalingskort, der i 2000 blev afløst af lov nr. 414 af 31. maj 2000 om visse betalingsmidler. Loven etablerer dels et offentligretligt tilsyn med virksomheder, der anvender eller udbyder betalingskortordninger mv., dels regulerer den en række aftale- og erstatningsretlige forhold, mellem den der udbyder, og den der anvender et sådant system.

Immaterialret

Et af de IT-lovgivningsområder, der har givet anledning til den mest intensive retspolitiske debat og til flest retsafgørelser, er *immaterialretten*. I 1989 blev ophavsretsloven ændret for bl.a. at give udtrykkelig hjemmel for ophavsretlig beskyttelse af IT-programmel. Loven blev igen ændret i 1992 efter vedtagelsen af Rådsdirektivet af 14. maj 1991 om retlig beskyttelse af edb-programmer, og med ophavsretsloven af 1995 blev den IT-retlige retsbeskyttelse udvidet, således at den ikke blot omfatter edb-programmer, men også data i digital form. Ved lov nr. 407 af 26. juni 1998 blev et EU-direktiv om databaser indført, og ved lov nr. 1051 af 17. december 2002 gennemførtes reglerne i det såkaldte Infosoc-direktiv. I 1987 indførtes halvlederloven, lov nr. 778 af 9. december 1987 om beskyttelse af halvlederprodukters udformning (topografi). Også denne lov udspringer af et direktiv. Senest har EU vedtaget direktiver om retlig beskyttelse af databaser og om ophavsret i informationssamfundet.

5.1.b. Konkrete afgørelser

Domspraksis

Det praktiske arbejde med IT-rettens problemer lider ofte under den begrænsede mængde retspraksis, der foreligger om en række af de vanskelige spørgsmål. Problemet var mere udtalt i IT-rettens barndom end i dag, men som det vil fremgå af denne bog er der fortsat talrige problemstillinger hvis løsning – i mangel af retspraksis – må søges på grundlag af en isoleret analyse, jf. herom indføringen i den analytiske metode i afsnit 2.1.d. Spørgsmålet om købelovens og produktansvarslovens anvendelighed på programmel og om den nærmere udformning af culpanormen på IT-området er eksempler herpå.

Branche-klagenævn

Der foreligger på nuværende tidspunkt (juni 2005) kun et enkelt branchenævn på IT-området, nemlig Teleankenævnet, jf. be-

mærkningerne herom s. 223. Som her anført viderefører nævnet det arbejde, der tidligere blev udført af det Telebrugernævn, der var nedsat i medfør af telekonkurrenceloven. I 2000 nedsattes et Klagenævn for Domænenavne, der i henhold til de aftaler, der indgås med brugerne af .dk-domænet, er kompetent til at behandle sager vedrørende .dk-domænenavne. I henhold til § 13 i internetdomæneloven (IDL) nedsætter VTU-ministeren et klagenævn for internetdomænenavne, der er omfattet af loven. I perioden fra lovens ikrafttræden og til der efter denne bestemmelse første gang er nedsat et klagenævn for internetdomænenavne samt fastsat regler for klagenævnets virksomhed mv. (jf. § 14, stk. 1), fungerer det hidtidige klagenævn for domænenavne, jf. lovens § 28, stk. 3.

I 2005 har forbrugerministeren forsøgt at få branchen til ligeledes at oprette et særskilt it-ankenævn, som kan tage sig af den stadigt stigende mængde af klager over computere og dermed aflaste Forbrugerklagenævnet fra dets arbejde på dette område, jf. herom straks nedenfor. Forslaget har hidtil mødt modstand fra detailhandlens side og er derfor endnu ikke realiseret.

Herudover vil enkelte andre mere generelt orienterede klagenævn lejlighedsvis blive præsenteret for IT-retlige problemstillinger, herunder *Erhvervsankenævnet* (bl.a. i relation til IT-sikkerheden i visse finansielle virksomheder) og *Klagenævnet for Udbud* (i relation til offentliggørelse af brugergrænseflader mv. ved visse offentlige udbud). Det største og mest interessante materiale af enkeltafgørelser på IT-området foreligger med *Forbrugerklagenævnet*s praksis, som er tilgængelig fra Forbrugerstyrelsens hjemmeside <www.fs.dk>. Nævnet har igennem de seneste år måttet tage stilling til en lang række af dagligdagens praktiske spørgsmål vedrørende køb og salg af alle form for IT-ydelser, lige fra PC'er incl. udstyr, mobiltelefoner, programmer og meget andet.

Erhvervsankenævnets retsgrundlag og praksis er behandlet af *Peer Schaumburg-Müller og Erik Werlauff* i Industriministeriets Erhvervsankenævn (1994). Se om Klagenævnet for Udbud, *Jacob Federspiel & Ulf Lund* i U1996B.414. For en nærmere gennemgang af arbejdet i Klagenævnet for Domænenavne henvises til afsnit 11.5.e.

Voldgift

Antallet af IT-retlige *voldgiftsafgørelser* er noget større end domsmaterialet. Her som i den civile retspleje gælder det imidlertid, at omkostningsincitamentet til at forlige sagerne er betydeligt. Dertil kommer, at mange voldgiftssager forliges efter proceduren, hvorved parterne ofte kan spare penge til voldgiftsretten ved blot at nøjes med dennes mundtlige tilkendegivelse om sa-

gens udfald. Voldgiftskendelser kan som bekendt ikke appelleres. For den retsdogmatiske analyse ligger det største problem dog i, at de voldgiftsafgørelser, der dog findes, ikke er samlet og offentliggjort ét sted. En af årsagerne til, at man vælger voldgift, ligger i ønsket om at hemmeligholde sagen for omverdenen, og dette ønske fører ofte til, at de involverede parter ikke ønsker de afsagte kendelser offentliggjort. I relation til de voldgiftsafgørelser, der afsiges af *ad hoc* voldgiftsretter (der er nedsat med sigte på den enkelte sag og uden for rammerne af en af de etablerede voldgiftsinstitutioner), er det dernæst vanskeligt overhovedet at samle det materiale af voldgiftskendelser, der kunne være af interesse.

5.1.c. Retspolitiske tendenser

I disse år præges IT-lovgivningsudviklingen først og fremmest af de nye problemer, der er opstået ved udbredelsen af det verdensomspændende Internet. Det forhold, at enhver borger, virksomhed og myndighed, der via telenettet tilslutter sig Internet, dermed i realtid og med minimale omkostninger kan sprede og modtage information fra enhver anden tilsluttet bruger i hele verden har ikke alene givet anledning til nye kontrol- og håndhævelsesproblemer, men indebærer tillige en forskydning af tidligere etablerede informationsbaserede magtforhold, som uden tvivl vil forandre samfundet ligeså stærkt som andre medier som telefonen, tv'et og radioen har gjort det.

Info-samfundet år 2000

I slutningen af marts 1994 nedsatte den danske regering et topersoners udvalg til at styre et projekt, der fik navnet "Informationssamfundet år 2000". Udvalget fik til opgave at udarbejde en række forslag, som bl.a. skulle formulere en overordnet dansk informationspolitik samt identificere særlige indsatsområder for de nærmeste år. Resultatet af dette arbejde er fremlagt i 1994 med *Dybkjær/Christensen*-rapporten (efter forfatterne, MEP *Lone Dybkjær* og daværende stiftamtmand *Søren Christensen*): Info-samfundet år 2000. Heri blev grundlaget skabt for den nuværende regerings opprioritering af de IT-politiske spørgsmål og for en betydelig del af det arbejde, der udføres i Forskningsministeriets IT-politiske søjle. Dybkjær/Christensen-rapporten giver en række anbefalinger, hvoraf hovedparten kredser om et ønske om, at Danmark udnytter sine muligheder i informationssamfundet bedst muligt, såvel inden for den offentlige sektor som i den private. Til rapporten om Info-samfundet år 2000 hører et omfattende bilagshæfte med specialstudier indenfor dele af de emne-

områder, rapporten behandler. I bilagshæftet finder man bl.a. udredninger om IT-retlige problemstillinger.

Handlingsplanerne

Info-2000-rapporten blev siden fulgt op med en række yderligere rapporter mv. og senere med årlige handlingsplaner fra det Ministerium for Videnskab, Teknologi og Udvikling, der blev etableret ved regeringsskiftet i 2001. I et tilbageblik over de talrige publikationer, der med farverige titler og omslag er udgået fra dette ministerium, synes der at være langt mellem de store ord og den konkrete handling. Problemet har været, at ministeriet kun har haft ressortkompetence inden for ganske få områder (reelt kun teleområdet), og at muligheden for at føre politik inden for de centrale ressortområder, der har været afgørende for udviklingen af "det digitale Danmark", har stået, og er faldet, med den politiske velvilje hos det embedsværk og de ministre, der havde ansvaret for disse områder. Denne velvilje har måske nok været til stede på det principielle plan, men erkendelsen af, hvilken tid og hvilken grundighed der skal til før man kan gennemføre digitale løsninger, har ofte været forskellig. Gennem de seneste år har man derimod set en øget lovgivningsaktivitet i de enkelte ressortministerier med henblik på at indføre digital teknologi i den offentlige forvaltning, i tinglysningen, i selskabsretten etc., og den lovgivningsmæssige tilpasning til netværkssamfundet er dermed for alvor kommet i fart.

EU-lovgivning

En stigende del af IT-lovgivningen udgår fra EU. Sådan må det næsten gå. Informationsindustrien er en af fællesskabets mest værdifulde sektorer, og tekniske handelshindringer mv. på dette område vil vanskeliggøre udviklingen af denne del af samfundsøkonomien. Arbejdet med regulering af telesektoren er allerede omtalt. I 1995 vedtoges direktivet om beskyttelse af personer i forbindelse med behandling af personoplysninger (95/46/EF) og i 1997 fulgte et direktiv (97/66/EF) om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren. Hertil kommer et væld af direktiver om immaterialretlig beskyttelse af forskellige IT-relaterede frembringelser, jf. nedenfor.

I forsøget på at sikre en koordineret IT-politik på europæisk plan har EU betjent sig af talrige virkemidler af retlig, økonomisk og politisk karakter. De første skridt blev taget i 1993 med Kommissionens hvidbog om "Growth, competitiveness, employment – the challenges and ways forward into the 21st century", der betonede vigtigheden af at tage højde for den "digitale revolution" og de heraf følgende strukturelle ændringer i samfundet. Hvidbogen gav politisk støtte til, at en gruppe prominente industrifolk mv. (*the Bangemann Task Force*) fremlagde deres konk-

rete visioner og forslag. Siden har der været et væld af rapporter, vismandsudredninger og beslutninger, der alle har peget i samme retning: Europa bør søge en lederposition i den nye digitale verden ved at udnytte sin mangfoldighed og veluddannede arbejdskraft. Og dette bør primært ske ved, at EU spiller rollen som motivator og kun træder til med regulerende retsforskrifter, når væsentlige hensyn er på spil. Det vil føre for vidt her at gå i detaljer om disse mange rapporter, der i form og indhold kan være vanskelige at skelne klart fra hinanden.

Immaterialretsområdet

Foruden disse generelle initiativer har EU taget en række konkrete skridt til at understøtte lovgivningen på de områder, der spiller en særlig rolle for informationssamfundets udvikling. Et sådant lovgivningsområde er først og fremmest immaterialretten. Immaterialrettigheder giver deres indehaver ret til at modsætte sig kopiering eller spredning af den information, som dækkes af hver enkelt immaterialret (ophavsret, patentret, varemærke mv.). I det omfang sådanne enerettigheder består, hæmmes den frie udveksling af information, hvilket kan være til skade for brugerne af den information og dermed også for samfundet. I det omfang man derimod ikke giver sådanne enerettigheder, kan dette få negative følger for frembringelse af ny information, eftersom man derved fratager udvikleren hans incitament til at investere de fornødne ressourcer heri. Denne afvejning kan være vanskelig at foretage, og dens udfald vil derfor ofte bero på nationale, kultur- og erhvervspolitiske overvejelser. Da dette samtidig giver en risiko for uensartede regler og dermed vanskeligheder for den virksomhed, der ønsker at markedsføre et informationsprodukt for hele unionen, har unionsmyndighederne på et meget tidligt tidspunkt fattet interesse for dette felt.

Se for en nærmere redegørelse over de direktiver og tilhørende grønbøger mv., der er udarbejdet med henblik på den ophavsretlige beskyttelse i relation til digitale udnyttelsesformer, *Peter Schønning*: Ophavsretsloven med kommentarer, 3. udg. (2003), s. 81 ff. Det seneste tema, der for alvor har givet anledning til retspolitisk debat, er Kommissionens forslag til direktiv om patentering af edb-programmel, se hertil s. 477.

5.1.d. Teknologisk og teknologineutral regulering

På de områder af IT-retten, hvor man har fundet det nødvendigt at lovregulere, står lovgiveren over et principielt beskrivelsesproblem: Skal lovreguleringen sigte mod den teknologi, man kender på lovgivningstidspunktet, således at reguleringen sigter *teknologispecifikt* mod denne, eller skal man forsøge at fremtidssikre

lovgivningen ved at operere med *teknologineutrale* betegnelser mv. og dermed gardere sig mod *konvergensproblemer*, jf. herom afsnit 2.1.c. Det siger sig selv, at man ikke kan besvare dette spørgsmål generelt for alle retsområder. På IT-strafferettens område er lovgiveren f.eks. bundet af det krav om "fuldstændig lovanalogi", kan udledes af straffelovens § 1, medens det på andre områder – f.eks. i relation til læren om digital aftaleindgåelse – i højere grad lader sig gøre at operere med bredere begreber, som er robuste overfor teknologiske omskift. Alligevel kan der anføres enkelte observationer:

International ret

Vender man sig til det internationale område er der en tydelig tendens til, at man søger at regulere teknologineutralt. De betydelige politiske og økonomiske omkostninger, der er forbundet med at skabe international konsensus begrunder, at man her søger at undgå hyppige revisioner af de internationale retskilder, og en af vejene hertil ligger netop i at anvende begreber, der ikke overhales af den tekniske udvikling. Prisen herfor betales til gengæld i en ofte tung begrebsanvendelse samt i en langsommere beslutningsproces, hvor man efter bedste evne søger at "fremtidssikre" problemstillingerne.

EU

I EU mærker man en tilsvarende tendens. Ønsket om en teknologineutral regulering søges bl.a. tilgodeset gennem en terminologi, hvorefter reguleringen omfatter "informationssamfundets tjenester". Herved forstås, jf. nærmere art. 1, nr. 2, i direktiv 98/34/EF som ændret ved direktiv 98/48/EF, EFT 1998 L 320/454, "enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ved hjælp af elektronisk databehandlingsudstyr (herunder digital komprimering) og dataoplagringsudstyr på individuel anmodning fra en tjenestemodtager". Begrebet omfatter ikke alene WWW-baseret informationsformidling, men også WAP-, SMS- og e-post baserede tjenester, jf. nærmere *Trzaskowski* i U2000B.643 f. og kritisk om de – betydelige – afgrænsningsproblemer *Justin Harrington* i 17 CLSR 3.174 ff. (2001).

- e-signaturer

Et væsentligt eksempel på brug af denne teknologineutrale metode er 1999-direktivet om elektroniske signaturer, der bevidst undlader at omtale den digitale signatur, til trods for, at digital signatur-teknologi for tiden er den eneste kendte brugbare teknologi til elektronisk signering af meddelelser. Til gengæld indeholder direktivet en regulering af en række af de *egenskaber*, som den digitale signatur besidder, jf. således for dansk ret LES § 3, nr. 2, i definitionen af den "avancerede elektroniske signatur" (hvis egenskaber opfyldes gennem digital signatur-teknologi) og § 4 om kvalificerede certifikater.

- telehemmelighed

Et andet eksempel er direktiv 2002/58 om behandling af personoplysninger og privatlivets fred i den elektroniske kommunikationssektor. I Kommissionens direktiv af 16. september 2002 om konkurrence på markederne for elektroniske kommunikationsnet og -tjenester (2002/77) er tidligere telefonibegreber f.eks. erstattet med mere generelle kommunikationsbegreber som f.eks. "kommunikation", "kommunikationstjeneste", "kommunikationsnet" mv.

Enkelte retsforskrifter forholder sig direkte til spørgsmålet om teknologi-neutralitet, således f.eks. Sundhedsstyrelsens vejledning om lægers journalføring (nr. 118 af 13. oktober 2003), der under et princip om "teknikneutralitet" fastslår, jf. pkt. 3.1, stk. 3, at der ikke gælder særlige regler for journalføring, afhængig af, hvilken teknik der anvendes.

5.2. Selvregulering

5.2.a. Problemstilling

Historisk baggrund

Da internettet i begyndelsen af 1990'erne gjorde sit indtog i samfundslivet meldte der sig et naturligt politisk ønske om at videreføre beskyttelsen af de samfundsværdier mv., som den eksisterende lovgivning omhandlede, til "informationssamfundet". Tankegangen var forståelig: Et samfund, der bygger på fysiske værdier og som indebærer adfærdsformer med fysisk kontakt og fysiske transaktioner, vil naturligt indføre aftaleretlige, strafferetlige og markedsretlige regler, der beskytter det fysiske. Men når disse værdier gradvis begynder at få ikke-fysisk (*immateriel*) form, opstår der et behov for at sikre en tilsvarende beskyttelse på dette plan. Opgaven med at tilpasse lovgivningen i denne retning – og i den forbindelse ikke mindst opgaven med at sikre den udfordring, der lå i selve nettets grænseløse karakter – stillede de politiske beslutningstagere overfor en overvældende, ja nærmest uoverstigelig, udfordring.

Det Columbus-æg, der i første omgang blev anvendt for at tage denne udfordring op, var at tilskynde markedet til *selvregulering*. Dette svar blev anvist i en række af de rapporter, der fremkom fra såvel EU som fra danske ministerier og sagkyndige udvalg mv., jf. nærmere redegørelsen i afsnit 5.1.c. Et eksempel herpå er den rapport om Danmarks IT-sikkerhedspolitik, som det daværende IT-sikkerhedsråd lagde frem i november 1996, se hertil s. 25 ff. Et andet eksempel er den løsning om delegering af

domæner under det danske .dk-topdomæne, der i 1999 blev gennemført ved etableringen af Dansk Internet Forum (DIFO), jf. nærmere s. 536 f.

Som årene er gået, og i takt med at de enkelte ressortministerier er blevet mere fortrolige med informationssamfundets retlige problemer, er det blevet mere naturligt at regulere sådanne samfundsspørgsmål ad lovgivningsvejen. Et væsentligt skridt i denne retning blev gennemført med e-handelsloven, der har rod i e-handelsdirektivet fra 2000. Et andet er gennemførelsen af internetdomæneloven fra 2005. Disse lovreformer har alle drejet sig om forhold, som aftalemidlet ikke nødvendigvis har været egnet til at regulere. På andre områder, og herunder navnlig i relationer mellem erhvervsdrivende, er der imidlertid fortsat rum for selvregulering som middel til at løse det digitale samfunds retlige problemer.

Begrebsafgrænsning

I sin yderste konsekvens kan enhver privat aftale siges at være udtryk for selvregulering, jf. nærmere *Åke Nilson* i 6 EDI Law Review 183 ff. (2000) om ICC's historiske rolle på dette område (standardkontrakter, INCOTERMS mv.). Men begrebet kan antage forskellige skikkelser beroende på de involverede aktører.

I det følgende anvendes det i tre betydninger, der bl.a. varierer efter de vekslende grader af offentlig deltagelse i regeldannelsen: myndighedsinitieret selvregulering, brancheregulering og kollegiale regler samt teknologisk understøttet selvregulering. Som det vil fremgå, er der langt fra tale om nye problemstillinger. Det *nye* i den megen tale om selvregulering i disse år ligger formentlig i det *pres*, hvormed man fra politisk hold søger at gennemføre selvreguleringsbestræbelserne, og i den heraf følgende *hastighed*, hvormed bestræbelserne søges ført ud i livet.

Aftalemodellen kan i princippet også involvere offentlige myndigheder, der i rollen som kunde eller udbyder understøtter en *aftalepraksis*. Eksempler herpå foreligger f.eks. i forbindelse med nedsættelsen af det danske EDI-råd, se hertil afsnit 5.2.b. En anden fremgangsmåde kan være, at virksomheder med en særlig dominans selv pålægger sig visse begrænsninger (*self-commitment*). Dette virkemiddel kendes f.eks. fra medieområdet, hvor aviser og televirksomheder ofte underlægger sig visse redaktionelle og andre begrænsninger for, hvilke annoncer mv. man ønsker at optage. I begge tilfælde kan sådanne tiltag have til formål at undgå, at der gennemføres lovgivning af et måske mere restriktivt indhold.

5.2.b. IT-branchen og dens brugere

Når man taler om selvregulering, er det branchen og dens brugere, der er i fokus. Det er dem, der "selv" skal finde normative løsninger på de problemer, som gennem *selv*reguleringen søges bragt i anvendelse i stedet for en egentlig *lov*regulering.

IT-branche foreningen

I Danmark repræsenteres systemleverandørerne af *IT-brancheforeningen* (tidligere Brancheforeningen Kontor og Data). Foreningen opslugte i 1991 ESF – EDB-systemleverandørernes forening, hvis navn fortsat optræder på en række aftaledokumenter.

Allerede i 1980 udsendte ESF en – i dag forældet – kontrakt om EDB-Servicebureaukørsel. I midten af 1980 udsendte ESF en standardkontrakt om system- og programudvikling. Denne kontrakt er senere blevet revideret. Efter K33's fremkomst og ikke mindst efter debatten herom tog ESF tillige initiativ til at udsende en tilsvarende totalkontrakt benævnt "ESF standardkontrakt vedrørende levering, installation og vedligeholdelse af et IT-system". Det var meningen, at kontrakten skulle revideres løbende, men dette er ikke sket. Dokumentet regulerer i hovedsagen samme spørgsmål som dem, der omfattes af K18 og K33. En række af de omdebatterede spørgsmål er dog ikke overraskende faldet ud til leverandørens fordel. Kontrakterne omtales nærmere i kapitel 21.

Internet-handel

I tilknytning til den hastigt voksende Internet-branche har en række særlige organisationer set dagens lys. *Foreningen for Dansk Internet Handel* (<www.fdih.dk>) har markeret sig med en række synspunkter i den offentlige debat, bl.a. om sikring af betalingskort på nettet og om fri ret til kryptering. En anden organisation er FAKDIS: Foreningen af Kommercielle Danske Internet Sites (<www.fakdis.dk>).

Dansk IT

Brugersiden har ikke opleveret en tilsvarende vækst i foreningsdannelser. Foruden Forbrugerrådet er det navnlig foreningen Dansk IT, der søger at være talerør for IT-brugernes synspunkter. Foreningen, der består af ca. 6.200 IT-brugere, har bl.a. været aktiv i høringsprocessen i forbindelse med de lovforslag, der har gennemført de seneste års reformer på teleområdet. Herudover medvirker Dansk IT ved udpegning er sagkyndige til brug for retssager og voldgiftssager om IT. Foreningen deltager ligeledes i arbejdet med udviklingen af nye statslige IT-kontrakter.

Staten

En gengivelse af den aftaleretlige retsdannelse på IT-området må dernæst inddrage den rolle *det offentlige* har spillet for aftaleudviklingen. Staten har fra gammel tid hentet vejledning ved offentlige IT-indkøb hos statslige instanser (oprindelig Administrationsdepartementet, senere Forskningsministeriet), og disse

instanser har hentet kyndig rådgivning til deres arbejde hos Statens faste advokatforbindelse, Kammeradvokaturen. Gennem dette arbejde er en række væsentlige standardaftaler udsprunget, herunder de aftaledokumenter for overdragelse af IT-systemer, der benævnes K18 og K33. Det seneste udslag af dette samarbejde er den statslige standardkontrakt K01, som i 2003 blev vedtaget af de toneangivende myndigheder og organisationer som *agreed document* for visse IT-transaktioner. Det pågår nu et udvalgsarbejde om en ny standardkontrakt med sigte på mere komplekse og længerevarende leverancer ("K02").

Interesse-organisationer

Herudover spiller IT-retten en så stor indirekte betydning for en række samfundssektorer, at det også er relevant at nævne de repræsentative organisationer, man finder her. Et eksempel herpå er *Finansrådet* (der bl.a. har medvirket til udarbejdelsen af flere adfærdskodekser på IT-området, herunder vedrørende home banking). *Danske Reklame- og Relationsbureauers Brancheforening* har i 1999 udsendt en Standardaftale for Web-samarbejde og et hertil hørende sæt retningslinier for aftaler om website-udvikling.

Aftalepraksis

IT-retlig aftalepraksis har på bedste vis forsøgt at følge trop med teknologiens udvikling og udbredelse. Der har været et stort pres på IT-aftalekoncipisterne. I mangel af veldefinerede IT-retlige regler er aftaleparterne henvist til at skabe deres egen ret. Kravene til en god og klar IT-aftale er størst, hvor der er store værdier på spil – enten fordi aftalens genstand er kostbar, eller fordi den forudsættes indplaceret i en følsom sammenhæng med risici for tab.

Den første IT-aftalepraksis former sig som en overbygning til den klassiske overdragelse af systemer fra leverandør til bruger. I sådanne aftaler er det klart, hvilke interesser de involverede parter har. Som nærmere udviklet nedenfor i afsnit 21.5.d, har denne interessemodsætning bl.a. resulteret i forskellige "skoler" for, hvorledes man fordeler risikoen for uforudsete omkostninger ved visse former for IT-udvikling.

5.2.c. Selvreguleringsformer

Som nævnt ovenfor kan selvregulering udfolde sig under vidt forskellige former. I en første gruppe kan man udskille den selvregulering, der sker på initiativ af en myndighed.

Den myndighedsinitierede selvregulering kendetegnes ved at udfolde sig under en underforstået trussel om, at den involverede myndighed tager skrappere midler i brug, enten ved at gøre brug

af en eksisterende hjemmel til at gribe ind med forbud, påbud eller bekendtgørelsesregulering eller ved at søge et lovgrundlag herfor etableret. Denne trussel har utvivlsomt været en medvirkende årsag til, at man netop på dette område har set nogle af de hidtil mest effektive forsøg på selvregulering herhjemme.

Et eksempel på (opfordring til) selvregulering igangsat af en myndighed er den *fælles holdning*, som de nordiske forbrugerombudsmænd udsendte i december 1998, der er revideret og udsendt i en ny skikkelse i oktober 2002 – nu som et fælles "standpunkt til handel og markedsføring på internettet". Opfordringen er udmøntet i den elektroniske mærkningsordning, der er indført i Danmark i 2000, jf. nærmere afsnit 15.5.b.

Udover disse eksempler kan en række EU-retsforskrifter ses som udtryk for en tilsvarende tankegang – omend præget af, at selvreguleringen i kraft af retsforskriftens bestemmelser er lagt i visse rammer. Artikel 27 i direktivet om *persondatabeskyttelse* pålægger således medlemsstaterne og Kommissionen at tilskynde til udarbejdelsen af *adfærdskodekser*, der afhængigt af de særlige forhold i de forskellige sektorer skal bidrage til en korrekt anvendelse af de nationale bestemmelser, medlemsstaterne vedtager til gennemførelsen af direktivet. Det pålægges ligeledes medlemsstaterne at lade brancheorganisationer mv., der har udarbejdet udkast til nationale adfærdskodekser, at kunne forelægge dem for den nationale myndighed til udtalelse. Artikel 16 i direktivet om *elektronisk handel* pålægger medlemsstaterne og Kommissionen at opfordre til, at erhvervssammenslutninger eller -organisationer på fællesskabsplan udarbejder adfærdskodekser, som skal bidrage til, at direktivforslagets materielle regler anvendes efter hensigten. Forslaget vil endvidere pålægge en pligt til at fremsende disse adfærdskodekser til Kommissionen samt at gøre dem tilgængelige elektronisk på fællesskabssprogene. Endvidere foreslås det, at forbrugersammenslutninger skal have ret til at blive inddraget i udarbejdelsen og iværksættelsen af adfærdskodekser, der kan vedrøre dem. I en række sammenhænge har EU-myndighederne søgt at løse de vanskelige problemer med spredning af såkaldt "skadeligt indhold" ("harmful content") på nettet, via selvregulering se herved COM(2001) 106 final, der indeholder resultaterne af en evaluering af virkningerne af de foranstaltninger, der er gennemført i opfølgning af rådets rekommendation af 24. september 1998 om beskyttelse af mindreårige og menneskelig værdighed.

Brancheregulering

En anden form for selvregulering er den, der helt og holdent styres og udspringer af en branches ønsker om at ordne sine forhold selv. En branchemæssig selvregulering, der udspringer af aktørernes følelse af, hvad der er god skik mv., vil ofte få større slagkraft. Ulempen er, at sådanne regler ofte ikke regulerer ligeså intenst som regler udstedt af en myndighed eller lovgiver.

Eksempler på *brancheregulering* med betydning for elektronisk handel er *ICC's* Guidelines on Marketing and Advertising using Electronic Media fra december 2004. Disse seneste retningslinjer træder i stedet for en første version fra 1996, der senere blev revideret i 1998. Retningslinjerne henviser til en række sektorspecifikke retningslinjer, f.eks. for Advertising Practice, Direct Marketing, Environmental Advertising, Sales Promotion, Sponsorship, Direct Selling og Marketing and Social Research. Se i øvrigt generelt om brancheregulering *Sten Bønsing*: Brancheregler og brancheproces (2001).

Betænkeligheder

Det er ikke uproblematisk at gøre brug af branchestyret selvregulering. Der kan være en fare for, at dominerende markedsaktører kommer til at sætte sig på regeldannelsen ud fra egne økonomiske interesser. Metoden kan derfor forekomme mindre velegnet på områder, hvor en sådan dominans foreligger. Dertil kommer problemerne ved at håndhæve de vedtagne regler. En branche bestående af udbydere, der er bundet sammen i et kollegialt eller organisatorisk fællesskab, er lettere at styre end en branche, hvor udbyderne kommer og går. Dette argument taler med en særlig vægt i relation til retshåndhævelsen på Internet, hvor informationerne flyder frit mellem landegrænserne og hvor årsagen til den virkning, man søger at ramme, kan befinde sig såvel geografisk som lovgivningsmæssigt "langt borte".

Selvforpligtelse

I konsekvens af en brancheregulering forekommer det ofte, at enkelte virksomheder underkaster sig en branchemæssig vedtagelse ved på forhånd at meddele potentielle kunder, at man er parat til at efterleve bestemte regelsæt, der ikke ellers ville være forpligtende. Også denne form for selvregulering har i princippet lange rødder. Den kendes bl.a. fra klagenævnsområdet, hvor det ofte forekommer, at virksomheder (f.eks. i kraft af medlemskab af en brancheorganisation) på forhånd underkaster sig et privat klagenævns kompetence. I forbindelse med elektronisk handel kendes sådanne *self commitments* i forbindelse med brugen af særlige mærkningsordninger.

Retlig funktion

En sådan erklæring kan enten udgøre et forpligtende *løfte* (der som sådant kan retshåndhæves) eller en *uforpligtende erklæring*, der ikke kan håndhæves direkte efter sit indhold, men som derimod kan tænkes at få indirekte betydning (f.eks. i relation til vurderingen af, om der foreligger adfærd i strid med "god markedsføringsskik", jf. markedsføringslovens § 1). Hvis en erhvervsdrivende f.eks. overfor en selvreguleringsinstans afgiver et forpligtende løfte, der tilsigter at få virkning overfor nuværende og kommende kunder som *tredjemandsløfte*, vil dette – alt efter sit indhold – kunne håndhæves.

Håndhævelse?

Kvaliteten af denne form for selvregulering beror på, om der skrides effektivt ind, hvis regelsættet overtrædes.

E-mærket

Den danske elektroniske mærkningsordning, e-mærket, er et selvreguleringsinitiativ gennemført af de organisationer, der repræsenterer brugere og leverandører i den danske e-handel (herunder Forbrugerrådet, Dansk Handel og Service, Finansrådet, HTS, Dansk Industri, Dansk IT, IT-Brancheforeningen og Foreningen for Dansk Internethandel). De pågældende organisationer har til formålet etableret en fond, e-handelsfonden, der udgør den juridiske identitet bag mærket. Ordningen fungerer ved, at e-handelsfonden indgår aftale med den virksomhed, der ønsker at bruge e-mærket. Virksomheden tiltræder et sæt retningslinjer, der forpligter den til at give en række oplysninger (herunder navnlig de, der i forvejen er påbudt i medfør af e-handelsloven), samt til at sikre, at funktioner til aftaleindgåelse holdes adskilt fra andre funktioner på sitet. Endvidere foreskrives særlige regler om betaling, eftersalgsservice og om behandling af personoplysninger. Ordningens administrator fører løbende kontrol med erhvervsdrivende, der har fået tildelt det elektroniske mærke. Kontrollen indebærer en vurdering af, om den erhvervsdrivende fortsat efterlever retningslinierne. Kontrollen kan gennemføres som stikprøve og uden varsel.

Udenlandske mærkningsordninger

TRUSTe er herhjemme markedsført af FDIH (Foreningen for Dansk Internet Handel). Det fremgår af den amerikanske hjemmeside (<www.truste.org>), at ordningen indbefatter et "TRUSTe oversight" program, hvorefter TRUSTe-licenshavere *overvåges* for at konstatere, om de opfylder de principper for privatlivsbeskyttelse, de har offentliggjort. Dernæst må selve indholdet af selvreguleringen være afbalanceret. Hvad angår dette krav fungerer TRUSTe som en slags fødselshjælper for formuleringen af den enkelte hjemmesides privatlivspolitik således, at der på den ene side sikres en regulering, der tager højde for den enkelte virksomheds behov og ønsker, samtidig med at visse generelle minimumskrav (herunder om gennemsigtighed, valgfrihed og datasikkerhed) opfyldes.

Tilsvarende gælder for det internationale *WebTrust* segl, der herhjemme markedsføres af FSR (Foreningen af Statsautoriserede Revisorer). Når en Internet-butik er godkendt efter reglerne herfor skal der gå 60 dage, før WebTrust-seglet kan sættes ind på hjemmesiden. I disse dage undersøger WebTrusts revisorer, om hjemmesiden lever op til de krav, der gælder for seglet.

Det erfaringsmateriale, der foreligger indenfor områder, hvor man har gennemført selvregulering, er endnu forholdsvis begrænset. Den

amerikansk-fødte TRUSTe-løsning adresserer alene problematikken om privatlivsbeskyttelse. Når effekten af denne selvregulering vurderes, må det imidlertid tages i betragtning, at de amerikanske myndigheder er underlagt et ikke ubetydeligt pres for at gennemtvinge selvregulering på dette område som følge af EU's persondatabeskyttelsesdirektiv fra 1995, der alene tillader dataeksport til tredjelande, der lever op til visse minimumskrav. Den selvregulering, man oplever indenfor persondatabeskyttelsesområdet, kan dermed siges at udfolde sig under truslen om lovindgreb af den ene eller den anden art.

Hvor grænsen går mellem sådanne løfter og mere uforpligtende erklæringer kan ikke siges generelt. Denne sondring mellem en viljeserklæring og en konstaterende erklæring hører til aftalerettens klassiske problemstillinger. Men selv om en erklæring ikke tillægges virkning som viljeserklæring, kan den dog få retlig betydning af andet indhold: Urigtige erklæringer kan indebære, at indgåede aftaler tilsidesættes som ugyldige pga. svig eller medføre erstatningsretlige sanktioner efter reglerne om *culpa in contrahendo*.

Denne form for selvregulering har de ældste rødder. En stor del af arbejdet med at udstede vejledende retningslinjer, standardkontrakter i form af *agreed documents*, anbefalinger og standarder (jf. herom i afsnit 5.3.) kan ses som udtryk herfor.

5.2.d. God skik-regler mv.

En særlig form for selvregulering, der har været oppe i tiden gennem de seneste år, består i, at en branche underlægger sig et sæt kollegiale eller etiske regler. Sådanne regler har IT-branchen også forsøgt at udvikle fra tid til anden. Forsøgene herpå har dog haft vekslende indhold og gennemslagskraft, bl.a. fordi de sjældent har været fulgt op med sanktioner. Enkelte, større, virksomheder har ligefrem givet regler for god forretningsmæssig adfærd for deres ansatte (f.eks. IBM's historiske *"Business conduct guidelines"*). Overholdelsen af sådanne regler er ligefrem en betingelse for medlemskab af visse brancheorganisationer.

Et sådant krav praktiserer en række brancheorganisationer, der organiserer liberale erhverv inden for rådgivning mv., se hertil *Bryde Andersen*: Advokatretten (2005), s. 87 ff. IT-branchen har imidlertid endnu ikke ført til fremkomsten af et tilsvarende liberalt erhverv for IT-professionelle. Det nærmeste man er kommet en god skik-regulering svarende til den, der kendes fra de liberale erhverv, er det daværende EDB-råds såkaldt "Etiske regler for datamatikere" fra 1982, se ITR.25 ("Syn og skøn og EDB"), s. 31 ff. Omend disse regler tog sigte på en noget mere snævert defineret kreds af programmører

mv., der udgjorde datidens primære IT-profession, er regelsættet karakteristisk for den form for regulering, man møder på disse professionsområder. Under en række få men generelle overskrifter fastslås "datamatikerens" pligt til at handle så hensynsfuldt og loyalt som muligt.

"God edb-skik"

I 1992 udsendte Foreningen af Statsautoriserede Revisorer, Foreningen af Interne Revisorer i Danmark og Foreningen for Informationskvalitet et sæt regler om "god edb-skik". Regelsættet adskiller sig fra de førnævnte ved at rette sig til virksomhedens ledelse, idet der sættes fokus på de forhold, "som ledelsen skal være opmærksom på, hvis den vil sikre sig imod ubehagelige overraskelser som følge af edb-anvendelse". Regelsættet betoner den forpligtelse, ledelsen har til at formulere en klar politik for anvendelsen af IT, således at rollerne omkring IT-anvendelsen er veldefinerede, beslutningerne formaliserede og IT-anvendelsen tilrettelagt på en måde, så der består et effektivt sikkerhedsnet og beredskab. Disse generelle synspunkter udmøntes herefter i mere konkrete anvisninger om, hvorledes forskellige dele af virksomheden bør indrette sig, bl.a. i forbindelse med brug, driftsafvikling, systemudvikling og sikkerhed.

Betydning

Uforpligtende regler som de førnævnte kan ikke forventes at påvirke retsanvendelsen og næppe heller det praktiske IT-liv. IT-retten kan næppe hente megen inspiration i disse forsøg på at kodificere god IT-adfærd mv. I konkrete sager må forholdene søges belyst gennem sagkyndige erklæringer og brancheudtalelser, og den retlige bedømmelse vil herefter ske efter en sammenligning mellem faktisk og ønsket adfærd. For en stor dels vedkommende gentager disse "etik-regler" blot almindelige retsregler inden for immaterial- og aftaleretten. I det omfang, de berører ikke-juridiske spørgsmål, findes "reguleringen" i form af en hensynsopregning. De vanskelige afvejningsspørgsmål, der opstår ved valget mellem forskelligartede – og mere eller mindre sikre – IT-strategier, berøres f.eks. ikke.

5.2.e. Teknologisk selvregulering

Til billedet af selvreguleringen på IT-området hører også den form for regulering, der betjener sig af teknologiske midler. Hermed tænkes ikke alene på den mulighed, en IT-leverandør har for gennem kopibeskyttelse eller andre spærrefunktioner at afskærme dele af sit system, men navnlig på brug af teknologiske filtreringssystemer, der kan fungere i samspil med forskellige typer af systemer til rating og kvalitetssikring. I det omfang man opbyg-

ger systemer til at klassificere hjemmesider, kan brugerne foretage til- og fravalg efter behov og ønsker, f.eks. således at børn har adgang via én indgang og voksne via en anden. En sådan klassifikation kan f.eks. knytte sig til en hjemmesides indhold af materiale af pornografisk eller voldeligt indhold. Brugeren kan herefter indstille sin browser, så den ikke vil modtage information med dette indhold.

PICS

Et eksempel herpå er den såkaldte *PICS*-løsning (Platform for Internet Content Selection, se <http://www.w3.org/PICS>), der er udviklet af The World Wide Web Consortium bl.a. med EU-støtte. Der er tale om en standard, som oprindeligt tilsigtede at give forældre mulighed for at filtrere, hvilke hjemmesider deres børn fik adgang til på nettet, men som nu understøtter en række andre formål, herunder håndhævelse af privatlivspolitikker. Standarden udbygges løbende med en lang række "rating services" tilpasset forskellige løsninger (som tilsvarende således forudsættes udviklet, så de bliver "PICS-kompatible"). Nogle af de filtrerings- og blokeringsløsninger, der anvendes i dag, bygger deres filtreringsmekanismer på beslutninger truffet af dertil udpegede paneler mv. For en oversigt over lister med filtreringssoftware, se <http://netparents.org>. Se også afsnit 15.5.e. om den tidligere nævnte *TRUSTe*-løsning, der understøtter selvregulering af privatlivsbeskyttelse.

5.3. Tekniske standarder

5.3.a. Begreb og funktion

Begreb

Uden for "the lawyers law" anvendes begrebet "standard" i en anden betydning end ved talen om "retsstandarder" mv. En standard er herefter en teknisk specifikation, som er godkendt af et anerkendt standardiseringsorgan til gentagen eller konstant anvendelse, men hvis overholdelse ikke er obligatorisk. Til forskel fra lovhjemlede tekniske forskrifter er der altså i almindelighed ingen pligt til at overholde en standard. En sådan pligt kræver til enhver tid særskilt hjemmel i aftale eller lovgivning.

Definitionen ovenfor anvendes i EU's forskellige direktiver om standardisering, se f.eks. art. 1, stk. 2, i direktiv 98/34/EF af 22. juni 1998 om en informationsprocedure for tekniske standarder og forskrifter. En noget snævrere definition af begrebet anvendes af den internationale standardiseringsorganisation ISO: "A technical specification available to the public, drawn up with the co-operation and consensus or general approval of all interests affected by it, based on the consolidated results of science, technology and experience, aimed at the

promotion of optimum community benefits and approved by a body recognised at the national, regional or international level".

Anvendelsesområde

Standarder kan tage sigte på alle forhold af teknisk eller praktisk art, lige fra skrivemaskinetastaturer, papirstørrelser, materialer, sproganvendelser og til fremgangsmåder, metodiker, dimensioner, ydeevner, sikkerhedsforskrifter eller produktionsprocesser. Der er altså ingen grænser for, hvilke forhold der kan reguleres af en standard, og standarder findes derfor inden for alle områder af samfundslivet – altså ikke kun på IT-området eller lignende teknisk prægede områder.

Standardiseringens betydning på IT-området er allerede omtalt i den historiske introduktion: Uden grundlæggende standarder har den enkelte producent været nødt til at "genopfinde hjulet" for at kunne sætte sin "bil" på markedet. I konsekvens heraf har man i udviklingens første år fået produkter, der ikke kunne "tale sammen" (såkaldt manglende *interoperabilitet*), hvilket blandt meget andet har vanskeliggjort teknisk vedligeholdelse, fremskaffelse af reservedele mv. og gjort forbrugerens valg uoverskueligt.

IT-standarder

At disse skadevirkninger har været særligt store på IT-området skyldes navnlig, at IT-systemer i stigende grad er sammensat af *moduler*. Et modulært opbygget system kan bestå af komponenter fra forskellige leverandører, hvad enten der er tale om hardware-enheder (lige fra halvlederchips og til hele systemenheder) eller om programmel udviklet af underleverandører (såkaldt tredjepartsprogrammel). Sammenkoblingen kan enten ske *fysisk*, således at komponenterne rent faktisk kan sættes sammen ved stik og indstikskort, eller *logisk*, således at det ene program kan kommunikere med det andet.

Standardisering er dermed ensbetydende med åbenhed og større konkurrence. Denne sammenhæng illustreres ved et blik på de standarder, der i sin tid konkurrerede om at blive dominerende for markedet for videokassetter, den amerikanske VHS-standard og den japanske *Betamax*-standard. Trods Betamax-standardens teknologiske fortrin blev slaget vundet af VHS-standarden, og det er i dag praktisk taget umuligt at erhverve en fabriksny *Betamax*-videomaskine.

Blandt de områder inden for den klassiske IT-ret, hvor disse standardiseringsinitiativer har spillet en særlig rolle, kan nævnes elektroniske signaturer. Ifølge artikel 3, stk. 5, i direktivet om elektroniske signaturer kan Kommissionen efter en særlig procedure offentliggøre referencenumre på almindeligt anerkendte standarder for elektroniske signatur-produkter. Der skal herefter gælde en formodningsre-

gel, hvorefter et elektronisk signatur-produkt, der opfylder sådanne standarder, skal formodes at overholde kravene i bekendtgørelsens bilag II, litra f, og bilag III (de kvalificerede krav). I 1999 bemyndigede Kommissionen en ekspertgruppe kaldet "European Electronic Signature Standardization Initiative" (EESSI) opgaven at analysere den fremtidige brug af standardisering inden for dette område, og resultatet af dette arbejde foreligger med en rapport af 28. juli 1999. Arbejdet hermed er siden videreført af ETSI, se nærmere <http://portal.etsi.org>. I Danmark udfoldes en værdifuld koordinerende indsats i det Forum for Digital Signatur (FDS), der er etableret under Dansk Standard.

Af disse grunde kan indholdet af en standard være altafgørende for, hvorledes konkurrencen udvikler sig på markedet for de produkter, standarden understøtter. Prisfaldet på mobiltelefoner, der benytter GSM-standarden, skyldes netop, at denne fælleseuropæiske standard har skabt et så stort marked, at stordriftsfordelene for alvor slår igennem i produktionen. Uden de standarder, der ligger til grund for Internet (TCP/IP, HTTP m.fl.), ville man savne det tekniske grundlag, der knytter de mange computere sammen i dette net. Havde man ikke standarder for digitale tv-signaler, ville det være vanskeligt at opbygge et fælles marked for salg af satellit-dekodere mv. og dermed et fælles marked for betalings-tv via satellit. Det samme kan siges om udbredelsen af den digitale video-disk (DVD'en), der ligeledes bygger på standarder for såvel datalagring som kryptering mv.

Problemer

Standardisering er dog ikke uproblematisk. En virksomhed, der "ejer" en standard, er nødt til at åbne indmaden af sit produkt for omverdenen og stille specifikationer mv. til almenhedens kundskab, hvis hans standard skal være generel. Men ofte vil disse specifikationer indeholde resultatet af kostbare udviklingsinvesteringer, som konkurrenterne uden videre kan få glæde af, hvis standarden kommer i *public domain*. Den måde, hvorpå et system afgiver og modtager data, kan f.eks. reducere behovet for maskinressourcer eller tilføje yderligere kvaliteter (f.eks. sikkerhed mod aflytning el.lign.). Dette problem er ikke alene relevant for de standarder, der ligger til grund for telekommunikation ved hjælp af telefon, telefax og ved udveksling af data på Internet, men også for producenter af udstyr, der skal tilsluttes andet udstyr (f.eks. chip-baserede spil, plug in enheder mv.).

For den producent, der skal efterleve en standard, kan standarden være både en fordel og en ulempe. Vel har producenten fordel af standardiseringen, hvis standarden åbner et stort marked for ham. Men understøtter standarden ikke et sådant marked, vil den blot være ensbetydende med, at producenten tvinges til at

gøre noget ved udformningen af sit produkt mv., som han måske ville have foretrukket at gøre anderledes. Standarden kan tvinge ham til at gå en omvej for at nå den tilsigtede tekniske løsning. Og hvis ikke omkostningerne ved at gå denne omvej hentes hjem over afsætningen, er der ingen økonomisk fornuft i at standardisere.

Omkostninger

Er standarden under udarbejdelse, kan leverandøren søge at få indflydelse på dens endelige udformning. Dette er imidlertid ikke uden omkostninger. Medlemskab i en arbejdsgruppe (jf. herom nedenfor) koster et årligt gebyr – almindeligvis mellem 1.000 og 6.000 kr. – der dækker udgifter til kopiering, møder og sekretariat. Dertil kommer de omkostninger, der kan måles i tid og besvær. Det stiller ofte store krav til tålmodigheden at skulle koordinere de mange ønsker, der gør sig gældende, når mange nuværende og kommende udbydere skal enes om en grænseflade eller funktion. Aktørerne i dette arbejde deltager for egen regning.

I IT-sikkerhedsrådets første oplæg til en dansk IT-sikkerhedspolitik (Forskningsministeriet, november 1996), anbefales det, at Danmark opprioriterer sin deltagelse i det internationale standardiseringsarbejde på IT-sikkerhedsområdet, se oplægspapiret s. 11.

Kvalitetskrav

Ideelt set bør en standard altid optimere den teknologi eller det produkt, den angår. Når nye teknologier kommer til, vil dette ideal ofte støde mod inertiens lov, når standarden rent faktisk indarbejdes. Da den QWERTY-standard, der bestemmer placeringen af typerne på skrivemaskinetastaturer verden over, i sin tid blev indført, skete det for at nedsætte skrivehastigheden, så to typer ikke stødte sammen på vej mod papiret. Bl.a. placerede man de ofte benyttede bogstaver T, E og R ubekvemt ved siden af hinanden over det sted, hvor venstre hånd placeres på tastaturet. I dag, hvor teknologien stort set har elimineret denne faktor, er der behov for en anden og mere effektiv standard. QWERTY-standarden er imidlertid en realitet, og de funktionelle argumenter i modsat retning kan ikke ændre den.

5.3.b. Terminologi

Funktions- og basisstandarder

Standardiserings-terminologien er ikke klar. Området florerer med forskellige termer, der udskiller standarderne i henseende til f.eks. præciseringsgrad, vedtagelsesform o.lign. Som *funktionsstandarder* betegner man efter én terminologi den måde, hvorpå andre standarder – *basisstandarder* – skal formuleres. Findes der ingen basisstandard, overlader funktionsstandarden producenten

en række muligheder, som i og for sig kun har aktualitet i enkelttilfælde.

Vedtagne standarder

En anden sondring knytter sig til, hvordan standarden er blevet indført. *Vedtagne standarder* er fremkommet som resultatet af et teknisk-kollegialt arbejde. Blandt de vedtagne standarder indtager de europæiske standarder (EN) en særlig rolle, jf. herom senere. Inden for denne gruppe dækker begrebet *harmoniseret standard* de standarder, der er blevet til i overensstemmelse med reglerne i direktiv 98/34/EF, se nærmere nedenfor. Visse standarder opstår helt uformelt, f.eks. ved at en branche rent faktisk vælger at følge en vis praksis.

De facto og de jure-standarder

En tredje sondring knytter sig til, hvilken instans der står for arbejdet med at udvikle standarden. En *de facto-standard* er opstået uden noget formaliseret forarbejde, f.eks. som resultatet af en producents valg af produktdesign. Sådanne standarder får deres virkning efter *follow the leader*-princippet ved, at en toneangivende leverandør (f.eks. IBM, Amdahl, Hewlett-Packard, Digital Equipment Corporation eller andre) – mere eller mindre utvetydigt – tilkendegiver, at man vil fremstille produkter af en given beskaffenhed. Modsat er en *de jure-standard* kendetegnet ved at følge de regler, der gælder for et standardiseringsorgan. En de jure-standard vil således altid været vedtaget.

Branchevedtagelser

I en mellemgruppe mellem de facto-standarder og vedtagne standarder står de, der udspringer af en *branchevedtagelse*, der ikke er nået i et standardiseringsorgan. Sådanne standarder – der ikke bærer nogen anerkendt betegnelse – er f.eks. dukket op som et modspil til de facto-standarder, der af forskellige årsager anses for utjenlige til deres formål.

Tre eksempler herpå kan nævnes. I slutningen af 1980'erne udviklede et antal IT-producenter standarden for den såkaldte EISA-bus, der skulle udgøre et alternativ til IBM's MCA-bus, og dermed løsrive IBM fra dette selskabs kontrol over de komponenter, der skal kommunikere med bussen. I en tilsvarende mellemgruppe finder man halv-officielle standardiseringsorganer, som f.eks. X/OPEN, der bl.a. arbejder med standardisering af styresystemer baseret på AT&T's UNIX-system. Arbejdet i X/OPEN-gruppen er støttet af EU-Kommissionen, der har meddelt den dispensation under TEF's konkurrenceregler. Et tredje eksempel er de standarder, som en række maskinproducenter har vedtaget vedrørende den såkaldte NC.

5.3.c. Særligt om teleområdet

Et af de væsentligste standardiseringsområder i det moderne informationssamfund er teleområdet. Som nævnt under den kom-

munikationsteoretiske gennemgang i afsnit 2.2. forudsætter enhver form for kommunikation anvendelse af et fælles sprog. Dette gælder, uanset om der er tale om kommunikation mellem personer eller mellem systemer. Ved kommunikation mellem systemer taler man om overholdelse af *protokoller*.

Telefoni

På teleområdet får standardiseringskaos direkte betydning for funktionaliteten. Derfor har standardiseringsarbejdet netop her lange traditioner. Den, der køber en telefon, kan som bekendt sætte sig i forbindelse med alle afkroge af jordkloden og slutte den til nettet overalt. Denne intense og effektive standardisering skyldes hovedsagelig de telemonopoler, der har været gældende på området i kraft af koncessionsordninger og statsmonopoler mv. Efter opløsningen af disse monopoler er det påkrævet med en stærk koordinering af udstyrets tekniske grænseflader mv.

Internet

Et andet standardiseringsområde angår *Internet-kommunikation*. Som tidligere anført bygger Internet på en række standarder for kommunikation mellem tilsluttede computere og terminaler. Den grundlæggende protokol er IP-protokollen (IP for Internet-Protokol), som siden 1980'erne har foreligget i en version 4. Denne standard anser nogle for at være for snæver, idet den bl.a. indeholder begrænsninger for, hvor mange adresser der kan kommunikeres fra og til. I disse år arbejder man på udviklingen af en ny såkaldt version 6 af denne protokol (kaldet IPv6).

De nævnte standarder blev oprindelig skabt af de personer, der deltog i udviklingen af ARPA-nettet. Nettet blev bygget op om et antal protokolstandarder, der sikrede det førnævnte princip for dataudveksling. Som følge af den kontakt, der består mellem DoD og de amerikanske universitetsforskningsmiljøer, blev ARPA-nettet gradvis taget i brug af universitetsverdenen. I 1983 vedtog man en protokol for den kommunikation, der sker på nettet, TCP/IP (Transmission Control Protocol/Internet Protocol), som i dag er grundstammen for Internet-kommunikation.

Hovedparten af standardiseringarbejdet vedrørende Internetkommunikation ligger i dag i World Wide Web Consortium og i Internet Engineering Task Force (IETF) under Internet Society, se <www.ietf.org>.

5.3.d. Vedtagelse af standarder

Som allerede nævnt beror værdien af en standard på, hvor udbredt den er. Derfor søger man at tilrettelægge standardiseringsarbejdet, så der opnås højest mulig konformitet blandt de kommende brugere. Dette kræver et koordinerende arbejde, som i

nutidens verden søges organiseret på både nationalt, regionalt (europæisk) og internationalt plan.

Standardiserings-organet

Det organ, der godkender og udsender en standard, kan være nationalt, europæisk eller internationalt. Typisk indgår organet i en organisation, der også har indtjening på at sælge den tekst, hvori standarden er nedfældet. Prisen for standarder er typisk høj, da standardiseringsorganerne herved søger at inddække nogle af de omkostninger, der har været forbundet med at producere standarden. Herhjemme står den selvejende institution Dansk Standard (DS) for det nationale standardiseringsarbejde. Det europæiske arbejde varetages af bl.a. CEN, CENELEC, ETSI m.fl. På den internationale scene finder man ISO, IEC, ITU-T m.fl. De standarder, der understøtter WWW, vedtages af World Wide Web Consortium, se <www.w3.org>. WWW Consortium står bl.a. for vedligeholdelsen af den vigtige HTML-standard for hypertekst-dokumenter på Internet og for udviklingen af de nye XML-standarder.

Dansk Standard

Dansk Standard (dengang: Dansk Standardiseringsråd) blev oprettet i 1926 under Industriministeriet på foranledning af Industrirådet og DIF. I henhold til de af ministeriet godkendte vedtægter er rådets formål at virke for standardisering i Danmark, bl.a. ved som medlem af ISO, CEN og INSTA "at virke for anvendelsen af International og Europæisk Standard i den udstrækning, det er foreneligt med danske forhold". Rådet fungerer endvidere som dansk WTO-informationscenter og som certificerende organ. Under rådets formål hører også "at virke for anvendelse af henvisninger til Dansk Standard i dansk lovgivning". Endelig er rådet dansk informations- og dokumentationscenter for standardisering. Rådet ledes af et repræsentantskab, et forretningsudvalg og en direktør.

I USA er det offentlige standardiseringsarbejde placeret under U.S. Department of Commerce, der herved rådgives af National Institute of Standards and Technology (NIST) – tidligere National Bureau of Standards (NBS). Ifølge en nyere lov skal Department of Commerce "promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary [i.e. Department of Commerce] determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems", se 40 U.S.C.A. § 759 (d), stk. 1.

Arbejdets igangsætning

Forslag om vedtagelse af en ny standard rejses typisk i en af de tekniske komitéer (Technical Committees eller TC), der hører til det nationale eller det internationale standardiseringsarbejde. En gruppe af fagfolk konstaterer et behov for et nærmere fastlagt

regelsæt og tager herefter kontakt med et standardiseringsorgan. Organet formidler den relevante kontakt med en eksisterende TC for at sikre den fornødne koordination. TC'en uddelegerer arbejdet med at afklare grundlaget for den nye standard samt med at præcisere dens indhold til en arbejdsgruppe eller flere (Working Group eller WG). Eventuelle del-emner behandles i en Sub-Committee (SC). Hver TC, SC eller WG har et sekretariat, som varetages af et af medlemslandene.

Åbenhed

Åbenhed er en væsentlig ingrediens under vedtagelse af de jure-standarder. DS har klare retningslinier for offentliggørelse af forslag til Dansk og International Standard, der bl.a. fastslår, at enhver, hvis interesse berøres af sagen, kan indsende bemærkninger. Fagtidsskrifter (som f.eks. ugeavisen Ingeniøren) indeholder løbende omtale af igangværende standardiseringsarbejder med opfordring til interesserede parter om at komme med forslag eller indsigelser. Kan sådanne forslag ikke tiltrædes, må dette efter reglerne for DS begrundes.

IT-standardisering

Det DS-standardiseringsarbejde, der har særlig interesse på IT-området, styres af tre grupper under DS – gruppe S142, S242 og S243. F.eks. arbejder gruppe S243 bl.a. med standarder for elektronisk dataudveksling inden for administration, handel og transport, herunder de EDIFACT-standarder, der danner grundlaget for fremtidens EDI-systemer.

5.3.e. Den EU-retlige dimension

I det økonomiske samfund har standarder flere funktioner. Kompatibilitetsstandarder tjener til at opbygge markeder, hvor der konkurreres på pris. Kvalitetsstandarder kan holde underlødige produkter ude. Da begge dele spiller en stor rolle for virksomhedernes indtjening, er der naturligt fokus på standardiseringsarbejdet. Ethvert højteknologisk samfund og enhver aktør indenfor det teknologiske brancheområde må derfor som en del af sin industripolitik have en standardiseringspolitik. En sådan politik er også blevet en del af Danmarks IT-sikkerhedspolitik, jf. IT-sikkerhedsrådets baggrundspapir herom, s. 25 ff. Problemet har en indlysende EU-retlig dimension, eftersom forskellige, nationale standarder, fører til forskellige markeder og hermed til barrierer for udveksling af varer og tjenester over landegrænser.

EN-systemet

Et mærkbart udslag af EU's standardiseringspolitik er, at en række nationale standarder i de kommende år vil blive erstattet af europæiske standarder, der bærer præfikset EN ("European Norm"). En EN-standard er godkendt på grundlag af vedtægterne

i en af de standardiseringsorganisationer, som EU har indgået aftale med. Et af disse er CEN, der omfatter alle europæiske (EU og EØS) standarder, der ikke dækkes af andre standardiseringsorganer. En anden er CENELEC, der har ansvaret for europæisk standardisering inden for det elektrotekniske område. En EN-standard er kun "bindende" på det folkeretlige plan. Den skal vedtages som national standard, og eventuelle afvigende nationale standarder skal ophæves, før den får virkning som national standard eller national retsforskrift.

Den hastighed, hvormed EU-myndighederne frembringer ny lovgivning, står i skarp kontrast til den træghed, hvormed internationale standarder bliver til. Vedtagelsen af en standard kan sagtens tage henved 10 år, og på det tidspunkt har teknologien måske bevæget sig langt væk fra det, der var grundlaget for at formulere standarden. Et sådant tidsforbrug er uacceptabelt, bl.a. fordi det vil lægge en dæmper på den industrielle udvikling, som standarden gerne skulle understøtte. Da EN-standarder må vedtages hurtigere, har man indført begrebet "foreløbige europæiske standarder", forkortet ENV (Europäische Norm für Versuchungsweise Anwendung), der efter en tre-årig forsøgsperiode vurderes med henblik på indførelse som endelig EN-standard.

Retsgrundlag

EU's standardiseringsarbejde understøttes af en række mere eller mindre formaliserede vedtagelser, hvis hovedlinie er, at medlemsstaterne skal undgå nationale sær-standarder på de områder, der har betydning for fællesskabets økonomiske politik. Hovedhjørnestenen i dette system findes i direktiv 98/34/EF, om en informationsprocedure med hensyn til tekniske standarder og forskrifter samt forskrifter for informationssamfundets tjenester (EFT 1998 L 204/37), som ændret ved direktiv 98/48, EFT 1998 L 217/18 (det såkaldte *transparensdirektiv*) med sigte på det sidste led: "informationssamfundets tjenester". Direktivet tilsigter at koordinere medlemsstaternes forslag om nationale tekniske forskrifter. Dette sker bl.a. gennem en ordning, hvorefter udkast til sådanne forskrifter fremsendes (notificeres) til Kommissionen, se hertil art. 2-4. Kommissionen og medlemsstaterne har herefter frist til at foreslå ændringer af den påtænkte foranstaltning med det formål at fjerne eller mindske de hindringer for den frie vareudveksling, som kan følge af foranstaltningen.

En tilsvarende notifikationspligt gælder i henhold til WTO-aftalen, se Erhvervsfremmestyrelsens cirkulære nr. 85 af 16. juni 1995.

Ved den ændring af direktivet, der fandt sted ved direktiv 98/48/EF, blev "informationssamfundets tjenester" som nævnt

medtaget, se om dette forslag KOM(96) 392 endelig udg. Hermed sigtes til "enhver tjeneste i informationssamfundet, dvs. enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager" (artikel 1, litra a), stk. 2). Som følge heraf er det pålagt medlemsstaterne – i overensstemmelse med direktivets almindelige regler – at udsætte vedtagelsen af lovgivning og bekendtgørelser, der inden for det afgrænsede område ("informationssamfundets tjenester") har karakter af "tekniske forskrifter". Visse lovgivningsområder – herunder lovgivning inden for den finansielle sektor – er dog undtaget.

Den "nye metode"

På grundlag af forløberen for 1998-direktivet (direktiv 83/189/EØF) indførte Rådet den 7. maj 1985 en ny metode i forbindelse med teknisk harmonisering og standarder, se EFT 1985 C 136/1. Tidligere indeholdt de EU-direktiver, der opstiller krav om tekniske egenskaber eller kvaliteter, en mængde tekniske detailstandarder, der var vanskelige for medlemsstaterne at overskue endsige gennemføre. Den nye metode, der anvendes i relation til tekniske specifikationer, hvortil der knytter sig en sikkerhedsmæssig, sundhedsmæssig eller offentlig interesse, går ud på, at direktiverne alene angiver en række "essential requirements" (f.eks. med relation til sikkerhed mv.), som må opfyldes, uanset om de pågældende produkter handles på tværs af medlemslande. Et produkt, der opfylder disse krav, og som er blevet mærket med det særlige CE-mærke, kan spredes frit over hele Fællesskabet. Mere detaljerede krav til produktets egenskaber kan herefter fastsættes i de tekniske standarder fra de europæiske og internationale standardiseringsorganer. Medmindre andet følger af fællesskabsregler, er sådanne krav ikke bindende. Den nye metode er siden indføjet i de direktiver, der har implementeret standardiseringspolitikken, f.eks. EMC-direktivet jf. nedenfor.

Den nye metode (der siden er blevet søgt gjort til en "global metode", se hertil rådets resolution af 21. december 1989, EFT 1990 C 10/01), har hidtil været anvendt i ca. 25 direktiver, hvoraf nogle tangerer IT-området, således direktiverne om maskiner (89/292/EØF), personligt beskyttelsesudstyr (89/686/EØF), visse medicinske instrumenter (90/385/EØF), ikke-automatiske vejeinstrumenter (90/384/EØF), og telekommunikationsudstyr (91/263/EØF). Se generelt hertil *Christopher Kuner* i 2 Business Law International (2000), 102 ff. Ved EF-domstolens præjudicielle afgørelse af 26. september 2000 (i sag C-443/98) er det i øvrigt bestemt, at en national domstol under behandlingen af en kontraktsretlig sag mellem private

ikke må anvende en national teknisk forskrift i en periode, hvor vedtagelsen af udsat efter direktivets såkaldte *stand-still*-procedure.

I dag, 20 år efter indførelsen af den "nye metode", er der opstået et revisionsbehov, jf. rådsbeslutningen af 10. november 2003 (2003/C 282/02), hvori Rådet opfordrer Kommissionen til at foreslå ændringer. Man har navnlig set et behov herfor i relation til den private *conformity assessment* (dvs. overensstemmelsesvurdering), ligesom det ønskes vurderet, om medlemsstaternes administration af *CE-mærket* (herunder afgrænsningen af, hvad der udgør "essential requirements") har været hensigtsmæssig.

Standardiseringsbeslutningen

Af særlig betydning for IT-området er den beslutning, rådet traf den 22. december 1986 om standardisering inden for informationsteknologi og telekommunikation (87/95/EØF), EFT 1987 L 36/31. Ifølge beslutningens artikel 5 træffer medlemsstaterne de fornødne foranstaltninger til, at der i offentlige indkøbsaftaler vedrørende informationsteknologi henvises til europæiske standarder, foreløbige europæiske standarder og godkendte internationale standarder. Dette indebærer bl.a., at Fællesskabet og medlemsstaternes respektive regeringer skal anvende ISO's standarder inden for IT-behandling. I konsekvens heraf skal medlemsstaternes statsinstitutioner ved anskaffelser af IT kræve europæiske eller andre internationale standarder på IT-området overholdt, efterhånden som disse specificeres.

Anvendelsesområder

De førnævnte standardiseringskrav er bl.a. udmøntet i de EU-retlige regler om offentlige myndigheders indkøb, jf. nærmere afsnit 12.2.d. EU-direktiverne om offentlige indkøb, der omtales nærmere i kapitlet om overdragelse, forpligter offentlige myndigheder i EU til at anvende tekniske forskrifter, der er udtryk for gennemførelse af europæiske standarder. Denne forpligtelse er i dansk ret indført ved § 5 i bekendtgørelse nr. 132 af 28. februar 1991 om anvendelse af standarder ved offentlige indkøb af informationsteknologi og ved fastsættelse af visse tekniske forskrifter. Reglerne søger tillige at tjene som løftestang for udbredelsen af de pågældende standarder, da det offentliges efterspørgsel kan forventes at smitte af på markedet som helhed.

Bevillingsfunktioner

Også når EU optræder som bevillingsmyndighed for forskning, søger man at konsolidere de europæiske standarder. Dette krav stilles typisk som vilkår for bevillinger under Kommissionens RACE og ESPRIT-projekter. Dernæst har EU ganske ofte støttet forskning, der tager sigte på standardiserings-følsomme teknologier.

Produktsikkerhed

Et tredje område for EU-standardiseringsarbejdet finder man i de EU-regler, der er under udarbejdelse om produktsikkerhed. Ifølge § 7 i lov om produktsikkerhed (lov nr. 364 af 18. maj 1994 med senere ændringer) *anses* et produkt eller en tjenesteydelse for sikkert i det omfang det er konstrueret og fremstillet henholdsvis udført "i overensstemmelse med de sundheds- og sikkerhedskrav, der er fastsat i lovgivningen", jf. stk. 1. Produktet anses dog kun for sikkert i henseende til *disse* sikkerhedsaspekter. Et produkt *formodes* dernæst at være sikkert, i det omfang det er i overensstemmelse med de sikkerheds- og sundhedskrav, der er fastsat i nationale standarder, som gennemfører europæiske standarder, hvis referencer Europa-Kommissionen i overensstemmelse med Europa-Parlamentets og Rådets direktiv om produktsikkerhed i almindelighed har offentliggjort i EF-Tidende, jf. stk. 2. Er der ikke fastsat sundheds- og sikkerhedskrav efter stk. 1 eller 2, vurderes et produkts eller en tjenesteydelses sikkerhed i forhold til (1) en dansk standard, der er baseret på andre europæiske standarder end dem, der er omhandlet i stk. 2, (2) en dansk standard, (3) henstillinger fra Europa-Kommissionen, som fastlægger retningslinjer for vurdering af produktsikkerhed, (4) adfærdskodekser for produktsikkerhed inden for den pågældende sektor eller (5) andre relevante forhold, herunder den aktuelle viden og teknologi samt den sikkerhed, som brugerne med rette kan forvente, jf. stk. 3. I det omfang der i EU-retten eller med hjemmel heri er fastsat harmoniserede sikkerhedskrav til produkter eller tjenesteydelser, træder disse i stedet for tilsvarende sikkerhedskrav i de i stk. 1-3 anførte forskrifter. En tilsvarende regulering findes i andre sektorspecifikke regler om bestemte produkters sikkerhed.

5.3.f. Retsvirkninger

Det ligger i kravet om, at standarden "ikke er obligatorisk", at den norm, den udtrykker, ikke i sig selv er juridisk forpligtende. Dette udgangspunkt modificeres dog dels ved den gennemslagskraft, der ligger i et standard-efterspørgende marked, dels af, at lovgivningen hyppigt inkorporerer standarder som en del af retsgrundlaget. Derfor er det vigtigt, at vedtagelse af standarder opfylder visse parlamentariske grundbetingelser.

- ved lov

En standard kan for det første opnå retsvirkninger ved lov. Talrige tekniske forskrifter inden for byggeri og anlæg henviser

til DS-standarder, og som nævnt vil EU's standardiseringspolitik frembringe flere regler af denne karakter, jf. nærmere i afsnit 5.3.e. I enkelte tilfælde sker det, at standarder ophøjes til bekendtgørelser. Det gælder f.eks. for bygningsreglementet og for stærkstrømsreglementet af 1962.

- ved aftale

I takt med, at en række standarder har vundet indpas som funktionelle forudsætninger for moderne IT-produkters funktionsduelighed, er et produkts overensstemmelse med disse standarder (ofte betegnet med udtrykket *kompatibilitet*) blevet en aftaleparameter. Det kræver f.eks. ikke særlig vedtagelse at støtte krav på, at en Internet-browser eller et Internet-mail-program opfylder gældende standarder for kommunikation på Internet. I offentlige udbudsaftaler optræder henvisningen til offentliggjorte standarder ikke alene som en aftalt betingelse; en sådan inkorporering er pålagt efter de EU-retlige regler om offentlige indkøb, jf. nærmere afsnit 23.2.c.

- som udfyldning

Selv om en standard ikke i sig selv kan derogere et andet retsgrundlag, kan den efter omstændighederne anvendes som udfyldende retsgrundlag, f.eks. i relation til upræcise lovbestemmelser. Når kbl. § 1 lader loven vige for "handelsbrug eller anden sædvane", er det den faktiske adfærd – ikke standarden – der kvalificerer. Omvendt kan der nævnes eksempler på talrige standarder, der må anses for bortfaldet ved desvetudo. Standardens juridiske gennemslagskraft beror altså på dens udbredelse og væsentlighed. *U 1989.1039 H* angik forudsætningerne for et løfte om at udbedre mangler ved et byggeri, der bestod i, at en byggestandard ikke var overholdt. Overtrædelsen havde kun begrænset betydning. Flertallet i Højesteret ville derfor ikke tilsidesætte aftalen, medens et mindretal ville. Ved dommen i *TBB 1999.7 V* fandtes det ikke godtgjort, at sælgeren af nogle afløbsbrønde havde indestået for, at leverancerne kunne opfylde tyske normkrav. Brøndene skulle leveres til en byggeplads i Tyskland, men der var ikke indgået udtrykkelig aftale om, at de tyske normkrav skulle opfyldes. I *FKNbrtn. 1985.36* henviste sælgeren af en stereo-forstærker til en ikke sædvanligt anvendt DIN-norm ved sin angivelse af udgangseffekten. Dette fandtes misvisende og udgjorde dermed en mangel.

ISO 9000-serien

På IT-området kan standarder navnlig få juridisk betydning i relation til vurderingen af en ydelses kvalitet og pålidelighed. ISO har i den række standarder, der er publiceret i DS/ISO 9000-serien (EN 29000), dels formuleret krav til kvalitetsstyringssystemer i kontraktsituationer, dels givet retningslinjer til brug i de mange situationer, hvor en virksomhed eller organisation ønsker at udvikle et kvalitetsstyringssystem og gennemføre det i praksis. Disse standarder er imidlertid processtandarder, der først og fremmest siger noget om leverandøren og kun indirekte noget om det produkt, han leverer. Et eksempel på en produktstandard, der kan tænkes at få betydning ved overdragelse af IT, er ISO 9126 (EN 29.126) fra 1990: "Information technology – software product evaluation – quality characteristics and guidelines for their use" og ISO 9127 (EN 29.127) fra 1989: "Information processing systems – user documentation and cover information for consumer software packages". ISO 9126 angiver seks kvalitetsegenskaber ved software, ISO 9127 opstiller en række krav til de brugervejledninger, der ledsager standardprogrammel. I det omfang, disse standarder vinder indpas, vil de utvivlsomt kunne påvirke de typeforudsætninger, der gør sig gældende i sådanne køb. Dette synes dog endnu ikke sket. ISO 9000-serien har været genstand for en righoldig litteratur, se bl.a. *Bøje Larsen*: ISO 9000 forfra og bagfra (1996).

5.3.g. Immaterialretlige spørgsmål

Udgangspunktet

Behovet for at udvikle åbne systemer og interoperable komponenter har ført til et skisma mellem standardisering og retsbeskyttelse. Problemet opstår i relation til to aspekter af en standardiseringsproces: Selve den sproglige beskrivelse, hvor ophavsrettens regler kan spille ind, og den tekniske fremgangsmåde, hvor patent- og brugsmodelsystemet kan få betydning.

- ophavsret

Når man har diskuteret, om standarder overhovedet burde kunne beskyttes *ophavsretligt* som litterære værker, bygger indvendingen herimod på principper svarende til de, der har ført til, at offentlige *rets*akter ikke ophavsretsbeskyttes, se f.eks. *Joseph Farrell* i 30 Jurimetrics Journal 35 (1989). Efter gældende ret er det dog udgangspunktet, at en standard, som udstederen effektivt søger at håndhæve en ophavsret til, også er undergivet en sådan beskyttelse. Men tendensen går også på dette område i retning af, at rettighedshaverne i givet fald undlader at håndhæve disse rettigheder, en praksis, der f.eks. ses ved at talrige standarder foreligger tilgængelige fra standardiseringsorganisationernes hjemmesider.

- Ophl. § 9

Ophl. § 9 fastslår, at love, administrative forskrifter, retsafgørelser og lignende offentlige aktstykker ikke er genstand for ophavsret; men udgangspunktet for denne bedømmelse er, om standarden *har* normerende karakter; ikke om den *tillægges* en nor-

merende virkning. Og da standarden pr. definition ikke er gennemtvingelig, må den betragtes som et faktisk fænomen, nemlig som manifestationen af den enighed, der er nået i standardiseringsorganet om, hvorledes man vil gribe et bestemt problem an.

Som udgangspunkt må det antages, at juridiske dokumenter er omfattet af ophavsretten, se hertil *Bryde Andersen*: Advokatretten (2005), s. 608 f. Som her antaget kan den ophavsretlige beskyttelse give anledning til vanskeligheder, når dokumentet genbruges og inspirerer til frembringelse af nye dokumenter mv. Det forhold, at advokater sjældent søger at gennemtvinge ophavsretten til deres dokumenter, medvirker til at cementere en generel retsopfattelse, hvorefter der – hvis ikke der foreligger et særligt grundlag for at nå til et andet resultat – består et vist frirum til at foretage ophavsretlige udnyttelseshandlinger. Om noget tilsvarende vil være gældende i relation til offentliggjorte standarder beror på, om det involverede standardiseringsorgan søger at fastholde en ophavsret til dokumentet, f.eks. for at finansiere de ofte betydelige omkostninger til mødeafholdelse og trykning. Er dette tilfældet, taler meget for at fastholde det almindelige ophavsretlige udgangspunkt. Er standarden derimod lagt ud til fri afbenyttelse, f.eks. fra standardiseringsorganets hjemmeside, taler meget for at lade reglerne om juridiske kontraktsdokumenter finde tilsvarende anvendelse.

- patentret mv.

Standarder, der beskriver en teknisk metode eller proces, kan tænkes at anvise fremgangsmåder mv., der er genstand for patentbeskyttelse. Når en sådan konflikt forekommer er der ingen tvivl om, at patentsystemet vinder, medmindre man i den enkelte situation befinder sig inden for et af de områder, der dækkes af patentudelukkelse, herunder visse ikke-erhvervsmæssige og forskningsmæssige anvendelser, jf. PL § 3, stk. 3. Patentsystemet har således ikke undtagelsesregler svarende til ophl. § 9. Dette betyder, at standarden da kun kan bruges, såfremt patenthaveren meddeler sit samtykke hertil.

I IT-praksis er problemet navnlig opstået i relation til standarder for telekommunikation. Skal rettighedshaveren kunne opretholde et patent i en standard (f.eks. et teknisk krav om, at alle GSM-basisstationer skal følge dette sorteringsprincip), vil han komme til at "eje" den pågældende teknologi. Og hvis ikke dette ejerskab modificeres, f.eks. gennem tvangslicens-lignende foranstaltninger, vil man opnå en situation, der er direkte i strid med de hensyn, standardiseringen tilsigtede.

ISO og IEC

ISO og IEC har længe haft vedtagne regler for immaterielle rettigheder i standarder, se herved ISO's Rules for reference to patented items in International Standards. EU-Kommissionen har ved forskellige lejligheder anbefalet, at standarder ikke gøres til genstand for immaterialrettigheder, og at standardiseringsorgan-

erne i tilfælde, hvor sådanne rettigheder er uundgåelige, sikrer, at markedet har mulighed for på rimelige betingelser at få licens på dem. Dermed indfører man en form for "frivillig tvangslicens": De således fastsatte spilleregler binder på forhånd deltagerne i standardiseringsarbejdet til at fraskrive sig den adgang, de ellers ville have haft, til at udøve deres aftalefrihed i afgørelsen af, hvem der skulle tildeles licens til de pågældende patenter.

Vil rettighedshaveren ikke give licens, kan dette etablere en dominerende stilling, der kan forfølges konkurrenceretligt efter TEF.

1992-henstillingen

En række af disse problemer blev lagt frem med Kommissionens meddelelse af 27. oktober 1992 om Intellektuel Ejendomsret og Standardisering, KOM(92) 445, endelig udg. Heri henstiller Kommissionen bl.a., at standarder benyttes på fair, rimelige og ikke-diskriminerende vilkår, hvad enten brugerne deltager i standardiseringsorganets arbejde eller ej, og at indehavere af immaterialrettigheder sikres rimelige vilkår mht. royalties mv., idet disse efter bedste evne må bestræbe sig på at identificere eventuelle immaterialrettigheder.

ETSI

Spørgsmålet har givet anledning til en intens debat ved den europæiske standardiseringsorganisation for telekommunikation, ETSI. Diskussionen opstod i forbindelsen med vedtagelsen af standarderne for GSM-telefoni og resulterede i en generel *Intellectual Property Rights Policy*, som i dag findes som et anneks 6 til ETSI's Rules of Procedure (dateret 22. november 2000). Ifølge punkt 3.2 heri fastslås det almindelige princip, at indehavere af immaterialrettigheder – uanset medlemskab af ETSI – "should be adequately and fairly rewarded for the use of their IPRs in the implementation of standards and technical specifications". Reglerne pålægger dernæst alle ETSI-medlemmer at orientere ETSI om "essential IPR's", som medlemmet bliver opmærksom på. Dette gælder i særlig grad, hvis medlemmet selv fremlægger et forslag til en standard eller teknisk specifikation. Bliver ETSI's generaldirektør gjort opmærksom herpå, skal han straks anmode rettighedshaveren om inden for 3 måneder at erklære, at denne er "prepared to grant irrevocable licences on fair, reasonable, and non-discriminatory terms and conditions" i henseende til produktion, distribution, brug (herunder vedligeholdelse) og anvendelse mv., jf. nærmere pkt. 6.1. Afgives en sådan erklæring ikke, skal ETSI's generalforsamling overveje brugbare alternative teknologier, som opfylder ETSI's tekniske krav uden at kollidere med immaterialrettigheder. Reglerne er tilgængelige fra <www.etsi.org>.

Ser man imidlertid sagen fra immaterialrets-indehaverens synspunkt, kan det også føles urimeligt, at en teknologisk løs-

ningsmetode, som har været kostbar at udvikle, og som samtidigt har så betydelige økonomiske nyttevirkninger for brugeren, skal ophøjes til standard og dermed falde i almenhedens ejendom ("public domain") med det resultat, at den præsterede investering reelt er tabt. ETSI-reglerne er landet på en kompromis-løsning, der indebærer, at de pågældende standarder stilles til rådighed – sædvanligvis mod betaling – under en mild form for tvang udfoldet mellem ETSI-partnerne.

ETSI's standardiseringspolitik kan siges at angå det problem, der opstår, når en vedtagen – *de jure* – standard er eller bliver genstand for en industriel eneret. At dette grænseområde volder problemer skyldes patenteringsprocessen: På det tidspunkt, hvor en standard *diskuteres* af et standardiseringsorgan med henblik på eventuel senere *vedtagelse*, kan det tænkes, at en producent, der deltager i standardiseringsarbejdet, netop planlægger at søge patentbeskyttelse på det princip (f.eks. en metode til at komprimere data under anvendelse af en bestemt protokol), som standarden vil omfatte. Men da akterne i patentsagen først bliver offentligt tilgængelige 18 måneder efter ansøgningstidspunktet (inden for hvilket tidspunkt ansøgningen må betragtes som virksomhedens erhvervshemmelighed), vil producenten ikke ønske at få disse oplysninger ud i standardiseringsforhandlingerne, som netop udføres i et samvirke mellem virksomheden og dens konkurrenter!

At ETSI-politikken har givet anledning til en så forholdsvis omfattende debat skyldes, at de jure-standarder ofte er i public domain (ganske som lovgivning og anden officiel information er det). Derimod er det den almindelige opfattelse, at private virksomheders eneretsstandarder netop kan holdes i ejerskab, idet sådanne standarder til gengæld ikke blåstemples som officielle, f.eks. i forbindelse med offentlige myndigheders indkøb.

Supplerende litteratur

IT-rettens *retskildelære* er i litteraturen primært behandlet i relation til konkrete problemstillinger. En god oversigt over selvreguleringens problemer findes i *Åke Nilson*s korte oversigtsartikel History – Is Self-Regulation a New Concept?, trykt i 6 The EDI Law Review 183 ff. (2000).

Det europæiske *standardiseringsområde* belyses gennem DG XIII-publikationen Standardisering inden for informationsteknologi og telekommunikation (1988) og i EU-Kommissionens grønbog om standardisering, KOM(90) 456. Se også *Rudolf Skantz*: Standardiseringsarbeidet i EU og EFTA-landene (trykt i Complex 5/91, s. 199 ff.), *Georges Ferné* i

6 CLSR (March-April 1991), s. 2 ff. og *Florence Nicolas*: Fælles standarder for erhvervslivet (Kommissionen, 1992). Visse EU-retlige sider af standardiseringsarbejdet behandles af *Elisabeth Thuesen* i Julebog fra Juridisk Institut ved Handelshøjskolen i København 1999, s. 109 ff.

De *parlamentariske aspekter* af standardiseringsarbejde er behandlet i *Robert G. Dixon, Jr.*: Standards development in the private sector – thoughts on interest representation and procedural fairness. Boston (1978). Herudover kan henvises til *Florence Nicolas & Jacques Repussard*: Fælles standarder for erhvervslivet. Udgivet af Europakommissionen (Luxembourg, 1994), samt den omfattende redegørelse hos *Harm Schepel & Joseph Falke*: Legal aspects of standardisation in the Member States of the EC and EFTA, vol. I – III (Luxembourg, 2000).

De retlige aspekter af selvregulering har hidtil kun givet anledning til sporadisk interesse i litteraturen. Se herved *Jean-Francois Leronge* i 8 EDI Law Review 1997 (2002). Se dernæst om brancheselvregulering *Sten Bønsing*: Brancheregler og brancheproces (2001).

Kapitel 6. IT-OPHAVSRET

6.1. Almindelig indføring

6.1.a. Materiel og immateriel retsbeskyttelse

Behovet

Hvad enten der er tale om programmer og data på en diskette eller om topografien i en chip, kan digital information genskabes til perfektion for omkostninger, der udgør et fragment af udviklingsomkostningerne. Stod en sådan kopiering åben for alle, kunne andre konkurrenter på markedet spare de udviklingsomkostninger, producenten havde afholdt for at nå frem til komponenten. Til gengæld ville der næppe være mange, der så ville investere i teknologisk udvikling. Derfor hersker der en almindelig udbredt enighed om, at teknologisk innovation bør nyde en eller anden form for beskyttelse mod kopiering, omend der ofte er uenighed om, hvad man nærmere bør beskytte og hvordan.

På det globale plan har U-lande som regel større interesse i frit at kunne benytte nye teknologier end I-lande (sml. debatten om pirateri mv.), ligesom de mere dominerende markedsaktører har større interesse heri end mindre (sml. debatten om reverse engineering). I de enkelte lande vil der typisk bestå en interessemodsætning mellem udviklere, producenter og brugere, se mine indlæg herom i Bilagshæftet til rapporten om Info-Samfundet år 2000 (1994), s. 113 ff. og i Vennebog til Mogens Koktvedgaard (1993), s. 402 ff. Se for et amerikansk perspektiv *Arthur R. Miller* i 106 Harvard Law Review 982 ff. (1993) og *OTA* i den store udredning "Intellectual Property Rights in an age of Electronics and Information (april 1986).

Funktion

Den immaterialretlige lovgivning giver *nogen* (den, der har udviklet ny teknologisk information eller den, der har erhvervet rettighederne hertil) eneret til at forbyde *andre* at kopiere, sprede eller udnytte denne information, alt inden for rammerne af de enkelte eneretsregler: Hvad der beskyttes, og mod hvad, afhænger af det enkelte immaterialretlige lovsystem. Hvor der ingen sådan hjemmel findes er det udgangspunktet, at information er fri (i "*public domain*"). I så fald kan alle frit genskabe og udnytte informationen uden retlige begrænsninger. Dette udgangspunkt om informationens frihed gælder også inden for andre områder af

den informationsretlige lovgivning: Fandtes der ingen lovgivning om personregistrering eller om beskyttelse af privatlivets fred, ville registrering og udnyttelse af personoplysninger som udgangspunkt frit kunne ske. Immaterialretten frembyder det mest gennemarbejdede regelkompleks, hvor hensynet til rettighedshaverens "ejendomsret" er afstemt med hensynet til almenhedens krav på informationsanvendelse. Retsområdet bygger på århundredgamle begreber og grundsætninger og har været genstand for en stadig modernisering.

Virkemåde

Som dermed antydet knytter de immaterialretlige eneretssystemer an til forskellige typer af informationsfrembringelser. Ser man på IT-anvendelsen er det dermed også vidt forskellige *komponenter* og *lovmæssigheder* i et IT-system, der kan tænkes underlagt en sådan beskyttelse. Variationerne gør sig gældende, såvel i henseende til hvad det er for et *aspekt*, der beskyttes, som i henseende til *hvor specifikt* beskyttelsen gælder. Visse eneretsregler (ophavsretten, reglerne i halvlederloven) beskytter f.eks. kun den *konkrete manifestation* og kun denne. Andre (f.eks. patentloven, brugsmodelloven og reglerne i markedsføringsloven om erhvervshemmeligheder) beskytter også mere generelle *løsningsprincipper og idégrundlag*, der først skal implementeres for at kunne udnyttes. Afgrænsningen af, hvad det er for aspekter af teknologien, der retsbeskyttes, og afklaringen af beskyttelsens indhold, frembyder et faktisk og juridisk beskrivelsesproblem, der navnlig opstår i forbindelse med den ophavsretlige beskyttelse.

Formålet med de følgende kapitler er at fremstille de særlige problemer, der opstår i forbindelse med retsbeskyttelse af IT. Kapitlerne kan læses uden forudgående kendskab til immaterialretten, men det vil i sagens natur øge forståelsen, hvis man har et sådant kendskab. Bortset fra en kort historisk og konventionsretlig introduktion giver kapitlet kun et fragmentarisk billede af de pågældende regler, nemlig kun i henseende til de dele deraf, der har IT-retlig relevans. Læsere, der ønsker et bredere kendskab til immaterialrettens regler, henvises til de almindelige immaterialretlige fremstillinger, navnlig *Koktvedgaard*: Lærebog i immaterialret, 7. udg. (2005).

6.1.b. IT-immaterialrettens historie

Problemstillingen

Det fremgik af den teknologihistoriske gennemgang i afsnit 1.2, at moderne IT er skabt i kølvandet på den elektroniske computer, transistoren og halvlederteknologien. I teknologiens første år

voldte det ikke vanskeligheder at beskytte disse basale teknologier. Man anvendte *patentrettens* regler, eftersom der var tale om videreudviklinger af traditionelle ingeniørdiscipliner inden for svagstrømselektronik, materialeteknologi mv., der altid har været faste kunder i patentsystemet. Men i takt med programsidens stigende betydning for systemernes funktionalitet blev der behov for en selvstændig beskyttelse af programsiden. Med halvlederteknologiens indtog (som det væsentligste medium for såvel lagrings- som beregningsfunktioner) opstod ligeledes et behov for at beskytte disse komponenter i deres konkrete udformninger. Og med globaliseringen af IT-området er disse spørgsmål i stigende grad kommet på dagsordenen for internationale handelspolitiske drøftelser, bl.a. inden for WTO.

Programbeskyttelsen

I slutningen af 1970'erne opstod en principiel diskussion om, hvorvidt programsiden skulle beskyttes efter reglerne om patent eller ophavsret, eller om man skulle indføre en helt ny rettighedstype. 1970'ernes teknologiudvikling havde skabt et marked for programmel, der hverken var udviklet af maskinleverandøren eller brugeren. Kunden kunne nu købe hardware hos én leverandør og programmer hos en anden eller ligefrem kopiere de programmer, han havde brug for, uden rettighedshaverens mellemkomst.

Sui generis-beskyttelse?

Valget stod dengang mellem ophavsretten, patentretten eller et særligt *sui generis* beskyttelsessystem. WIPO, der er det særlige agentur under FN, der bl.a. administrerer Bernerkonventionen, anbefalede i 1978 indførelsen af et sui generis regelsæt til beskyttelse af programmel, se disse "Model provisions on the protection of computer software" i betænkning 1064/1986, s. 100 f. Men som det ofte sker, tog den nødvendige politiske proces for lang tid. IT-industrien kunne ikke vente på politikerne. Et par år inden WIPO's modellovbestemmelser forelå, havde et regeringsudvalg under den amerikanske kongres, *CONTU* (Commission on New Technological Uses of Copyrighted Works), taget spørgsmålet under behandling. Dette førte til et forslag, der blev indført i amerikansk ophavsret i 1980, hvorefter programmer blev beskyttet efter reglerne i *Copyright Act*. Dette valg af beskyttelsesform har siden stået fast.

I dag er alle enige om, at programbeskyttelsen primært skal baseres på det *ophavsretlige* system, der er etableret med Bernerkonventionen. Nyere praksis – navnlig fra USA – synes dog at åbne op for en stadig videre adgang til at *patentere* programrelaterede opfindelser; men hvor en sådan patenteringsadgang foreligger, er der ikke tale om et enten-eller, men om et både-og, idet de to beskyttelsessystemer dækker hver sit aspekt af programmet

(den konkrete udformning som et ophavsretligt beskyttet *værk*, henholdsvis den i programmet anvendte innovative løsningsmetode som en patenterbar *opfindelse*). Denne ramme er ikke alene lagt i amerikansk ophavsret og i EU's direktiv om retlig beskyttelse af edb-programmer (91/250/EØF), men tillige i WTO-aftalerne og senest WIPO's traktat om ophavsret fra 1996, jf. nærmere nedenfor.

Dette fundamentale udgangspunkt betyder bl.a., at programmernes retsbeskyttelse følger af et eksisterende, internationalt beskyttelsessystem, der har rod i to verdensomspændende konventioner:

Bernerkonventionen

Bernerkonventionen til værn for litterære og kunstneriske værker (af 9. september 1886, som revideret i Paris den 24. juli 1971) opstiller et princip om national behandling: Medlemsstaterne skal behandle værker skabt af deres egne statsborgere på samme måde som værker skabt af udlændinge, se konventionens art. 5. Udenlandske værker, der sælges og markedsføres i Danmark, omfattes således af dansk ophavsret bl.a. i henseende til kravet om værkshøjde. Et værk, der ikke nyder beskyttelse i Tyskland, kan derfor godt tænkes at være beskyttet efter dansk ophavsret. Se nærmere herom Kulturministeriets anordning nr. 964 af 12. december 1995. Dernæst pålægger Bernerkonventionen unionslandene at yde visse minimumsrettigheder. Pligten gælder principielt kun i forhold til ophavsmænd fra andre medlemslande, men den vil i praksis også få virkning for medlemslandets egne ophavsmænd. Beskyttelsestiden skal være på mindst 50 år regnet fra ophavsmandens dødsår (art. 7, stk. 1). Herudover skal ophavsmandens personlige rettigheder sikres (art. 6 bis). Endelig forbydes medlemslandene at lade beskyttelsen bero på opfyldelse af formaliteter som f.eks. registrering (art. 5, stk. 2).

Ligesom Bernerkonventionen bygger 1952-Verdenskonventionen om ophavsret på princippet om national behandling samt om visse minimumsrettigheder. Da konventionen i mange henseender ikke påtvinger en ligeså stærk beskyttelse, som Bernerkonventionen gør, havde den i mange år en langt bredere tilslutning, herunder fra lande i den tredje verden. Dens praktiske betydning er stort set forsvundet, efter at de store lande, USA og Rusland, har tiltrådt Bernerkonventionen. Se i øvrigt den historiske oversigt over immaterialrettens udvikling hos *Jens Schovsbo* i NIR 1998.470 ff.

WIPO Copyright Treaty

I december 1996 vedtog WIPO en ny traktat om ophavsret – the WIPO Copyright Treaty. Danmark er ikke part i denne traktat, som er behandlet og ratificeret af EU-kommissionen, se hertil EFT

2000 L 89/09. Som før nævnt bekræfter traktaten bl.a., at edb-programmer skal beskyttes som litterære værker i medfør af reglerne i Bernerkonventionen (art. 4), og at den ophavsretlige beskyttelse ikke omfatter idéer, procedurer samt fremgangsmåder eller matematiske begreber som sådanne. Om databaser hedder det kort, at "compilation of data or other material, in any form, which by reason of the selection or arrangement of their contents constitute intellectual creations, are protected as such", idet det i tillæg hertil hedder, at denne beskyttelse ikke omfatter "the data or the material itself", ligesom den ikke berører den ophavsretlige beskyttelse for de værker, databasen består af. Til traktaten hører et såkaldt Agreed Statement, der bl.a. berører nogle af de mere følsomme spørgsmål, herunder om den digitale reproduktion af programmer og digitale værker, der indgår som en nødvendig del af IT-anvendelsen, indebærer eksemplarfremstilling. Se nærmere om forhandlingerne *Henry Olsson* i NIR 1997.107 ff. og *Thomas Vinje* i NIR 1997.207 ff.

6.1.c. International påvirkning

Med den internationale handel med retsbeskyttede produkter har immaterialretten fået en uomgængelig international dimension. Navnlig har amerikanske retsstrømninger betydning for, hvordan vi i Europa indretter vor lovgivning, ligesom amerikansk praksis smitter af på aftalepraksis. Denne kontakt har allerede vist sig legislativt i relation til problematikken om lønmodtageres ophavsret, jf. nu ophl. § 59, men præger tillige den EU-retlige lovgivningsproces, der fremover må forventes at blive den primære IT-ophavsretlige retskilde. Også WIPO's Copyright Treaty fra 1996 kan anskues som en kombination af begge systemer.

Ved studiet af fremmede ophavsretlige systemer må man sondre mellem to traditioner: Den anglo-amerikanske "copyright"-tradition og den kontinentaleuropæiske "author's right"-tradition.

Author's right

Efter *kontinentaleuropæisk* ophavsret, hvortil bl.a. nordisk ophavsret hører, anskues ophavsretten som en personlig ret, hvis eksistens tilskrives visse kreative handlinger, som et menneske har foretaget. Derfor betragtes ophavsretten altid som opstået hos forfatteren, kunstneren eller den, der i øvrigt har frembragt det pågældende værk. Af samme grund betegnes disse kontinentaleuropæiske systemer som *"author's right"*-systemer. "The author" er hovedpersonen. Han er altid den originære (dvs. oprindelige) ophavsmand, uanset om han ved aftale eller i kraft af lovgiv-

ning har afstået sit værk til andre. Selv om man ikke kan tale om "authors" i relation til opfindelser og frembringelser, der beskyttes som patenter eller brugsmodeller, bygger disse regelsystemer ligeledes på forestillingen om frembringeren som indehaver af retten, se hertil § 3 i lov om arbejdstageres opfindelser. Art. 4 c i Pariserkonventionen af 1883 om beskyttelse af industriel ejendomsret fastslår ligeledes opfinderens ret til at blive nævnt som sådan i patentbrevet, jf. PL § 8, stk. 4.

Copyright

Anglo-amerikansk ophavsret bygger derimod på ophavsretten som noget, retssystemet tilstår rettighedshaveren. Ophavsretten er her udviklet i forlængelse af tidligere tiders privilegiesystemer, jf. nærmere herom *Schmidt* (1989), s. 19 ff. Den, der besad et sådant privilegium (typisk et forlagshus), havde eneretten til at kopiere det eller de værker, som privilegiet dækkede. Af samme grund betegnes eneretten i disse systemer som *"copyright"*-systemer. Ophavsretten ses her primært som en eneret til at kopiere, som retssystemet tildeler "nogen" – primært værkets frembringer, men i mange tilfælde også den virksomhed, hos hvem frembringeren er ansat.

Forskelle

Forskellen mellem de to retstraditioner træder frem både i selve lovreguleringen og i den teoretiske systematisering af ophavsretlige spørgsmål. For det første antager kontinentaleuropæisk ophavsret, at ophavsrettigheder kun kan opstå *originært* hos mennesker. I det omfang en juridisk person har en ophavsret, vil dette altid være i kraft af en rettighedsovergang. For det andet hører de personlige rettigheder (*droit moral* og paternitetsretten, jf. herom senere) ikke naturligt hjemme i de anglo-amerikanske ophavsretssystemer – et forhold, der i sin tid var med til at hindre USA's tilslutning til Bernerkonventionen. Endelig afspejles forskellen i den ophavsretlige tænkning. Fremstillinger af amerikansk IT-ophavsret er i højere grad koncentreret om den enkelte værkstype, hvor den kontinentaleuropæiske tradition tager udgangspunkt i den proces, hvorved det færdige værk skabes. For en anglo-amerikansk betragtning er "*what's worth copying, worth protecting*". For en kontinentaleuropæisk tanke skal retten stedse afspejle den personlighed, ophavsmanden har lagt i sit værk.

Denne "Sweat of the brow"-doktrin er dog mærkbart nedtonet med Supreme Court's dom i *Feist Publications, Inc., v. Rural Telephone Service Company, Inc.*, 499 U.S. 340 (1991), hvor retten bl.a. udtalte, at "copyright rewards originality, not effort". Sagen ville falde anderledes ud, hvis de pågældende data var sammensat ud fra en selvstændig vurdering. Dette var f.eks. tilfældet i *CCC Information Services, Inc. v. Maclean Hunter Market Reports et al.*, 44 F.3d 61 (2nd

Cir., 1994), der handlede om en database over brugte biler med angivelse af den enkelte bils værdi i forskellige geografiske områder. Da basen dermed var udtryk for frembringerens professionelle ekspertise og originalitet nød den ophavsretlig beskyttelse.

Selvom der er megen inspiration at hente i den ganske fyldige amerikanske retspraksis på IT-ophavsrettens område, må en sådan retssammenligning altså ske med lempe. Dels præges amerikansk ret generelt af synspunkter, der må forekomme fremmedartede for vor egen tænkemåde. Dels suppleres amerikansk ophavsret med andre alternative beskyttelsessystemer end dansk: På den ene side er konkurrencebeskyttelsen (jf. for dansk ret mfl. § 1) svag i USA; beskyttelsen knyttes primært til hemmeligholdelse. På den anden side er patentsystemet – selv på softwareområdet – formentlig langt stærkere, jf. nærmere nedenfor i afsnit 10.1. Retsstillingen på sådanne naboområder kan ikke undgå at præge den ophavsretlige retsanvendelse.

WTO

I konsekvens af GATT-samarbejdets udvidelse fra de klassiske varekategorier og over mod tjenesteydelsesområdet har man ved den seneste revision pålagt medlemsstaterne at håndhæve de centrale immaterialrettigheder. Reglerne herom findes i den såkaldte TRIPS-protokol (TRIPS = Trade Related Intellectual Property RightS), der bl.a. foreskriver beskyttelse af edb-programmer og databaser. Det fastslås bl.a. heri, at der ikke skal være beskyttelse af "methods of operation" i edb-programmel.

EU

Den største påvirkning af den moderne immaterialret kommer imidlertid fra EU. EU-kommissionen tog sit første immaterialretlige initiativ på IT-området i 1989 med sin Grønbog om ophavsret og den teknologiske udfordring, som suppleredes med en opfølgningsgrønbog af 20. november 1996 (KOM(1996) 568 endelig udg.). På IT-området har EU allerede gennemført tre væsentlige beskyttelsesdirektiver, nemlig 1986-direktivet om beskyttelse af halvlederprodukter, 1991-direktivet om beskyttelse af edb-programmer og 1996-direktivet om beskyttelse af databaser. Foruden disse direktiver har en række almene direktiver betydning for IT-immaterialretten, herunder de ophavsretlige direktiver om udlån og udlejning af ophavsretligt beskyttede værker samt direktivet om beskyttelsestidens længde.

INFOSOC-direktivet

Senest er det såkaldte INFOSOC-direktiv (Europa-parlamentets og Rådets direktiv om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet) blevet vedtaget (2001/29/EF), se om direktivet og dets forhistorie *Martin Kyst* i U2001B.305 ff. Direktivet havde haft en lang og besværlig gang, idet en række af de vanskelige retlige afgræns-

ningsspørgsmål – herunder om, hvornår en flygtig digital kopi er et eksemplar i ophavsretlig forstand – gav anledning til betydelig principiel enighed. Det blev i sin tid foreslået af Kommissionen den 10. december 1997 (KOM(97) 629) i opfølgning af WIPO-traktaterne fra december 1996. Det er nu indført i dansk ret lov ved lov nr. 1015 af 17. december 2002 om ændring af ophavsretsloven.

Praktiske konsekvenser

EU-reguleringen betyder bl.a., at de berørte dele af dansk ret skal tillægges en EU-retlig fortolkning. I konkrete sager vil der endvidere kunne ske (og i Højesteret, *skal* der ske) præjudiciel forelæggelse for EF-domstolen af spørgsmål, der angår fortolkningen af de bagved liggende direktiver mv., se TEF art. 234 og *Bryde Andersen og Rasmussen* i EU-ret & Menneskeret 1997.207 ff. De omkostninger, en sådan forelæggelse er forbundet med, målt i tid og penge, var stærkt medvirkende til, at en større sag om beskyttelse af edb-programmer og om programmers overgang i ansættelsesforhold blev forligt under sagsførelsen ved Højesteret, se afsnit 7.2.a.

6.1.d. De modstående hensyn

De immaterialretlige regler tilgodeser både rettighedshaveren og samfundet. Samfundet får glæde af de beskyttede frembringelser, og rettighedshaverne kan få økonomisk udkomme af den eneret, beskyttelsen indebærer, og som samtidig inciterer til at udvikle og udnytte ny teknologi mv. Det er imidlertid langt fra givet, hvilket balancepunkt man skal vælge. Isoleret set kan en immaterialret skabe et begrænset monopol, der som sådant afskærer konkurrence med heraf følgende risiko for højere priser, færre udbydere og forbrugsmuligheder og ringere kvalitet. Set fra et synspunkt om informationsfrihed kan enerettigheder hæmme den frie udveksling af informationer: Ophavsrettigheder til information, der flyder på Internet, kan således ses som en slags begrænsning i ytringsfriheden. Enerettigheder til teknologisk information (patenterede opfindelser mv.) kan dernæst ses i et Nord-Syd-perspektiv som den rige verdens monopolisering af teknologi og *knowhow* til skade for den fattige. Når der opstår uklarhed om ophavsrettens indhold, må disse hensyn afbalanceres overfor de modstående hensyn til ophavsmanden. Det gælder ikke blot i den retspolitiske proces, men efter omstændighederne også ved fortolkningen af de enkelte regler. Se for en nærmere drøftelse af dette spørgsmål mit indlæg i Vennebog til Mogens Koktvedgaard (1993), s. 402 ff.

Det følger heraf, at enhver begrænsning i den frie ret til at kopiere og videreformidle information, må have hjemmel. En sådan hjemmel vil nemlig sikre, at den nødvendige afvejning mellem informationshensynet og hensynet til frembringeren er blevet foretaget. Denne afvejning fremstår klart, når man ser på ophavsretten til det skrevne eller talte ord. Udviklingen af den menneskelige civilisation beror i høj grad på, at vi har kunnet inspirere hinanden. En konsekvent gennemført tanke om, at enhver tanke eller ethvert udsagn skulle "tilhøre" deres frembringer, ville medføre helt ulidelige konsekvenser.

Hensynet til informationsforbrugeren bæres af grundlæggende forestillinger om personlig frihed og udfoldelse. Retten til at modtage information er f.eks. så indlysende, at modtageren ikke bør afkræves nogen særlig begrundelse for sit informationsønske. Det ville føles dybt uetisk, hvis bibliotekaren på et folkebibliotek aftvang sin låner en forklaring på, hvad hans egentlige motiv var til at låne en bestemt bog. Jeg har redegjort nærmere for dette princip i mit bidrag til bilagshæftet til rapporten om Info-samfundet år 2000 (1994), s. 127 ff. Som her anført gennemhulles udgangspunktet bl.a. ved reglerne i lovgivningen om persondatabeskyttelse, offentlighedsloven, arkivlovgivningen og immaterialretten, jf. om sidstnævnte retsområde straks nedenfor. Som ligeledes anført kan man argumentere økonomisk/rationelt for en regel om informationsfrihed: Kun hvis information spredes, bliver den brugt, og kun hvis den bliver brugt opnår den sin værdi for samfundet. Informationsfrihed er for så vidt en nødvendig ingrediens i et samfundssystem, der bygger på forestillinger om, at den optimale ressourceudnyttelse sker under markedsvilkår. Denne betragtning er genstand for *Thomas Riis*' afhandling om Ophavsret og Retsøkonomi (1996). Et vægtigt indlæg i debatten om informationsfrihed og ophavsret på nettet foreligger i øvrigt med *John Perry Barlow*s artikel i tidsskriftet WIRED 2.03 (March 1994), s. 84 ff., der senest – og med særligt sigte på en verserende amerikansk sag om de såkaldte *Napster*-tjenester – er fulgt op med et indlæg i WIRED 9.10 (October 2000), s. 240 ff.

Brugerhensynet

I nyere ophavsretlig retspolitik er brugerhensynet kommet til at spille en stigende rolle. Forklaringen herpå ligger hovedsagelig i, at "brugerne" ikke længere optræder i skikkelse af den svage forbruger, men i stigende grad som professionelt virkende aktører, der enten optræder i kraft af et branchemæssigt tilhørsforhold eller under dække af den industri, der forsyner dem med det udstyr, hvorfra de beskyttede værker anvendes. Den retspolitiske betydning af disse interesser trådte første gang frem under drøftelserne forud for 1991-direktivet om retlig beskyttelse af edb-programmer. Senere har den manifesteret sig i global sammenhæng under forhandlingerne forud for the WIPO Copyright Trea-

ty, der – i konsekvens heraf – i sin præambel udtrykkeligt påpeger nødvendigheden af at afbalancere "the Rights of authors and the larger public interests, particularly education, research and access to information, as reflected in the Berne Convention". Denne drøftelse er i øvrigt en væsentlig årsag til de vanskelige diskussioner, der førte til 2001-direktivet om ophavsret og beslægtede rettigheder i informationssamfundet.

En detaljeret interesseafvejning desangående bør som udgangspunkt ske i tilknytning til de konkrete retsproblemer, f.eks. i diskussionen om betingelserne for retsbeskyttelse, kopibegrebet etc. Der gør sig nemlig vidt forskellige hensyn gældende i relation til de enkelte rettighedstyper. Hvornår der bør anerkendes en eneret, kan således ikke isoleres fra spørgsmålet om, hvad denne ret nærmere skal indebære. Hvis den pågældende rettighedstype medfører beherskede eneretspositioner, svækkes de konkurrenceretlige argumenter for at være tilbageholdende med at tildele denne ret. Er eneretten omvendt stærk, kan der være grund til tilbageholdenhed. Vil man f.eks. i amerikansk ret beskytte programmets brugergrænseflade, skaber dette stærke konkurrencefordele for de producenter, hvis produkter bliver standard-sættende.

I nyere teori er dette skisma gjort til genstand for flere selvstændige undersøgelser. I sin disputats om Teknologi og immaterialret (1989) s. 69 ff., navnlig s. 71, argumenterer *Per Håkon Schmidt* ud fra hensynet til den frie konkurrence for et højt værkshøjdekrav (dvs. høje krav til programmets individualitet), idet han til gengæld vil gøre beskyttelsen "for dem, der kommer gennem nåleøjet," stærkere. Se tilsvarende *Schmidt* i Vennebog til Mogens Koktvedgaard (1993), s. 45. Synspunktet fører efter min opfattelse til uacceptable resultater, fordi det uvægerlig vil give risiko for monopoldannelser mv. Vil man argumentere for en almindelig skærpelse af kravene til programmers værkshøjde ud fra konkurrencehensynet, må dette forudsætte, at der er konkurrencerelevante kvaliteter knyttet til programmet. Dette har principielt intet at gøre med, hvilket individuelt præg programmets ophavsmand har sat på det. En bred beskyttelse for programmer, der præges af en høj individualitet, vil enten være uden betydning (nemlig hvis programmet ikke har noget marked), eller kunne føre til utålelige enerettigheder. Se i samme retning *Marianne Levin* i TfR 1990.219 og *Kristian E. Beyer* i Justitia, 1999, nr. 4, s. 83 f. *Thomas Riis* har i Ophavsret og Retsøkonomi (1996) analyseret en række ophavsretlige problemer i et retsøkonomisk perspektiv. Undersøgelsen konkluderer, at den retsøkonomiske metode næppe er velegnet til at beskrive gældende ophavsret, bl.a. fordi denne har andet end økonomiske begrundelser (s. 304). *Jens Schovsbo* har i Grænsefladespørgsmål mellem immaterialretten og konkurrenceretten

(1996) analyseret tre problemfelter inden for ophavsretten, varemærkeretten og mønsterretten med henblik på at afklare betydningen af konkurrencemæssige synspunkter inden for disse immaterialretlige retsområder.

6.1.e. Beskrivelsesproblemer

Uhåndterlige kopier

IT-immaterialretten frembyder talrige beskrivelsesproblemer. Foruden de, der skyldes teknologiens *immaterielle* beskaffenhed og tekniske kompleksitet, opstår der selv på det håndgribelige brugerniveau beskrivelsesproblemer i relation til de forskelligartede *funktioner*, programmerne udfører henholdsvis under udvikling og afvikling. De færreste IT-brugere har tankerne på de kopier mv., der undervejs udføres af programmet (f.eks. til RAM, buffere etc.). En yderligere vanskelighed ligger i, at de enkelte informationstyper kan være vanskelige at *afgrænse* fra hinanden. Når et "edb-program" – som i denne fremstilling – defineres som en serie koder til en processor, er det åbenbart, at en række af de værkselementer, der indgår i det produkt, man under betegnelsen "edb-program" sætter i sin PC, ikke er programmer, men f.eks. musik, levende billeder, manualer mv.

Information og medium

Et andet problem knytter sig til det samspil mellem informationen og medium, der foregår i IT-systemet. Under hidtidige informationsteknologier har det været nogenlunde indlysende, hvor informationen – og dermed "værket", "opfindelsen" etc. – befandt sig. Sådan er det ikke med den teknologiske information, der har betydning for moderne IT. Et program kan befinde sig på ethvert medium, der er indrettet til at kunne lagre digital information. For nogle af disse medier vil programkopien ikke efterlade sig spor (det gælder f.eks. disketter og harddisks), medens andre medier vil bære varigt præg af den pågældende information (det gælder f.eks. klassiske CD-ROM-skiver). For endnu andre medier gælder det, at selve mediet konstrueres således, at det netop er i stand til at håndtere en type information. Dette gælder således for de såkaldte halvlederprodukter.

Krydsende rettigheder

At den enkelte informationsmængde kan tænkes lagret efter så forskelligartede tekniske principper betyder bl.a., at der kan tænkes vidt forskellige typer af enerettigheder i relation til samme informationsbehandling. En halvlederchip kan i sig selv være beskyttet af reglerne i halvlederloven; men det enkelte halvlederprodukt kan være dækket af et patent eller en brugsmodelrettighed. Dertil kommer, at de programmer, der indbygges i halvlederproduktet, kan være beskyttet efter ophavsretlige regler. Hvis programmet dernæst styrer afviklingen af information, der er

understøttet af/undergivet særskilt beskyttelse (f.eks. musik, fotos eller levende billeder), vil også de hertil svarende beskyttelsessystemer kunne give hjemmel for retspositioner. Hertil kommer de retsvirkninger, der kan følge af indgåede aftaler, enten *inter partes* eller i kraft af retsregler (herunder navnlig mfl. § 10), der knytter retsvirkninger til visse aftaler (om hemmeligholdelse af erhvervshemmeligheder mv.).

Nye dimensioner

Et tredje problem opstår, når man som grundlag for IT-anvendelsen anvender medier – som f.eks. Internet – der i deres virkemåde får hidtidige grænser for, hvad der er muligt i tid og over afstande, til at forsvinde. Når en dansk bruger fra en PC kan kalde op til en amerikansk hjemmeside og høre musik, foretager han en udnyttelseshandling, som kan tænkes at udgøre en eksemplarfremstilling i Danmark og/eller en form for radioaflytning i USA. Musikken transmitteres gennem en række datapakker, der undervejs lagres for korte øjeblikke på de routere og servere, som nettet består af. Hvilke af disse lagringer mv., der har ophavsretlig betydning, er endnu ikke fuldt opklaret.

Man kan næppe generelt forvente den slags beskrivelsesproblemer løst af lovgiveren. Erfaringen synes at vise, at politiske debatter om højteknologisk lovgivning får en tendens til at løbe af sporet med skæbnesvangre konsekvenser for den efterfølgende retstilstand: Problemstillingen ser enkel ud på overskriftsniveau; men når diskussionen først bevæger sig nedefter i materien, fremstår en række komplekse sondringer og afvejninger, der har en tendens til at køre politikerne trætte. Det er ofte set, at lovforslag om ændringer, der fra begyndelsen fremstod som rent lovtekniske, undervejs i den politiske proces har forandret bane, således at der pludselig er kommet helt andre emner på dagsordenen. Forløbene omkring 1991-direktivet om ophavsretlig beskyttelse af edb-programmer og 1995-ophavsretsloven (særligt om bibliotekernes adgang til at foretage udlån af visse værker) er eksempler herpå. Andre, og måske mere slående, eksempler uden for IT-immaterialretten kan hentes fra lovgivningen om persondatabeskyttelse.

6.2. De beskyttede frembringelser

6.2.a. Ophavsretten i resumé

Retsfaktum

Ifølge ophl. § 1 har den, som frembringer et litterært eller kunstnerisk *værk*, ophavsret til værket, hvad enten dette fremtræder som en i skrift eller tale udtrykt skønlitterær eller faglitterær fremstilling, som musikværk eller sceneværk, som filmværk eller fotografisk værk, som værk af billedkunst, bygningskunst eller brugskunst, eller det er kommet til udtryk på anden måde. Uden værk, ingen ophavsret (jf. dog nedenfor om de særlige regler i lovens kapitel 5).

Retsfølge

Foreligger der et værk, fastslår § 2 retsfølgen af den ophavsretlige beskyttelse. Efter denne bestemmelse har ophavsmanden – med de i loven angivne undtagelser – *eneret* til at råde over værket "ved at fremstille eksemplarer af det og ved at gøre det tilgængeligt for almenheden, i oprindelig eller ændret skikkelse, i oversættelse, omarbejdet i anden litteratur- eller kunstart eller i anden teknik". Det er vigtigt at understrege, at der er tale om en *eneret*, som til gengæld kun gælder som udtrykkeligt anført: Ved fremstilling af *eksemplarer* af værket og ved at dette gøres *tilgængeligt for almenheden* på de i § 2, stk. 3, særligt specificerede måder, jf. nærmere afsnit 6.3.c. En udnyttelseshandling, der *ikke* har denne karakter (f.eks. at brugeren har *nytte* af en databehandling udført via et edb-program eller *inspireres* af et litterært værk) rammes derfor ikke af den ophavsretlige beskyttelse, hvis ikke den også indebærer en eksemplarfremstilling eller spredning.

Begrænsninger

På grund af denne slagkraft er ophavsretsloven forsynet med en række undtagelser, der tilsigter at afbalancere rettighedshaverens interesser med brugernes. Om disse gælder det generelt, at de indtræder, når ophavsmanden i en eller anden form har lagt sit værk frem for almenheden. Den, der ønsker en fuld og uindskrænket sikkerhed mod nogen form for uhjemlet udnyttelse af et ophavsbeskyttet litterært værk, bør derfor holde det for sig selv! Men når han "spreder" det til almenheden (f.eks. gennem udgivelse eller overdragelse af eksemplarer), kommer hans interesse i at opretholde en total eneret på kollisionskurs med samfundets interesse i at videreudvikle og dermed genanvende information. Ophavsretten bygger på den tanke, at det offentliggjorte værk bør være en *åndelig impuls*, som ophavsmanden ikke bør have herredømme over, og at visse handlinger, som det vil være vanskeligt at håndhæve i *privatsfæren*, ikke bør være omfattet af eneretten.

Disse modifikationer findes i ophl. kapitel 2, hvis regler om brugerens ret til at fremstille reserve- og sikkerhedskopier mv., jf. § 36, stk. 1, nr. 2, omtales i afsnit 7.4.b. Hertil føjer sig § 12 stk. 2, nr. 3-5, der afskærer kopiering til privat brug af edb-programmer og databaser i digital form og enkelte eksemplarer af andre værker i digital form, medmindre dette udelukkende sker til personlig brug for fremstilleren eller dennes husstand, jf. nærmere herom i afsnit 6.4.a. Foruden de justeringer, lovgiveren har lagt ind i loven, vil der løbende være et behov for, at også domstolene foretager tilpasninger. I det omfang, der ikke findes sådanne undtagelser, er det op til parterne at tilvejebringe den fornødne balance i aftaledannelsen, se nærmere herom nedenfor i afsnit 7.4.e.

Andre beskyttede handlinger?

Principielt var der intet til hinder for, at ophavsretten knyttede an til andre udnyttelsesformer. Når loven knytter an til eksemplarfremstilling og spredning, skyldes det dels de økonomiske aspekter, der ligger heri, dels det praktiske forhold, at udnyttelsen er let at bevise og dermed håndterlig i retsanvendelsen. Det store marked for ophavsretligt beskyttede produkter (musikværker, programmer etc.) eksisterer netop i kraft af eksemplarfremstillinger og overdragelser mv. Ved affattelsen af den særlige beskyttelse af databaser, der er hjemlet i ophl. § 71, stk. 2, har man således ladet andre udnyttelsesformer være afgørende for beskyttelsen.

Ideelle rettigheder

Som nævnt ovenfor anskuer de kontinentaleuropæiske ophavsretlige systemer, hvortil dansk ophavsret hører, ophavsretten som en personlig ret, hvortil der ikke alene er knyttet enerettigheder af økonomisk art, men også visse ideelle rettigheder. De personlige rettigheder hjemles ved ophl. § 3, der fastslår frembringerens *droit moral* og *droit de paternité*, jf. nærmere afsnit 6.3.h. Hvor de ideelle rettigheder kendetegnes ved at være uoverdragelige og stedsevarende og dermed nært knyttet til skaberen og hans personlighed, viser de økonomiske rettigheder sig ved ophavsmandens eneret til at råde over værket. Enhver, der ønsker at udnytte værket ved f.eks. at fremstille eksemplarer af det, må have ophavsmandens samtykke hertil. Den økonomiske dimension fremkommer ved, at dette samtykke kan gives mod betaling.

6.2.b. Det ophavsretlige værksbegreb

Funktion

Når man benytter udtrykket "værk" om en intellektuel frembringelse, har man dermed allerede konstateret, at der er tale om en frembringelse, der kan nyde ophavsretlig beskyttelse. Strengt taget er dette dog ikke ensbetydende med, at der også gælder en eneret: Beskyttelsen kan således være ophørt, fordi ophavsretstiden er udløbet (som det f.eks. gælder for det *Mona Lisa*-ikon, der

anvendes som cursor i visse brugergrænseflader), at ophavsmanden klart har markeret, at han ikke agter at gøre sin ophavsret gældende (som det gælder for rettighederne til det såkaldte LINUX-programmel), at værket er skabt i et land, som Danmark ikke har overenskomst med (og som vi derfor heller ikke har pligt til at beskytte efter ophavsretslovens regler), eller at man befinder sig inden for en af ophavsrettens talrige undtagelsesregler.

Et "værk" er i bred forstand resultatet af en *menneskelig* frembringelsesindsats inden for de ophavsretlige hovedområder kunst og litteratur. Hvis man betragter ethvert menneskeligt udtryk som båret af et sprog (jf. nærmere indføringen i den matematiske kommunikationsteori i afsnit 2.2.b.), kan man omformulere ophl. § 1 således: "Den, som *manifesterer* en *informationsmængde* ved hjælp af *litteratursproget eller et kunstnerisk sprog*, har ophavsret til *denne information* (hvis den er tilstrækkeligt original), hvad enten manifestationen fremtræder som en *i skriftmedier eller talte medier* udtrykt skønlitterær eller faglitterær fremstilling ... eller den er kommet til udtryk *ved brug af andre medier*". Se nærmere om denne betragtning min afhandling i NIR 1995.616 ff. Denne omformulering anskueliggør, at der ingen begrænsninger er i, hvilke *medier* der kan tænkes at manifestere et kunstnerisk eller litterært værk, og at der heller ingen begrænsninger gælder i relation til de *udtryksformer*, gennem hvilke værket får sit særpræg. For så vidt er det ikke overraskende, at også frembringelser, der har skikkelse af edb-programmer, HTML-opmarkeringer eller hjemmesidedesign kan udgøre ophavsretlige værker, jf. i øvrigt ophl. § 1, stk. 3.

Idé-grundlag

Det er dog ikke enhver original menneskelig frembringelse, der kvalificerer som ophavsretligt værk. I ophavsretten plejer man at lægge en grænse mod de mere generelle tankemæssige frembringelser og antage, at selve den idé, der beskriver, hvordan disse instruktioner skal udføres og hvilket resultat, de skal udvirke, ikke kan begrunde en ophavsretlig beskyttelse. Svaret herpå er klart, og det beror ikke på, at der er tale om edb-programmer: Det er det konkrete *udtryk* – i modsætning til den abstrakte *idé* – der beskyttes. En klassisk illustration af denne tanke er, at maler NN får ophavsret til *sit* maleri af solnedgangen over Vesterhavet, men at denne ret ikke afskærer andre malere fra at få ophavsret til deres maleri over ganske samme tema.

Overført til IT kan *programmøren* altså få ophavsretlig beskyttelse til et program, der kan systematisere filer på en bestemt måde, men ikke på selve denne måde at systematisere filer på, ligesom *web-masteren* kan få ophavsret til sin tilrettelæggelse af

en hjemmeside efter et bestemt design-princip (hvor menustrukturen f.eks. lægges skråt henover skærmen), men ikke for brugen af selve dette princip ved konstruktion af hjemmesider. Beskyttelsen samler sig altså om en nærmere angiven type af manifestationer, der foreligger fra ophavsmandens hånd.

§ 101 (b) i den amerikanske *Copyright Act* formulerer dette således, at "copyright protection for an original work of authorship (in no case does) extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work", sml. den ledende amerikanske højesteretsdom fra 1879 i sagen *Baker v. Selden* (101 U.S. 99), der ikke gav ophavsretsbeskyttelse til et arkiveringssystem og den lignende afgørelse i *U 1960.237 Ø* om idéen til publikationen "Skatten". I art. 1, stk. 2, i Rådsdirektivet om retlig beskyttelse af programmer siges det udtrykkeligt, at idéer og principper, som ligger til grund for de enkelte elementer i et program, herunder sådanne idéer og principper, som ligger til grund for dets grænseflader, ikke nyder ophavsretlig beskyttelse efter direktivet. Se nærmere hertil *Morten Rosenmeier*: Værkslæren i ophavsretten (2001), s. 66 ff.

Afgrænsning

Sondringen mellem idé og udtryk udgør vel et håndfast slagord med en vis pædagogisk værdi. Men den giver intet svar på, hvad der kan beskyttes som ophavsretligt værk. Hertil kommer, at sondringen har forskellige implikationer inden for de forskellige værkskategorier: Visse værkstyper (f.eks. maleriet) er mere idébundne end andre (f.eks. den skønlitterære roman), forstået således at udmøntningen af en og samme idé levner et mindre spillerum for udfoldelsen af det kreative udtryk. I praksis vil sondringen mellem idé og udtryk bero på, hvor "smal" eller "bred" idéen, henholdsvis udtrykket, er. Den "manifestation", der på skrift formulerer plottet i en roman i forhold til den færdige roman, vil i én henseende have karakter af et idéindhold, samtidig med at den i en anden (nemlig som tekstmængde) må betragtes som et færdigt værk.

Denne tanke er på programområdet bl.a. udtrykt i den principielle afgørelse i sagen *Computer Associates v. Altai*, se herom nedenfor, med bemærkningen, at "each subroutine is itself a program, and thus, may be said to have its own "idea"." I NIR 1997.76 f. fastholder *Hanne Bender* sondringen mellem idé og udtryk som grundlag for en beskrivelse af brugergrænsefladens ophavsretlige beskyttelse. *Michael Plogell* (1996), s. 18 ff., foreslår en sondring mellem idé, koncept og udtryk. Mellemkategorien – koncept – kan alt efter omstændighederne beskrive de tilfælde, der giver grundlag for ophavs-

retlig eller patentretlig beskyttelse. Sondringen er velegnet til at beskrive de konkrete spørgsmål, der gør sig gældende og kan for så vidt være egnet til at kaste lys over de centrale problemstillinger i læren om retsbeskyttelse. Som antydet indeholder den imidlertid ikke i sig selv nogen retligt relevant skillelinje. Sondringen mellem idé og udtryk har også betydning ved afgørelsen af, hvorledes formater til tv-programmer beskyttes, sml. herved dommen i *U 1999.1762 ØLK*, der nægtede ophavsretlig beskyttelse af et tv-quiz-program, men anerkendte et fogedforbud baseret på mfl. § 1. Resultatet kritiseres af den procederende advokat (*Torben Steffensen*) i U2000B.196 ff. Spørgsmålet behandles af *Hanne Kirk Deichmann*: Programkoncepter. Ophavsret til tv-formater (2003). Et eksempel på den vanskelige grænse mellem idé og udtryk er dommen i *U 2002.1645 Ø*, der i overensstemmelse med en skønserklæring antog ophavsretlig beskyttelse for et "dispositionsforslag" til et kontorbyggeri. Forslaget indeholdt en generel beskrivelse af byggeriet med tilhørende tegninger, der viste en buet bygning med tre "fingre" mod en skov. Landsretten når til sin konklusion efter en "helhedsbedømmelse."

Metoder

Det er dermed også slået fast, at der ikke kan erhverves ophavsret til programmeringsmetoder eller almindelige principper for opbygning af databaser eller hjemmesider. En metode er i sig selv ikke noget værk, selv om den kan *præge* et værk. Metoden lever i og med ophavsmanden og kommer til udtryk i den måde, hvorpå han færdiggør sine enkelte værker. Ej heller kan man opnå ophavsret til en særlig model for programudvikling (f.eks. Yourdon, SYSKON el.lign.) eller til en særlig kombination af værktøjer, maskinmiljøer, styresystemer mv., uanset hvor original den pågældende kombination eller teknik måtte være. Enkelte modifikationer i dette udgangspunkt kan dog gøres efter reglerne om samleværker, se hertil under 6.2.e.

Grundlæggende samfundshensyn taler for dette resultat. Tænkte man sig f.eks., at *Charlie Parker* og *Dizzie Gillespie* havde ophavsret til *be-bop* musikken, havde dette kunnet blokere hele denne del af jazz-musikken langt ind i indeværende århundrede. Og knyttede man f.eks. ophavsret til nutidens former for struktureret programmering, ville dette føre til en uacceptabel centralisering og formentlig også retardering af den almindelige videreudvikling af teknologien. Ophavsret til sådanne stilformer mv. synes da heller ikke påberåbt i praksis. End ikke erfaringerne fra udlandet antyder noget ønske om at få eneret til forskellige program-"stilarter" gennem ophavsretten. Tværtimod kan der være en generel faglig interesse i at understøtte udviklingen af generelle programmørfærdigheder. For medarbejderne giver dette mulighed for at dygtiggøre sig på tværs af ansættelsessted og brancheskel. For arbejdsgiversiden vil sådanne færdigheder give større valgfrihed ved ansættelse af programmører.

Værkstyper

Selv om ophavsretten er blevet til med sigte på den klassiske kunst og litteratur, beskytter ophavsretten en bred vifte af forskellige værkstyper. Når det gælder de litterære værker er det eneste fællestræk, at værket er konstrueret ved hjælp af bogstaver og tegn ("littera" = tegn). Der er således intet til hinder for at betragte en *hjemmeside* eller en *e-mail* som et litterært værk (hvis det har den fornødne originalitet), jf. tilsvarende *Wagle & Ødegaard* (1997), s. 129. Når det gælder de kunstneriske værker er der principielt heller ingen begrænsninger i, hvilke frembringelser der kan beskyttes som sådanne – blot det kan konstateres, at der er tale om et kunstnerisk udtryk, der har den fornødne originalitet.

Dobbelt-frembringelser

Ophavsretten beskytter ikke mod dobbeltfrembringelser: Skulle det ske, at programmør A kom til at skrive et program, der var identisk med det, programmør B allerede havde skrevet, får begge programmører ophavsret. Sandsynligheden herfor er dog ikke stor, navnlig ikke, hvis man i overensstemmelse med det nedenfor anførte justerer originalitetskravet, så det netop knytter sig til, om der består en vis sandsynlighed for dobbeltfrembringelser. Men den teoretiske mulighed for en dobbeltfrembringelse kan give anledning til bevisproblemer ved håndhævelsen af retsbeskyttelsen, nemlig hvis en påstået krænker hævder at have udviklet det pågældende værk ved en af ophavsmanden uafhængig indsats, sml. straks nedenfor bl.a. om *U 1993.17 H*.

6.2.c. Originalitetskravet

Uanset om der er tale om programmel, anden litteratur eller brugskunst, opnås der kun ophavsretlig beskyttelse, hvis frembringelsen besidder den egenskab, der i nyere ophavsretlig teori og lovgivning udtrykkes med ordet *originalitet* og som i tidligere terminologi benævnes som ophavsretlig *værkshøjde*, jf. om denne begrebsjustering *Koktvedgaard* i Festskrift til Karnell (1999), s. 341 ff. Efter den almindelige antagelse, jf. *Koktvedgaard* (2005), s. 61 ff., betyder dette, at værket er frembragt ved ophavsmandens *personlige, skabende indsats*. Kravet kan vel ikke læses direkte af loven, og dets indhold og rækkevidde giver ofte anledning til tvivl. Men at det gælder, fremgår af hele ophavsretslovens tankegang om "værket" som noget "udtrykt". Dernæst finder man kravet i flere EU-direktiver på ophavsrettens område, se art. 1, stk. 3, i direktiv 91/250/EØF om edb-programmer og i direktiv 96/9/EF om retlig beskyttelse af databaser. De personlige rettigheder (krav om navngivning, modsættelse af krænkende an-

vendelse mv.) giver da også kun mening, hvis der er en "personlighed" i værket, som i givet fald krænkes. Se generelt om originalitetskravet *Rosenmeier* (2001), s. 89-117 (om edb-programmer navnlig s. 206 ff.) samt *Per Jonas Nordell* i NIR 2001.73 ff.

Maskinelle frembringelser

I kravet om originalitet underforstås, at værket skal være *menneskeskabt*. Der må altså kunne udpeges en ophavsmand bag det, uanset om denne har betjent sig af tekniske mekanismer under den skabende proces. Værkets "egenart" må kunne henføres til denne skabende person – eller kreds af skabende personer – og ikke blot være udslag af udefra kommende omstændigheder. Et program*værk* kan ganske enkelt ikke skabes af en processor, jf. afsnit 9.1. om frembringelser skabt ved IT.

Variationer

Kravene til originalitet varierer alt efter, hvilken type værk der er tale om. For traditionelle litterære værker inden for kunst og faglitteratur sættes det relativt lavt. Det volder således ingen tvivl at fastslå, at programmets dokumentation skal vurderes i overensstemmelse med de regler, der gælder for andre tekniske tekster mv., ligesom dets grafik og animation skal følge praksis for de pågældende litterære og kunstneriske værker.

- litteratur

Skeler man til de litterære værkers område, har domstolene undertiden antaget ganske beskedne krav til størrelsen af et værk for at opnå originalitet. I enkelte tilfælde er enkelte sætninger (i form af filmtitler mv.) anset som litterære værker, se til illustration *U 1951.725 H* ("Hvem ringer klokkerne for?"), der ganske vist er afsagt før 1961-ophavsretsloven, og *U 1966.676 Ø* ("Nabo til Nordpolen"), der næppe kan fastholdes. I nyere praksis synes kravene – med rette – at være skærpet. Se således *U 1983.630 Ø*, der dog ikke tog direkte stilling til, om sætningen "ud i det blå" kunne beskyttes ophavsretligt, *U 1986.272 SH*, der nægtede beskyttelse af "Lige på en studs" og senest *U 1998.1385 SH*, der afviste ophavsret til ordene "I von Scholtens Fodspor", der blev anvendt som slogan og varemærke. Se ligeledes *Koktvedgaard* (2005), s. 66, *Palle Bo Madsen* (1997), s. 38 f. og *Rosenmeier* (2001), s. 147 ff.

- programkode

Overføres denne tankegang til programområdet er det nærliggende at indlægge et krav om, at et program – uanset sit originale præg – må have *et vist omfang*, for at en ophavsretlig beskyttelse som selvstændigt *værk* kan komme på tale. Sådanne krav stilles imidlertid ikke. Det er ikke noget absolut krav, at et program skal have en vis størrelse for at være beskyttet. Men i praksis fører kravet om *originalitet* til, at der kræves et vist omfang. Inden for rammerne af et programmeringssprog kan det således være van-

skeligt at udvise den fornødne originalitet, hvis ikke man frembringer en vis mængde kode.

- brugskunst

Frembringelser, der hovedsagelig tjener funktionelle formål, må generelt opfylde skrappere krav om originalitet. Dette ses mest tydeligt i praksis om ophavsretlig beskyttelse af brugskunst, jf. *U 1981.946 H* om et bordstel og *U 1978.337 H* om en transformerstation. Som anført nedenfor kan sådanne betragtninger få betydning i relation til de aspekter af programmet, der har æstetisk art og retter sig mod brugeren, herunder i brugergrænsefladen.

Det har været foreslået, at de formalsprog, der anvendes ved edb-programmering, må betragtes som udtryk for samme begrænsning i det kreative spillerum som de funktionelle begrænsninger, der gælder ved design af brugskunst. En sådan betragtning vil indebære, at kravene til originalitet må skærpes i tilsvarende omfang. I sin disputats om Teknologi og immaterialret (1989), se navnlig s. 178 ff. og 209 ff., har *Per Håkon Schmidt* gjort dette synspunkt gældende. Synspunktet støttes på, at "edb-sproget" er mindre *nuanceret* end naturlige sprog (s. 210), og at programmets tiltænkte *funktion* gør det nødvendigt at foretage en egentlig kvalitetsvurdering af programmerne. Dermed "ligner" programmerne i højere grad brugskunsten end de litterære værker. Og netop på brugskunstens område "kræves noget særligt, hvis et generationslangt monopol skal indrømmes". Se ligeledes *Schmidt* i Vennebog til Mogens Koktvedgaard (1993), s. 39 ff., bl.a. med note 15, s. 45.

Schmidt sondrer imidlertid ikke mellem forskellige aspekter af frembringelsesprocessen, men forudsætter generelt, at et programværk er en i afgørende henseender prædetermineret proces, der ikke efterlader samme spektrum af valgmuligheder som frembringeren af et almindeligt litterært værk har. Det er imidlertid værd at understrege, at mulighederne for at være kreativ inden for rammerne af et formalsprog er mindst lige så store som inden for rammerne af et naturligt sprog. Hvor det naturlige sprog gør det muligt at fremkalde komplekse associationsformer gennem få ord og uforudsete virkemidler, forudsætter det formelle sprog ganske vist en dækningsgrad, der har nærmest matematisk præcision, men til gengæld betyder den kolossale kapacitet i moderne IT-systemer, at der sjældent gælder grænser for, "hvor meget" programmøren kan "sige" i en given sammenhæng, dvs. hvor mange kommandoer han kan placere i programværket. Selv om valget af den enkelte instruktion er mere begrænset for programværkernes vedkommende (ligesom valget af bogstaver jo også er begrænset for andre litterære værker), er muligheden for at overføre information helt den samme. Det er med andre ord repræsentations*formen* – ikke programstoffets potentielle infor-

mationsmængde og mulighederne for kreativitet – der adskiller programmer fra andre litterære værker. En god indføring i problemerne omkring kreativitet i programudvikling findes i øvrigt i *Anthony Lawrence Clapes*' bog: Software, copyright and competition – the "look and feel" of the law (New York, 1989).

Direktivet

Diskussionen er i hovedsagen afgjort ved programdirektivet (91/250/EØF). Ifølge dettes art. 1, stk. 3 – der dog ikke er implementeret gennem en specifik ændring af ophl. – kan man kun stille den betingelse for den ophavsretlige beskyttelse, at programmet "er originalt i den forstand, at det er ophavsmandens egen intellektuelle frembringelse". Direktivteksten præciserer udtrykkeligt, at der ikke gælder andre kriterier for, om et program er berettiget til beskyttelse. Dermed er det slået fast, at kravene til edb-programmers originalitet ikke skal vurderes i lyset af den strenge praksis, der gælder for brugskunst.

Tommelfingerregel

I praksis må dette originalitetskrav forstås således, at risikoen for *dobbeltfrembringelser* udgør en praktisk tommelfingerregel. Den "nedre" grænse går altså der, hvor den kreativitet, som A på forhånd kan udøve, er således afstukket, at A's frembringelse alt andet lige vil blive lig B's. Dette kriterium tager netop hensyn til interessen i at understøtte den almindelige konkurrence: Hver enkelt udvikler får ophavsret til sit eget program, medmindre andre udviklere må forventes at udvikle helt identiske programmer, hvorved programmet må siges at være i public domain. Se tilsvarende *Plogell* (1996), s. 22 ff. og muligvis *Schmidt* (1998), s. 35 f., *Rosenmeier* (2001), generelt s. 132 ff. og særligt om edb-programmer, s. 209 ff. og *Schønning* (2003), s. 145.

Tipsdommen

Dobbeltfrembringelseslæren synes anvendt i *U 1993.17 H*, der er den eneste afgørelse, Højesteret har truffet om programmers retsbeskyttelse. Sagen drejede sig om ophavsretten til såkaldte tipssystemer. Et tipssystem er en metode til at udfylde et større antal tipskuponer efter en systematik, der efter visse regler definerer eller minimerer en risiko. Selve "tipssystemet" er altså strengt taget ikke et edb-program; men i praksis afvikles disse systemer ved hjælp af edb-programmer, der udskriver tipskuponerne efter brugerens valg af hel- og halvgarderinger mv., og under sagens førelse synes der at have været enighed mellem parterne om, at man betragtede sagens genstand som edb-programmel. Den pågældende sag udsprang af en strid mellem forskellige leverandører af IT-baserede tipssystemer. En forhandler gjorde gældende, at en anden havde krænket hans ophavsret til tipssystemet "Data-tips". Denne anden bestred, at kravene til værkshøjde var opfyldt. Et udmeldt syn og skøn konstaterede, at de grundlæggende idéer og metoder ved konstruktion af tipssy-

stemer er så enkle, at der vil være stor sandsynlighed for, at to forskellige konstruktører, der har kendskab til disse idéer og metoder, uafhængigt af hinanden vil udvikle det samme system. Efter en konkret gennemgang af de fem tipssystemer, sagen angik, antog Sø- og Handelsretten og senere Højesteret, at disse fem systemer ikke nød ophavsretlig beskyttelse.

Af anden praksis kan nævnes en dom afsagt af Hovrätten för Västra Sverige i *NIR 1988.310*, der bl.a. angik et kalkuleringsprogram, hvis kildetekst fyldte 250 A4-sider, og som det havde taget 20 mandår at udvikle. Tingsrätten havde fastslået, at programmet havde karakter af et teknisk hjælpemiddel og dermed savnede et skabende element. Hovrätten lagde til grund, at programmer udgør tekniske hjælpemidler til ved brug af computerens ressourcer at nå et tilsigtet resultat, og at der "(v)id utarbetande av program av ej alltför enkel art torde (finnas) åtskilliga valmöjligheter ... för utformaren .... såväl en hög grad av kunskap och förmåga till logiskt tänkande som intuition för att på enklaste och effektivaste sätt nå fram till det bästa resultatet". Under hensyntagen til ophavsretslovens vide værksbegreb fandt Hovrätten, at programmer "under förutsättning att de är en produkt av ett inte obetydligt andligt skapande" udgør et ophavsretligt værk. I tidligere *tysk* praksis har man udviklet strengere værkshøjdekrav, der alene ville give ophavsret til et begrænset antal af de programmer, der er i omsætning, se herved Lærebog i edb-ret (1991), s. 200 f. Den hårdhændede tyske praksis var en væsentlig grund til, at EU-kommissionen med Rådsdirektivet om retlig beskyttelse af programmer tog initiativ til at harmonisere værkshøjdekravene på programområdet. Efter direktivets art. 9, stk. 2, finder bestemmelserne heri tillige anvendelse på programmer, der er udviklet før den 1. januar 1993 (direktivets ikrafttrædelsesdato).

Lavkvalitetsprogrammel

At knytte værkshøjdebestemmelsen for programmer til risikoen for dobbeltfrembringelser kan i særlige tilfælde føre til stødende resultater, hvis det forstås som et unuanceret krav om, at programmørens "personlighed" skal komme til syne i programmet. Man kan dermed komme til at præmiere det program, der er inkonsekvent, uordentligt, fejlbehæftet og vanskeligt at vedligeholde, fordi det reflekterer programmørens personlighed mod til gengæld at nægte beskyttelse for det gode, strømlinede og "upersonlige" program, der udmærker sig ved overskuelig systematik og person-uafhængighed. Kravet om originalitet må derfor primært fungere som en markering af, at værket må have en kompleksitet, der i hele sin opbygning muliggør et sådant særpræg under udviklingsprocessen, at det færdige program vil adskille sig fra andre programmer med samme funktioner.

Teknisk kvalitet

Man kan derimod ikke forlange, at programværket skal besidde en særlig teknisk kvalitet svarende til den, man f.eks. vil stille

inden for patentretten, ligeså lidt som et sådant krav stilles for den almindelige brugskunst. I præamblen til Rådsdirektivet om retlig beskyttelse af programmer er det udtrykkeligt anført, at de kriterier, der skal lægges til grund for at afgøre, om et program er originalt eller ej, ikke skal omfatte afprøvning af programmets kvalitetsmæssige eller æstetiske værdi. Dette aspekt kan derimod få betydning i relation til programmets *brugergrænseflade*, for så vidt denne betragtes som brugskunst, se hertil nedenfor under 7.3.c.

Størrelse

Heller ikke antallet af programinstruktioner har som udgangspunkt betydning for værkshøjdevurderingen. Derimod ligger det klart, at den, der skriver et program, har større spillerum for sin originalitet, hvis han udtrykker sig over 10.000 programkoder, end hvis han kun anvender 10 eller 20. Skyldes programmets størrelse imidlertid kun en uhensigtsmæssig struktur, der lader samme funktioner udføre af flere forskellige moduler i stedet for at ligge ét sted, hvorfra de kan kaldes, vil størrelsen ikke nødvendigvis være udtryk for originalitet.

Markeds-udbredelse

Programmets markedsmæssige udbredelse fremholdes undertiden som en ophavsretlig indikation. Således har det været hævdet, at et program, der kan sælges som standardvare, også må formodes at være beskyttet. At salgbare programmer ofte vil nyde ophavsretsbeskyttelse er imidlertid ikke en funktion af salgbarheden, men af, at markedet ofte vil præmiere velfungerende programmer.

Bevisspørgsmål

Den domstol, der skal påkende en sag om ophavsretlig originalitet, vil typisk have vanskeligt ved at få noget klart billede af, om dette krav er opfyldt. Ofte foretager domstolene denne vurdering uden sagkyndige erklæringer, se f.eks. ERA 3.216 (Århus byrets dom af 13. januar 1988) og Københavns Byrets dom af 18. oktober 1989; men det kan være risikabelt for rettighedshaveren at forlade sig herpå.

6.2.d. Bearbejdninger

Problemstillingen

Det forhold, at ophavsretten også omfatter bearbejdninger af det beskyttede værk, jf. ophl. § 2, stk. 1 ("i ændret skikkelse"), har stor betydning på hele det digitale område. Mange tekster – programmer eller andre litterære værker – der én gang er lagret i digital form, har en tendens til at blive holdt i live i form af løbende opdateringer og tilretninger. Dermed kan der opstå en flerhed af rettighedshavere til det reviderede – bearbejdede – værk. Mest slående er dette på programområdet, hvor første ver-

sion af et program kan leve videre i årtier i kraft af de opdateringer og ændringer, programmet undergår. Dermed kan klassiske eller basale programmer anvendes gennem adskillige IT-generationer, jf. nærmere *Bing* i NIR 1999.295 ff. Men det samme kan siges om databaser, hjemmesider og større skriftlige fremstillinger, der er genstand for digital værksudnyttelse.

Ophavsretligt giver dette anledning til to problemer: Hvornår kan den *oprindelige ophavsmand* modsætte sig bearbejdninger? Og hvorledes er retsstillingen mellem den oprindelige ophavsmand og *bearbejderen*, hvis der rent faktisk sker en bearbejdning?

Retten til bearbejdningen

Den oprindelige ophavsmand vil som udgangspunkt kunne modsætte sig en bearbejdning af værket, der resulterer i, at værket gøres tilgængeligt for almenheden i denne ændrede skikkelse. Dette gælder, hvad enten bearbejdningen har karakter af "oversættelse" eller "omarbejdelse i anden litteratur- eller kunstart eller i anden teknik". Denne regel er klart udtalt i ophl. § 2. Derimod kan rettighedshaveren ikke modsætte sig en bearbejdning af værket, der ikke gøres tilgængelig for almenheden, f.eks. fordi den sker i det private hjem eller til privat forskningsmæssig anvendelse. Den ret, brugeren dermed har til at bearbejde værket i lukkede miljøer (altså uden tilgængeliggørelse for almenheden), har dog kun selvstændig betydning, når værket foreligger i ikke-digital form, f.eks. nedskrevet i en bog. Dette skyldes, at bearbejdninger af programværker (og andre værker) i digital form i praksis kun kan ske gennem en eksemplarfremstilling og efter de særlige, restriktive, begrænsninger der gælder herfor, jf. nedenfor om ophl. §§ 12, stk. 2, nr. 3-5 og 36-37. Selv hvor der er sket en egentlig overdragelse af en ophavsret – og ikke blot tilstået en licens – følger det af ophl. § 56, stk. 1, at erhververen ikke har ret til at ændre i værket, medmindre ændringen er sædvanlig eller åbenbart forudsat.

Ifølge art. 4 (b) i direktiv 91/250/EØF om retlig beskyttelse af edb-programmer omfatter ophavsretten til et edb-program tillige retten til at "oversætte" dette. Da oversættelse af edb-programmel i form af *kompilering* er et naturligt og nødvendigt led i enhver programanvendelse, må det antages, at dette led i bestemmelsen sigter til oversættelse fra et programmeringssprog til et andet, se tilsvarende *Jon Bing* i NIR 1999.283. Derimod må den rent maskinelle oversættelse ("*kompilering*") af et edb-program betragtes som en eksemplarfremstilling, sml. herved ophl. § 2, stk. 2, der fastslår, at begrebet eksemplarfremstilling også omfatter det forhold, at værket overføres på indretninger, som kan gengive det. Alt efter sin beskaffenhed kan en *konvertering* af programmet, hvorved

programmøren udøver forskellige typer af valg, udgøre en bearbejdning af det. Forskellen ligger i, at den programmør, der forestår oversættelsen, alene har ophavsret til oversættelsen, hvis der er udvist den fornødne originalitet (hvilket der ikke nødvendigvis vil være, hvis der er tale om oversættelse mellem to programmeringssprog, der har nogenlunde ensartet opbygning). Er der derimod tale om en bearbejdning, vil der som udgangspunkt være spillerum for originalitet i selve bearbejdningsprocessen.

Samtykketilfælde

I mange tilfælde vil ophavsmanden imidlertid have givet udtrykkeligt eller stiltiende samtykke til, at bearbejderen kan ændre i værket. Dette kan f.eks. tænkes, hvis værket er frembragt i et samvirke mellem flere – f.eks. interessenter i et interessentskab – og under den aftale eller klart markerede forudsætning, at værket siden skal kunne revideres i samvirkets interesse. Problemet opstår ikke i ansættelsesforhold, hvor det følger af ophl. § 59, at arbejdsgiveren opnår (hele) ophavsretten til sådanne programmer, der frembringes af en arbejdstager under udførelsen af dennes arbejde eller efter arbejdsgiverens instruktioner, jf. nærmere herom i afsnit 6.5.c.

Bearbejderens ret

Den, der bearbejder et værk, har ret til sin bearbejdning, under forudsætning af, at denne besidder den fornødne originalitet, jf. nærmere *Schønning* (1998), s. 181 f. Dette begreb søges almindeligvis afgrænset "nedad" således, at den rent *tekniske medhjælp* ikke antages at opnå medophavsret. Det afgørende er, hvilke grænser "medhjælpen" er underlagt i sine valgmuligheder og dermed i sin mulighed for at udfolde originalitet. En web-master, der efter en klar instruktion *rentegner* en skitse med henblik på indlæggelse på en hjemmeside, vil som udgangspunkt ikke opnå medophavsret hertil, idet han ikke forventes at udøve nogen valgmuligheder, der afspejler originalitet.

Edb-programmel

I relation til edb-programmel må det på den ene side antages, at *fejlretninger*, hvorved enkelte kommandoer ændres, ikke vil kunne opfylde originalitetskravene. Er der derimod tale om at tilføje bestanddele af kode, der isoleret set kunne være beskyttet som selvstændige værker, vil der på den anden side være ophavsret hertil efter almindelige regler. Vanskeligheden knytter sig til mellemområdet, hvor bearbejdningen har karakter af en *gennemskrivning*. Her må man anlægge et konkret skøn. Et andet problem knytter sig i den forbindelse til den bearbejdning af et programværk, der sker i forbindelse med dets *implementering og tilpasning* til en specifik installation.

Brugskunst

Problemstillingen kendes ligeledes på brugskunstens område, hvor arkitekter og formgivere ofte samarbejder under udviklingsprocessen. *U 1989.1016 H* statuerede f.eks. medophavsret til en

kaffekande, som B havde udviklet på grundlag af et forberedende design udført sammen med A. Dommen går ganske vidt i anerkendelse af medophavsret og når tilsyneladende sit resultat uden noget bevis for, hvilken specifik rolle A havde spillet omkring formgivningen. Se også *U 1965.720 Ø*. En vis inspiration for problemkredsen kan i øvrigt hentes i patentretten, hvor tilsvarende samejekonstruktioner opstår, se hertil min kommentar til Lov om arbejdstageres opfindelser (1995), s. 67 ff. Dommen i *Ashton-Tate v. Ross*, 916 F.2d 517 (1990) frakendte en person, hvis bidrag til udviklingen af et spreadsheet-program bestod af en liste over programmets brugerinterface, medophavsret til det. Se i øvrigt til problemstillingen *Wagle & Ødegaard* (1997), s. 200 ff. og 213 f.

Afbrudte samarbejdsforhold

I visse samarbejdsforhold kan det volde tvivl, om et færdigt værk er en "bearbejdelse" af en førsteudgave eller et samleværk: A og B er gået sammen om at udvikle et program, men A forlader samarbejdet inden det er færdigt, hvorpå B færdiggør systemet alene. Situationen kan da enten være den, at A undervejs i udviklingsprocessen har frembragt færdige "del-værker" (moduler mv.), som han er eneophavsmand til, og som B i givet fald må frikøbe rettighederne til. Eller også kan der være tale om, at A's indsats smelter sammen med B's på en måde, så den ikke kan udskilles. I så fald vil der foreligge et fællesværk, som B i medfør af ophl. § 6 må respektere A's medophavsret til.

Se nærmere hertil *Bing* i NIR 1999.296 f. med henvisning til den norske lagmannsdom trykt i NIR 1999.411 ff. og L&D 56/1998.8 ff.: Trods et stort antal bearbejdninger fandt retten, at ophavsmanden til det således udviklede program ikke havde frembragt et nyt og selvstændigt værk.

6.2.e. Samleværker

Begreb

Når et antal litterære eller kunstneriske værker mv. eller dele heraf sammenstilles, kan der opstå et såkaldt *samleværk*, jf. ophl. § 5. Det klassiske eksempel herpå er antologien, hvor en redaktør (ophavsmanden) skaber noget "nyt" ved at bringe en række forfatteres enkeltværker sammen. I informationsalderen er *databasen* blevet et mindst ligeså praktisk eksempel, og også på programsiden er der plads for denne særlige beskyttelse, f.eks. når et program bliver til gennem såkaldt *CASE*-programmering, ved sammensætning af en række på forhånd udviklede programmoduler. I den ophavsretlige terminologi må sådanne sammenstillinger rubriceres som samleværker, der, fordi de ikke (som sam-

leværk betragtet) rummer instruktioner til en processor, *ikke også* er edb-programmer. Derimod må de enkelte moduler i sammenstillingen – såfremt de indeholder sådanne instruktioner – rubriceres som selvstændige programværker.

Ophl. § 5 knytter ophavsret til *sammenstillingen*, altså dette at man ved at sammenstille værker eller dele af værker frembringer et litterært eller kunstnerisk samleværk. Den ret, skaberen ("sammenstilleren") hermed opnår, gør dog ingen indskrænkning i ophavsretten til de enkelte værker. Kunne den det, ville ophavsretten til en artikel eller novelle ikke være meget værd.

Originalitetskravet

Ligesom andre værker skal et samleværk besidde den fornødne originalitet for at kunne beskyttes ophavsretligt. En kronologisk sammenstilling af en given forfatters "samlede værker" vil således ikke opnå beskyttelse (allerede fordi det pr. definition kun kan sammenstilles på én måde), og helt samme resultat må man nå til, hvis en database inden for et bestemt vidensområde indeholder en komplet datasamling (f.eks. kursen på samtlige børsnoterede selskaber på Københavns Fondsbørs en bestemt dag præsenteret i alfabetisk rækkefølge). Samleværksbeskyttelsen fører dermed til det ejendommelige paradoks, at mulighederne for at beskytte databasen bliver mindre, jo mere fuldstændig databasen er. Dette problem er baggrunden for, at der er indført en særlig *sui generis* beskyttelse af databaser, se herom afsnit 8.4.

Man kan diskutere, om samleværksreglerne også beskytter sammenstillinger af elementer, der ikke er værker (f.eks. samlinger af kataloger og tabeller, der beskyttes efter ophl. § 71, værker under værkshøjdekravet, lovlige citater, jf. § 22, eller offentlige aktstykker mv., jf. § 9), når de pågældende sammenstillinger har den fornødne originalitet. Se hertil betænkning 1064/1986: Ophavsret og edb, s. 20 f., der som eksempel herpå nævner selektive bibliografier o.lign. Alternativet hertil måtte være at beskytte sådanne sammenstillinger som selvstændige litterære værker, således som dette skete i *U 1975.30 H*, der anså en tekstløs billedbog som et litterært værk, og *U 1980.689 Ø*, der beskyttede en naturkalender, der for hver dag indeholdt en kort beskrivelse af en naturbegivenhed, som sådant. Da praksis har vist sig åben overfor en sådan beskyttelse, har spørgsmålet ikke den store praktiske betydning, jf. bemærkningerne i afsnit 8.2.c. om programantologier. Ved dommen i *U 1962.254 SH* fandt Sø- og Handelsretten f.eks., at "Ingeniørens indkøbsbog" – en samling af tekniske annoncer og firmabeskrivelser fra ca. 1000 virksomheder – var et ophavsretligt værk, der som sådant var beskyttet mod efterligning. Dommen er afsagt på grundlag af retstilstanden før kata-

logreglens indførelse, og retten kan derfor have følt et behov for at sikre frembringelsen en beskyttelse ved at rubricere den som et værk.

6.2.f. Fællesværker

Begreb

Når et program skrives af flere ophavsmænd, vil den enkeltes indsats ofte ikke kunne udskilles fra helheden. Programkoden vil foreligge i en form, der ikke gør det muligt at fastslå, hvem der har skrevet hvad. Sådanne værker kaldes for fællesværker: De er skabt i fællesskab, og i medfør af § 6 tilfalder ophavsretten derfor de involverede ophavsmænd i fællesskab, ganske som det gælder for ejendomsretlige samejer. Den ene forfatter kan derfor ikke uden den andens samtykke beslutte sig til at disponere over værket, f.eks. ved at markedsføre det. Dog fastslår § 6, at enhver af ophavsmændene kan påtale retskrænkelser, f.eks. når programmet kopieres ulovligt. Ønsker B at frigøre sig for sine forpligtelser overfor A, må dette ske efter retningslinjer som for opløsning af samejer. De eventuelle personlige rettigheder, A måtte have til systemet, kan B derimod ikke frigøre sig for.

Et fællesværks tilblivelse kan rammende sammenlignes med, hvordan en familiesang bliver til. Typisk forfattes sådanne værker af et "forfatterkollegium", hvoraf én sidder med pennen i hånden og skriver ned; en anden kaster en idé ud som forslag til et vers; en tredje finder den enkelte versefod; en fjerde én der rimer herpå etc. etc. I sådanne tilfælde vil alle – på nær den, der fik idéen, henholdsvis førte pennen – få andel i ophavsretten. På tilsvarende vis foregår samarbejdet i større projektforløb ved, at en gruppe formulerer de basale strategier, f.eks. valg af udviklingsværktøjer, hovedfunktioner og systemarkitektur. En anden foretager nedbrydningen i del-moduler. En tredje personkreds har ansvaret for, at der er kongruens mellem de forskellige delmoduler. En fjerde gruppe sørger for, at arbejdsopgaverne formuleres i overensstemmelse hermed. Først på det femte plan, der måske repræsenterer under 20 % af den samlede udviklingstid, bliver den endelige kode skrevet.

Blandede tilfælde

Både inden for de klassiske samleværkers område (antologier) og på programområdet vil den redigerende indsats undertiden indebære forfatterisk virksomhed. Hvor redaktøren bidrager med et forord, vil den udviklingsansvarlige måske skrive et lille program, der binder nogle moduler sammen. Ophavsretligt foreligger der to forskellige værkstyper. Samleværksbeskyttelsen retter sig mod sammenstillingen af værker. Forfattes der dertil særskil-

te værker, er disse undergivet den primære ophavsret. Smelter værkerne sammen, således at det ikke (længere) er praktisk muligt at udskille de enkelte værkskomponenter fra hinanden, må frembringelsen rubriceres som et ophavsretligt fællesværk, jf. ophl. § 6.

6.3. Enerettens omfang

6.3.a. Eksemplarfremstilling

Som nævnt ovenfor indebærer den ophavsretlige eneret bl.a. en ret til eksemplarfremstilling, jf. § 2. Det er underordnet, hvilket medium der anvendes til eksemplarfremstillingen. Ophl. § 2, stk. 1, medtager også den eksemplarfremstilling, der gør værket tilgængeligt for almenheden "i ... anden teknik". Dernæst anses efter stk. 2 også enhver direkte eller indirekte, midlertidig eller permanent og hel eller delvis eksemplarfremstilling på en hvilken som helst måde og i en hvilken som helst form som eksemplarfremstilling, jf. ophl. § 2, stk. 2, 1. pkt. Bestemmelsen indfører art. 5, stk. 1, i Infosoc-direktivet, der betegner sådanne udnyttelseshandlinger som "midlertidige reproduktionshandlinger", jf. nærmere afsnit 6.3.b. Ligeledes anses som fremstilling af eksemplarer også det forhold, at værket overføres på indretninger, som kan gengive det, jf. ophl. § 1, stk. 2, 2. pkt. Denne bestemmelse, som stammer fra Bernerkonventionens art. 9, stk. 3, søger at præcisere det væsentlige forhold, at der ikke stilles noget krav om, at et ophavsretligt eksemplar er *synbart* eller at det i øvrigt foreligger i en form, der fremstår som *færdigt og funktionelt*.

Det er derfor uden betydning for den ophavsretlige beskyttelse, om et program er lagret i computerens hardware (f.eks. i en ROM-kreds), magnetisk (f.eks. på diskette), optisk (f.eks. på CD-ROM) eller på anden vis, sml. art. 1, stk. 2, i direktiv 91/250/EØF. Ligeledes er det uden betydning for beskyttelsen, hvilket *format* eksemplaret foreligger i. Kilde- og objektkode anses (også) her som ækvivalente værker, der beskyttes på samme måde. Der trækkes hverken fra eller lægges noget til ved at oversætte (kompilere) et program fra kilde- til objektkode. Ved den lovændring, der fandt sted i 2001, er det i ophl. § 11, stk. 3, blevet præciseret, at det dog ikke er tilladt at fremstille eksemplarer af et værk på grundlag af en gengivelse af værket, der er sket i strid med den ophavsretlige eneret, jf. ophl. § 2. Denne regel blev ved indførelsen af Infosoc-direktivet i 2002 udvidet, således at også eksem-

plarer, som er fremstillet på grundlag af en omgåelse af en teknisk foranstaltning i strid med ophl. § 75c, stk. 1, afskærer adgangen til yderligere eksemplarfremstilling på grundlag af reglerne i ophl. kapitel 3.

De beskyttede handlinger

I relation til værkets genskabelse sondrer ophavsretsloven mellem "eksemplarfremstilling" og "anden udnyttelse". Eksemplarfremstilling indebærer, at man genskaber værket i fuldstændigt den samme udformning, det havde fra programmørens hånd. Dette er praktisk muligt, når værket har en flygtig tilknytning til sit medium, således som forholdet er for f.eks. videogrammer, tekstsider til fotokopiering og programdisketter. Ved anden udnyttelse genskabes kun visse aspekter, og der må anlægges en nærmere vurdering af, om der består den fornødne *ækvivalens*.

Ækvivalenslæren

Læren om ophavsretlig ækvivalens er navnlig udviklet inden for de områder af ophavsretten, hvor værkerne har brugsfunktionel karakter, herunder navnlig brugskunsten og arkitekturen, se hertil *Schmidt* (1989), s. 69 ff. *U 1993.17 H*, nægtede netop ophavsret til fem tipssystemer, hvorved spørgsmålet om ækvivalens bortfaldt. Se ligeledes den vidtgående *U 2002.1645 Ø,* der antog, at et byggeprojekt om et kontorbyggeri måtte anses for en "videreførelse" af nogle skitseforslag og et dispositionsforslag til et lignende kontorbyggeri, og at ophavsretten til disse skitseforslag mv. var krænket på grund af deres "slående lighed" hermed. Som begrundelse for sit resultat henviser landsretten bl.a. til, at tegningen ikke kunne være blevet til uden kendskab til den tidligere tegning. Selve denne begrundelse kan dog ikke bære et sådant resultat: At man udformer en kontorbygning med "fingre" har karakter af en idé, der ikke kan beskyttes som sådan, jf. bemærkningerne i afsnit 6.2.b. (s. 289). Og i selve den subjektive vurdering af, hvor grænsen går mellem "idé" og "udtryk" spiller det ikke nogen afgørende rolle, om frembringeren af det nye værk har været inspireret af et tidligere. Den ophavsretlige ækvivalenslære vedrørende edb-programmer behandles bl.a. af *Thomas Riis* (2002), s. 37 f. med henvisning til den norske lagmanns-dom i *Rettens Gang* 1999.330 (*NIR 1999.411*).

Bedømmelsens genstand

I relation til den ophavsretlige beskyttelse af programkoden må ækvivalens-vurderingen tage udgangspunkt i programmets instruktioner, således som de kommer til udtryk i kildeteksten (som da må bringes frem for den dømmende ret – et spørgsmål, der i sig selv kan give anledning til processuelle spørgsmål, hvis den ene part gør gældende, at der er tale om erhvervshemmeligheder). Det er her, "værket" er materialiseret, her ophavsmandens originalitet er kommet til udtryk og her, krænkeren i givet

fald har været på spil. Der er tale om en kompliceret og omfattende procedure, som under sagsførelse almindeligvis vil kræve medvirken af en eller flere syn- og skønspersoner. Opgaven består ganske enkelt i at sammenligne teksterne i henseende til struktur, betegnelse for de enkelte program-"kald" samt de enkelte programinstruktioner, jf. nærmere *Bing* i NIR 1999.291 ff. og 297 ff., sidstnævnte sted med omtale af de tekniske muligheder, der er for at optimere dette sammenligningsarbejde.

Er der flere ophavsmænd, kan man også vurdere den sammenstilling af del-moduler mv., der manifesterer programmet som samleværk. Ækvivalensbedømmelsen kan ligeledes knytte sig til programmets uddata i form af skærmbilleder, tekst, grafik eller lyd. I så fald anskuer man ikke programmet, men de selvstændige værkstyper (f.eks. klassisk-litterære eller kunstneriske værker mv.), som programmet er medium for. Denne værksbedømmelse vil ske som for enhver anden form for tekst, billede mv.

Indexeringer

I forbindelse med den stigende anvendelse af Internet-søgerobotter er det blevet aktuelt at afklare, hvorledes den *indexering*, der indgår som et nødvendigt element heraf, skal betragtes. Indexeringen indebærer, at en række informationer fra nettets hjemmesider hentes herfra og lægges ned på robottens server, hvor de danner et gigantisk stikordsregister med henvisninger til de pågældende hjemmesider. Fordelene ved en sådan indexering ligger i, at brugeren i den enkelte søgning sparer transmissions- og opkoblingstid til de talrige hjemmesider, hvorfra informationen hentes ned. Han søger i stedet i indexet, som herefter peger videre til de enkelte hjemmesider. Dette index opdateres automatisk med bestemte intervaller, f.eks. dagligt eller hver time.

- diskussion

På den ene side kan det være vanskeligt at hævde, at et stikordsregister, der indeholder alle ord i en bog, udgør en kopi af bogen, eftersom de fleste ord optræder flere gange i bogen, uanset de kun står en gang i stikordsregisteret. Men det særlige for et hypertekst-baseret index er, at hvert ord er forsynet med information om, hvilke andre ord det optræder sammen med. Derfor kan man argumentere for, at indexet må betragtes som en overførelse af "bogen" (og her, hjemmesiden) til en indretning, der er egnet til at gengive denne, jf. ophl. § 2, stk. 2. Selv om denne betragtning har meget for sig, er resultatet ikke utvivlsomt. Der kan således også argumenteres for, at indexet som "indretning" slet ikke tager sigte på gengivelse, og at det kun med betydeligt besvær vil kunne udvirke en gengivelse af de pågældende værker.

Spørgsmålet må anes for tvivlsomt. Som udgangspunkt spiller det dog næppe nogen større praktisk rolle, eftersom en formåls-

betragtning (nettet som noget, der netop kendetegnes ved at være opbygget af links) også her må føre til, at det eksemplar, man måtte konkludere at der forelå, må anses for lovligt, jf. ophl. § 36, stk. 1, nr. 1.

6.3.b. Midlertidige eksemplarer

Teknisk problem

Når man anvender programmel i en computer, sker dette på grundlag af en mangfoldighed af kopieringer af programmel og data; kopieringer, der i vekslende omfang styres af systemet eller brugeren. En fornuftig bruger vil allerede sikre sig mod uheld på systemet ved at *sikkerhedskopiere* programmer og data. Flytning af filer fra gammelt til nyt medium sker i to led, der ligeledes indebærer en kopiering: 1. Kopiering til nyt medium. 2. Sletning fra gammelt medium. Endelig genererer mange programmer selv kopier af programdele mv., som led i selve IT-anvendelsen – navnlig sker der en kopiering, når applikationen eller dele af den indlæses i *systemets RAM*, uden hvilken programmet slet ikke kunne give sine instruktioner til processoren.

Eksemplar-begrebet

Alle disse kopier kan siges at være midlertidige, idet de alene tjener en teknisk funktion, der udtømmes ved afslutningen af den proces, der automatisk igangsætter kopieringshandlingen. Spørgsmålet er nu, hvilke af disse mange kopier der kan betragtes som "eksemplarer" i ophavsretlig forstand. Svaret på dette spørgsmål har tidligere givet anledning til betydelig tvivl. En betydelig del af denne tvivl er afskåret efter indførelsen af Infosoc-direktivet. Som før nævnt følger det nu af ophl. § 2, at begrebet eksemplarfremstilling omfatter "enhver direkte eller indirekte, midlertidig eller permanent og hel eller delvis eksemplarfremstilling på en hvilken som helst måde og i en hvilken som helst form". Bestemmelsen gennemfører Infosoc-direktivets art. 5, stk. 1, der undtager visse "midlertidige reproduktionshandlinger" fra den ophavsretlige eneret. De reproduktionshandlinger, der undtages, er de flygtige eller tilfældige, som udgør en integrerende og væsentlig del af en teknisk proces, og som udelukkende har til formål at muliggøre "(a) en mellemmands transmission i et netværk mellem tredjemænd, eller (b) en lovlig brug af et værk eller en anden frembringelse". Disse handlinger undtages dog kun fra den ophavsretlige eneret, hvis de "ikke har selvstændig økonomisk værdi", jf. ophl. § 11a (generelt). Dette kriterium er ikke sammenfaldende med kriterierne i den legale licens i § 36, stk. 1, nr. 1, og stk. 2 (for edb-programmer og databaser). Nærmere om denne bestemmelse i afsnit 7.4.b.

Selv om denne lovændring har løst de fleste af dagliglivets praktisk forekommende spørgsmål om den ophavsretlige lovlighed af midlertidige eksemplarer, tilbagestår et generelt – og på det teoretiske plan fortsat væsentligt – beskrivelsesproblem om, hvad der i det hele taget udgør et "eksemplar" henholdsvis en "reproduktion" af dette eksemplar. Problemet kan få praktisk betydning i flere situationer. For det første indebærer anvendelsen af de førnævnte regler flere retlige kvalifikationsbetingelser, der kan give anledning til tvivl. Det gælder f.eks. spørgsmålet, om de nævnte midlertidige reproduktionshandlinger indebærer en "lovlig brug" samt den generelle betingelse om, hvorvidt brugen har "selvstændig økonomisk værdi". Hvis ikke disse krav er opfyldt, kan ophavsmanden modsætte sig, at der fremstilles et "eksemplar". For det andet har afgrænsningen af, hvornår der foreligger et "eksemplar", betydning for det praktiske arbejde med licensering af edb-programmel og databaser.

Derfor er der fortsat behov for en selvstændig analyse af, hvornår en teknisk gengivelse af bits hidrørende fra et program, et litterært værk eller en anden beskyttet frembringelse udgør et "eksemplar" i ophavsretlig forstand.

RAM-kopier

Når spørgsmålet drøftes i relation til RAM-hukommelsen, kan det være nødvendigt at sondre mellem forskellige typer af RAM-kopier. Navnlig må man sondre mellem den dynamiske RAM (DRAM) og den statiske RAM (SRAM). Den statiske RAM, der f.eks. kendes fra USB-lagerenheder og fra de clips, der lagrer fotos i digitale kameraer, kendetegnes ved, at informationen bliver liggende i hukommelsen, uanset om strømmen afbrydes. Forholdet kan nærmest sammenlignes med et stykke metal, der drages til en elektromagnet, men som falder til jorden, når strømmen slukkes og elektromagneten derfor slipper sit tag i metalstykket. Den dynamiske RAM – som er den hyppigst anvendte teknologi i moderne IT-systemer – indebærer derimod, at der sker en løbende opdatering ("genopfriskning") af hver enkelt celle i hukommelsen millisekund efter millisekund. Hvor der – ikke mindst pga. ligheden med den magnetiske harddisk-kopiering – næppe kan være den store tvivl om, at information fikseret i en statisk RAM indebærer en eksemplarfremstilling, kan det give anledning til tvivl, om DRAM-kopier udgør eksemplarer.

Programdirektivet

Ifølge art. 4, litra a), i Rådsdirektivet om retlig beskyttelse af programmer omfatter ophavsmandens eneret bl.a. retten til at tillade eller foretage varig eller midlertidig, hel eller delvis reproduktion af programmet på en hvilken som helst måde og i en hvilken som helst form. Det tilføjes hertil, at *hvis* indlæsning,

visning på skærm, kørsel, overførsel eller lagring af programmet nødvendiggør reproduktion af programmet, så kræver en sådan reproduktion rettighedshaverens tilladelse. Bestemmelsen forudsætter dermed, at en lagring, visning eller kørsel af et program kan ske uden en delvis fiksering, og sondrer dermed mellem de omtalte små-kopier, der sker i forbindelse med den rene visning, kørsel, overførsel mv., og den delvise "reproduktion", der frembringer en mere varig kopi. Kun denne sidste har ophavsretlig relevans. De andre kan ophavsmanden ikke modsætte sig.

Diskussion

Ved vurderingen af dette – som andre af IT-rettens tvivlsområder – er det rimeligt at skele til den konkurrencemæssige betydning af mulige fortolkninger. Kun i de tilfælde, hvor der består en risiko for, at rettighedshaveren udsættes for utilbørlig plagiering, ligger der et argument for at udvide retsbeskyttelsen. Indlæsningen af programmer og data i RAM kan have helt permanent karakter, uanset de principielt "kun" bliver der, så længe computeren er tændt og RAM-lageret dermed er aktivt. Da visse computere – navnlig visse bærbare modeller – har faciliteter, der gør det muligt for brugeren at afbryde strømmen, uden at RAM-lageret mistes, og da andre computere ganske enkelt aldrig slukkes, kan det meget vel tænkes, at en RAM-kopi eksisterer i uger, ja sågar måneder og år. Derfor vil det være problematisk at indbygge en tidsbetingelse eller lignende krav i definitionen af det ophavsretlige eksemplarbegreb. Allerede ved afgrænsningen af den benyttelsesret, der skal være gældende for brugeren af et edb-program, vil et sådant kriterium volde vanskeligheder: Hvor længe skal computeren være tændt, før man kan tale om en eksemplaranvendelse? Ville man frakende sådanne kopier deres karakter af "eksemplarer" betød det, at en økonomisk væsentlig udnyttelseshandling ville være undtaget fra den ophavsretlige beskyttelse.

Konklusion

Efter min opfattelse må det derfor antages, at kopiering til RAM udgør en eksemplarfremstilling, der dækkes af den ophavsretlige eneret, uanset om der er tale om SRAM eller DRAM teknologi. Med sin noget uklare sondring mellem "reproduktion" og "kopiering" i bemærkningerne til art. 4 i forslaget til Rådsdirektivet om retlig beskyttelse af programmer (der knytter an til, om der efterlades "spor", når kørslen er afsluttet) er det netop forudsat, at begge dele bør falde inden for den ophavsretlige eneret. Af samme grund giver ophl. §§ 36-37 hjemmel for visse undtagelser fra ophavsretten. Disse spørgsmål behandles nærmere i forbindelse med licensproblemerne i afsnit 7.4.

I overensstemmelse med konklusionen ovenfor har man i amerikansk retspraksis fastslået, at RAM-kopier var ophavsretlige eksemplarer, se herved *MAI Systems Corp. v. Peak Computer*, 991 F.2d 511 (9th Cir. 1993). Afgørelsen har dog givet anledning til en del uro, jf. nærmere *Rosenoer*: CyberLaw (1996), s. 22 ff. og *Katariina Rajala* i NIR 1999.103 ff. med henvisning til senere praksis, der dog følger linjen fra MAI-sagen. Spørgsmålet drøftes indgående af *Therese Steen* i Eksemplarfremstilling av litterære verk til privat bruk (Complex 1/97), s. 12 ff., af *Wagle & Ødegaard* (1997), s. 157 ff. (der sondrer mellem, hvad man vil nå til efter "traditionel" henholdsvis "digital" ophavsret) og af *Jon Bing* i Rettslige aspekter ved digital kringkasting, Complex 6/97, s. 41 ff. Det generelle billede er, at spørgsmålet er tvivlsomt, men at RAM-kopiering i dag – ikke mindst af pragmatiske grunde – må siges at udgøre en eksemplarfremstilling. Se tilsvarende *Schønning* (1998), s. 138, for svensk *Lindberg & Westman* (1999), s. 169, og for finsk *Katariina Rajala* a.st. s. 119 f.

Efter denne opfattelse foreligger der herefter en "eksemplarfremstilling", når der er indtrådt en *fiksering* af værket til et medium eller en mere *varig tilknytning* til mediet, der i relation til værkets anvendelse må sidestilles med en fiksering. Fikseringskravet er som nævnt lagt til grund fra udenlandske ophavsretsordninger (herunder amerikansk ret) og knytter an til forhold, der har central ophavsretlig betydning. Den mere varige tilknytning må, hvis den skal sidestilles med en fiksering, fremtræde som i en helt tilsvarende skikkelse.

I en sammenligning kan man sige, at et spejlbillede ikke er "fikseret" i spejlet, da det dannes gennem en løbende passage af lys, der rammer spejlet, hvorimod en blyantsstreg er fikseret på papiret (selvom den kan fjernes med et viskelæder), idet papiret inden dette sker bærer den pågældende information i sig og principielt kunne gøres til genstand for faktiske foranstaltninger mv. (modsat spejlet). Denne betragtning skulle i sig selv lede til, at der kun foreligger en fiksering i en SRAM og i forbindelse med caching til harddisk; men da indlæsning på DRAM fremtræder på ganske samme måde, må den sidestilles hermed. SRAM-indlæsning kan således ikke sammenlignes med et spejlbillede: Hvor spejlbilledet af det emne, der reflekteres i spejlet, løbende vil ændre sig afhængigt af lys- og atmosfæreforhold, vil den datamængde, der findes i en DRAM, fremtræde i 100% identisk form, selvom den løbende gentages i takt med processorens clock-frekvens.

Internetkopieringer

En særlig problemstilling opstår i relation til den eksemplarfremstilling, der sker over åbne digitale net (Internet mv.). Ikke alene er antallet af eksemplarfremstillinger her ganske ukendt

(enhver transmission af information via digitale net sker ved et stort antal eksemplarfremstillinger undervejs fra afsender til modtager), men det vil tilmed være stort set umuligt at konstatere, på hvilke medier, hvor og hvor længe disse eksemplarfremstillinger finder sted. Dermed vil det også være umuligt at føre beviser for, at den tidsmæssige udstrækning af eksemplarfremstillingerne var ensbetydende med, at en ophavsret var krænket.

Selv om det lægges til grund, at de kopieringer af et værk, der sker under værkets transmission fra A til B via serverne på Internet, falder under den ophavsretlige eneret, kan man rejse spørgsmålet, om der også foreligger en "kopiering" i hver af de pakker, som den meddelelse, der repræsenterer værket, deles op i som følge af de anvendte protokoller. Som nævnt neden for i afsnit 7.1.b. om "partitioneringsproblemet" kan denne afgrænsning give anledning til vanskeligheder. Men hvis formålet med pakkeopdelingen alene er at sikre, at værket kan genskabes hos modtageren, må det klare udgangspunkt være, at denne mellemliggende handling falder inden for den ophavsretlige eneret, sml. herved det princip (som fremgår af Bernerkonventionens artikel 9, stk. 3), der finder udtryk i ophl. § 2, stk. 2, 2. pkt.

Ophl. § 11a

Med ophl. § 11a, der er indført på grundlag af Infosoc-direktivets art. 5, stk. 1, kan ophavsmanden ikke modsætte sig udførelse af midlertidige eksemplarer, der er flygtige eller tilfældige, og som udgør en integreret og væsentlig del af en teknisk proces, når de pågældende eksemplarer "udelukkende har til formål at muliggøre ... en mellemmands transmission af et værk i et netværk mellem tredjemænd". Det kræves dog, at udførelsen af de nævnte eksemplarer "ikke har selvstændig økonomisk værdi".

Ved fortolkningen af denne bestemmelse giver kravet om den "selvstændige" økonomiske værdi anledning til tvivl. I præambelen til Infosoc-direktivet (betragtning 33) fastslås det, at denne undtagelse også bør dække "browsing samt handlinger, der muliggør lagringer i cache-hukommelsen, herunder sådanne, som bidrager til, at transmissionssystemerne fungerer effektivt, forudsat at mellemmanden ikke ændrer informationen og ikke foretager indgreb i den lovlige anvendelse af teknologi, som er almindelig anerkendt og anvendt af industrien, med det formål at skaffe sig data om anvendelsen af informationen." Herved sigtes til artikel 13 i e-handelsdirektivet, der er indført i dansk ret med e-handelslovens § 14. Meningen må herefter være, at selv en oplagring af informationen, der har en vis varighed, ikke krænker ophavsmandens eneret, så længe denne oplagring ikke gøres til genstand for en selvstændig (forstået som adskilt fra selve kom-

munikationshandlingen) økonomisk udnyttelse. Hvis brugeren derimod på kommercielt grundlag giver andre end de kommunikerende parter adgang til den pågældende, kræves ophavsmandens samtykke. En adgang, der alene har teknisk karakter, eller som har til formål at opfylde et myndighedspålæg (f.eks. i forbindelse med et straffeprocessuelt indgreb i meddelelseshemmeligheden) krænker derimod ikke ophavsretten.

Visning på skærm

Hermed må man formentlig også antage, at der indtræder eksemplarfremstilling, når et digitalt lagret værk (f.eks. et foto eller et værk af billedkunst) vises på skærm. Dette resultat må i hvert fald kunne fastholdes, hvis der er tale om en skærmtype, der *fikserer* de enkelte elementer af billedet, hvorimod spørgsmålet må betragtes som tvivlsomt, hvis ikke der sker nogen fiksering i skærmen. Fiksering sker f.eks. ved brug af de TFT-farveskærme, der er almindelige i bærbart udstyr og på visse stationære fladskærme: Skærmbilledet dannes ved lysudladninger fra et stort antal tætsiddende transistorer, der er placeret i en matrix på skærmen, og som udlæser billeddata fra et tilsvarende antal hukommelsesceller i RAM. Skulle man følge betragtningen om, at flygtige fikseringer ikke udgør "eksemplarer", måtte en sådan projektion alternativt skulle betragtes som en "visning" eller "fremførelse", se hertil straks nedenfor og diskussionen hos *Wagle & Ødegaard* (1997), s. 181 f. og 172 f., *Lindberg & Westman* (1999), s. 172 f. og *Riis* (2002), s. 44 f.

En praktisk konsekvens af kun at betragte en digital gengivelse af et værk på skærmen som en visning eller fremførelse (men *ikke* samtidigt som en eksemplarfremstilling) vil være, at ophavsmanden ikke vil kunne modsætte sig en offentlig brug af værket efter den almindelige regel i ophl. § 2, stk. 3, nr. 2-3, såfremt visningen sker på grundlag af et eksemplar, der er *udgivet*. Dette skyldes konsumptionsreglen i ophl. § 20, der alene gør undtagelse (stk. 2) for tv-visning samt visning af litterære og musikalske værker, "hvis værkets indhold derved gøres tilgængeligt for almenheden". Anses forholdet derimod som en eksemplarfremstilling – som hævdet i nærværende fremstilling – vil også den private fiksering på skærmen falde indenfor ophavsmandens eneret, jf. lovens § 12, stk. 2, nr. 5. Dette vil f.eks. betyde, at man ikke uden ophavsmandens samtykke kan placere en terminal i et offentligt lokale til almindelig anvendelse, hvis anvendelsen af den pågældende terminal indebærer, at værker vises på skærmen.

Subjektive krav?

Man kan diskutere, om der i det ophavsretlige eksemplarbegreb bør indgå subjektive krav om formålet med de pågældende kopier mv. I *U 1997.691 H* antog Højesteret, at et ugeblads gengivelse af et bundt pengesedler ikke indebar en eksemplarfremstilling af

de kunstværker, pengesedlerne indeholdt, idet deres primære formål lå i den symbolværdi, sedlerne repræsenterer. Tilsvarende kunne det overvejes, om eksemplarer, der ikke udføres med henblik på tekniske funktioner, men f.eks. frembringes ved fejlbetjening el.lign., ikke skulle udgøre eksemplarer. En sådan fortolkning, som der ikke er dækning for hverken i lov eller forarbejder, vil imidlertid føre til vanskelige afgrænsninger og heraf følgende omgåelsesmuligheder mv. Som før nævnt bør de hensyn til den godtroende bruger, som betragtningen kunne tilgodese, snarere varetages i forbindelse med anvendelsen af de ophavsretlige retsfølger (straf, erstatning mv.), frem for gennem tillempninger af dette basale element af retsfaktum.

6.3.c. Tilgængeliggørelse for almenheden

Oversigt

Ved siden af retten til eksemplarfremstilling giver ophavsretsloven ophavsmanden eneret til at gøre værket "tilgængeligt for almenheden". Efter lovens § 2, stk. 3, dækker dette tre former for udnyttelse, der omtales nærmere i de følgende afsnit, men som oversigtsmæssigt kan præsenteres som følger.

Den første udnyttelsesform går ud på, at eksemplarer af værket (f.eks. programpakker) udbydes til salg, udlejning eller udlån eller på anden måde spredes til almenheden, jf. ophl. § 2, stk. 3, nr. 1. Denne udnyttelse betegnes i ophavsretlig terminologi som spredning og omtales nærmere i afsnit 6.3.d. Spredning er alene omfattet af denne eneret, når den sker til "almenheden", jf. herom senere.

Den anden udnyttelsesform går ud på, at eksemplarer af værket "vises offentligt", jf. ophl. § 2, stk. 3, nr. 2. Begge disse ordkomponenter – visningen, og kravet om offentlighed – giver anledning til afgrænsningsproblemer. De spørgsmål, der har at gøre med selve visningen behandles i afsnit 6.3.e.

Den tredje udnyttelsesform sker, når værket "fremføres offentligt". Som offentlig fremførelse efter stk. 3, nr. 3, anses også trådbunden eller trådløs overføring af værker til almenheden, herunder udsendelse i radio eller fjernsyn og tilrådighedsstillelse af værker på en sådan måde, at almenheden får adgang til dem på et individuelt valgt sted og tidspunkt, jf. ophl. § 2, stk. 4, nr. 1. Nærmere om denne afgrænsning neden for i afsnit 6.3.f.

Visning og fremførelse

Man kan med en vis ret gøre gældende, at sondringen mellem visning og fremførelse slet ikke er egnet til at danne grundlag for afgrænsningen af ophavsmandens eneret i disse sammenhænge, jf. *Nordell* i TfR 1999.489 f. Som loven fremstår, er det imidlertid

nødvendigt at lægge en klar begrebssondring. Afgrænsningen har bl.a. betydning ved afgrænsningen af konsumptionsreglerne i §§ 20 og 21: Hvor man har en almindelig ret til at "vise" et eksemplar af et værk – herunder et programværk – når dette er udgivet, er det kun tilladt at "fremføre" det, når tilhørerne eller tilskuerne har adgang uden betaling, hvis ikke fremførelsen er det væsentlige ved den pågældende foranstaltning, jf. ophl. § 21, stk. 1, nr. 1. Samme bestemmelses stk. 3 synes i øvrigt – ved sin placering – at forudsætte, at der foreligger fremførelse, når "filmværker, musikværker og værker i digital form stilles til rådighed ved hjælp af teknisk udstyr" (f.eks. fra en terminal). Den pågældende bestemmelse giver en ret hertil "til personligt gennemsyn eller studium". Eksemplarfremstilling (udover den, der følger af § 36, stk. 1) er dog ikke tilladt.

"Almenheden"

Fælles for de tre kategorier af beskyttede handlinger er, at de skal være sket overfor "almenheden". Begrebet giver anledning til betydelige afgrænsningsproblemer, der har stor praktisk betydning også uden for det digitale område, jf. nærmere *Schønning* (1998) s. 148 ff. Som udgangspunkt er det afgørende, om den kreds, der nås gennem tilgængeliggørelsen, kan afgrænses som ubestemt. I grænsetilfælde kan det spille ind, hvor mange personer der rent faktisk nås; men principielt er det numeriske antal ikke afgørende. Hvis man f.eks. sætter sit omstillingsbord til at spille pausemusik, medens den opkaldende part venter på at blive stillet igennem, er denne musik gjort tilgængelig for almenheden, selv om ingen ringer op.

Grænsetilfælde har bl.a. foreligget i relation til arbejdspladser, hvor der spilles musik: Principielt udgør medarbejderne på en arbejdsplads en sluttet kreds, eftersom de alene er tilstede på grundlag af et aftaleforhold, der typisk har en vis varighed. Efter at Højesteret i *U 1952.269 H* fandt, at fremførelse af musik i en fabrik med 2.150 medarbejdere udgjorde en offentlig fremførelse er det nu i § 2, stk. 4, nr. 2, præciseret at fremførelse i en erhvervsvirksomhed, der finder sted for en større kreds, som ellers måtte som "ikkeoffentlig", anses som offentlig fremførelse. I nyere retspraksis har man f.eks. antaget, at der ikke foreligger offentlig fremførelse, når musik afspilles i fritids- og ungdomsklubber (*U 1999.2011 H*) og i gymnastikforeninger (*U 2004.2134 H*).

Net-spredning

Begrebet "almenheden" omfatter med sikkerhed også tilgængeliggørelse af værker i digital form (gennem spredning af digitale eksemplarer eller ved digitale udsendelsesformer), der ikke ad teknisk vej er reserveret en mere snævert afgrænset kreds. I

relation til spredning af værker over telenet (f.eks. Internet) er kriteriet, hvordan den kreds af personer, der har *muligheden* for at tilslutte sig nettet og identificere det pågældende værk, er afgrænset. Det har derimod ikke betydning, om de rent faktisk *tilegner sig* værket, jf. *Wagle & Ødegaard* (1997), s. 183 f. Dette afgrænsningskriterium fører med sikkerhed til, at kommunikation af værket fra bruger til bruger (*one to one*) ikke udgør en tilgængeliggørelse til almenheden. Den nærmeste analogi er her, at værket sendes via en telefax fra A til B. Udsendes værket derimod til almenheden i krypteret form, således at det kun er den kreds af personer, der er udstyret med en særlig kode eller krypteringsnøgle mv., der vil kunne tilegne sig det, knytter afgrænsningen sig til denne særlige kreds, sml. herom den norske højesteretsdom i *Rt. 1995.35* og *Wagle & Ødegaard* (1997), s. 187 f. om begrænset distribution af piratkopierede dekoderkort.

Ikke kendte hjemmesider

Vanskelige grænsedragninger kan derimod opstå, hvis et værk stilles til rådighed fra en hjemmeside, hvis tilstedeværelse på nettet ikke er almindeligt kendt. Ligger værket således på en hjemmeside, hvorfra der ikke er etableret DNS-service, kan hjemmesiden kun nås med kendskab til dens IP-nummer. Et sådant IP-nummer kan man i praksis ikke regne sig frem til, endsige huske med henblik på genbrug (modsat en hjemmeside, der nærmest pr. definition er beregnet til at blive husket). En tilgængeliggørelse under sådanne omstændigheder kan derfor alene betragtes som sket til "almenheden", hvis kendskabet til det pågældende IP-nummer offentliggøres på anden vis. Tilsvarende må formentlig antages, hvis hjemmesiden i øvrigt er skjult for den almindelige almenhed, f.eks. ved ikke at optræde i en portal el.lign. og heller ikke at være gjort synbar for de almindeligt anvendte Internet-søgerobotter.

6.3.d. Spredning

Problemstilling

Ophavsretten til et værk giver for det første rettighedshaveren ret til at forbyde spredning af værket. Herved forstås bl.a., jf. ophl. § 2, stk. 3, nr. 1, at "eksemplarer af værket udbydes til salg, udlejning eller udlån eller på anden måde spredes til almenheden". Disse tre – væsentligste – udnyttelsesformer fremtræder som eksempler, idet eneretten også gælder anden spredning til almenheden, f.eks. gennem gave.

Funktion

Når bestemmelsen læses er det vigtigt at frigøre tanken fra den undtagelsesbestemmelse, der for de fleste praktiske formål modificerer dens anvendelsesområde, nemlig konsumptionsreglen i

ophl. § 19. Uden § 19 ville § 2, stk. 3, nr. 1, således – korrekt anvendt – være til hinder for, at man kunne forære gamle aviser bort til genbrugsindsamlinger eller sælge brugte bøger antikvarisk. Som bestemmelsen står, giver den – isoleret set – ophavsmanden en eneret til at kontrollere enhver transaktion, hvorved et eksemplar af et værk bringes videre fra den aktuelle besidder til en ny.

Når begrebet afgrænses, er det vigtigt at holde fast ved kravet om, at spredningen skal ske "til almenheden", jf. bemærkningerne straks ovenfor. Heri ligger først og fremmest en afgrænsning overfor privatsfæren: Selv uden § 19 ville det fortsat være muligt at købe en CD for at forære den til en ven. Derimod må det som udgangspunkt antages, at overdragelse, der finder sted mellem virksomheder, sker til "almenheden". Dette udgangspunkt kan dog modificeres, hvis de pågældende virksomheder er knyttet varigt sammen af særlige forpligtelser, f.eks. hvis de indgår i en joint venture eller er koncernforbundne under fælles aktiv styring. Kriteriet – der ikke er meget præcist – må være, om den forretningsmæssige transaktion, der begrunder spredningshandlingen (salget, udlejningen, udlånet) udspringer af en markedsmæssig vurdering af, hvilken part det er mest profitabelt at indgå aftale med, eller om aftaleparten er givet på forhånd i kraft af de særlige bånd, der binder parterne sammen.

Digital spredning?

Spredningsreglen er i sin tid affattet med sigte på spredning af fysiske eksemplarer: En bog, et maleri, en grammofonplade. I sådanne tilfælde opstår der ikke tvivl om, hvornår spredningen er gennemført: Det er den, når erhververen har opnået en mere varig besiddelse over det *medium*, der materialiserer værket. En sådan tvivl kan imidlertid opstå, når værket ikke er knyttet fast til et medium, men i sin tid er overdraget i rent digital form, således at den første erhverver så at sige har stillet sit eget medium til rådighed. Sådan er situationen f.eks., når et værk hentes fra en Internet-hjemmeside. Men situationen er meget lig dette, når værket overdrages på et medium, som straks efter værkets installation ikke længere forventes at udføre nogen funktion for brugen af værket. Det spørgsmål opstår så, hvornår man i disse "digitale" tilfælde kan tale om en spredning af værket.

Når spørgsmålet rejses kan der indledningsvis være grund til at slå fast, at der ingen retssystematisk begrundelse er for at behandle værker, der overdrages i rent digital form, anderledes i relation til konsumptionsadgangen end værker, der overdrages integreret i et medium. Opgaven må derfor være at udskille de "digitale" tilfælde, der minder mest om den fysiske overdragelse

(og som derfor må betragtes som spredninger, jf. § 2, stk. 3, nr. 1, og følge de almindelige konsumptionsregler) fra de, der må indrubriceres på anden vis.

Licenstilfælde

For det første er det vigtigt at udskille de tilfælde, hvor der ikke foreligger en eksemplaroverdragelse af værket, men hvor erhververens ret til at råde over værket hviler på en gyldig *licensaftale* med rettighedshaveren eller den (f.eks. en forhandler), der er berettiget til at tegne rettighedshaveren. I disse tilfælde må det følge af licensaftalens indhold, hvilken ret der består til videreoverdragelse. Udgangspunktet er her, at licenstageren ikke kan sætte en anden i sit sted, eftersom dette vil indebære et debitorskifte, der som sådant kræver kreditors samtykke. Indebærer aftalen imidlertid, at aftalen fuldt ud er opfyldt fra debitors (licenstagerens) side, og har debitor ikke påtaget sig forpligtelser, der går videre end, hvad der følger af den almindelige ophavsretlige regulering, må formodningen være for, at licenstageren kan sætte en anden licenstager i sit sted.

Eksemplartilfælde

Når værket overdrages uden en sådan aftale – altså som en *eksemplaroverdragelse* – på et *digitalt medium*, der efter værkets installation har opbrugt sin funktion, må det antages, at dette medium fortsat tjener en vis *symbolfunktion* som afgiver af en formodning for, at mediets besidder ikke alene er berettiget til at benytte programmet, jf. terminologien i ophl. § 36 stk. 1, men som også har det i sin magt at udvirke en overdragelse af eksemplaret. Dette giver anledning til vanskelige spørgsmål om, hvorvidt retten til at benytte et program bortfalder, såfremt originalmediet stjæles. Nærmere herom i afsnit 12.3.

Tekniske begrænsninger

Overdrages værket uden medium, men således, at der til den enkelte "solgte" installation udleveres en kode, et licensnummer eller en anden indretning, der gør det muligt at aktivere værket, gælder principielt det samme. I mangel af modstående aftale må det antages, at den person, der har rådighed over det pågældende nummer, er retmæssig bruger af programmet og kan effektuere en overdragelse af det ved at give licensnummeret videre (og herefter destruere det eller i hvert fald effektivt ophøre med brugen af det). Sådanne eksempler kendes ikke alene ved køb af værker på nettet, men også i aftaleforhold, hvor der f.eks. sælges "multiple license agreements", der giver 25 ikke på forhånd navngivne brugere i en virksomhed ret til at få udleveret det pågældende licensnummer.

Konsumption

Efter ophl. § 19 kan eksemplarer af litterære værker, som med ophavsmandens samtykke er *solgt eller på anden måde overdraget til andre*, som hovedregel frit spredes videre. Som netop

nævnt vil en sådan overdragelse bl.a. kunne tænkes gennemført i digital form ved overdragelse af et medium eller et licensnummer. Denne konsumptionsadgang indebærer først og fremmest, at ophavsmanden (rettighedshaveren) ikke – i mangel af aftale – kan modsætte sig *videresalg*, *gaveoverdragelser* og (med forbehold af bl.a. programområdet) *udlån* af det pågældende værk. Hvis ikke en sådan fravigelse fandtes, ville man som nævnt f.eks. ikke kunne aflevere gamle aviser til en spejderindsamling.

Begrundelse

Den nærmere afgrænsning af disse konsumptionsregler udspringer af en hensynsafvejning, der inddrager de særlige hensyn, der gør sig gældende på IT-området. På grund af den enkle kopieringsmulighed vil udlån eller udlejning af maskinlæsbare programmer eller digitale værker i maskinlæsbar form kunne åbne mulighed for en helt ukontrolleret kopiering til skade for ophavsmanden, se nærmere min artikel i U1986B.361 ff. Ud fra sådanne hensyn indførte man allerede ved 1989-ændringen af ophavsretsloven en særlig undtagelse fra den almindelige spredningsret, hvorefter "eksemplarer af programmer, som er udgivet i maskinlæsbar form" ikke uden ophavsmandens samtykke kan spredes gennem udlån eller udlejning. En tilsvarende regel blev indført ved art. 4, litra c), i Rådsdirektivet om retlig beskyttelse af programmer, hvorefter enhver form for offentlig spredning, herunder udlejning, af det originale program eller kopier deraf, er omfattet af ophavsmandens eneret.

- udlejning

Der indtræder ikke konsumption i relation til udlejning af værker, jf. § 19, stk. 2, bortset fra værker af bygningskunst og brugskunst. Selvom rettighedshaveren til et musikværk har givet tilladelse til, at værket sælges på en musik-CD, skal han med andre ord give sit samtykke til (i praksis: have betaling for), at sådanne solgte CD'er gøres til genstand for udlejning. Tilsvarende gælder for værker, der indeholder edb-programmer eller information i digital form.

Derimod kan der ske udlån af CD'er, således som dette også praktiseres fra visse musikbiblioteker, jf. nærmere nedenfor.

- leasing

Man kan diskutere, om forbuddet mod udlejning også omfatter edb-programmel, der gøres til genstand for finansiel leasing. For det første kan man her drøfte, om der overhovedet sker en overdragelse ved finansiel leasing: Hvis værket bliver, hvor det hele tiden er, kan det føles anstrengt at sige, at det er gjort til genstand for en "spredning". Det synes for det første nærliggende at betragte tilfælde af *finansiel leasing* ved sale and lease back som en finansieringsform, der må betragtes på samme måde som sikkerhedsstillelse ved pant og altså ikke som en overdragelse i sig selv.

En overdragelse (og spredning) vil således kun komme på tale, hvis der indtræder misligholdelse af den underliggende låneaftale, eller hvis aktivet mister sin værdi for leasingtageren (brugeren), og i så fald må den heraf følgende – mulige – overdragelse håndteres for sig (og eventuelt afskæres ophavsretligt). Er der derimod tale om *operationel leasing*, bør forholdet vurderes som en spredningshandling. Som nærmere anført i *ET* s. 156, har sådanne transaktioner væsentlige lighedspunkter med almindelige lejeforhold: Genstanden kommer fra A og kommer først i kraft af leasingaftalen over i B's besiddelse.

Omvendt må man efter almindelige grundsætninger om omgåelse også antage, at salg, der sker med henblik på tilbagekøb, indebærer leje eller udlån. Dette gælder formentlig uanset, hvilke beløb der udveksles mellem parterne. Se tilsvarende *Schønning* (2003), s. 154, med henvisning til lovmotiverne.

- udlån

Med ophl. § 19, stk. 3, gælder nu den undtagelse fra den almindelige konsumptionsregel, at ophavsmandens samtykke kræves til spredning af eksemplarer af edb-programmer i digitaliseret form gennem *udlån*. Det lokale folkebibliotek kan altså ikke indkøbe et antal programpakker med et udbredt tekstbehandlingssystem for derefter at låne disse programpakker ud. Derimod kan biblioteket godt udlåne bøger, hvor læseren kan stifte bekendtskab med programkoden i kildetekstformat. At man har indført en sådan regel hænger netop sammen med, at sådanne udlån kunne forventes at blive ganske kortvarige, nemlig svarende til den tid der ville medgå til en kopiering af de pågældende programmer! Tilsvarende betænkeligheder gør sig ikke gældende i relation til bogen med kildetekst.

- integrerede udlån

Samme hensyn gør sig for så vidt gældende for værker i digitaliseret form, f.eks. elektroniske ordbøger, leksika mv. I tiden efter indførelsen af 1989-loven anså rettighedshaverne imidlertid ikke dette område for at udgøre noget væsentligt problem, eftersom sådanne værker under alle omstændigheder ville være således integreret med det programsystem, der styrede søgning og fremvisning mv., at det alligevel ikke lod sig gøre at låne selve den digitale bog ud, uden også – ulovligt – at skulle låne søgeprogrammet mv. Efter pres fra biblioteksområdet blev denne retstilstand imidlertid ændret i sidste time før vedtagelsen af 1995-ophavsretsloven, idet § 19, stk. 3, andet pkt., nu gør udlån af edb-programmer mulig, hvis programmet "udgør en del af et litterært værk og udlånes sammen med dette". Med denne regel er det nu muligt for folkebibliotekerne at udlåne elektroniske ordbøger, der udelukkende indeholder litterære værker, selv om de afvikles

ved hjælp af programmel. Derimod er det ikke muligt at udlåne multimediaværker, der tillige indeholder andet end litterære værker, f.eks. fotos, levende billeder og musik.

I UBIS-udvalgets betænkning vedrørende Bibliotekerne i Informationssamfundet, nr. 1347/1997, foreslås denne bestemmelse udvidet, således at der på grundlag af en aftalelicens gives hjemmel til almindeligt udlån af edb-programmer. Forslaget blev ikke gennemført. Ved den ændring af ophavsretsloven, der fandt sted ved lov nr. 407 af 26. juni 1998, blev det derimod præciseret, at den legale programlicens i ophl. § 36, jf. nærmere afsnit 10.2.b., kan udøves af "den, der har ret til at benytte edb-programmet", hvilket også omfatter låneren.

Udlån og udlejning af programmer, der enten er i public domain eller som indgår i en sharewareordning, der omfatter Danmark, finder undertiden sted ved offentlige biblioteker og institutioner.

Library of Congress har i 1993 (men med senere ændringer) udsendt et sæt *regulations* om shareware, se tillige part 201, § 201.26. Efter disse bestemmelser kan rettighedshaveren gennem deponering i Library of Congress fastslå de vilkår, der skal gælde for et shareware-produkt. Bestemmelserne indeholder også en definition af shareware-begrebet. Dette begreb omfatter "copyrighted software which is distributed for the purposes of testing and review, subject to the condition that payment to the copyright owner is required after a person who has secured a copy decides to use the software". Tilsvarende defineres public domain som "software which has been publicly distributed with an explicit disclaimer of copyright protection by the copyright owner". Der er fastsat en afgift på 20$ for deponering i medfør af disse regler. Reglerne findes på <www.loc.gov>

Fremførelse

Som omtalt i afsnit 6.3.f. giver ophl. § 21, stk. 3, hjemmel til en særlig adgang til fremførelse af værker i digital form, nemlig i form af såkaldt præsensbenyttelse (til personligt gennemsyn eller studium på stedet ved hjælp af teknisk udstyr) på offentlige biblioteker. Denne adgang forudsætter, at det pågældende værk er offentliggjort, jf. ophl. § 8, stk. 1. De særlige problemer vedrørende bibliotekers brug af værker i digital form er behandlet i Vejledning til bibliotekerne om visse konsekvenser af den nye lov om ophavsret, udsendt af Statens Bibliotekstjeneste, 30. juni 1995.

6.3.e. Visning

Problemstillingen

I ophavsrettens første år havde eneretten til *eksemplarfremstilling* og til at *sprede* de fremstillede eksemplarer størst betydning. Behovet herfor blev navnlig aktualiseret af rotationspressen, der

skabte det første industrialiserede marked for værker, se hertil *Koktvedgaard* (2005), s. 19 ff. Men med fremkomsten af film, lydoptagelse og fonogramproduktion samt elektroniske medier som radio og tv opstod behovet for også at beskytte sådanne udnyttelsesformer. Dette behov blev løst gennem ophavsmandens eneret til at gøre værket tilgængeligt for almenheden.

I sin oprindelige skikkelse blev denne retsvirkning af ophavsretten formuleret som en ret til offentlig fremførelse eller visning. De to begreber henviste hver for sig til, hvordan forskellige typer af værker efter deres karakter kunne nå et offentligt rum: Et billede måtte i givet fald *vises*, et stykke musik *fremføres* etc. Alligevel var – og er – det begrebsteoretiske grundlag for denne sondring klart: En *fremførelse* indebærer, at værket når sit publikum gennem en aktiv proces. Denne proces kan foranstaltes af en udøvende kunstner, af en person, der yder en faktisk bistand eller af en teknisk anordning (f.eks. en radiosender). Derimod indebærer en *visning*, at værket blot placeres på en måde, hvor offentligheden kommer i kontakt med det, uden at denne kontakt i øvrigt forudsætter yderligere processer.

Hverken begreberne eller deres begrundelser var – og er – særligt skarpe, og det har længe været klart, at talrige udnyttelseshandlinger kan ligge i et grænseområde, der berører begge begreber. F.eks. er det almindeligt at tale om, at en film "vises" på tv, selv om den tekniske proces, hvorved denne visning gennemføres, netop indebærer en teknisk proces (udsendelseshandlingen) fra brugernes side. I takt med den teknologiske udvikling blev afgrænsningsspørgsmål som disse stadigt vanskeligere, og vanskelighederne kulminerede med udbredelsen af de Internetbaserede transmissionsformer med en sådan kompleksitet og retsusikkerhed, at der måtte en afklaring til.

WCT og Infosoc

Første skridt hen imod en afklaring blev nået med vedtagelsen af the WIPO Copyright Treaty i 1996. I opfølgning af denne traktat tog EU-kommissionen skridt til at foreslå det direktiv, der nu kendes som Infosoc-direktivet, og som i dag er indført ved den revision af ophl. § 2, der fandt sted i december 2002. Direktivet har dog ikke ført til nogen ændring i opfattelsen af visningsbegrebet. Der er således ikke taget stilling til, om det forhold, at et digitalt billede "vises" på en skærm i kraft af en på forhånd styret proces, hvorved elektroniske impulser og billedelementer (pixels) arbejder sammen, indebærer, at det, der udadtil fremstår som en "visning", i realiteten skal betragtes som en "fremførelse".

Udgangspunkt

I overensstemmelse med den opfattelse, der var gældende inden indførelsen af Infosoc-direktivet, må det antages, at det ophavsretlige begreb "visning" i den digitale verden også omfatter sådanne tekniske processer, der alene har til formål at simulere en visuel effekt, der modsvarer en ikke-elektronisk grafisk visning. Ligesom visningsbegrebet også omfatter den fysiske fremvisning af et eksemplar, der sker ved hjælp af en fysisk anordning (f.eks. et lysbilledapparat) må det antages, at visning ved hjælp af en pc og en lyskanon udgør "visning". Se hertil bemærkningerne i betænkning 1064/1986, s. 23. Her går grænsen så også. I det omfang den pågældende skærm anvendes under en proces, hvor billedets indhold løbende ændres eller tilpasses, bevæger man sig fra visningsbegrebet og over i begrebet fremførelse (og eventuelt også i det hertil hørende underbegreb, *communication to the public*). Se tilsvarende *Thomas Riis* (2002), s. 44 f.

Edb-programmer

Man kan på denne baggrund spørge, om et edb-program "vises" eller "fremføres" offentligt, når det afvikles fra en computer, hvortil offentligheden (f.eks. tv-seere, der ser en undervisningsudsendelse) har adgang. Ved afgørelsen af dette spørgsmål er det vigtigt at sondre. Hvis programmets *kildetekst* hentes frem på skærmen, og dette sker under en proces, hvor der ikke sker forandringer heri, vil der foreligge en visning. Indgår kildeteksten derimod i et dynamisk forløb, hvor der under afviklingen sker forandringer heri, vil der foreligge en fremførelse. Det forhold, at et program afvikles *uden* at man ser selve programinstruktionerne, vil i givet fald indebære en *fremførelse* af programmet, jf. nærmere om denne problemstilling i afsnit 6.3.f.

Under brugerens almindelige benyttelse af en applikation "vises" kun de tekstelementer og den lyd, som programmet er forberedt til at vise, og disse elementer rummer pr. definition ikke "programmet" (forstået som serien af koder til processoren), men de af programmøren udvalgte værkselementer til brugergrænsefladen. Disse værkselementer kan meget vel være beskyttet efter andre (ikke-programrelaterede) regelsæt, jf. nærmere afsnit 7.3. Typisk vil rettighedshaveren have sikret sig kontrol over selve programinstruktionerne ved at holde kildeteksten hemmelig.

Konsumption

Hvor fremførelse af et værk – bortset fra de i § 21 omhandlede tilfælde – kræver tilladelse fra ophavsmanden, kan værket "vises" offentligt, når det er *udgivet*, se ophl. § 20. Har man købt et eksemplar af et edb-program eller et andet værk i digital form, er det altså lovligt at vise dets informationsindhold, f.eks. ved at stille terminaler, der gør dette, til rådighed for offentligheden i forbindelse med kursusvirksomhed. Denne mulighed har dog be-

grænset betydning på programområdet, hvor muligheden for – meningsfuldt – at vise de instruktioner, der ligger på programmediet, er begrænsede. Derimod kan den have praktisk betydning ved brug af andre litterære værker i digital form, f.eks. fra hjemmesider.

6.3.f. Fremførelse

Problemstilling

I sit historiske udspring, jf. bemærkningerne herom s.619 f.*, har eneretten til offentlig fremførelse primært haft betydning for beskyttelsen af sceneværker, film og andre kunstneriske værker, som når deres publikum i kraft af en selvstændig *indsats* fra en udøvende kunstner: Et digt læses op, et teaterstykke opføres etc. Som nævnt kan en fremførelse også ske på grundlag af en ikke-kunstnerisk, ja ligefrem rent teknisk, proces. Da denne proces kan forløbe forskellig alt afhængigt af, hvilken type værk der er tale om, omfatter eneretten til fremførelse tilsvarende forskellige udnyttelsessituationer, alt efter hvilket værk man har at gøre med. Udnyttelsen af edb-programmer (der fremføres i en rent teknisk proces) sker f.eks. på en helt anden måde end udnyttelsen af en biograffilm (der fremføres ved hjælp af en filmfremviser, et videoapparat eller anden indretning) eller af et digt (der som nævnt kan fremføres ved at blive læst op).

I det følgende sættes fokus på disse forskellige udnyttelsessituationer. Når fokus rettes mod de enkelte udnyttelsessituationer er det væsentligt at sondre mellem *selve* fremførelsen og de *eksemplarfremstillinger*, der finder sted som led i den handling, hvorved værket fremføres.

Analytisk udgangspunkt

Ophavsretten er en meget stringent eneret, der stedse fokuserer på enkelte retspositioner. Selv om man befinder sig i en sammenhæng, som det kan føles naturligt at opfatte som en enhed, er det nødvendigt at forholde sig særskilt til de enkelte udnyttelseshandlinger, den indebærer. Når der f.eks. i forbindelse med en fremførelse af et værk også sker en eksemplarfremstilling af værket eller af dele af det, må forholdet således både vurderes som et tilfælde af *eksemplarfremstilling* og som et tilfælde af *fremførelse*.

Download og anden eksemplarfremstilling

Er der derimod alene tale om, at et værk *downloades* på brugerens udstyr, f.eks. en harrdisk eller MP3-afspiller, uden at der i den forbindelse *samtidig* sker en offentlig fremførelse, er fremførelsesretten uden selvstændig betydning. Det centrale i denne udnyttelse ligger i den eksemplarfremstilling, som her finder sted, og som der i de fleste tilfælde vil kræves tilladelse til, jf. de almindelige regler herom i afsnit 6.3.a.

Edb-programmer

Edb-programmer hører til den kategori af litterære værker, der alene tjener tekniske funktioner. For at få nytte af et edb-program er det nødvendigt at gøre programmet til genstand for en teknisk proces som nærmere beskrevet i kapitel 3. Som nævnt s. 311 må det antages, at brugerens anvendelse af et edb-program i ophavsretlig forstand indebærer en fremførelse. Denne antagelse har rod i betænkning 1064/1986, der tilsvarende antager, at en gengivelse af selve kildeteksten (eller – måske af mindre interesse – af objektkoden) i givet fald ville udgøre en "visning". Antagelsen kan forekomme forskruet, eftersom man er langt fra de begrundelser, der i sin tid lå bag fremførelsesbegrebet. Men den er ikke langt fra de eksempler på fremførelse, der angives i ophl. § 2, stk. 4, nr. 1. Ved at medtage denne udnyttelseshandling under den ophavsretlige eneret tilføjes et element, som har betydning, hvor en udnyttelse ikke er udtømt med de eksemplarfremstillinger, der finder sted under benyttelsen af programmet, f.eks. fordi der er tale om at benytte programmets *funktioner* (offentligt) i en situation, hvor retten til disse eksemplarfremstillinger er hjemlet.

Streaming og webcasting

Stilles værket til rådighed for brugere i et offentligt rum på en sådan måde, at brugerne kan benytte det ved såkaldt *streaming*, dvs. under en proces, hvor overførelsen finder sted samtidig med at værket opleves, foreligger en fremførelse. Når en radio- eller tv-udsendelse formidles på denne vis taler man om *web-casting* (et begreb der viderefører begrebet *broadcasting*, som anvendes inden for radiofoni) Da radiofonier (dvs. virksomheder, der udfører broadcasting) har mulighed for at opnå aftalelicens efter reglerne i ophl. §§ 30-31, har begrebet selvstændig betydning. Streaming kan dog også forekomme uden for radio- og tv-området, f.eks. i forbindelse med brug af transmission af begivenheder ved hjælp af web-kamera mv. Her er der ikke tale om, at værket (eller den beskyttede frembringelse der er tale om) gøres til genstand for en eksemplarfremstilling. Derimod vil denne transmissionsform udgøre en fremførelse, eftersom der er tale om en proces, der bringer værket frem til brugeren, jf. de generelle bemærkninger herom s. 322. Anderledes hvis radiostationen alene stiller sine programmer til rådighed med henblik på download, f.eks. til en MP3-afspiller. En sådan "*podcasting*" må alene betragtes som en foranstaltning, der muliggør eksemplarfremstilling af de pågældende værker (filer).

"Communication to the public"

Med indførelsen af Infosoc-direktivet ved lov nr. 1051 af 17. december 2002, er ophl. § 2, stk. 2, nr. 3, forsynet med en yderligere underinddeling af fremførelsesbegrebet. På grundlag af direktivets art. 3 er der indført et nyt begreb, der i direktivets engel-

ske tekst betegnes som "*communication to the public*", og som i dansk sprogbrug har fået betegnelsen "overføring til almenheden" (om end den engelske sprogbrug også anvendes i dansk sprogbrug). Med dette begreb sigtes navnlig til Internet-transmissioner, der igangsættes ved at brugeren *selv* ("on demand") sætter den tekniske proces i gang, der udvirker dataoverførelsen, f.eks. aktiverer et link. Heri ligger nemlig en central forskel mellem Internet-brug af værker og den traditionelle æterbårne radiotransmission. Hvor radiotransmission indebærer en ophavsretlig brug af værket allerede i den proces, hvorved værket via lydbølgerne bringes ud i atmosfæren, ville man uden præciseringen i § 1, stk. 4, nr. 1, kunne argumentere for, at der jo ikke var sket nogen fremførelse af værket ved at dette lægges tilrette på en server med henblik på senere brug, eftersom den udnyttelseshandling, der i ophavsretlig (og økonomisk) henseende har interesse, jo først indtræder, når brugeren rent faktisk foretager sig noget for at hente værket.

Udsendelse

Det fremgår af ophl. § 2, stk. 4, nr. 1, at udsendelse i radio og fjernsyn er en delmængde af begrebet "overføring af værker til almenheden". Det eneste punkt, hvormed denne udnyttelse adskiller sig fra de øvrige eksempler på overføring af værker til almenheden, ligger i det manglende *on demand*-element.

Linking mv.

Hverken ophl. eller Infosoc-direktivet tager stilling til, om det falder inden for ophavsmandens eneret at etablere et link til et værk, der befinder sig på nettet. Hvis det pågældende værk udgør et ulovligt eksemplar, er dette spørgsmål uden selvstændig betydning, idet et link, der peger hen til værket, da vil udgøre en medvirkenshandling, der kan sanktioneres særskilt, hvis der foreligger den fornødne uagtsomhed, se nærmere hertil afsnit 17.1.d. Men spørgsmålet har praktisk betydning i de tilfælde, hvor værket befinder sig på nettet i kraft af rettighedshaverens samtykke.

Det kan måske umiddelbart undre, at rettighedshaveren kan have et ønske om at modsætte sig, at andre således linker hen til et værk, rettighedshaveren selv har placeret. Men ønsket kan være begrundet i markedsføringshensyn eller i rettighedshaverens interesse i at være eneste kilde til det pågældende værk. Dernæst kan rettighedshaveren være interesseret i at undgå en bevisførelse om, hvorvidt der ved *ulovlig* brug foreligger den fornødne subjektive tilregnelse (forsæt eller uagtsomhed) hos den, der linker til et ulovligt eksemplar af et værk, men som gør gældende, at han anså dette eksemplar for lovligt. Derfor har spørgsmålet praktisk betydning.

Vurderingen af dette spørgsmål er faldet forskelligt ud ved de retsinstanser, der har bedømt det. I *U 2001.1572 V* fandt Vestre Landsret med tvivlsom føje, at to unge mennesker ved at oprette direkte links til musiknumre, som andre ulovligt havde uploadet, selvstændigt havde "tilgængeliggjort musiknumrene for almenheden på en måde, der måtte sidestilles med offentlig fremførelse, jf. ophavsretslovens § 2". Et tilsvarende resultat nåede Högsta Domstolen til i *NJA 2000.292*. Disse afgørelser bør dog ikke betragtes som gældende dansk ret, og senere praksis fra Vestre Landsret har da også undladt at gentage denne fortolkning, se herved *U 2005.60 V*. Det forekommer anstrengt at tale om, at der her sker en visning eller *fremførelse*. Selv om *fremførelsesbegrebet* – som fremhævet af Högsta Domstolen – i sin tid blev indført for at dække udnyttelseshandlinger, der er komplementære til eksemplarfremstilling, forudsætter fremførelsen en teknisk proces (eller kunstnerisk fortolkning el.lign.), der er andet og mere end blot dette at vise værket frem (hvilket et link jo ikke gør i sig selv). En sådan proces er det vanskeligt at få øje på, blot ved at der etableres et link til værket. Skulle selve denne link antages at være en fremførelse, måtte det være nærliggende også at antage, at den henvisning til værket, der sker gennem offentliggørelsen af linket i en bog eller avisartikel, vil være en fremførelse. Et sådant fortolkningsresultat vil føre til uantagelige konsekvenser.

Derfor er det velbegrundet, at den norske Høyesterett med sin (enstemmige) dom i *Rt. 2005.41* udtrykkeligt har lagt afstand til denne retsopfattelse. I dommen (præmis 53) betones blandt andet det forhold, at de pågældende musikfiler ubesværet kunne være hentet gennem brug af web-adresserne for de pågældende udbydere, altså uden det mellemliggende link. Og i lyset af det straf- og erstatningsansvar, der følger med antagelsen om, at et link skulle være retsstridig, medens den direkte henvisning skulle være lovlig, bør der – som fremhævet af retten – kunne gives "en noenlunde tilfredsstillende begrunnelse for hvorfor bruk av den ene metoden rammes, men ikke den andre." Retten tilføjer i den forbindelse, at rettighedshaverne ikke har kunnet give nogen tilstrækkelig begrundelse for dette.

Konsumption

Den eneret, rettighedshaveren har til fremførelse af et program, modificeres, når programmet er "udgivet", hvilket det er, jf. § 8, stk. 2, "når eksemplarer af værket med ophavsmandens samtykke er bragt i handelen eller på anden måde spredt blandt almenheden". Ifølge ophl. § 21 kan et udgivet værk, som ikke er et sceneværk, fremføres offentligt ved lejligheder, hvor tilhørerne

eller tilskuerne har adgang uden betaling, hvis fremførelse ikke er det væsentlige ved den pågældende foranstaltning, og hvis denne ikke finder sted i erhvervsøjemed.

Bestemmelsen er ikke formuleret med sigte på edb-programmel og andre værker i digital form, men finder desuagtet anvendelse også for sådanne værker. For at en sådan anvendelse kan gennemføres, må begreberne tilpasses. Det er således nærliggende at læse kravet om "adgang" til også at indbefatte tilfælde, hvor der er tale om en rent telematisk forbindelse, f.eks. til en hjemmeside, hvor værket befinder sig. Hvis formålet med den pågældende hjemmeside ikke udelukkende er at fremføre det pågældende værk, vil retten til at gennemføre en sådan fremførelse således være konsumeret. Problemet kan få betydning, hvis fremførelsen kan finde sted uden brug af en samtidig eksemplarfremstilling af værket. Konklusionen har dog beskeden praktisk betydning, hvis det netop antages, at læsningen af værket på brugerens skærm udgør en eksemplarfremstilling, jf. bemærkningerne herom i afsnit 6.3.b.

Der gælder en udvidet adgang til offentlig fremførelse, når fremførelsen sker til brug ved gudstjeneste eller – hvad der har større praktisk betydning på IT-området – undervisning, se hertil § 21, stk. 1. Rettighedshaveren kan altså ikke modsætte sig, at et udgivet programværk benyttes i forbindelse med en demonstration til undervisningsbrug, selvom der er tale om kommerciel kursusvirksomhed. Adgangen til fremførelse i kommerciel undervisningsvirksomhed gælder dog ikke databaser, jf. § 21, stk. 2, andet led, der blev indsat i ophavsretsloven ved lov nr. 407 af 26. juni 1998, og som indfører databasedirektivets art. 6, stk. 2, litra b. Erhvervsmæssig undervisningsmæssig brug af et multimediaværk, der sker for en offentlig forsamling, kræver altså tilladelse fra rettighedshaveren.

Præsensbenyttelse

Til bestemmelsen føjer sig som allerede nævnt en særlig regel om bl.a. udgivne digitale værker, § 21, stk. 3. Sådanne værker kan stilles til rådighed for enkeltpersoner på offentlige biblioteker til personligt gennemsyn eller studium på stedet ved hjælp af teknisk udstyr (*præsensbenyttelse*). At disse værker skal være "offentliggjorte" indebærer, at biblioteket mv. også kan stille digitale værker til rådighed for omverdenen, såfremt bibliotekets udnyttelsesret til disse værker baserer sig på en *licensaftale* med rettighedshaveren (eller dennes repræsentant), medmindre den indgåede aftale direkte forbyder en sådan anvendelse. Før december 2002, hvor bestemmelsen blev ændret som følge af Infosocdirektivet, var bibliotekernes adgang til præsensbenyttelse be-

tinget af, at værket var udgivet, jf. ophl. § 8, stk. 2. Værket skulle med andre ord være spredt blandt almenheden. Med den nye formulering er det også muligt at udlåne et værk, der (lovligt) er hentet ned fra en database. Eksemplarfremstilling af sådanne værker er dog alene tilladt i det omfang dette følger af andre regler, herunder ophl. § 11a, stk. 1 (der dog ikke omhandler edb-programmer og databaser, jf. stk. 2).

6.3.g. Udstrækning i tid og rum

Varighed

I tid vedvarer ophavsretten til et litterært værk, jf. ophl. § 63, indtil 70 år er forløbet efter ophavsmandens dødsår eller – for fællesværkers vedkommende – til den længstlevende med-ophavsmands dødsår. Hvis værket er offentliggjort uden ophavsmandens navn, alment kendte pseudonym eller mærke, varer ophavsretten, indtil 70 år er forløbet efter udløbet af det år, da værket blev offentliggjort, ophl. § 63, stk. 2. Da talrige programværker markedsføres uden angivelse af navnet på de medvirkende ophavsmænd, vil ophavstiden ofte skulle beregnes fra offentliggørelsestidspunktet. Selve dette kan være et argument for at kreditere programforfattere.

I de tilfælde, hvor ophavsmandens navn er angivet ved offentliggørelsen, kan denne gyldighedstid blive ganske langvarig. For programmer, der bearbejdes, jf. ophl. § 4, stk. 1, som led i en teknisk vedligeholdelse eller opdatering, vil ophavsretten til det bearbejdede program bestå indtil 70 år efter dødsåret for den ophavsmand, der har stået for det seneste bidrag, det være sig til den oprindelige eller omarbejdede version. For programmer, der har basal betydning (f.eks. styresystemer og kompiler-programmer/oversættere til programmeringssprog), kan dette give en ganske langvarig reel beskyttelsestid. F.eks. blev grundlaget for UNIX-styresystemet lagt allerede i midten af 1960'erne.

Territorium

Dansk ophavsret kan kun håndhæves inden for *dansk territorium*. Mangfoldiggøres et dansk værk ulovligt i Tyskland, må denne krænkelse retsforfølges i Tyskland. I kraft af de førnævnte internationale konventioner beskyttes værket imidlertid efter visse minimumsregler.

Disse problemer opstår primært i relation til piratkopiering i lande, der ikke håndhæver reglerne om minimumsbeskyttelse. Med sigte herpå hjemler ophl. § 77 bødestraf for indførelse af eksemplarer af visse værker (herunder programmer), der er fremstillet uden for Danmark under sådanne omstændigheder, at en tilsvarende fremstilling i Danmark ville være i strid med loven,

hvis indførelsen sker med henblik på at gøre disse eksemplarer tilgængelige for almenheden. Bestemmelsen tillader med andre ord import af værker mv., der set i forhold til dansk ophavsret (men derimod ikke stedets ophavsret) er kopieret i udlandet på en måde, der ikke ville være lovlig i Danmark, *uanset* om denne udlandskopiering målrettet tager sigte på indførelse af værket i Danmark med henblik på erhvervsmæssig anvendelse. Det eneste, den forbyder, er indførelse af værker med henblik på distribution mv. (tilgængeliggørelse) i Danmark.

Hvis begrebet "indførelse" ikke også omfatter den situation, der foreligger, når en person i Danmark under de i bestemmelsen nævnte omstændigheder henter et værk hjem fra en fremmed database, f.eks. via World Wide Web, vil man hermed have åbnet et hul i ophavsretsloven, som for næsten enhver betragtning må siges at være uacceptabelt. Man vil nemlig da kunne forestille sig, at der i områder af verden, der ikke anerkender nogen ophavsretlig beskyttelse, blev etableret databaser med de kommercielt mest interessante værker (herunder edb-programmer) fra vor egen civilisation. Disse værker kunne herefter kvit og frit hentes hjem af private og erhvervsmæssige brugere, blot dette ikke skete med henblik på tilgængeliggørelse for almenheden. Selv om rettighedshaveren ikke er sikret nogen generel "importret", har et sådant hul i den ophavsretlige beskyttelse aldrig været tilsigtet. Som jeg nærmere har redegjort for i NIR 1995.616 ff., må forholdet betragtes således, at der foretages *eksemplarfremstilling* af værket i Danmark, når en bruger i Danmark henter værket ned fra hjemmesiden; ikke, at værket fæstnet på et medium "indføres" sammen med mediet.

I forbindelse med indførelsen af ophavsretsloven af 1995 blev det bl.a. overvejet at indføre en importret for rettighedshaveren, men Kulturministeriet ønskede ikke en sådan regel indført.

6.3.h. De ideelle rettigheder

Efter ophl. § 3 har ophavsmanden krav på at blive navngivet i overensstemmelse med, "hvad god skik kræver". Navngivelsen skal såvel ske på eksemplarer af værket, som når dette gøres tilgængeligt for almenheden. Ligeledes er det bestemt, at værket ikke må "ændres eller gøres tilgængeligt for almenheden på en måde eller i en sammenhæng, der er krænkende for ophavsmandens litterære eller kunstneriske anseelse eller egenart".

Da denne personlige side af ophavsretten pr. definition ikke har økonomisk betydning, ofres den sjældent den store interesse

i den stærkt konkurrenceprægede IT-branche. Rådsdirektivet om retlig beskyttelse af programmer forudsætter vel i art. 2, stk. 3, at de personlige rettigheder eksisterer, når man i denne bestemmelse alene lader de "økonomiske" rettigheder til et program udviklet under et ansættelsesforhold tilfalde arbejdsgiveren. Men i øvrigt gælder der en almindelig antagelse, hvorefter *droit moral* ikke spiller nogen større rolle for programmel. Se f.eks. EU-kommissionens Grønbog om ophavsret (1989), pkt. 1.4.9 og 5.6.27, *Koktvedgaard* (1999), s. 116, Betænkning 1064/1986, s. 64 f., *Schmidt* (1989), s. 50 ff. og *Blume*: Retsbeskyttelse af edb (1989), s. 29, men derimod *Simon Newman* i 13 CLSR 96 (1997).

Edb-programmer

Når man diskuterer *droit moral* for programmer, er det vigtigt at præcisere, hvilke aspekter af programmet der drøftes. Tænkes der på programmets uddata (f.eks. i form af skærmbilleder og lyd), kan den kreative proces tænkes at resultere i en mangfoldighed af litterære og kunstneriske værker, der – trods det, at de "findes" i et program – ikke udgør et programværk. Helt tydeligt er dette på multimedia-området, men også i relation til de programmer, der afvikles på moderne softwareapplikationer, hvor lagerkapaciteter ikke lægger begrænsninger i omfanget af den programkode, der kan overdrages. Udbredelsen af populære spilprogrammer må utvivlsomt tilskrives disse kvaliteter, og på dette område er det da også fast praksis, at ophavsmændene krediteres på samme måde som ved filmværker, enten ved programmets opstart eller ved at brugeren kan kalde en særlig menu, hvor bidragydernes navne ruller ned.

Det vanskelige problem om *droit moral* angår den kreativitet, der kommer til udtryk i selve kildeteksten. Her kan det – i dag – være vanskeligt at sige noget klart om, hvad der er "god skik". Formentlig er området i bevægelse, måske på grund af praksis på multimedia-området, måske fordi en navngivning alt andet lige vil sikre en længerevarende beskyttelse, jf. ophl. § 63, stk. 2. Programudbyderne synes ikke at følge noget mønster for forfatterkrediteringer i programmel, der er så fast, at man på forhånd kan fastlægge de gældende grænser. Enkelte programmer er ligefrem opkaldt efter deres ophavsmand (dette gælder f.eks. *Peter Norton*s utilities til PC-systemer), og i visse tilfælde krediteres programmøren ved programmets opstart eller ved aktivering af en særlig kommando i programmet, ligesom på multimedia-området.

Open Source-løsninger

En særlig problemstilling vedrørende kreditering er opstået inden for markedet for open source-programmel, jf. nærmere redegørelsen i afsnit 9.4.b. Som her anført er det en væsentlig

komponent i de licensvilkår, der ledsager sådanne programmer (f.eks. de, der markedsføres under GNU-GPL), at licenstageren skal sikre bibeholdelsen af ophavsmandens navn i kildeteksten. Baggrunden herfor ligger i, at ophavsmandens incitament til at deltage i udviklingen af disse programmer bl.a. motiveres med ønsket om at opnå den anerkendelse, senere brugere og videreudviklere vil vise, f.eks. når programmet anvendes som grundlag for bearbejdning og videreudvikling. Da formålet med at distribuere programmel under *open source*-licenser netop er at bidrage til den almindelige udveksling af informationer, befinder man sig i det klassiske område for såvel citatret som kreditering, jf. tilsvarende *Folker* i NIR 2005.174 f.

Multimedier mv.

Særlige spørgsmål om *droit moral* opstår, når værker anvendes og vises ved hjælp af medier, der ikke tillader en fuldstændig, endsige teknisk korrekt, gengivelse. Hvis et maleri eller en filmsekvens f.eks. skal anvendes i et digitalt leksikon, vil det med nutidens teknologi ikke være muligt at undgå et vist kvalitetstab. I *U 1997.975 Ø* tog Østre Landsret stilling til, om beskæring af filmværker i forbindelse med fremvisning på tv er uberettiget i medfør af ophl. § 3, stk. 2. Sagen var rejst af en amerikansk filminstruktør, hvis film, *Three Days of the Condor*, var blevet vist i dansk tv i en såkaldt panscannet udgave, hvorved tv-formatets mere kvadratiske billede flytter sig frem og tilbage over cinemascope-formatets mere rektangulære billedformat. Landsretten slog fast, at tilpasning ved panscanning af widescreen medførte bortskæring af en betydelig del af billederne med den følge, at billedkompositionen i en række sekvenser måtte betragtes som "lemlæstede", at detaljer af betydning for personkarakteristikken var udgået, og at der var opstået uoverensstemmelser mellem billeder og dialog. Den omfattende beskæring havde ikke været teknisk nødvendig for at muliggøre filmens visning på tv, idet filmen havde kunnet vises i det originale format, om end i et mindre billede. Derfor fandtes denne brug af værket i sig selv at udgøre en krænkelse af kunstnerens anseelse og egenart, jf. ophl. § 3, stk. 2. Rettens bemærkning om, at den omfattende beskæring ikke havde været teknisk nødvendig, indicerer, at fremvisningen af et kunstnerisk værk i digital form på en skærmterminal ikke i sig selv indebærer en krænkelse af *droit moral*.

Lønmodtagerproblemet

Spørgsmålet om *droit moral* er ofte inddraget i debatten om lønmodtageres ophavsret til programmel, der dog ikke har ført til faste retningslinier for ophavsretlig kreditering mv. At man ofte krediterer programmøren i programmets kildetekst, skyldes primært den teknisk begrundede interesse i at kunne finde frem til

programmøren med henblik på tekniske afklaringer. Problemet har dog fået fornyet aktualitet med multimedia-produkterne. Der er imidlertid det væsentlige samspil mellem *droit moral*- og lønmodtagerproblematikken, at den arbejdsgiver, der ikke krediterer sine medarbejdere for kreative frembringelser, vil fremstå mindre troværdig, når han efterfølgende – for at opnå ophavsretlig beskyttelse – vil hævde, at disse frembringelser har kunstnerisk karakter. Ligeså åbenbart det er at angive navnet på møbelarkitekten, i markedsføringen for den arkitekttegnede stol, ligeså nærliggende bør det være for den industrielle multimedia-producent at kreditere de medarbejdere, der står bag værkets æstetiske kvaliteter.

Art. 9 i TRIPS-protokollen undtager udtrykkeligt "moral rights" fra henvisningen til Bernerkonventionen.

6.3.i. Rettens håndhævelse

Håndhævelsen af ophavsretten til et programværk sker efter samme regler som dem, der gælder for håndhævelsen af andre retsbeskyttede værker, jf. ophl. kapitel 7 og *Koktvedgaard* (2005), kapitel VIII. De retsmidler, der står til rådighed, er fogedforbud, straf, tilintetgørelse (hvilket primært har betydning overfor pirateri), inddragelse, konfiskation, godtgørelse og erstatning. Som hovedregel skal disse retsmidler effektueres efter rettighedshaverens initiativ, og det er derfor vigtigt at vide, hvilke fordele og ulemper de hver for sig byder på.

Fogedforbud

Reglerne om fogedforbud følger af rpl. kapitel 57 (§§ 641 ff.) og giver fogedretterne mulighed for at pålægge private mv. "at undlade handlinger, som strider mod rekvirentens ret". Som betingelse for forbuds nedlæggelse kan fogedretten bestemme, at rekvirenten skal stille sikkerhed for den skade og ulempe, som kan påføres rekvisitus ved forbuddet. For den lille rettighedshaver er de sikkerhedsbeløb, fogedretterne kræver, ganske høje. Er rettighedshaveren i tvivl om mulighederne for at gennemføre sit krav, kan dette tale for ikke at gå denne vej, men i stedet anlægge almindeligt søgsmål med påstand om anerkendelse af retten.

Beslaglæggelse

Rpl. § 645, stk. 2, giver fogedretten hjemmel til at beslaglægge rørligt gods, "såfremt det anvendes eller har været anvendt ved overtrædelse af forbuddet, eller såfremt der er bestemte grunde til at antage, at det vil blive anvendt til sådant formål". Med henvisningen til "rørligt gods" kræves det, at bestemmelsen kun kan anvendes i relation til det medium, hvorpå programmel og andre værker i digital form manifesteres, f.eks. CD-skiver. Beslaglæg-

gelse kan betinges af sikkerhedsstillelse, og det bestemmes ved dommen i den senere forbudssag, hvorledes der skal forholdes med det beslaglagte gods, rpl. § 649, stk. 1. Det kan enten tilbagegives til rekvisitus eller konfiskeres. Sker der konfiskation, kan det konfiskerede efter anmodning anvendes til dækning af rekvirentens erstatningskrav.

Ved forordning 3295/94, EFT 1994 L 341/8 har Rådet givet regler om foranstaltninger med henblik på at forbyde overgang til fri omsætning mv. af varemærkeforfalskede og piratkopierede varer. Forordningen, der træder i stedet for forordning nr. 3482/86, gør det muligt for en rettighedshaver at få toldvæsenets bistand til at hindre indførelsen af varer, der krænker visse immaterialrettigheder, hvorved rettighedshaveren undgår selv at skulle retsforfølge hver enkelt krænker. Men hvor 1986-forordningen kun gav hjemmel i relation til varemærkeforfalskninger, gælder den nye forordning også for krænkelser af ophavsrettigheder og mønsterrettigheder. Begrebet "piratkopierede varer" defineres som "varer, som er eller indeholder kopier, som er fremstillet, uden at indehaveren af ophavsretten eller de beslægtede rettigheder eller indehaveren af en rettighed til et design eller mønster (mønsterindehaveren), hvad enten det er registreret under national ret eller ej, eller en af denne gyldigt bemyndiget person i fremstillingslandet har samtykket heri, dersom fremstillingen af disse kopier krænker den pågældende rettighed ifølge lovgivningen i Fællesskabet eller i den medlemsstat, hvor toldmyndighederne er blevet anmodet om at gribe ind." Toldmyndighederne har ret til at gribe umiddelbart ind over for varer, der mistænkes for at være piratkopierede eller varemærkeforfalskninger uden at skulle afvente udfaldet af en national retsafgørelse. Den rettighedshaver, der mener sig krænket, henvender sig til toldmyndighederne, og en sådan indgriben kan i givet fald betinges af, at den berettigede stiller sikkerhed.

Straf

Hjemmel til at pålægge straf for ophavsretlige retskrænkelser findes i ophl. §§ 76-80. Hovedreglen om straf for krænkelse af de økonomiske rettigheder følger af § 76, der som udgangspunkt giver hjemmel for bødestraf. Bestemmelsens andet stykke giver dog under kvalificerede omstændigheder mulighed for at idømme straf i form af fængsel indtil 1 år og 6 måneder. Bestemmelsen hjemler ligeledes straf, hvis gengivelsen eller eksemplarfremstillingen er begået forsætligt og under skærpende omstændigheder. Skærpende omstændigheder anses navnlig for at foreligge, hvis overtrædelserne sker erhvervsmæssigt, hvis der fremstilles eller blandt almenheden spredes et betydeligt antal eksemplarer, eller hvis værker og frembringelser gengives på en sådan måde, at almenheden får adgang til dem på et individuelt valgt sted og tidspunkt, jf. § 2, stk. 4, nr. 1, 2. led. Se herved *TfK 2001.615 Ø*, hvor T, som havde fremstillet mindst 5.424 cd'er

ved ulovlig kopiering (og solgt mindst 2.419 af disse), blev idømt en bøde på kr. 25.000 samt udbyttekonfiskation af kr. 60.000 og af det anvendte udstyr.

Foruden denne strafhjemmel foreskriver strfl. § 299b straf med fængsel indtil 6 år for den, der for derigennem at skaffe sig eller andre uberettiget vinding eller som i øvrigt under særligt skærpende omstændigheder gør sig skyldig i ophavsretskrænkelser af særlig grov karakter, jf. ophl. § 76, stk. 2, eller ulovlig import af særlig grov karakter, jf. ophl. § 77, stk. 2. Bestemmelsen blev indsat efter forslaget i betænkning 1417/2002, se herved s. 74 ff. og 147 ff. I forslaget betones netop det behov, der er for at strafsanktionere ophavsretsstridige handlinger begået på internettet.

At forsætskravet ofte volder vanskeligheder i sådanne sager, viser Københavns Byrets dom af 4. december 1995: Indehaverne af et anpartsselskab, der solgte edb-udstyr, var tiltalt for overtrædelse af ophavsretslovens regler ved at have solgt ulovligt kopierede eksemplarer af MS-DOS- og Windows-styresystemerne til en samlet værdi af 2.252.803 kr. De tiltalte nægtede sig skyldige, idet de påberåbte sig ukendskab til, at de pågældende programmer var ulovligt kopierede. De pågældende programpakker var ikke forsynet med det hologram, som Microsoft benytter til at certificere programpakkers lovlighed, men Microsoft havde ikke altid fulgt denne praksis. Under henvisning til bevisusikkerheden om de tiltaltes forsæt til at begå ophavsretsbrud blev begge frifundet.

Inddragelse mv.

Foruden disse retsmidler kan den forurettede i medfør af ophl. § 84 få dom for, at eksemplarer af værket skal inddrages til fordel for ham eller overdrages til ham mod et vederlag, der ikke overstiger fremstillingsomkostningerne. I stedet for inddragelse eller overdragelse kan det bestemmes, at eksemplarerne helt eller delvis skal tilintetgøres eller på anden måde gøres uanvendelige til ulovlig brug, § 84, stk. 2. Denne bestemmelse vil ofte kunne anvendes i tilfælde af ulovlig programanvendelse, idet "tilintetgørelsen" blot kan ske ved effektiv sletning eller overskrivelse af det pågældende programmedium.

Erstatning

Reglerne om erstatning for krænkelser af en ophavsret findes i ophl. § 83, stk. 1. Ifølge denne bestemmelse har den, som forsætligt eller uagtsomt overtræder en af de i §§ 76 og 77 nævnte bestemmelser, pligt til at udrede rimeligt vederlag for udnyttelsen samt erstatning for den yderligere skade, som overtrædelsen måtte have medført. I overensstemmelse med den almindelige culparegel stilles der altså kun krav om (simpel) uagtsomhed. I praksis er det imidlertid sjældent den subjektive tilregnelse (skyldgra-

den), der volder tvivl, men derimod tabets opgørelse. Praksis på dette punkt lægger vægt på, hvilke oplysninger der foreligger om den konkrete udnyttelse. Savnes der præcise oplysninger herom, udmåles ofte runde beløb i erstatning, se f.eks *U 1999.326 Ø*, hvor Microsoft fik tilkendt 1 mio. kr. i erstatning for piratkopierede programmer udført af en forhandler, *U 1983.976 Ø*, der i en sag om piratkopiering af videofilm tilkendte en erstatning på 1,2 mio. kr., *U 2001.1572 V*, der pålagde en 15-årig dreng at betale 100.000 kr. i erstatning og godtgørelse for ikke-økonomisk skade forvoldt ved etablering af links til piratkopierede musikværker og *U 2005.1393 H*, der idømte et kopicenter erstatningsansvar for 400.000 kr. for i "mindst" 349 tilfælde at have kopieret faglitterære værker ulovligt.

U 2005.60 V

Er der derimod mere præcise oplysninger på bordet (hvilket ofte vil være tilfældet, hvis krænkelsen er begået på nettet, hvorfra der foreligger log-oplysninger om tidspunkt, værkstype mv.), er der grundlag for en tilsvarende mere præcis tabsopgørelse. Et illustrerende eksempel herpå er dommen i *U 2005.60 V*. I denne sag var det oplyst, at der havde været i alt 2.673 registrerede brugere på den pågældende hjemmeside, hvoraf 20% (svarende til 535 personer) måtte antages at have udvekslet ulovlige kopier af film indbyrdes. Retten statuerede, at hovedparten af de ulovligt kopierede og udvekslede film var nyudgivne film, der ville have været solgt til fuld pris, hvis de var blevet solgt som DVD-film. Under hensyn hertil og til, at film i DivX-format kvalitetsmæssigt ligger meget tæt på DVD-film, fandt retten det forsvarligt at fastsætte salgsprisen til gennemsnitligt 100 kr. pr. film excl. moms: "Da denne salgspris også indeholder udgifter til fremstilling og distribution samt andre driftsudgifter, skal det rimelige vederlag, som appellanterne har krav på, fastsættes til et lavere beløb svarende til dækningsbidraget. På baggrund af de oplysninger om størrelsen af de variable omkostninger, som appellanterne fremkom med i byretten, fastsættes disse til 30 kr. Det rimelige vederlag, som tilkommer appellanterne, opgøres skønsmæssigt og angår ulovlig kopiering på en måde, som appellanterne efter det oplyste ikke ville have tilladt selv mod vederlag." Det rimelige vederlag blev herefter fastsat til 70 kr. pr. film excl. moms.

- markedsforstyrrelse

Et særligt problem i opgørelsen af den erstatning, der tilkommer rettighedshaveren som følge af en immaterialretlig krænkelse, angår erstatningen for den såkaldte markedsforstyrrelse. Hermed forstås generelt det tab, den krænkede lider ved ikke længere at kunne sælge sine produkter til den højere pris, markedet forventede inden retskrænkelsen, sml. *Koktvedgaard* (2005), s. 463.

Denne udgiftspost har primært betydning på et marked, hvor der foregår en reel konkurrence mellem lovlige og ulovlige produkter, og hvor rettighedshaveren derfor tvinges til at sætte sine priser ned, når der opstår en konkurrence med et plagiatprodukt, der udbydes på samme måde som originalproduktet, se f.eks. *U 2004.1302 H* om en nederdel, *U 2004.1085 H* om et reolsystem og *U 2001.747 H* om en barnestol. Man bør derimod nære skepsis overfor denne post, når værker krænkes ved, at eksemplarer i rent digital form gratis stilles til rådighed på nettet. I disse tilfælde er det klart for brugeren, at han foretager sig noget ulovligt, og typisk vil udsigten til et erstatnings- og strafferetligt ansvar afskrække ham fra at erhverve det ulovlige eksemplar. I Konkurrencestyrelsens Konkurrenceredegørelse fra juni 2005, s. 149, er det f.eks. lagt til grund, at piratkopiering kun har begrænset indflydelse på det lovlige salg af cd'er. Hertil kommer, at den pris, piratbrugeren sparer ved ikke at købe værket, ofte vil være så høj, at han aldrig ville have erhvervet værket på lovlig vis i det omfang han har erhvervet værket ved ulovlig kopiering. Derfor har markedsforstyrrelsen på piratområdet en helt egenartet karakter, som gør det påkrævet at afprøve dens præmisser i hver enkelt situation, således som det også skete i *U 2005.60 V*, hvor retten nægtede Dansk Journalistforbund erstatning for markedsforstyrrelse ("da vederlaget for undertekster til DVD-film ikke relaterer sig til antallet af solgte DVD-film").

- kontroludgifter

I nær forbindelse med erstatningen for markedsforstyrrelse er den erstatning, rettighedshaveren efter omstændighederne kan opnå for sine kontrolforanstaltninger, dvs. som en andel af hans udgifter til at overvåge, om krænkelser finder sted. Dansk retspraksis anerkender, at en sådan udgiftspost – der udelukkende kan henføres til de ulovlige handlinger, der er tale om at retsforfølge – kan fradrages. Det siger sig selv, at en sådan erstatning nødvendigvis – for det første – må være skønsmæssig, og at det nødvendige skøn – for det andet – kan anlægges efter forskelligartede kriterier: Hvor nogle domme har foretaget en helt skønsmæssig vurdering (se f.eks. *U 2001.1572 V* og *U 2005.60 V*), synes andre domme at binde erstatningsvurderingen op på en numerisk opgørelse over antallet af ulovlige kopier mv. Således fandt *U 2005.60 V*, at den ulovlige kopiering af film havde påført rettighedshaverne "yderligere skade i form af udgifter til kontrol mv. og i form af tab som følge af markedsforstyrrelse på grund af den yderligere ulovlige udbredelse af de film, appellanterne har ophavsretten til." Retten fandt herefter, at erstatningen for mar-

kedsforstyrrelse mv. måtte udmåles til et beløb svarende til vederlaget, dvs. efter et princip om "dobbelt op".

- skønsafvejningen

Som anført oven for giver sager om erstatning for ophavsretlige krænkelser anledning til usikkerhed på grund af de mange skønselementer, der indgår i de enkelte erstatningsposter: Hvor meget er værket blevet kopieret? Hvilken indflydelse ville den ulovlige kopiering have haft på salget og prisdannelsen? Vil krænkeren alligevel (f.eks. for at få adgang til emballage og manualer) på et tidspunkt købe værket? I denne afvejning kan der være behov for at sondre mellem den ulovlige kopiering, der typisk vil indebære, at krænkeren *ikke* anskaffer sig en lovlig kopi, f.eks. kopiering af en DVD-film, på den ene side, og på den anden side den kopiering, der bl.a. bæres af et ønske om at stifte bekendtskab med værket med henblik på en eventuel senere anskaffelse. Omvendt bør det også spille ind, om den uautoriserede programkopiering af visse værker (herunder også musik) kan få betydning for markedets kendskab til disse værker. På grund af kompleksiteten i denne afvejning bør man derfor – navnlig i tilfælde af omfattende kopieringer mv. – være tilbageholdende med at antage erstatningskrav, der bygger på rent numeriske optællinger af antallet af ulovlige kopier, suppleret med "dobbelt op"-beløb for markedsforstyrrelse mv.

Lempelse

Er den immaterialretlige krænkelse forvoldt af en person, der ikke udøver egentlig erhvervsmæssig virksomhed, vil der ofte være grundlag for at lempe erstatningsansvaret i henhold til den almindelige lempelsesregel i erstatningsansvarslovens § 24. En sådan lempelse skete f.eks. i *U 2005.60 V* og praktiseres ofte i de forligsaftaler, der indgås mellem Antipiratgruppen og den enkelte krænker.

Ansvarsgennembrud

Erstatningsansvaret for ophavsretlige krænkelser påhviler som udgangspunkt den fysiske person, der har udført de handlinger, der har udløst de ulovlige kopier mv. At låne en computer til en anden indebærer ikke en objektiv hæftelse for de handlinger, der herefter begås på computeren. Når et barn begår ophavsretskrænkelser ved brug af forældrenes Internet-forbindelser, er det med andre ord barnet, der er erstatningsansvarlig – med de almindelige modifikationer i dette ansvar, der følger af erstatningsrettens regler. Er krænkelsen udført i regi af et helejet selskab har domstolene undertiden antaget ansvarsgennembrud på dette område, se f.eks. *U 2005.1019 V* (ulovlig visning af tv-transmitteret boksekamp) og *U 1999.326 Ø*.

Godtgørelse

Ophl. § 83, stk. 3, giver udtrykkelig hjemmel for tilkendelse af *godtgørelse* for ikke-økonomisk skade. Denne bestemmelse kan

næppe formodes at få nogen særligt stor betydning i relation til de egentlige edb-programmer (se dog den noget særprægede afgørelse i ERA 3.27 om ulovlig kopiering af programdokumentationen), hvorimod den sagtens kan komme til at spille en rolle i relation til multimedia-værker og databaser. Et af de synspunkter, der fra ophavsmændenes side er gjort gældende i den retspolitiske diskussion om medarbejderes ret til værker, der gøres til genstand for nye digitale udnyttelsesformer, har netop været, at den enkelte forfatter kan føle et sådant ansvar for sit værk, at en anvendelse af dette værk i en uventet og uønsket sammenhæng kan føles som en ideel belastning.

Mandatarspørgsmål

Omkostningerne ved at forfølge edb-pirater (som sjældent vil kunne betale idømte erstatningsbeløb) vil ofte afskære den enkelte rettighedshaver fra at tage initiativ. Derfor forestås retsforfølgning af den egentlige piratkopiering som regel af interesseorganisationer, der optræder på vegne af en flerhed af rettighedshavere, danske såvel som udenlandske.

Sådanne organisationsformer er velkendte på det ophavsretlige område, jf. i det hele redegørelsen i betænkning 912/1981 om Licenskonstruktioner og fotokopiering med omtale af fuldmagtsproblematikken s. 44 ff. i relation til den *lovlige* udnyttelse af værker og andre beskyttede frembringelser. På det digitale område har navnlig to organisationer betydning. I Danmark har en række organisationer inden for film og musikbranchen samlet deres arbejde med at bekæmpe ulovlig kopiering og distribution af film og musikværker i *AntiPiratGruppen* (se <www.antipiratgruppen.dk>). Med udspring i USA stiftede en række virksomheder og organisationer inden for softwareområdet i 1988 den globalt orienterede *Business Software Alliance* (se <www.bsa.org/denmark>).

Som hovedregel må sådanne interesseorganisationer kunne dokumentere deres beføjelse til at gøre ophavsretlige krav gældende ved fuldmagter fra de tilsluttede rettighedshavere. En byretsdom afsagt den 20. juni 1989 af retten i Helsinge (BS 1683/1987) har imidlertid antaget søgsmålsret på grundlag af forklaringer om indholdet af vedtægterne for det daværende SUS (Sammenslutningen af Udbydere af Standardprogrammel). Almindeligvis må sagsøgte enten kunne forlange dokumentation for, at oppebårne beløb kommer rettighedshaverne til gode, eller at de rettighedshavere, hvis interesser berøres af den pågældende sag, har givet gyldigt samtykke til en kollektiv opkrævning.

Bevis for plagiering

Der er ingen særregler om beviset for plagiering af et programværk. Et særligt problem opstår her, fordi den, der har rådighed over programmets kildetekst, uden vanskelighed kan frem-

bringe et plagierende program, der i oversat form vil fremtræde med en helt anden objektkode. I EU's Grønbog om ophavsret (1989) overvejede man at indføre regler, hvorefter bevisbyrden overgår til den påståede krænker, når først rettighedshaveren for domstolene har fremlagt de forskellige versioner af sit eget program, hvortil han har adgang, og godtgør en rimelig begrundet mistanke om kopiering. Se hertil Grønbogen, pkt. 4.5.31, der dog ikke fandt vej til 1991-rådsdirektivet om retlig beskyttelse af edb-programmer (91/250). Sådanne generelle regler har fra tid til anden været foreslået indført i patentloven.

Bevissikring

Efter reglerne i rpl. kap. 57a, som indsat ved lov nr. 216 af 28. marts 2001, er der givet særlige regler om bevissikring i sager, hvor der er mistanke om krænkelse af immaterialrettigheder. Reglerne er indsat på grundlag af et forarbejde i betænkning 1385/2000. Ønsket om at få indført disse regler er gjort gældende af rettighedshaverorganisationer (herunder først og fremmest den førnævnte dominerede *Business Software Alliance*) der fandt, at Danmark havde pligt til at indføre sådanne regler i medfør af TRIPS-protokollerne. Som det vil fremgå af det følgende er der tale om en indgribende procesregulering, der går langt videre end man hidtil har set på det privatretlige område.

Bevissikring er imidlertid blevet en fast ingrediens i rettighedshavernes arbejde med overvågning af ophavsretlige krænkelser, herunder navnlig sådanne, der foregår på nettet og under såkaldte net-parties. Det var f.eks. en bevissikring, der lå til grund for den sag, der fandt sin afgørelse i *U 2005.60 V*. Brugen af dette retsmiddel kan undertiden forekomme hårdhændet overfor de ikke-erhvervsmæssige krænkere, der ofte er inde i billedet. *U 2002.1065 VLK* godkendte f.eks. en fogedforretning mod en 14-årig med henblik på bevissikring af piratkopieret materiale. Den 14-årige havde deltaget i et net-party sammen med ca. 300 andre deltagere, og det fandtes sandsynliggjort, at han her i ikke ubetydeligt omfang havde foretaget ulovlig kopiering af beskyttede værker. Landsretten fandt, at den 14-åriges værge ikke kunne tilkaldes uden væsentlig forsinkelse, og da der endvidere ikke var andre personer over 18 år til stede, som ville varetage hans interesser, måtte forretningen gennemføres i medfør af rpl. § 656 a, stk. 4, sidste pkt., altså som om rekvisitus ikke var til stede. Fogedforretningen fandtes således gennemført med rette. Se for en gennemgang af det erfaringsmateriale, der foreligger med reglerne, *Clement Salung Petersen* i U 2005B.10 ff.

- grundbetingelser

Ifølge rpl. § 653 kan fogedretten efter begæring fra en rettighedshaver (eller dennes beføjede repræsentant) træffe bestem-

melse om, at der hos rekvisitus skal foretages en *undersøgelse* med henblik på at sikre bevis for en immaterialretlig krænkelse. Betingelsen herfor er, at rekvirenten kan sandsynliggøre, at rekvisitus som led i erhvervsvirksomhed eller i øvrigt i ikke ubetydeligt omfang har begået en krænkelse, og der er grund til at antage, at bevis herfor kan findes i de lokaler, der ønskes undersøgt. Se hertil nærmere § 653, stk. 1, nr. 1 og 2. De krænkelser, der kan begrunde et sådant retsskridt, er nærmere angivet i § 653, stk. 2, der angiver en nærmest komplet oversigt over immaterialretten.

- sandsynlighedskravet

Kravene til denne sandsynliggørelse fremgår ikke af loven; men der må som minimum stilles krav svarende til dem, der ville kunne have begrundet en ransagning efter de straffeprocessuelle regler. Dernæst skal der anlægges en proportionalitetsvurdering, jf. rpl. § 653, stk. 4: Undersøgelsen må ikke påføre rekvisitus skade eller ulempe, som står i misforhold til rettighedshavernes interesse i dens gennemførelse. Det har f.eks. ikke været meningen, at en undersøgelseshandling som den, der nu er skabt hjemmel til, kan sættes i værk for at sikre beviset for mere bagatelagtige overtrædelser i form af almindelig "uorden" i licensforholdene. En formodning for, at en kunde har glemt at forny den licens, han har til en tidligere version af en programpakke, så den svarer til en opdateret version, bør derfor ikke kunne begrunde en bevisanmodning efter dette regelsæt. Krænkelserne skal have et vist omfang, før der kan skrides til så væsentlige indgreb i privatsfæren.

- fremgangsmåde

Som grundlag for en bevissikring skal der foreligge en begæring, der nærmere angiver de oplysninger, rekvirenten påberåber sig som grundlag for sin mistanke, jf. § 653a, stk. 1. Som udgangspunkt skal rekvisitus herefter indkaldes til fogedretten. En sådan indkaldelse kan dog undlades, hvis den må antages at medføre risiko for, at genstande, dokumenter, edb-oplysninger eller andre af de oplysninger, der er omfattet af begæringen, vil blive unddraget, jf. nærmere § 653a, stk. 2. Har rekvisitus ikke været underrettet, skal han dog have adgang til at tilkalde en advokat, jf. § 653a, stk. 5. Forretningen skal i så fald udsættes, indtil advokaten er kommet til stede, medmindre dette vil medføre unødig forsinkelse eller risiko for bevisunddragelse. Har rekvisitus ikke været til stede, skal fogedretten uden unødigt ophold give meddelelse om det passerede. Herefter kan rekvisitus inden 1 uge efter modtagelsen af denne underretning forlange genoptagelse.

Undersøgelse kan foretages, selv om rekvisitus ikke giver møde eller ikke kan træffes, jf. § 653a, stk. 4. Er rekvisitus ikke

til stede, når fogeden banker på døren, skal fogeden først opfordre andre personer over 18 år, som er til stede, og som må antages at have kendskab til rekvisiti forhold (f.eks. forældre til mindreårige børn eller medarbejdere i erhvervsvirksomheder), til at varetage rekvisiti interesse under forretningen. Er heller ikke sådanne personer til stede, skal forretningen som udgangspunkt udsættes, jf. nærmere § 653a, stk. 4. Udsættelse kan dog undlades, hvis der foreligger særlige omstændigheder – f.eks. klare indikationer om, at bevismidler er ved at blive fjernet.

- omfang

Selve undersøgelsen gennemføres ved fogedrettens foranstaltning. I de – hyppige – tilfælde, hvor undersøgelsens genstand befinder sig på et digitalt medium, kan fogedretten foretage beslaglæggelse af sådanne medier eller andre genstande og dokumenter, jf. § 653b, stk. 1. Materialet opbevares herefter af fogedretten eller den, retten bemyndiger hertil (f.eks. den tilknyttede bistandsyder), jf. § 653b, stk. 3.

Da fogedretten ikke selv forventes at have de fornødne tekniske forudsætninger for at kunne foretage en sådan kopiering, giver § 653b, stk. 2, fogedretten adgang til at udpege uvildige sagkyndige som bistandsydere, f.eks. en statsautoriseret revisor. Denne udarbejder herefter en rapport over undersøgelsens resultat, jf. § 653b, stk. 4. Rekvirenten og/eller dennes repræsentant har ret til at være til stede under selve undersøgelseshandlingen for dermed at kunne medvirke til, at der ikke overdrages oplysninger i et omfang, der går videre end begrundet i den krænkelsesmistanke, der ligger til grund for begæringen.

- justifikationssag

Der er tale om et foreløbigt retsskridt, som rettighedshaveren alene kan foretage på grundlag af sikkerhedsstillelse, jf. § 653a, stk. 6 (medmindre fogedretten undtagelsesvis bestemmer andet), og som senest 4 uger efter undersøgelsens afslutning skal følges til dørs med en justifikationssag, jf. § 653c. Viser det sig, at undersøgelsen er gennemført med urette, påhviler der rettighedshaveren et *objektivt* erstatningsansvar, jf. § 653c, stk. 3.

- vurdering

Som nævnt er det ganske vidtgående regler, der hermed er indført i dansk lovgivning. Under lovforarbejdet gav reglerne bl.a. anledning til modstand fra Advokatrådets side; men der udspillede sig ingen større retspolitisk debat om deres hensigtsmæssighed, se herved mit indlæg i Datasikkerhedsbladet nr. 37, december 2000, s. 12 ff. Fraværet af denne debat kan undre, når det tages i betragtning, hvor vidtgående indgreb, der kan tænkes foretaget på grundlag af regelsættet. Enhver rettighedshaver, der mener at kunne dokumentere en vis sandsynlighed for, at rettigheder, der tilkommer ham er blevet krænket, har nu fået adgang

til – med fogedens hjælp – at skaffe sig adgang til andre privatpersoner eller virksomheder og der få indblik i forhold, som ellers ville være hermetisk aflukket for omverdenen. Dette er naturligvis gunstigt for de pågældende rettighedshavere; men når man sammenligner med tilfælde, hvor den bevismæssige usikkerhed udspringer af et kontraktsforhold, er det vanskeligt at se, at den bevissituation, rettighedshaverne står i, er mærkbart anderledes end andre aftaleparters stilling i andre tilfælde, hvor der foreligger mistanke om en misligholdelsessituation, som det kan være vanskeligt at bevise. Man kender systemer som de, der hermed er indført i dansk ret, fra andre retssystemer (se bl.a. *PA* s. 430 ff. om de amerikanske regler om *discovery*). Uden for det offentligretlige og straffeprocessuelle område har de dog hidtil været ukendte i dansk ret.

Ifølge Justitsministeriets bemærkninger til lovforslaget var Danmark ikke – som hævdet af rettighedshaverorganisationerne – tvunget til at gennemføre dette regelsæt på grund af TRIPS-reglerne. Man må altså gå ud fra, at der er tale om et frivilligt retspolitisk valg fra den danske lovgivers side. Den periode, man nu bevæger sig ind i, hvor reglerne skal omsættes til praktisk anvendelse, giver derfor anledning til at mane til forsigtighed og – som nævnt – navnlig stille store krav til karakteren af den "mistanke", der begrunder en anvendelse af regelsættet, samt anlægge en nøje proportionalitetsvurdering, når kravene til en bevisbegæring vurderes.

6.4. Indskrænkninger i ophavsretten

6.4.a. Privatkopiering

Ifølge ophl. § 12, stk. 1, har brugeren af et værk, der er offentliggjort af rettighedshaveren (hvilket ifølge ophl. § 8, stk. 1, er tilfældet, når værket lovligt er gjort tilgængeligt for almenheden) ret til at fremstille eller lade fremstille "enkelte eksemplarer til sin private brug". Denne ret markerer en *undtagelse* fra den hovedregel, der fastslås i ophl. § 2, stk. 1, om at ophavsretten medfører eneret til at fremstille eksemplarer af værket. Undtagelsen i § 12, stk. 1, indebærer bl.a., at den, der lovligt har købt et program med dokumentation, kan frembringe enkelte fotokopier af dokumentationen, f.eks. for at have centrale passager ved hånden, hvis et program på den bærbare computer skulle drille under ophold i sommerhuset. En sådan kopieringsret for brugeren gæl-

der derimod ikke i forbindelse med *erhvervsvirksomhed* herunder ved kommerciel undervisningsvirksomhed. Undtagelsen i § 12, stk. 1, er således udtrykkeligt afgrænset til den *private* sfære, jf. nærmere herom *Schønning* (2003), s. 248 ff. Ligeledes antages det, at *juridiske personer* – hvad enten de optræder i kommercielt, offentligretligt eller almennyttigt regi – er afskåret fra at udføre privatkopiering efter reglerne i § 12, stk. 1.

Teknisk medhjælp

Undtagelsen i stk. 1 er generelt begrænset ved ophl. § 12, stk. 5, der forbyder eksemplarfremstilling af musikværker og filmværker ved brug af teknisk udstyr, der er stillet til rådighed for almenheden på biblioteker, i forretningslokaler eller på andre offentligt tilgængelige steder. Det samme gælder for litterære værker, såfremt det tekniske udstyr er stillet til rådighed i erhvervsøjemed. Gennem denne regel hindres omgåelse af forbuddet mod digital privat eksemplarfremstilling. Bestemmelsen forbyder dermed brug af kopieringsudstyr i indkøbscentre eller kopiforretninger til fremstilling af eksemplarer til privat brug.

Værksspecifikke undtagelser

Undtagelsen i § 12, stk. 1, er dernæst begrænset ved reglerne i § 12, stk. 2, hvoraf nr. 3-5 har betydning på det digitale område. Disse regler forbyder brugeren at fremstille eksemplarer af edb-programmer i digitaliseret form (3), at fremstille eksemplarer i digital form af databaser, når eksemplarfremstillingen sker på grundlag af en gengivelse af databasen i digital form (4), og at fremstille enkelte eksemplarer i digital form af andre værker end edb-programmer og databaser, medmindre det udelukkende sker til personlig brug for fremstilleren eller dennes husstand (5).

Edb-programmer

Forbuddet i § 12, stk. 2, nr. 3, mod at foretage eksemplarfremstilling af edb-programmer i *digitaliseret form* følger af art. 4 i programdirektivet (91/250). Da edb-programmer anvendes i kraft af en række teknisk betingede kopieringshandlinger, har det været nødvendigt at forsyne denne begrænsning i brugerens adgang til at foretage eksemplarfremstillinger med en legal programlicens, der er indeholdt i ophl. § 36, jf. nærmere herom i afsnit 7.4.b. Hvor omfanget af denne licens, som det fremgår, kan give anledning til tvivl, volder det sjældent særlig tvivl, om der er foretaget en digital eksemplarfremstilling i medfør af § 12, stk. 1, nr. 3. Bestemmelsen tager således primært sigte til programmet i maskinlæsbar form, dvs i objektkodeform, jf. *Schønning* (2003), s. 254. Foreligger programmet i kildetekstversion, vil denne version også være omfattet, hvis kildeteksten – hvilket normalt vil være tilfældet – uden videre kan oversættes til objektkode ved hjælp af den *compiler*, der hører til det pågældende programmeringssprog. Et program, der er skrevet ud på papir, er derimod

ikke "maskinlæsbart", selv om teksten på papiret ubesværet kan læses maskinelt af en skanner.

Databaser

Forbuddet i § 12, stk. 2, nr. 4, mod at foretage privatkopiering af databaser i digital form følger af artikel 5-6 i databasedirektivet (96/6), der ifølge art. 6, stk. 2, litra a, kun giver adgang til at tillade privatkopiering af databaser, når der er tale om eksemplarfremstilling til privat brug af en *ikke-elektronisk* database, dvs. en database i analog form. Forbuddet gælder således digital kopiering, der sker på grundlag af et digitalt eksemplar. Der er således mulighed for at uddrage *analoge* kopier (f.eks. ved udprint) af en database til privat brug efter den almindelige regel i § 12, stk. 1. Brugeren af en database må derfor udlede sin ret til at foretage nødvendige brugskopieringer af basen på grundlag af ophl. § 36, stk. 2, der er præceptiv, jf. § 36, stk. 3. Se nærmere herom afsnit 8.2.c. Bestemmelsen omhandler kun databaser. Se nærmere om dette begreb i afsnit 8.1.

Andre digitale værker

Ophl. § 12, stk. 2, nr. 5, indeholder endelig en praktisk væsentlig adgang til at fremstille "enkelte eksemplarer i digital form af andre værker end edb-programmer og databaser, medmindre det udelukkende sker til personlig brug for fremstilleren eller dennes husstand." Ophavsmandens samtykke kræves dog til fremstilling af eksemplarer i digital form på grundlag af et eksemplar, der er lånt eller lejet. Det er derfor ikke tilladt – uden ophavsmandens samtykke – at fremstille private digitale eksemplarer af musik-cd'er eller DVD-film, man har lånt, hvad enten eksemplarfremstillingen sker til en ny CD, til harddisk eller til MP3-afspiller. Det er ligeledes uden betydning, om der kopieres fra et medium, hvor værket ligger i statisk form, eller om der kopieres fra en radiospredning, streaming eller lignende.

Som bestemmelsen er formuleret, er den ikke begrænset til tilfælde, hvor eksemplarfremstillingen sker på grundlag af en gengivelse af værket i digital form. Modsat retsstillingen før 2001-lovændringen, kræver det nu tilladelse fra rettighedshaveren, hvis man uden for husstanden vil kopiere værker fra et analogt medium (f.eks. ved almindelig ikke-digital radiotransmission) og til et digitalt (f.eks. til MP3-afspiller eller CD). Det er altså både *analog-digital* og *digital-digital*-kopiering, der er omfattet. Uden for husstandens grænser må man altså ikke downloade et litterært værk fra nettet uden at sikre sig, at rettighedshaveren er indforstået hermed (en indforståelse, der almindeligvis må antages at foreligge ved værkets blotte eksistens på hjemmesiden uden angivelse af et modsat rettet udtrykkeligt kopieringsforbud), eller overspille analog lyd til digitalt medium. Ligeledes

kræver det tilladelse uden for husstandens rammer at *inde* en tekst eller et billede til digitalt medium.

"Husstanden"

Med § 12, stk. 2, nr. 5, er der indført et nyt husstandskriterium i dansk ophavsret. Herved forstås ifølge lovbemærkningerne "en fysisk persons privatsfære", idet den nærmere afgrænsning af dette begreb overlades til en konkret bedømmelse, hvor der bl.a. skal lægges vægt på, om der er tale om bofællesskaber med fælles husholdning eller andre momenter, der peger på en i dagligdagen personlig forbundet personkreds. Som hermed antydet, volder afgrænsningen betydelige problemer: Udveksling af digitale filer mellem kollegiebeboere vil formentlig falde uden for husstandsbegrebet, hvorimod udveksling mellem et kollektivs beboere vil falde inden for. Det er således lettere at karakterisere de tilfælde, der med sikkerhed falder uden for begrebet. Hertil hører undervisnings- og erhvervsvirksomheder, institutioner og andre sammenhænge mellem deltagere, hvis samkvem i højere grad må anses for motiveret ved funktionelle gøremål end ønsket om personligt samkvem. En vis øvre grænse ligger dog i, at der i alle tilfælde kun må fremstilles "enkelte eksemplarer". Heri ligger ingen absolut talmæssig grænse. Der må, som anført i forarbejderne, anlægges et skøn, der bl.a. inddrager værkets sårbarhed overfor kopiering.

Digital-analog

Ophl. § 12, stk. 2, nr. 5, afskærer ikke analog kopiering af den digitale tekst, f.eks. i forbindelse med almindelig udprintning. At man gennem brug af moderne ingsudstyr har mulighed for at gøre en udprintet tekst "maskinlæsbar", gør ingen forandring i dette resultat, så længe udprintningen ikke tager sigte på at blive "læst" af en maskine. De tilfælde, hvor dette er tilfældet (f.eks. ved brug af stregkode eller tal til maskinaflæsning), har dog ingen nævneværdig ophavsretlig interesse. Om retten til sådanne eksemplarfremstillinger fra digitalt til analogt medium gælder den almindelige adgang til privat eksemplarfremstilling i medfør af ophl. § 12, stk. 1.

6.4.b. Citatret

Den ophavsretlige citatret, der er hjemlet ved ophl. § 22, giver ret til at citere fra et offentliggjort værk "i overensstemmelse med god skik og i det omfang, som betinges af formålet". Traditionelt er denne ret betragtet som en nødvendig forudsætning for den informationsudveksling, som et kultursamfund ikke kan være foruden. For en lang række værker generer citatretten da heller ikke ophavsmanden. Tværtimod vil henvisninger til et værk ofte

bidrage til udbredelsen af kendskabet til det og dermed skabe et større marked for værket. Men citatretten og de begrundelser, den bygger på, har ikke rigtig gyldighed på programområdet, selv om den efter sin formulering dækker alle værksarter.

Efter en naturlig forståelse tager begrebet "citat" sigte på, at man i tale eller skrift (ordret) ytrer sig om en anden person eller et sted i et skrift, jf. også betænkning 1197/1990, s. 168. Den citerende "bruger" vel den citeredes værk; men han hidfører det på den anden side en værdiforøgelse ved den ytring, hvori værket citeres. Hermed varetages det hensyn til informationsudveksling, der begrunder denne undtagelse fra ophavsmandens eneret. Som almindelig regel kan man nok sige, at citater fra værker, der almindeligvis "købes" hos rettighedshaveren, og som underminerer dette marked, ikke er lovlige, sml. f.eks. *U 1993.180 Ø* (hvor et kommercielt tv-selskabs benyttelse af 1 minut og 7 sekunder fra et tv-interview ansås at overskride citatretten), men derimod *U 1991.744 Ø* (hvor en anvendelse af en to-minutters samlejescene i en tv-udsendelse udgjorde et lovligt citat). Se omvendt *U 1984.881 Ø*, der – under dissens – antog, at affotografering af et billede af dronningen fra transmissionen af nytårstalen faldt inden for den ophavsretlige citatret. Dommen er næppe rigtig. Kendelsen i *U 1998.525 ØLK* drejede sig om en situation, hvor en person fra sin hjemmeside havde indlagt musikprøver af fra 30 til 40 sekunders varighed fra ca. 300 ud af 450 forskellige musiktitler. Idet der var tale om kopiering med salg for øje var dette ikke hjemlet i medfør af ophl. § 22.

Diskussion

Det er på denne baggrund tvivlsomt, om man med hjemmel i citatretten frit kan genskabe stumper af et program, f.eks. til at understøtte egne programmer mv. *For* at anerkende en citatret taler det, at man i 1995-ophavsretsloven ikke gav særlige regler herom, således som man har gjort det på andre "inkompatible" områder af IT-ophavsretten, og at rettighedshaverens økonomiske belastning ved en sådan udnyttelse vel ikke adskiller sig mærkbart fra den, andre litterære rettighedshavere må tåle. *Imod* taler det forhold, at man ved "citering" af programstof i objektkode gør noget, der ligger ret fjernt fra den retspolitiske begrundelse for citatretten. Når spørgsmålet ikke er afklaret, må der tillægges lovens ordlyd vægt. Resultatet må derfor være, at objektkode-"citater" også er omfattet af § 22, idet retten til at foretage den slags citater – som i øvrigt – forudsætter "god skik", sml. den førnævnte markedsbetragtning: Et citat, der har til formål at undgå at skulle købe et produkt, der udbydes på det almindelige marked, er konkurrencetruende for ophavsmanden og kan næppe

betragtes som "god skik", jf. betænkning 1197/1990, s. 167. Fonte og drivere må således erhverves hos rettighedshaveren, selv om de kun udgør begrænsede bestanddele af større systemer.

Fair use mv.

Dansk ophavsret rummer ikke – som f.eks. anglo-amerikansk – et generalforbehold om *fair use* eller *fair dealing*, der giver hjemmel til at modificere retsanvendelsen, hvor den ellers ville føre til stødende resultater, se herved section 107 af den amerikanske *Copyright Act* (der bl.a. foreskriver, at der skal tages højde for "the effect of the use upon the potential market for or value of the copyrighted work"). De undtagelser, vi opererer med, er snævert afgrænset til særlige former for kopiering og citering, jf. nærmere ophl. §§ 12 og 22.

Særligt om multimedia

Citatretten må antages at få sin væsentligste betydning i relation til de værkselementer, der indgår i multimedia-værker. Det er endnu ikke afklaret, hvad der i relation til sådanne værker må anses som "god skik". På den ene side ligger det klart, at man i kommercielle produktioner inden for det traditionelle filmområde i almindelighed opererer med betaling for benyttelse af værkssekvenser. På den anden side må det erkendes, at der netop på dette område endnu ikke har etableret sig nogen fast praksis for, hvad der betales for, sml. herved *U 1999.547 Ø*, hvor musikbenyttelse i en videotrailer ikke fandtes omfattet af citatretten. Adgangen til at foretage sådanne citater vil formentlig blive præget af den velvillighed, hvormed de berørte rettighedshavere tilbyder ophavsretlige tilladelser (licenser) på rimelige økonomiske vilkår. Problemet vil muligvis finde retspolitiske løsninger gennem regler om tvangslicens.

En række forvaltningsorganisationer, herunder KODA og Gramex, tilbyder aftaler, der dækker ophavsretlig udnyttelse af musik og andre beskyttede værker og præstationer via Internet. Aftalerne indgås med indehaveren af den pågældende hjemmeside, som tilstås en ikke-eksklusiv licens til at anvende værkerne i uændret form til andet end reklamebrug med pligt til kreditering og uden ret til ændring.

6.4.c. Ændringsret

Som anført ovenfor indebærer den ophavsretlige eneret bl.a. retten til at gøre værket tilgængeligt i "ændret skikkelse", jf. § 2, stk. 1. Hertil føjer sig ophl. § 3, stk. 2, der ud fra ideelle overvejelser giver ophavsmanden ret til at modsætte sig en ændring, der er krænkende for hans litterære eller kunstneriske anseelse eller egenart. I talrige tilfælde kan man imidlertid ikke undgå, at digitale værker, herunder programmer, ændres som led i deres forudsatte brug. Dette kan f.eks. følge af reglerne om privatkopiering

eller i medfør af de særlige regler i § 36, stk. 1, nr. 1, om kopiering af edb-programmer med henblik på fejlrettelse. I ophl. § 11, stk. 2, slås det fast, at sådanne ændringer ikke må gå videre, "end den tilladte brug kræver". Reglerne herom omtales i afsnit 7.4.b.

6.4.d. Konsumption

En væsentlig indskrænkning i ophavsmandens eneret følger af reglerne om konsumption. Da disse regler knytter sig til hver af de enerettigheder, ophl. § 2, stk. 3, tildeler ophavsmanden, er de behandlet ovenfor i tilknytning til hver af de nævnte enerettigheder. For eneretten til offentlig *spredning*, jf. ophl. § 2, stk. 3, nr. 1, følger konsumptionsreglerne af lovens § 19, jf. nærmere afsnit 6.3.d. For eneretten til offentlig *visning*, jf. ophl. § 2, stk. 3, nr. 2, følger konsumptionsreglerne af ophl. § 20, jf. herom afsnit 6.3.e. Og for eneretten til offentlig *fremførelse*, jf. ophl. § 2, stk. 3, nr. 3, følger konsumptionsadgangen af ophl. § 21, jf. nærmere afsnit 6.3.f. Der henvises i det hele til behandlingen af problemstillingen de anførte steder.

6.5. Det ophavsretlige rettighedssubjekt

6.5.a. Problemstillingen

Udgangspunktet

Efter ophl. § 1 er udgangspunktet, at den, der *frembringer* et litterært eller kunstnerisk værk, har ophavsret til værket. Dette hænger efter kontinental ophavsret sammen med, at ophavsretten grundlæggende betragtes som en personlig ret. I ansættelsesforhold kommer dette *ophavsretlige* udgangspunkt i konflikt med den *arbejdsretlige* hovedregel om, at det er arbejdsgiveren, der høster frugterne af den ansattes arbejde. I aftaler med konsulenter kan der opstå interessemodsætninger, hvor klientens interesse i frit at kunne råde over det programværk, konsulenten udvikler, kan komme i konflikt med konsulentens interesse i at kunne genbruge sit erfaringsmateriale og sine værktøjer.

Uanset om disse spørgsmål opstår under en ansættelsesaftale, i konsulentforhold eller i andre rettighedsrelaterede transaktioner, er der nogle fælles udgangspunkter, der kan udledes af aftaleretlige *fortolkningsprincipper* og af ophavsrettens grundlæggende *kendetegn*. Som fremhævet af *Koktvedgaard* (2005), s. 103, gælder det engelske mundheld om, at "you cannot eat your cake and have it" ikke på ophavsrettens område: De ophavsretli-

ge beføjelser giver ophavsmanden ret til at tillade vidt forskellige former for værksudnyttelse og i vidt forskellige henseender. Sælger man hele ophavsretten til et edb-program, kan dette efter omstændighederne lægge væsentlige begrænsninger i muligheden for at genbruge programdele samt moduler fra firmaets programbibliotek. Omvendt tilsiger aftale- og forudsætningssynspunkter ikke, at der tilstås udvikleren flere rettigheder, end han har behov for.

Knophs tanke

I sit skelsættende værk Åndsretten (1936) gav nordmanden *Ragnar Knoph* et svar på dette spørgsmål, der siden er blevet stående som et etableret udgangspunkt i nordisk ophavsret. "Synspunktet må være", skrev Knoph (s. 84), "at prinsipalen vinner den rett over åndsverket som er nødvendig og rimelig, hvis arbeidsaftalen skal nå sitt formål, men heller ikke mere. En avis må derfor ha rett til å trykke op sin journalists eller sin tegners arbeider så ofte den vil, men får ikke rett til å selge dem til andre, eller til å gi dem ut i bogform eller som mappe".

Journalist-dommen

Knoph's synspunkt genfindes i en toneangivende dansk højesteretsdom, der netop angik en journalists ophavsret til sin artikel, *U 1978.901 H*. Dommen antog, at en journalist, der havde skrevet en artikel som led i sit ansættelsesforhold til dagbladet Politiken, havde retten til forud for Politiken at retsforfølge en ophavsretlig krænkelse af den pågældende artikel. I Højesterets præmisser udtales det generelt, at journalistens ophavsret pga. hans ansættelsesforhold til Politiken ikke var overgået til bladet "i videre omfang end nødvendigt af hensyn til Politikens sædvanlige virksomhed".

En tilsvarende – og endda mere vidtgående – afgørelse foreligger med *U 1982.926 Ø* om en journalist ansat ved Ritzaus Bureau. Et tidsskrift uden for bureauets kreds havde optrykt en af journalistens artikler. Journalisten fik medhold i, at dette optryk var uberettiget, fordi det pågældende tidsskrift ikke hørte til bureauets sædvanlige kundekreds. Se også *U 1993.180 Ø* om ansatte ved en lokalradiostation. Se ligeledes straks nedenfor om *U 1994.349 H*. I en ØLD af 22. januar 1990 blev tilsvarende synspunkter gjort gældende af en medarbejder ved Værdipapircentralen (VP) efter VP's salg til den tilsvarende norske central af et programsystem, som bl.a. han havde været med til at udvikle. Dommen kom imidlertid ikke ind på spørgsmålet, da Landsretten ikke fandt dokumentation for, at det pågældende system havde fornøden værkshøjde, jf. nedenfor. Se i øvrigt betænkning 1197/1990, s. 66 ff., der i detaljeret form gengiver reglerne om ophavsret i ansættelsesforhold, men som ikke skønner det hensigtsmæssigt at foretage en sådan regulering "bl.a. fordi der her er tale om et retsområde, som er under en konstant og tæt påvirkning af den teknologiske udvikling". Med Supreme Courts dom af 25.

juni 2001 i sagen *New York Times et al. v. Tasini et al.*, 533 U.S. 483 (2001), er det i øvrigt antaget, at en free-lance journalist ikke ved blot at stille sin artikel til rådighed for et dagblad hermed havde givet bladet ret til at genanvende artiklen i en elektronisk database. Flertallets præmisser (5-2), der er ført i pennen af dommer Ginsburg, betoner, at aftaleforholdet med journalisten – i mangel af særskilt vedtagelse – ikke gav støtte for en så vidtgående ret, som en videreudnyttelse i databaser ville repræsentere.

6.5.b. Konsulenter

Det skitserede udgangspunkt kan uden videre overføres til IT-opdrag, der involverer konsulenter og andre selvstændigt virkende bistandsydere, der frembringer programkode for en opdragsgiver. Har bistandsyderen specialudviklet et edb-program, og er der ikke indgået nærmere aftale om rettighedsfordelingen, vil aftalen alene overføre de rettigheder, der er nødvendige for at tilgodese det overordnede formål med denne aftale, til kunden. Dette vil typisk indebære, at kunden – uden modstående aftale – indtræder i retten til uindskrænket og tidsubegrænset at anvende programmet inden for sin egen organisation. Om kunden f.eks. har ret til at udbyde programmet i fri handel eller anvende det i en anden sammenhæng end den oprindeligt tiltænkte, vil bero på karakteren af kundens virksomhed ved aftalens indgåelse. Da konsulenter sjældent forventes at få indgående kendskab til kundens planer for fremtidig virksomhed, vil det være i kundens interesse at orientere konsulenten om mulige "nye" udnyttelsesformer for dermed at skabe det forudsætningsgrundlag, der vil tildele kunden rettighederne i disse henseender.

Der findes ingen nyere afgørelser om konsulenter, der belyser disse principper. I *U 1994.349 H* havde to personer i perioden fra 1985 – 1987 været ansat ved et produktionsselskab (Kanal 2 Broadcast ApS), der havde til formål at producere, drive og administrere et betalings-TV i det storkøbenhavnske område. I denne egenskab havde de medvirket til at skabe et antal TV-udsendelser. Disse TV-udsendelser havde TV-selskabet genudsendt uden forinden at sikre sig medarbejdernes godkendelse. Højesteret fandt, at medarbejdernes ansættelse var så fast, at selskabet var indtrådt i deres ophavsrettigheder "i det omfang, dette på produktionstidspunktet var nødvendigt for appellantens (TV-selskabets) sædvanlige virksomhed". De to journalister var således ansat til at producere tv-programmer, hvis nærmere indhold og omfang ikke på forhånd var klarlagt. De fik fast månedsløn – også i perioder, hvor der ikke produceredes programmer – de fik feriegodtgørelse, og deres ansættelsesforhold var ikke tidsbegrænsede. Dermed opstod det andet spørgsmål, om der i det

foreliggende ansættelsesforhold var sket en sådan overdragelse af medarbejdernes ophavsrettigheder, at genudsendelserne havde været berettiget. Ej heller på dette punkt fik de to medarbejdere medhold. Højesteret bemærkede i den forbindelse, at muligheden for genudsendelse måtte anses for "sædvanlig for en TV-virksomhed som appellantens". Spørgsmålet er i øvrigt behandlet hos *Hanne Bender*: Edb-rettigheder (1998), s. 179 ff. og hos *Torvund* i NIR 1999.123 ff., der bl.a. peger på en uensartethed, der gør sig gældende på programområdet sammenlignet med andre former for ophavsretlige opdrag.

Aftaleforhandling

Spørgsmålet giver ofte anledning til intens debat, når det rejses i aftaleforhandlingen. *Konsulenten* vil kunne gøre gældende, at det udviklede program er baseret på hans særlige knowhow, og at opdragsgiveren med sit krav vil tiltage sig flere rettigheder, end han har købt og betalt for. Tilsvarende vil en total overførelse af rettigheder til opdragsgiveren afskære konsulenten fra at genbruge rettighedselementer, som det ikke kan skade opdragsgiveren, at der sker genbrug af. Heroverfor vil *opdragsgiveren* kunne gøre gældende, at han har betalt for arbejdet og derfor også må få de rettigheder, arbejdet resulterer i. Ofte beror sådanne diskussioner på misforståelser om ophavsrettens indhold. For det første er der rig mulighed for at genbruge rettighedselementer uden at det kommer modparten i kontraktsforholdet til skade. For det andet dækker ophavsrettigheder ikke de generelle idéer og principper, men kun det færdige produkt. Selv om ophavsret overgår til kunden, afskæres konsulenten altså ikke fra at udnytte sin almindelige know how i anden sammenhæng.

Udgangspunkt

En forhandling om udnyttelsesretten til et værk bør baseres på to enkle udgangspunkter: For det første har hver af parterne en interesse i at få noget til gengæld for den investering, de præsterer i transaktionen. For det andet må det sikres, at de retspositioner, der defineres for hver af parterne, ikke fører til efterfølgende uforudsete begrænsninger i anvendeligheden. Begge synspunkter understreger behovet for præcise beskrivelser af de ophavsretlige retspositioner, der overdrages.

Konkurrence-begrænsninger

Selv om aftalen mellem parterne har overført et antal ophavsretlige beføjelser til bistandsyderen, får denne ikke nødvendigvis ret til at udnytte disse rettigheder, som han vil. Aftaleforholdet påfører bl.a. parterne en pligt til at handle loyalt og hensynsfuldt, der giver støtte for visse begrænsninger i adgangen til at udføre handlinger, der enten påfører medkontrahenten en uventet og urimelig konkurrence eller reducerer dennes interesse i ydelsen, jf. nærmere *Koktvedgaard:* Immaterialretspositioner (1965), s. 275 ff., 290 f. I ansættelsesforhold opstilles en hovedregel om, at overdrageren i almindelighed ikke må give sig til at konkurrere

med den virksomhed, der gerne skulle realiseres ved ophavsretserhvervelse, men tilsvarende gælder i andre aftaleforhold, sml. dommen i *U 1982.4 H* om *Jacobsens slankekure*.

Jacobsen havde udgivet 4 bøger om sine slankekure på Samlerens forlag, der havde udfoldet en betydelig reklamevirksomhed og realiseret en stor salgssucces på bøgerne. 5 år efter udsendte Jacobsen en 3-ugers slankekur på et konkurrerende forlag efter forinden at have udgivet teksten hertil som en ugebladsserie. Uanset han ikke havde påtaget sig nogen udtrykkelig forpligtelse til at afstå fra at udgive konkurrerende bøger, fandt Højesteret, at Jacobsen ved sine aftaler med Samlerens forlag havde givet dette ret til at foretage genoptryk af disse bøger. Under henvisning til, at de konkurrerende bøger påførte Samlerens forlag en ubillig konkurrence, antog Højesteret, at udgivelserne var retsstridige, og idømte erstatning. Se ligeledes *U 1964.221 H*, hvor digteren *Piet Hein* havde indgået aftale med medicinalselskabet H. Lundbeck & Co om at levere et antal "gruks" med tegninger til reklamebrug. Aftalen blev hævet af Lundbeck, da man fandt ud af, at Piet Hein også leverede gruks til et andet medicinalfirma med henblik på annoncering, omend af et andet indhold og udformning. Denne ophævelse fandt Højesteret var berettiget, da det måtte stå klart for Piet Hein, at Lundbeck tilsigtede en eneret til de leverede gruks. Dommen er vanskelig at forene med den meget lignende situation, der forelå i *U 1984.1122 SH*, og som næppe kan opretholdes.

6.5.c. Arbejdstagere

Ifølge ophl. § 59 overgår ophavsretten til et edb-program, der er frembragt af en arbejdstager under udførelsen af dennes arbejde eller efter arbejdsgiverens anvisninger, til arbejdsgiveren. Bestemmelsen, der har rod i art. 2, stk. 3, i Rådsdirektivet om retlig beskyttelse af edb-programmer, gælder medmindre andet er aftalt. Den omfatter kun "edb-programmer". Frembringer medarbejderen et multimedia-værk eller en database, der ikke er et programværk, jf. bemærkningerne herom i afsnit 7.1.c., gælder lovgivningens almindelige regler om ophavsrettens overgang i ansættelsesforhold, jf. ovenfor. Dernæst gælder bestemmelsen kun for "arbejdstagere", dvs. personer, der befinder sig i ansættelsesforhold med deraf normalt følgende instruktionsbeføjelse for arbejdsgiveren.

Personel afgrænsning

Et særligt problem opstår i relation til personer ansat i forskningsmæssige stillinger. Forstår man kravet om "tjenestestilling" efter pålydende, måtte sådanne ansættelser behandles på samme måde som andre ansættelsesforhold, hvorved rettighederne tilkom forskningsinstitutionen. Dette harmonerer vel med den

praksis, der følges inden for visse forskningsstillinger og på visse sektorforskningsinstitutter, f.eks. Risø og Meteorologisk Institut. Der har hidtil været udbredt enighed om, at ophl. § 59 ikke har virkning for universitetsansatte eller andre skabere, der udfører deres arbejde som led i en "fri" forskning. Betragtningen er, at skulle de ophavsretlige frugter af denne forskning tilfalde universitetet, ville dette skabe et arsenal af rettigheder, som det aldrig har været tanken med bestemmelsen at etablere. Som anført i bemærkningerne i min kommentar til Lov om arbejdstageres opfindelser (1995) s. 50, må denne opfattelse dog nok tages op til revision, hvis universiteternes patenteringspraksis ændrer sig i aktiv retning. Dette er muligvis ved at ske i disse år.

Ifølge § 8 i lov om opfindelser ved universiteter og sektorforskningsinstitutioner, nr. 347 af 2. juni 1999 har den institution (dvs. universitet eller sektorforskningsinstitution, jf. § 6), hvortil en arbejdstager er knyttet, krav på at få de rettigheder, der er knyttet til en opfindelse, overdraget til sig, hvis arbejdstager har gjort opfindelsen som led i sit arbejde på institutionen. I bemærkningerne til lovforslagets § 3, der definerer begrebet "opfindelse", lægger ministeren til grund, at institutionerne allerede råder over de rettigheder, der knytter sig til udviklede edb-programmer. Dette må antages, for så vidt den pågældende institution har optrådt i en arbejdsgiverrolle i relation til den pågældende programfrembringelse. Er dette ikke tilfældet – programmet er f.eks. skrevet på egen hånd, uden at programfrembringelsen har haft sammenhæng med et forskningsprojekt, der har involveret andre medarbejdere ved institutionen – må det antages, at medarbejderen selv råder over samtlige ophavsrettigheder vedrørende programmet. Se i øvrigt *Jens Schovsbo*: Lov om opfindelser ved offentlige forskningsinstitutioner (2001), s. 101 ff., der ligeledes argumenterer for en indskrænkende fortolkning af denne regel i relation til edb-programrelaterede opfindelser.

Saglig afgrænsning

§ 59 rammer ikke alle de programmer, den ansatte udfører. Programmer udviklet i medarbejderens fritid falder udenfor bestemmelsen, medmindre fritidsarbejdet er udført efter anvisning (f.eks. ved overarbejde). Omvendt må det antages, at medarbejderens brug af arbejdsgiverens maskinel i arbejdstiden (f.eks. i ledige stunder) ikke i sig selv giver arbejdsgiveren ophavsret. Her er programmet netop ikke frembragt "som led i" et ansættelsesforhold. Med lovmotivernes henvisning til, at der skal foreligge et ansættelsesforhold med heraf følgende instruktionsbeføjelse, er det afgørende for vurderingen, om arbejdsgiveren – direkte eller indirekte – har kunnet pålægge funktionæren at udføre den pågældende programmering. Det er ikke afgørende, om medarbejderen er særligt uddannet eller specifikt ansat til netop at stå for programmering. Netop på dette punkt har § 59 gjort op med

den hidtil gældende retstilstand, der lagde vægt på forudsætningerne i forskellige relationer, jf. nærmere nedenfor.

Stiltiende overdragelse

Et særligt spørgsmål opstår, når rettighederne til et program indehaves af medarbejderen, men hvor denne senere har ladet arbejdsgiveren udnytte det og f.eks. ligefrem ladet andre ansatte videreudvikle på det. Dette kan f.eks. forekomme i relation til programmel, som den ansatte har udviklet før han blev ansat. Sådanne tilfælde må løses efter aftaleretlige regler om passivitet. I *U 1989.228 H* havde en person uden for sin arbejdstid udført 125 ophavsretligt beskyttede designs til tæpper, men ladet arbejdsgiveren udnytte disse designs til tæppeproduktion. Efter ansættelsesforholdets ophør opstod der tvist om, hvorvidt arbejdsgiveren fortsat havde ret til at anvende de pågældende designs. Højesteret lagde vægt på, at den ansatte havde ladet arbejdsgiveren benytte de pågældende designs til bestilling af prøvetæpper, der indgik i virksomhedens salgsmateriale, uden at tage eller forbeholde sig designer-honorar. Under disse omstændigheder var arbejdsgiveren ikke afskåret fra fortsat at benytte de pågældende designs.

Supplerende litteratur

Forståelsen af de *almene problemer* i forbindelse med retsbeskyttelse af edb-teknologi nås bedst i den almene immaterialret. Herom henvises navnlig til *Mogens Koktvedgaard*: Lærebog i immaterialret, 5. udg. (1999), til *Palle Bo Madsen*: Markedsret, del 2, 3. udg. (1997) og til *Ragnar Knophs* stadig aktuelle klassiker: Åndsretten. Oslo, (1936). Ophavsretsloven er righoldigt kommenteret af *Peter Schønning*, 2. udg. (1998).

Den bedste samlede systematiske fremstilling af de ophavsretlige problemer, der udspringer af den digitale økonomi, foreligger med *Wagle & Ødegaard* (1997): Ophavsrett i en digital verden (Oslo, 1997). Andre samlede fremstillinger foreligger med *Peter Blume:* Retsbeskyttelse af EDB (1989), *Per Håkon Schmidt*: Retsbeskyttelse af edb-programmer (1998) og *Thomas Riis*: Immaterielret & IT (2001). Se i øvrigt *Mads Bryde Andersen*: Ophavsretten og den nye teknologi, NIR 1995.616 ff.

Fra den tidlige tidsskriftslitteratur kan henvises til *Koktvedgaard* i U1983B.317 ff. og U1989B.297 ff. Herudover indeholder hver årgang af NIR righoldige afhandlinger om IT-ophavsretlige problemer.

Kapitel 7. PROGRAMBESKYTTELSEN

7.1. Almene spørgsmål

7.1.a. Det retssystematiske valg

Konsekvenser

At man rubricerer programkode som et litterært værk indebærer, at *genstanden* for den ophavsretlige beskyttelse samt beskyttelsens *retsvirkninger* (varighed, eneret mv.) dermed er lagt fast. Herom gælder – medmindre andet er bestemt – ophavsretslovens regler om litterære værker. Derimod er det imidlertid ikke givet, at selve retsanvendelsen i enhver henseende skal ske i overensstemmelse med den tradition, ophavsretten har udviklet for andre litterære værker. For det første giver loven en række særregler om edb-programmer, se f.eks. § 12, stk. 2, nr. 3, § 19, stk. 3, §§ 36-37, § 59 og § 78. For det andet fremtræder edb-programmer på talrige punkter markant anderledes end andre litterære værker. Der foreligger med andre ord et *beskrivelsesproblem*, som den juridiske teori og praksis må søge at løse.

Brugerens synsvinkel

Som anført i den historiske redegørelse har selve indplaceringen af programkoderne som en særlig slags "litteratur" ikke været uproblematisk, eftersom programmer i iøjnefaldende henseender adskiller sig fra andre litterære værker. Programmet "læses" ikke af brugeren, men af processoren, og "læsningen" sker med henblik på rent tekniske funktioner. Selv om man anskuer processoren som brugerens forlængede arm, kan der påpeges forskelle. Hvor læseren af et litterært værk ved, hvad han læser, ved brugeren ikke nødvendigvis, hvilke programmer systemet anvender, og hvordan (et problem, der – som det fremgår af afsnit 6.3.b. – bl.a. volder vanskeligheder for afgørelsen af, hvornår der foreligger eksemplarfremstilling). Dertil kommer, at ét og samme program – uden at være bearbejdet – kan fremtræde på vidt forskellige typer af medier (diskette, CD, halvlederchip, harddisk etc.), primært fordi programmets tilknytning til det digitale medium er langt flygtigere end bogstavets tilknytning til papiret. En mærkbar konsekvens heraf er, at forskellen mellem programmets salgspris og mediets værdi er langt større end forskellen mellem bogens salgspris og papirets værdi.

Skaberens synsvinkel

Også set fra skaberens synsvinkel er der mærkbare forskelle. Hvor forfatteren til en litterær tekst kan "udfordre" sit naturlige sprog inden for forholdsvis frie grænser og ligefrem opfinde nye ord mv., er programmøren bundet af de håndfaste grænser, der gælder for det programmeringssprog, han anvender. Overholder han ikke dets syntaksregler mv., kører programmet ganske enkelt ikke! Omvendt ligger det klart, at formalsproget åbner talrige andre udtryksmuligheder for programmøren. Tids- og pladsmæssige begrænsninger har sjældent samme betydning som i det talte sprog. Hvor forfatteren til en litterær tekst altid må respektere visse rammer for, hvor længe hans publikum holder ud, er der med nutidens teknologi ingen grænser for, hvor mange og detaljerede kommandoer og statements en programmør kan udtrykke sig med. Man antager således, at Windows 2000-pakken har et samlet omfang på mellem 35 og 60 millioner kodelinjer, se herved *Bruce Schneier* (2000), s. 210.

Fællesnævneren

Selv om der er talrige forskelle mellem edb-programmer og andre litterære værker, består der en afgørende strukturlighed, der gør det velbegrundet, at edb-programmer er rubriceret som litterære værker. Både programmer og klassiske litterære værker betjener sig nemlig af et litterært *sprog*. Sprogelementet er centralt for begrebet litterært værk, der efter forarbejderne til den tidligere ophavsretslov, defineres som "alle værker, som der er udtrykt ved sprogets hjælp". Se herved FT 1959-60, till. A, sp. 2683, der betoner, at der ikke kan stilles krav til værkets omfang eller med hensyn til det formål, det skal tjene. Den sproglige karakter mærkes først og fremmest i den – kommunikative – proces, hvorunder programmer bliver til: Programmøren koder i et programmeringssprog og frembringer derved det ophavsretlige *udtryk*.

Begrebet litterært værk defineres ikke i loven. Baseret på dets sproglige sammensætning (littera=bogstav) omfatter det værker, der sammensætter sig af bogstaver eller lignende tegn. I overensstemmelse hermed definerer den amerikanske Copyright Act (se 17 U.S.C. 101) begrebet som "works other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, manuscripts, phonorecords, film, tapes, disks, or cards". At edb-programmer skal henregnes til kategorien litterære værker efter Bernerkonventionens regler er i øvrigt lagt til grund i WIPO Copyright Treaty (1996), art. 4.

7.1.b. Programbegrebet

Processor-instruktioner

Når ophl. § 1, stk. 3, taler om edb-programmer, sigter bestemmelsen til de koder ("instruktioner"), der i overensstemmelse med reglerne i et programmeringssprog bringer processoren i stand til at udføre den funktion, programmøren tilsigtede, jf. i det hele den tekniske fremstilling i 3.2.a. Det er altså systemets *input*, begrebet sigter til. Den effekt, programmet genererer under anvendelsen (*output*-siden), omfattes ikke af *programbeskyttelsen*, men kan derimod tænkes beskyttet efter andre regelsystemer, herunder de ophavsretlige regler om litteratur og kunst (herunder brugskunst). Hvis programmøren koder processoren til at spille en melodi, vil dette program – foruden programkoderne – indeholde et *eksemplar* af det pågældende musikværk, og når programmet afvikles, vil denne afspilning være en *fremførelse* af denne musik (jf. om dette begreb afsnit 6.3.f.).

Modsat *Hanne Bender* i NIR 1997.75 f., NIR 1999.17 ff., og generelt i EDB-rettigheder (1998), der f.eks. finder, at et skærmbillede ikke er et "selvstændigt digitalt værk", og at hjemmel for beskyttelse heraf derfor må ligge i ophl. § 1, stk. 3. A.st. s. 78 anerkendes det dog, at skærmbilleder kan beskyttes efter § 1, stk. 1. Som fremhævet af *Torvund* i Ånd og Rett – festskrift til Birger Stuevold Lassen (1997), s. 1027 ff., er "litteraturmetaforen", altså forestillingen om, at programmets kildekode udgør kommandoer i en tekst svarende til ord i dagligsprogets sætninger, kommet under pres i takt med udviklingen af grafisk orienterede værktøjer, hvor kildeteksten fremtræder i form af kasser og pile, der markerer relationer mellem programmets forskellige objekter. Da værktøjer af denne art alene udgør konverteringer af det, der til syvende og sidst fremtræder som binære kommandoer til processoren, bringer iagttagelsen ikke den grundlæggende ophavsretlige rubricering af edb-programmet i fare. Derimod giver den anledning til overvejelser om, hvilke elementer af kildeteksten der er genstand for programbeskyttelsen, jf. *Torvund* sst. s. 1031 f., hvor det konkluderes, at retsbeskyttelsen må tilkomme den, hvis indsats har givet programmet dets særpræg. Se i øvrigt om programbegrebet *Wagle & Ødegaard* (1997), s. 71 ff.

Partitioneringsproblemet

Som begrebet "edb-program" er lagt fast, har det ingen naturlig ramme. Alle "serier" af kodeinstruktioner til en processor falder principielt inden for. Hvor man ofte vil have en forestilling om, hvornår en "menneskelæsbar" tekst har et omfang, der almindeligvis vil rubricere den som et "digt", en "novelle" eller en "videnskabelig tidsskriftsartikel", er det eneste fælles kendetegn for programmet dets evne til at nå processoren og herigennem udføre en *funktion*. Da der således ingen funktionelle begrænsninger gælder for, hvornår noget er "et program", opstår spørgsmålet

om, hvor grænsen skal sættes for, hvad der er et værk, eller blot en del af et værk. Dette spørgsmål betegnes undertiden som *partitioneringsproblemet*, jf. således *Wagle & Ødegaard* (1997), s. 173 ff., Se ligeledes *Bing* i Wege zum japanischen Recht, Festschrift für Zentaro Kitigawa zum 60. Geburtstag am 5. April 1992 (Duncker & Humblot, Berlin, 1992), s. 829 ff. og samme i NIR 1999.291 ff.

Problemet har betydning i to henseender: Hvor meget skal der til, for at et program opnår ophavsretlig beskyttelse? Og hvor stor en del af et program må der kopieres, før man kan sige, at ophavsretten er krænket. Problemet opstår generelt for værker, der ikke har noget afsluttet hele (edb-programmer, samleværker og databaser). Der kan næppe opstilles nogen eksakt formel for et svar, og i konkrete sager er man derfor nødt til at søge tilbage i almene betragtninger: En opdeling, der fører til beskyttelse for så små værkselementer, at der reelt opnås en idé-beskyttelse, kan således ikke tillades. Omvendt vil en opdeling, der gør det muligt for konkurrerende virksomheder at tilegne sig frugterne af væsentlige investeringer, heller ikke tillades.

Sidstnævnte problematik må principielt udskilles fra læren om programcitater, se hertil afsnit 6.4.b. Hvis et uddrag af et programværk ikke i sig selv har programkarakter, befinder det sig i *public domain*, og enhver kan da frit bruge det. Citatretten er derimod et indgreb i et ophavsretlig beskyttet værk, der kun kan udøves i overensstemmelse med de særlige regler herfor (værket skal være offentliggjort, citatet skal ske i overensstemmelse med "god skik" og kun i det omfang, der betinges af formålet, jf. nærmere ophl. § 22).

Bruger-information

Af den samlede mængde maskinlæsbar *information* i et "edb-program" (f.eks. materialiseret på en CD-ROM), er det derfor kun en begrænset del, der kan karakteriseres som *edb-programmel*, jf. nærmere om denne centrale sondring i afsnit 3.2.f. Den information, der bringes frem på skærmen, når man f.eks. læser filen i et tekstbehandlingsprogram, er ikke et "program", da den ikke er skrevet som instruktioner til en processor: Der er tale om menneskelæsbar information, der skrives med sigte på en læser. At informationen i den valgte tekniske ramme er *maskinlæsbar* forandrer ikke herved. Det maskinlæsbare er ikke nødvendigvis *eksekverbart*, dvs. i stand til at udføre en teknisk kommando i overensstemmelse med et programmeringssprog.

7.1.c. Mellemformer

Trods denne principielt skarpe sondring findes der en række frembringelser, som det kan være vanskeligt at placere i grænselandet mellem programbegrebet og databegrebet.

Dokumentation

For det første kan man spørge, hvorledes programmets dokumentation, dvs. de tekster mv., der angiver dets funktionalitet og brugergrænseflader, skal rubriceres. Man sondrer almindeligvis mellem *systemdokumentation*, der med henblik på fejlrettelse mv. primært retter sig mod programudviklere og systemfejl, og *brugerdokumentation*, der beskriver, hvordan slutbrugeren anvender programmet, og som i sagens natur derfor primært retter sig mod denne.

Som udgangspunkt ligger det klart, at den sprogligt nedfældede beskrivelse af programmets funktioner mv. må betragtes som et litterært værk, der ikke (også) er et edb-program. Inden for denne kategori er der tale om et litterært værk af *beskrivende art*, jf. § 1, stk. 1, dvs. en slags faglitteratur. Problemet er, om dette også gælder den maskinlæsbare dokumentation, f.eks. de *pop-up* menu'er, der aktiveres via programmets "hjælp"-funktioner. Selv om disse dele af programmet meddeler sig til brugeren ved hjælp af programkomponenter, er der ingen tvivl om rubriceringen. Det samme gælder om de kommentarer mv. (statements), som programmøren anfører i selve programkildeteksten for at understøtte programmets opdatering og videreudvikling: De pågældende sætninger mv. retter sig således ikke mod processoren (som netop vil ignorere dem, når programmet oversættes, eller rettere: "kompileres", til objektkode), men mod *programmøren*. Den i og for sig tilfældige omstændighed, at de optræder i fysisk sammenhæng med programkoden, gør ingen forandring heri. Spørgsmålet har dog næppe større praktisk betydning, da der i alle tilfælde vil være beskyttelse – givet at kravene til originalitet er opfyldte.

I forbindelse med programmets oversættelse fra kildetekst til maskinkode sker der dog den ændring, at en række af programmørens bemærkninger til kildeteksten (til glæde for sig selv og senere udviklere) forsvinder – al den stund de jo ikke retter sig til processoren. Den heraf følgende asymmetri mellem kildetekst og objektkode spiller dog ingen *ophavsretlig* rolle, eftersom disse bemærkninger netop *ikke* retter sig til processoren: I det omfang programmøren indlægger den slags kommentarer i kildeteksten må forholdet rettelig betragtes således, at han frembringer et litterært værk, der ikke er et edb-program. Problemet opstår kun, hvis de pågældende bemærk-

ninger optræder i forbindelse med den øvrige programkildetekst. Der er imidlertid sjældent nogen kommerciel eller anden interesse i at kopiere bemærkningerne som sådanne.

Integrerede dataobjekter

Et andet grænseeksempel herpå er de dataobjekter, der integreres i de fleste af nutidens programmer. For at øge brugervenligheden og i den forbindelse ikke mindst den æstetiske oplevelse af at bruge et program, er det almindeligt at forsyne programmet med en række *visuelle og lydlige indtryk*, der ofte vil komme til udtryk som litterære eller kunstneriske værker. Ved programmets opstart eller under venteperioder vil man kunne høre små musikkompositioner afspillet, og for at bistå brugeren med hjælp under programanvendelsen vil der ofte fremtræde et antal tekstelementer i digitaliseret form (blandt hvilke nogle kan tænkes at være litterære værker) i form af hjælpemenuer mv. Navnlig for programmer inden for underholdningsgenren kan mængden af "klassisk" ophavsretlig information (musik, musikindspilninger, kunst, fotos mv.) være ganske betydelig. Beskyttelsen af disse programelementer følger reglerne om de almindelige litterære og kunstneriske værker samt databaser, jf. nærmere afsnit 6.2.

Anderledes *Wagle & Ødegaard* (1997), s. 77, der afviser at lægge nogen klar sondring mellem denne form for integreret dokumentation og programmel, selv om dette vil indebære en udvidelse af programbegrebet. Begrundelsen herfor (nemlig at der i så fald vil gælde forskellige regler for de forskellige komponenter af programmet) kan dog næppe være afgørende. Samme problemkreds har man i forvejen ikke blot for programbeskyttelsen, men også inden for talrige andre værkskategorier (f.eks. film).

Opmarkeringer

Et tredje væsentligt grænsetilfælde er de opmarkeringer af tekstmasser, som bl.a. er nødvendige for at forberede et dokument til *hypertekst*-applikationer, f.eks. elektroniske bøger eller hjemmesider. I det omfang disse opmarkeringer understøtter muligheden for at foretage et "spring" hen til anden tekst, når brugeren aktiverer koden (og dermed forsyner systemet med data), kan man i en vis forstand hævde, at disse koder udgør instruktioner til en processor. Men på den anden side ligger det klart, at disse spring ikke effektueres i en programmæssig ramme: Hypertekst-koden er en integreret bestanddel af et hele, der fremstår som almindelig tekst. At den i kraft af den browser, teksten læses fra, effektuerer et hypertekst-spring, bør ikke kunne forandre tekstens karakter af data. I overensstemmelse med denne sidste betragtning må det antages, at sådanne opmarkeringer, trods deres tilsyneladende lighed med programfrembringelser, ikke skal betragtes som så-

danne, se tilsvarende *Wagle & Ødegaard* (1997), s. 80 ff., *Lindberg & Westman* (1999), s. 158 f. og *Nordell* i NIR 1999.489.

Instruktionsfiler

I nær forbindelse hermed kan for det fjerde nævnes sådanne filer, der vel ikke udgør integrerede dele af et edb-program, men som i sig rummer data, der betragtes som instruktioner, når filen kaldes fra en programfil. Et eksempel herpå er de såkaldte systemkonfigureringsfiler (i DOS-styresystemet f.eks. config.sys). I overensstemmelse med det foran antagne er den almindelige opfattelse også her, at sådanne filer ikke skal betragtes som edb-programmel, se tilsvarende *Hanne Bender* (1998), s. 75 f. Hvis filerne har en vis størrelse og kompleksitet kan det være aktuelt at bringe reglerne om katalogbeskyttelse i anvendelse, jf. ophl. § 71 og nærmere kapitel 8.

Makroer

For det femte kan man spørge, hvorledes programmeringsmakroer bør betragtes. En makro er en sammenfletning af en flerhed af funktioner, som brugeren af et program – f.eks. et tekstbehandlingsprogram – kan frembringe for dermed at undgå gang på gang at skulle udføre de enkelte indtastninger. Problemet er, at de enkelte instruktioner i makroen strengt taget har karakter af "inddata" til det program, der anvendes, hvad enten der er tale om nøgne data (som f.eks. navn og adresse til brug for frembringelse af et brevpapir) eller om aktivering af eksekverbare kommandoer. I henseende til frembringelsesprocessen er lighedspunkterne med programudviklingen så iøjnefaldende, at det forekommer rigtigst at rubricere makroer i kategorier af edb-programmer: For det første samler makroen en "*serie af instruktioner*", der til syvende og sidst når den processor, der er programmeret til at læse den. For det andet rummer den tekniske ramme, der gælder for makro-indlæsningen, et *formalsprog*, der i teknisk henseende modsvarer det, der gælder for andre programmeringssprog. At betragte makro-frembringelser som programmer stemmer i øvrigt med teknisk jargon, der ofte taler om "makro-programmering".

Programmeringssprog

Man kan endelig spørge, om programmeringssprog kan beskyttes ophavsretligt. Når spørgsmålet rejses, er det nødvendigt at sondre mellem programmeringssproget *som sådant* – dvs. i skikkelse af de regler for dets syntaks og semantik mv., der skal anvendes, når man betjener sig af det – henholdsvis det *program*, der *implementerer* disse sprogregler, først og fremmest i forbindelse med funktioner til frembringelse og oversættelse (kompilering) af edb-programmer skrevet i det pågældende sprog.

- oversættere

At oversætterprogrammer kan beskyttes ophavsretligt er utvivlsomt. Det eneste spørgsmål, man kan rejse, er om den ophavsret-

lige beskyttelse, som programmør A (forudsat fornøden originalitet) opnår til sit oversætterprogram til sproget X, forhindrer programmør B i at frembringe et andet (originalt) oversætterprogram til sproget X. Svaret herpå beror på de almindelige regler om ophavsretlig *idé-beskyttelse*, jf. afsnit 6.2.b., og om beskyttelse af *brugergrænseflader*, jf. afsnit 7.3. Selve dette at implementere et programmeringssprogs syntaks og grammatik må som udgangspunkt betragtes som implementering af en idé, der ikke kan beskyttes ophavsretligt. Hvis ikke programmør B i sin brugergrænseflade har ladet selvstændigt beskyttede elementer i programmør A's brugergrænseflade indgå, må udgangspunktet være, at programmør B's ophavsret til sit oversætterprogram kan gøres gældende helt uafhængigt af programmør A's.

- i sig selv

At et programmeringssprog i sig selv ikke er et "program" er utvivlsomt: Det indeholder ikke som sådant "instruktioner til processoren". Dets formål er derimod at understøtte muligheden af, at en anden end sprogets skaber *formulerer* sådanne instruktioner. Ligeså utvivlsomt er det, at et programmeringsværktøj, der baseres på sproget, er et program. Derimod kan man overveje, om programmeringssproget kan beskyttes efter andre ophavsretlige regler, herunder som almindeligt litterært værk eller database. Stillet generelt må dette spørgsmål formentlig også besvares benægtende: En beskyttelse som almindeligt litterært værk vil alene ramme den specifikke beskrivelse af sproget; men da et programmeringssprogs grammatik og syntaks – ligesom det gælder for et naturligt sprog – kan beskrives på mange forskellige måder, vil en sådan beskyttelse ikke ramme selve sproget som innovativ frembringelse.

I overensstemmelse hermed har den australske High Court nægtet et programmeringssprog beskyttelse som edb-program i sagen *Data Access Corporation v. Powerflex Services PTY Ltd* [1999] HCA 49.

7.2. Programkodens retsbeskyttelse

7.2.a. Kildetekst

Når man taler om ophavsret til edb-programmer sigtes normalt til de enkelte instruktioner i programmet, dvs. programmet i sin kildetekst- eller objektkodeversion. Som tidligere nævnt *kunne* man overveje at betragte kildeteksten på linje med program*dokumentationen*, eftersom kildetekstens kommandoer jo først skal oversættes (kompileres) til objektkode, før de kan læses af pro-

cessoren. At man ikke desto mindre må betragte kildeteksten som et programværk skyldes, at den udtrykker de enkelte kommandoer. Det fremgår således direkte af slutningsordene til ophl. § 1, stk. 1, at beskyttelsen gælder uanset den form, hvori det enkelte værk er kommet til udtryk.

Et af de spørgsmål, der tidligst har givet anledning til tvivl, ikke mindst i amerikansk ophavsretspraksis, er, om selve *strukturen* i programmets kildetekst, herunder de enkelte *sekvenser* af programkommandoer, kan beskyttes ophavsretligt. Spørgsmålet har primært betydning i tilfælde, hvor en programmør forlader et projekt (og et ansættelsesforhold) for i konkurrerende øjemed at frembringe et program, som minder om det, han kom fra. Det nye program skrives fra grunden; men med programmørens erfaring fra det tidligere projekt får det grundlæggende strukturelle lighedspunkter med det, programmøren forlod. Spørgsmålet er nu, hvornår det nye program rettighedsmæssigt er frigjort fra det gamle.

Når spørgsmålet vurderes, er det nærliggende at tage udgangspunkt i ophl. § 4, stk. 2. Efter denne bestemmelse er ophavsretten til et nyt og selvstændigt værk, som er frembragt gennem "fri benyttelse" af et andet, ikke afhængigt af ophavsretten til det oprindelige værk. Man er klart uden for denne regel, hvis der medtages ("stjæles") kode fra det oprindelige program. Men hvis ikke det oprindelige programs struktur i sig selv udgør et ophavsretligt beskyttet værk, kan bestemmelsen ikke umiddelbart anvendes, når det netop kun er strukturen – men ikke de enkelte programkommandoer – der går igen. Dermed bliver det et kritisk spørgsmål, om selve strukturen i et program er et beskyttet værkselement.

Spørgsmålet kan også opstå i andre tilfælde end i samarbejdsrelationer, f.eks. når det ved en almindelig afprøvning af programmets idégrundlag, jf. ophl. § 36, stk. 1, nr. 3, er muligt at få indblik i de principper, der er lagt til grund for de enkelte programelementer.

Diskussion

I drøftelsen af dette spørgsmål er det nærliggende at skele til reglerne om samleværker, jf. ophl. § 5, der i visse henseender kan siges at hjemle en beskyttelse af programstrukturen, jf. ligeledes *Riis* (1998), s. 139 f. Det må således antages, at man kan opnå ophavsretlig samleværksbeskyttelse af den "programredaktionelle" indsats, der består i at sammensætte programobjekter, som andre har skrevet. En sådan form for programmering er en kendt teknik i den form for CASE-programmering, der tillader brugeren – mod licensbetaling – at gøre brug af forskellige "præfabrikerede" programmoduler. Beskyttelsen forudsætter blot, at sammensætningen af disse moduler – i fornødent omfang – bærer præg af

originalitet, jf. de almindelige regler herom. Beskyttelsen dækker nemlig kun den *originale* sammenstilling af moduler og objekter i det færdige program. Men jo mere integreret den redaktionelle indsats er i selve kodningsarbejdet, desto vanskeligere bliver det at hævde en sådan beskyttelse, sml. herved *Lindberg & Westman* (1999), s. 160, der – med rette – fremhæver, at man normalt heller ikke opnår samleværksbeskyttelse til en film, selv om den tilsvarende består af et antal delværker. Som afgrænsningskriterium foreslår forfatterne, at man lægger vægt på, om delene er "passive og hvilende" eller om de indgår som bestanddele i noget nyt og selvstændigt.

En synsvinkel som den her hævdede ligger forudsætningsvis til grund for § 2, stk. 2, i halvlederloven, der i tilslutning til betingelsen om, at topografien skal være resultatet af frembringerens egen intellektuelle indsats, fastslår, at topografier bestående af elementer, der er almindelige inden for halvlederindustrien, kun beskyttes, "hvis kombinationen af disse elementer" besidder denne kvalitet. Se i samme retning pkt. 2.7 i *forslaget* til Rådsdirektiv om retlig beskyttelse af programmer (EFT 1989 C 91/6), hvor det fremhæves, at "programmets originalitet kan ligge i udvælgelsen og kompilationen af ... i øvrigt banale elementer".

I det omfang der således *kan* dokumenteres den fornødne originalitet i den "indholdsfortegnelse", der ligger til grund for en sådan "programantologi", må det antages, at der også kan opnås ophavsret til den heri liggende struktur. Men det er væsentligt at slå fast, at der ingen nødvendig sammenhæng er mellem programmets indre struktur og den opbygning, brugeren oplever gennem menuens punkter: En og samme grænseflade (og programfunktion) kan opnås gennem uendeligt mange forskellige udformninger af en programkildetekst. Derfor dækker denne beskyttelse ikke programmets "idé", f.eks. en særlig form for tekstbehandling. Om beskyttelsen af de *funktioner*, programmet udfører, f.eks. via sin menustruktur, se nedenfor i afsnit 7.3.c.

Egne delværker

Heri ligger også, at den, der skriver et program fra grunden, kan opnå en slags indirekte strukturbeskyttelse ved som led i denne frembringelse at "redigere" den samlede komposition af *egne* delprogrammer. Dette spørgsmål *kan* få betydning i tilfælde, hvor programmets delelementer ikke beskyttes, fordi de ikke opfylder originalitetskravene. Problemet kan umiddelbart synes teoretisk; men det har praktisk juridisk betydning, fordi samleværker efter ophavsretsloven betragtes som litterære værker, der *ikke* er edb-programmer, jf. § 1, stk. 1. Hvis man er i en situation, hvor del-programmerne befinder sig under originalitetsgrænsen (eller anvendes med rettighedshaverens samtykke), må man ka-

rakterisere den samlede frembringelse som et samleværk. Dermed gælder de særlige regler, loven opstiller for edb-programmer, ikke (hvorimod reglerne om andre værker i digital form gælder). I praksis betyder dette f.eks., at det således etablerede samleværk kan *udlånes* i medfør af ophl. § 19, stk. 3.

Styret kodning

Det kan være vanskeligt at udpege ophavsmanden til programmer, der er blevet til under en styret proces, hvor der er lagt ufravigelige tekniske rammer for kodningen. Hvis sådanne rammer udtømmer programmørens muligheder for at være kreativ, vil han være afskåret fra at opnå ophavsret, og ophavsretten vil i stedet opstå hos programredaktøren som den reelt kreative part. Problemet opstår kun, hvis styringen gennemføres så stramt, at programmøren er afskåret fra at tilføje det færdige værk et individuelt præg. Programmøren må da betragtes som "teknisk medhjælp", jf. betænkning 1064/1986, s. 43 og *Koktvedgaard* (2005), s. 96 f. Talrige værker inden for den klassiske ophavsret (f.eks. avisartikler, ordbogsbidrag mv.) frembringes indenfor præcist fastsatte rammer, f.eks. for LIX-tal, sprogstil eller ordvalg, uden at ophavsretten af denne grund udelukkende placeres hos den styrende kraft (f.eks. redaktøren).

Pseudokode

Problemet kan blive aktuelt, når der anvendes pseudokode under programmeringen, hvilket ofte sker under struktureret programudvikling (SPU). Pseudokode-teknikken indebærer ikke i sig selv, at ophavsretten opstår hos den styrende instans (der ofte vil være helt eller delvis den samme som programmøren), jf. allerede det forhold, at man typisk supplerer ved at gøre brug af såkaldt *walk through*, hvor den enkelte programmørs delværk gøres til genstand for kritik blandt dennes kolleger. Se i det hele hertil afsnit 3.2.d.

VP-sagen

I en utrykt dom vedrørende Værdipapircentralens edb-programmel (ØLD 22.1.1990) var dette spørgsmål til behandling. Da Værdipapircentralen udviklede VP-systemet, søgte man at opnå en så høj grad af personuafhængighed som muligt. Der var mange personer involveret i udviklingsprocessen, der tog flere år. Derfor var det vigtigt, at den enkelte programmør uden videre kunne erstattes af en anden.

Under sagen gjorde en enkelt programmør gældende, at han havde en del af ophavsretten til det samlede system. Den pågældende havde haft status som "delprojektleder" ved systemets opbygning. Dette indebar, at han havde skrevet kode, været med til at udfærdige de specifikationer, hvorefter koden skulle skrives, og koordineret hele den indsats, medlemmerne i hans delprojektgruppe udførte. Trods vidneforklaringer, der dokumenterede, at

programmøren havde skrevet kode på lige fod med hovedparten af de øvrige programmører, der skrev VP-systemet, fandt landsretten det ikke godtgjort, at programmøren havde "udarbejdet eller medvirket ved udarbejdelsen af programmer eller dele deraf, der i en sådan grad er resultatet af en skabende ånds- og eller intellektuel indsats og præget af individualitet, at disse nyder beskyttelse efter loven om ophavsrettigheder". Afgørelsen ville formentlig falde anderledes ud, hvis den skulle bedømmes på grundlag af det senere vedtagne programdirektiv (91/250/EØF), der netop fastslår, at der ikke kan stilles andre krav end, at programmet skal være ophavsmandens "egen intellektuelle frembringelse", og netop i lyset af dette blev sagen forligt for Højesteret, efter at der var indhentet et syn og skøn, der viste, at sagsøgeren i et vist omfang havde haft mulighed for at udvise individualitet i sit programmeringsarbejde.

I en offentliggjort forligstekst mellem parterne dateret den 30. juli 1992, tilslutter de sig skønsmandens vurdering: At den omhandlede medarbejder "principielt har haft mulighed for at udfolde en selvstændigt skabende indsats". Under henvisning til det originalitetskriterium, der er anført i programdirektivet (91/250/EØF) om, at programmet skal være udtryk for programmørens "egen intellektuelle frembringelse", erklærer parterne sig enige om, "at en VP-medarbejder, der har udført funktioner vedrørende systemanalyse og -udformning som de, den i sagen omhandlede medarbejder varetog, vil kunne have status som medophavsmand til VP-systemet". Da dommen på grund af direktivet imidlertid ikke længere har præjudikatværdi, besluttede Finansforbundet sig til at frafalde krav i anledning af salget af VP-systemet. Forbundet afskærer sig dog ikke fra i andre konkrete sager at rejse lignende ophavsretlige krav, ligesom spørgsmålet vil kunne inddrages i fremtidige overenskomstforhandlinger.

7.2.b. Forarbejder

Skriftligt nedfældede forarbejder mv. til et program beskyttes som almindelige litterære værker, der ikke er programmer, sml. den svenske højesteretsdom i *NJA 1998.563* (*NIR 1999.253*), hvor nogle byggetegninger antoges at have værkshøjde. I henseende til kravene om originalitet (værkshøjde) gælder altså de almindelige krav, man vil stille herom til andre tekstuelle og grafiske fremstillinger, jf. herom afsnit 6.2. For så vidt angår de grafiske værker af beskrivende art – f.eks. flow-charts, diagrammer, skitser mv. – følger beskyttelsen af ophl. § 1, stk. 2. Da ophavsretten til det forberedende designmateriale ikke giver ophavsret til det heri nedfældede idégrundlag, se nærmere herom afsnit 6.2.b., er værdien af denne beskyttelse dog beskeden. Så

længe man befinder sig på undfangelsesstadiet i en kreativ proces, hvor der alene er idéer, planer og muligheder på bordet, fratager man ikke andre retten til at fuldføre disse planer i en ny – og fra "plan-værket" adskilt – manifestation. Denne begrænsning i den ophavsretlige beskyttelse kan vel føles som en svaghed navnlig på IT-området, hvor den væsentligste værdiskabelse netop ligger i disse innovative idé-elementer. Svagheden afbødes dog i nogen grad gennem muligheden for at patentere programrelaterede opfindelser, jf. nærmere herom i afsnit 10.1.d.

I Rådsdirektiv 91/250/EØF om retlig beskyttelse af programmer, art. 1, stk. 1, antages udtrykket "program" også at omfatte "forberedende designmateriale" hertil. Bestemmelsen giver anledning til betydelig usikkerhed, jf. nærmere *Bing* i NIR 1999.284 f. Usikkerheden skyldes, at der jo i en vis forstand ingen grænser er for, hvilke frembringelser der kan siges at udgøre de indledende skridt til det færdige program. En afgrænsning er derfor nødvendig, og den må foretages under hensyntagen til ophavsrettens grundlæggende principper. Det kan således ikke antages, at det *idégrundlag*, der er nedfældet i det forberedende designmateriale, hermed opnår ophavsretlig beskyttelse, jf. udtrykkeligt samme artikels stk. 2, 2. pkt. Antog man denne konsekvens, ville vejen være åbnet for en bredere idé-beskyttelse. Meningen med at inkorporere designmaterialet i programdefinitionen er formentlig at lægge samme begrænsninger i anvendelsen af dette materiale som i anvendelsen af selve programmet, f.eks. i forbindelse med dekompilering (*reverse engineering* mv.), se herom nedenfor afsnit 7.4.g. Dette peger i givet fald på en afgrænsning af begrebet til udkast af en mere præcis beskaffenhed, herunder pseudokode mv.

Bearbejdede forarbejder

Et særligt problem foreligger, hvis forarbejdet udgør selve det grundlag, på hvilket den yderligere programmering bygges. Problemet kan skitseres med et eksempel fra litteraturens verden: Hvis en forfatter i en samtale skitserer idéen til et drama, er det almindeligt antaget, at der ikke foreligger nogen ophavsretskrænkelse, hvis en udenforstående tilhører benytter sig af, hvad han har hørt, og gengiver det i et værk, han selv frembringer. Den slags krænkelser kan derimod tænkes omfattet af reglerne om utilbørlig konkurrence eller af personlighedsretten. Men situationen begynder gradvis at forandre sig, hvis forfatteren nedfælder idéen til det pågældende værk på skrift, og tredjemand herefter får fingre i teksten og arbejder videre med den. Man kan da argumentere for, at der ved nedfældelsen manifesteres et litterært værk, og at en videre bearbejdning af dette (f.eks. ved filmatisering af den skitserede historie), rummer en *ophavsretlig bearbejdning* af værket, jf. ophl. § 4, stk. 1, sml. drøftelsen hos *Wagle & Ødegaard* (1997), s. 156 f.

Det er imidlertid vigtigt at fastholde, at der på det principielle plan ikke er stor forskel mellem de to eksempler. Det forhold, at en tekst skrives ned, giver den ikke isoleret set nogen stærkere ophavsretlig beskyttelse, end hvis den blot udtrykkes mundtligt. Ifølge ophl. § 1 gælder ophavsretten således uanset hvordan, værket er kommet til udtryk. Men at temaet rent faktisk *er* manifesteret skriftligt kan gøre det bevismæssigt lettere for en domstol at nå frem til, at der ikke blot er tale om et løsere udtryk for en abstrakt idé. Denne bevisvirkning vil umærkelig få den praktiske betydning, at man lettere vil statuere krænkelse af et ophavsretligt værk, hvis forlægget er nedfældet på tryk, end hvis der blot er tale om en løsere skitseret idé.

I en videreførelse af dette eksempel er det lettere at opnå en idé-lignende ophavsretsbeskyttelse til et programværk, hvis dele af det på et tidligt stadium i forberedelsen er blevet kodet. Navnlig når det færdige program bygger på den kodning, der er udført på et tidligt tidspunkt i forberedelsesprocessen, må man nå til, at det færdige program udgør bearbejdninger af den oprindelige programkode.

7.2.c. Programmanifestationen

Er en moderne vaskemaskine et eksemplar af et edb-program? For enhver praktisk betragtning er svaret på dette spørgsmål naturligvis nej. Men i den ophavsretlige terminologi giver det anledning til at spørge, hvilke manifestationer af et edb-program der med rette kan betragtes som "et programeksemplar". Og her er det en kendsgerning, at alle moderne vaskemaskiner – ligesom megen anden husholdningselektronik – indeholder talrige programkomponenter. Spørgsmålet har først og fremmest betydning i relation til den ophavsretlige eneret til spredning (og ikke mindst reglerne om, hvornår denne eneret er konsumeret), da retten hertil forudsætter, at et eksemplar af programmet udbydes til salg, udlejning eller udlån mv.

Det antages almindeligvis, at svaret på det konkret stillede spørgsmål er nej, se således *Bing* i NIR 1995.406 og *Wagle & Ødegaard* (1997), s. 84. At man føler sig sikker herpå skyldes ikke mindst en opfattelse af, hvad der er den typiske forudsætning bag brugen af det pågældende udstyr mv.: Hverken rettighedshaveren eller forbrugeren oplever forholdet som "brug" af et edb-program: Ingen af de beføjelser, som normalt tilkommer en programbruger (f.eks. retten til sikkerhedskopiering og fejlretning, jf. ophl. § 36) har heller praktisk betydning. Men så snart

blikket vendes mod transaktioner, hvor disse beføjelser er relevante, må det fastholdes, at også mindre programkomponenter i et digitalt værk af anden karakter gør den samlede manifestation til et eksemplar af det pågældende program.

Denne opfattelse ligger bl.a. til grund for den særlige regel i ophl. § 19, stk. 3, 2. pkt., der giver *biblioteker* ret til at udlåne "et eksemplar af et edb-program i digitaliseret form", når dette udgør "en del af et litterært værk og udlånes sammen med dette". Der er tale om en undtagelsesbestemmelse, der næppe kan fortolkes udvidende til også at omfatte andre værker end litterære værker, der styres af et edb-program. Styrer edb-programmet et produkt, der omfatter kunstneriske værker (f.eks. inden for multimedia-området), er bestemmelsen uanvendelig.

7.2.d. Opsætninger

I forbindelse med installation af et programsystem vil der ofte skulle foretages en række tilpasninger, som sætter systemet i stand til at fungere optimalt i den pågældende konfiguration, i det følgende kaldet systemets *opsætning*. Ofte kan disse opsætninger identificeres til særskilte filer eller tabeller, som dermed vil fremtræde som selvstændige frembringelser. Spørgsmålet er nu, hvilken retlig status disse frembringelser skal have.

Som udgangspunkt er det her nærliggende at anvende den almindelige regel i ophl. § 4, stk. 1, om bearbejdelser. Ganske vist tager denne bestemmelse primært sigte på bearbejdelser, der i deres nye skikkelse er integreret med det oprindelige værk, men det bagvedliggende princip bør ligefuldt finde anvendelse. Spørgsmålet om, hvem der har retten til denne bearbejdelse, må herefter løses efter de almindelige regler om ophavsrettens subjekt, jf. herved afsnit 6.5.

Hvis opsætningen foretages hos kunden af programudvikleren på et standardsystem, som sælges til almenheden, kan der dog opstå særlige spørgsmål om, hvorvidt kunden har ret til at overdrage opsætningen til andre brugere af det pågældende system. Som udgangspunkt må det her antages, at det "værk", bearbejdelsen repræsenterer, er "på anden måde overdraget til andre", jf. ophl. § 19. Dette resultat gælder i hvert fald det leverede program i sin opsatte form. Derimod vil det kræve særlig aftalehjemmel at fremtvinge en udlevering af den specifikation, leverandøren (bearbejderen) selv har gjort af sin opsætning. Ofte vil opsætningen repræsentere kompliceret og værdifuld *knowhow*, som leverandøren vil lide konkurrencemæssige retstab ved at skulle give fra sig. Problemet kan f.eks. opstå, hvis kunden outsourcer sin egen drift for at overgå til en facility management-løsning.

7.3. Beskyttelse af grænseflader

7.3.a. Problemstillingen

Umiddelbart kan det forekomme overraskende at diskutere beskyttelse af et programs grænseflader mod andre programmer (de tekniske grænseflader) eller mod brugerne (brugergrænsefladen) som en del af læren om beskyttelse af edb-programmer. Programmet defineres jo netop med udgangspunkt i de enkelte instruktioner i processoren, og som vi så ovenfor i gennemgangen af denne beskyttelse er det for så vidt underordnet herfor, hvilke resultater disse programinstruktioner udvirker. Imidlertid er drøftelsen om programmets brugergrænseflader traditionelt blevet rubriceret som en del af programbeskyttelsen, selv om den strengt taget drejer sig om reglerne om andre litterære eller kunstneriske værker.

Begreb

Et programs brugergrænseflade er indbegrebet af den information, brugeren må være i besiddelse af for at kunne bruge det. Denne afgrænsning er imidlertid ikke brugbar som grundlag for en afgrænsning af, hvilke elementer af brugergrænsefladen, der kan tænkes beskyttet som ophavsretlige *værker* eller *værksbearbejdninger*. Her kan man for det første udsondre de elementer af brugergrænsefladen der kan udskilles i *selvstændige værkskategorier*. Beskyttelsen er her problemløs: Kan der udpeges et værk i brugergrænsefladen (f.eks. et ikon eller en illustration), gælder de almindelige regler om, hvornår dette værk må gøres til genstand for eksemplarfremstilling og spredning mv. Et anderledes vanskeligt problem opstår, når det overvejes at gøre den mere ubestemmelige følelse af at arbejde med en bestemt brugergrænseflade til genstand for beskyttelse. Dette problem betegnes ofte som beskyttelsen af programmets *look and feel*, jf. nærmere herom i afsnit 7.3.c.

Begge typer af brugergrænsefladebeskyttelse har stor praktisk betydning, fordi IT-brugere ofte vil vælge applikationer efter en vurdering af, hvor let det er at lære at betjene dem. Problemet om selve brugergrænsefladens udseende spillede en stor rolle for de første generationer af PC-applikationer, men efter udbredelsen af den grafiske brugergrænseflade med "rullemenuer", "vinduer", "dialogbokse", "menubjælker" med faste grupper af kommandoer etc., har der dannet sig visse standarder for, hvordan brugergrænsefladen bygges op, og det individuelle spillerum er derfor blevet noget mindre, jf. nærmere *Bing* i NIR 1999.285 ff.

Den ophavsretlige beskyttelse af brugergrænseflader har principielt intet at gøre med beskyttelsen af selve edb-programmet. Når et program defineres som et antal instruktioner til en processor, må de værkselementer, der træder frem over for brugeren, som nævnt betragtes som værker af en *anden art*. At dette må være den korrekte betragtning følger i øvrigt af, at samme brugergrænseflade kan tilvejebringes gennem en ubegrænset flerhed af kildetekstkombinationer. Derfor kan man ikke antage, at den sammenstilling af funktioner, der ligger i en programmenu, udgør et ophavsretligt samleværk. Sammenstillingen har ikke litterær karakter, og anerkendelsen af en sådan beskyttelse ville åbne op for en næsten ubegrænset ophavsbeskyttelse af forskellige funktionssammenstillinger på det industrielle område (betjeningspaneler, tastaturer mv.).

Anden beskyttelse

En beskyttelse af disse aspekter kan her i Norden også støttes på de konkurrenceretlige regler om "god markedsføringsskik", således som disse f.eks. er anvendt i norsk praksis med byretsdommen af 20. juni 1989 fra retten i Strømmen. Afgørelsen, der er truffet med professor Birger Stuevold Lassen som meddommer, er trykt i Lov&Data nr. 19/1989, s. 2-3, og i *Bryde Andersen:* Edb-ret, lovgivning, retsafgørelser, kontrakter, s. 138 ff. Den er kommenteret af *Bing* i NIR 1999.287 f. Se ligeledes fra amerikansk praksis dommen i *Integrated Cash Management Services, Inc., v. Digital Transactions, Inc.*, 920 F.2d 171 (1990). Beskyttelsen har imidlertid begrænset gennemslagskraft, dels fordi den er national (den genfindes f.eks. ikke i amerikansk ret), dels fordi den til stadighed beror på en vurdering af de relevante konkurrencerelationer i det enkelte sagsforhold (man betjener sig altså ikke af systembegreber, som det ophavsretlige *værksbegreb* med dets veldefinerede retsfølger).

7.3.b. Værkskomponenter i brugergrænsefladen

Grafik og lyd

Foruden koderne til processoren kan en programapplikation indeholde værkselementer, der kommer til udtryk som billede (herunder som grafisk værk eller som computer-genereret film), som lyd (f.eks. gennem sampling eller tone-generering) eller som tekst (f.eks. dokumentation, hjælpe-menuer etc.). Et komplet billede af den ophavsretlige beskyttelse af programmer må også inddrage disse forskelligartede værkstyper.

Enkelte elementer i programmets grafik må som nævnt rubriceres som "tegninger og andre i grafisk eller plastisk form udførte værker af beskrivende art", jf. ophl. § 1, stk. 2 – ganske som et

digitalt lagret fotografi må betragtes som henholdsvis et fotografisk *værk*, jf. de almindelige regler i ophl. § 1, stk. 1, eller som et fotografisk *billede* (der altså ikke opfylder de ophavsretlige krav til originalitet), jf. ophl. § 70, der hjemler en særlig 50-årig beskyttelse heraf fra udgangen af det år, da billedet blev fremstillet. Ligeledes kan de lydsignaler, programmet genererer – f.eks. en særlig strofe eller den underlægningsmusik, der ledsager indlæsningen af de omfattende mængder af kode under opstart – udgøre et *musikværk*. Sådanne værkselementer beskyttes efter de almindelige regler, der gælder for de pågældende værkstyper. Enkelte grafiske elementer, som f.eks. *ikoner* og *baggrundsmønstre*, kan beskyttes som f.eks. varemærke eller design, jf. nærmere afsnit 10.3., se f.eks. *Apple Computer, Inc. v. Microsoft Corp.*, 821 F.Supp. 616 (N.D. Cal. 1993), 35 F.3d 1435 (9th Cir. 1994).

Præstationsbeskyttelse

Lyd spiller en stigende rolle for brugen af nutidens IT-applikationer. Ikke alene afgiver programmerne en stigende mængde information ved lydsekvenser (f.eks. genkendelseslyde ved opstart, fejlmeldinger, "banke på"-signaler mv.); lyden tjener ligeledes til at levendegøre de hændelser, der udspiller sig på skærmen i talrige multimediaapplikationer: En dør lukkes i, der lyder skridt, en motorcykel brøler afsted etc. De ophavsretlige muligheder for at beskytte sådanne lydsekvenser er begrænsede: Selv om det kan kræve megen kyndighed og betydelige omkostninger at frembringe den rigtige "*sound*", befinder vi os uden for det ophavsretlige værksbegreb. Af samme grund er også reglerne om fremførelse af ophavsretlige værker, jf. ophl. § 65, ude af billedet, da denne beskyttelse drejer sig om en "udøvende kunstners fremførelse af et litterært eller kunstnerisk værk."

Derimod giver ophl. § 66, som hører til blandt de ophavsretlige "naborettigheder", fremstilleren en eneret til eftergørelse eller tilgængeliggørelse til almenheden af "lydoptagelser", jf. nærmere afsnit 8.7.b.

Anden beskyttelse

Gennem de senere år er det blevet praksis ved en række varemærkekontorer at beskytte såkaldte lydmærker, se hertil *Wallberg* i NIR 1997.1. Denne praksis, der indtil videre primært har haft betydning for fysiske produkter som f.eks. motorcykler, shavere mv., kan imidlertid også få betydning i relation til brugen af et programværk: Gennem værkets markedsføring og offentliggørelse vil man efter reglerne i varemærkelovens § 4 kunne realisere en erhvervsmæssig brug, der kan indebære en krænkelse af varemærketten til det pågældende lydmærke, såfremt der ikke foreligger samtykke hertil. En sådan beskyttelse er dog forholdsvis snæver og vil – ikke mindst pga. de involverede omkostninger

til erhvervelse af beskyttelsen – formentlig kun være aktuel for de ganske få typer af programmer, hvor sådanne stilistiske detaljer kan formodes at have betydning for efterspørgslen.

7.3.c. "Look and feel"

Direktivet

Rådsdirektivet om retlig beskyttelse af programmer synes principielt at åbne mulighed for beskyttelse af brugergrænsefladen, omend direktivteksten er noget uklar på dette punkt. Efter præambelen omfatter begrebet grænseflade også brugergrænseflader, men art. 1, stk. 2, 2. pkt., fastslår herefter, at (bl.a.) de idéer og principper, der ligger til grund for programmets grænseflader, ikke nyder ophavsretlig beskyttelse efter direktivet. Beskyttelsen er altså mulig, medmindre grænsefladen er udtryk for en "idé", sml. om dette noget uhåndterbare begreb oven for under 6.2.b. Realiteten er nok, at direktivet af politiske grunde har undladt at tage stilling til spørgsmålet, der herefter må løses i retsanvendelsen.

USA

Når spørgsmålet er kontroversielt, skyldes det, at situationen – som allerede antydet – sikkert er en anden i USA. Gennem 1980'erne har amerikansk retspraksis gradvist udvidet det ophavsretlige værksbegreb til ikke kun at omfatte det litterære værks litterære elementer, men også det, der med et slagord er blevet kaldt "the look and feel".

Første skridt blev taget med den pudsige sag om den talende bjørn "Teddy Roxpin", der ved hjælp af kassettebånd programmeredes til at fortælle historier. Se *Worlds of Wonder, Inc. v. Vector Intercontinental, Inc.*, 653 F.Supp. 135 (1986). Den ophavsret, der her blev lagt til grund, knyttede sig imidlertid til et audiovisuelt værk (en værkstype, der ikke anerkendes som sådan af dansk ophavsret). Skridtet mod beskyttelse af programmets ikke-litterære elementer blev første gang taget i *Whelan Associates v. Jaslow Dental Laboratory*, 797 F.d. 1222 (1986), og senere med *Broderbund Software, Inc. v. Unison World*, 648 F.Supp. 1127 (1986) og *Johnson Controls v. Phoenix Control Systems*, 886 F.2d 1173 (1989). I sagen *Digital Communications v. Softclone Distributing*, 659 F.Supp. 449 (1987), der angik et program til asynkron datakommunikation, blev der givet beskyttelse af et skærmbillede som "compilation", dvs. samleværk (s. 463). En god oversigt over den amerikanske udvikling på området findes hos *Per Jonas Nordell* i NIR 1999.37 ff.

- CA v. Altai

Ved dommen i *Computer Associates Inc. v. Altai Inc.*, 982 F.2d 693 (1992) fandt appelretten for Second Circuit, at funktionelle elementer af et program, der kom til syne i brugergrænsefladen

uden her at komme til udtryk som selvstændige litterære værker, kunne beskyttes af ophavsretten. Grundlaget for denne beskyttelse fandt retten i en såkaldt *abstraction-filtration-comparison*-test, jf. nærmere *Riis* (1998), s. 137 ff. Tanken er, at ethvert edb-program vil rumme en flerhed af idéer og udtryk, og at man derfor ikke kan benytte denne generelle begrebssondring ved afgørelsen af, hvad der beskyttes. Selve dette princip er allerede lagt til grund i den foregående gennemgang: Man starter med at gennemføre en *abstraktion*, hvorved de forskellige niveauer af programmet adskilles fra hinanden, f.eks. betragtet som idé, som samleværk, som litterær struktur og som specifik kodning. Når dette er sket, *filtrerer* man de aspekter af programmet fra, som ikke har ophavsretlig beskyttelse, idet man konstaterer, at de befinder sig i *public domain*. De tilbageværende værkselementer – og altså ikke programmet som sådan – danner herefter grundlag for sammenligningen ("*comparison*") mellem det beskyttede program og det program, der påstås at krænke ophavsretten hertil. Denne del af testen har alene relation til krænkelsestilfælde.

Sagen angik et brugerprogram, der var programmeret til IBM mainframes, og som kunne køres under forskellige styresystemer. Efter krav fra CA gennemskrev Altai programmet ved anvendelse af *clean-room* teknik (se hertil neden for afsnit 7.4.g.). Spørgsmålet var nu, om det nye program, der teknisk set havde samme funktioner som det tidligere, krænkede CA-programmet. Linien fra *CA v. Altai* er siden fulgt op af senere retspraksis i senere circuit-jurisdiktioner, se hertil *David Hayes*' syv artikler i CLSR, senest i 12 CLSR 338 ff. (1996). Fra 5th Circuit foreligger *Engineering Dynamics v. Structural Software*, 26 F3rd 1335 (1994), fra 9th Circuit *Atari v. Nintendo*, 975 F2d 832, og fra 10th *Gates Rubber v. Bando*, 9 F3d 823 (1993). Også i England har testen været anvendt, se *Richardson v. Flanders* ([1993] FSR 497), hvorimod den er afvist i *Ibcos v. Barclays*, [1994] FSR 275, se hertil *Peter Stone* i 13 CLSR 15 ff. (1997). En helt tilsvarende filtreringstankegang er i øvrigt lagt til grund i *U 2001.747 H*, hvor Højesteret foretager en afgrænsning af de værkselementer til den såkaldte "Tripp-Trapp" barnestol, der efter udløbet af et patent på stolen fortsat nød ophavsretlig beskyttelse.

- Lotus v. Borland

Den amerikanske appelret for 1. circuit (kreds) afsagde i 1995 en endnu mere restriktiv afgørelse i henseende til beskyttelse af brugergrænseflader i sagen *Lotus v. Borland*. Lotus havde nedlagt påstand om, at det af Borland udviklede Quattro program krænkede Lotus-programmet "1-2-3", fordi Borland havde anvendt samme menustruktur og makro-principper som anvendt i Lotus 1-2-3. Retten afviste, at selve kommandostrukturen i Lotus 1-2-3 kunne beskyttes efter ophavsrettens regler.

De nærmere omstændigheder i sagen var følgende: I begyndelsen af 1980'erne udviklede Lotus sit berømte regneark 1-2-3, der inden længe blev førende i edb-industrien. I 1987 introducerede Borland sit første Quattro program. Selv om Borland skrev programmet i sin egen kode, indeholdt det stort set en identisk kopi af hele menustrukturen i 1-2-3. Samtidigt indeholdt det en såkaldt *Key Reader*-interface, som gjorde det muligt for Quattro at læse makroer, der var skrevet til 1-2-3, uden at disse makroer skulle skrives om i Quattro's sprog. Efter at Lotus havde rejst sag mod Borland i byretten fandt dommer *Keeton* (der er kendt som en stærk tilhænger af en intens ophavsretlig beskyttelse, bl.a. fra sin meget omtalte dom i sagen Lotus v. Paperback, jf. herom Lærebog i edb-ret, s. 197), at Borland dermed havde krænket Lotus' ophavsret. Derimod fandt appelretten, at kommando-hierarkiet i Lotus-menuen fremtrådte som en metode for brugeren til at anvende systemet, og at det derfor måtte betragtes som en "method of operation", som ikke kunne beskyttes efter reglerne i den amerikanske ophavsretslov. Det var således uden betydning, at der i dette kommandohierarki indgik elementer, der kunne siges at være udtryk for ophavsmandens personlighed. Med denne afgørelse forelå nu en modstridende retspraksis på appelretsniveau i USA. Tendensen har bevæget sig fra en meget stærk beskyttelse i den praksis for beskyttelse af "look and feel", der blev grundlagt med dommen i *Whelan v. Jaslow* (1987), til nu igen at begrænse den ophavsretlige beskyttelse til programmets litterære udtryk (dvs. først og fremmest selve koden) og til at nægte beskyttelse af den grafiske brugergrænseflade. Nogen føderal opfattelse af dette vigtige spørgsmål får vi først, når Supreme Court får lejlighed til at tage stilling. Lotus-sagen blev ganske vist påkendt i begyndelsen af 1996, men da en af rettens dommere måtte udtræde af sagen på grund af inhabilitet, deltog alene 8 dommere, som delte sig ligeligt, hvorved retten undlod at træffe afgørelse i sagen. Se nærmere om sagen *Riis* (1998), s. 143 f.

Dansk ret

Som det vil være fremgået, er den metode, der er lagt til grund i *Computer Associates v. Altai*, henholdsvis i *Lotus v. Borland*, i harmoni med de principper for analytisk beskrivelse i IT-retten, der er lagt til grund i denne bog. Det punkt, der kan give anledning til tvivl i dansk ret, er altså ikke selve metoden, men derimod enkelte af de værkselementer, der overvejes beskyttet.

Et af de spørgsmål, der herved påkalder sig størst interesse, er de elementer af programmet, der fastslår, hvorledes enkelte taster anvendes, hvor på skærmen der "klikkes" og hvilke lydimpulser der udtrykker bestemte typer af funktioner mv. Som det fremgår, er holdningen i nogle jurisdiktioner (som antaget i Altai og Lotus-sagerne), at sådanne værkselementer ikke kan beskyttes, medmindre man kan filtrere et værkselement bort, som kan stå alene og i sig selv kan siges at opfylde beskyttelseskravene.

Brugskunst?

I dansk ret vil man givetvis kunne beskytte sådanne funktionelle aspekter som *brugskunst*. Ligeså rummeligt begrebet "kunst" er på det kulturelle område, lige så vidt er brugskunst-begrebet på det industrielle. Det må imidlertid haves i erindring, at man netop på dette område stiller strengere krav til ophavsmandens originalitet end i relation til litterære værker. Erkendes må det vel også, at der er gode grunde til at være tilbageholdende. Det hensyn til den teknologiske udvikling, som almindeligvis fremhæves til støtte for ophavsretlig beskyttelse, har ikke ligeså stor vægt i relation til disse aspekter af et program, som det har, når talen er om at beskytte helt nye programtyper mv. Brugergrænsefladen er jo intet mål i sig selv, men en nødvendig rekvisit i et programværk, der skal betjenes af brugere. En større eller mindre beskyttelse heraf vil næppe hverken tilskynde eller afskære programudvikling. Tværtimod vil en for stærk beskyttelse af brugergrænsefladen kunne være til skade for markedet og herved navnlig for brugerne. Den typiske bruger vil investere betydelige ressourcer i at lære brugergrænsefladen at kende. Denne investering nyttiggøres ved køb af nye programmer med tilsvarende brugergrænseflader.

Betydning

Da de første sager om beskyttelse af grafiske brugergrænseflader kom frem, var der stor selvstændig innovation forbundet med den enkelte brugergrænseflade. Markedet befandt sig i en overgangsfase fra den tidlige tegn-orienterede skærm-teknologi, hvor kommandoer blev indtastet i menupunkter, og var på vej mod point-and-click-systemernes langt mere brugervenlige miljøer. Situationen i dag er den, at der i kraft af den massive udbredelse af Windows-systemerne og af den popularitet, der ikke mindst blev forgængeren – Apple Macintosh-teknologien – til del, har fæstnet sig visse almene standarder for, hvorledes brugeren kommunikerer med systemet via en vindues-orienteret grafisk skærm forbundet med mus mv. De sager, der har været ført mellem de toneangivende leverandører af disse systemer om retten til den oprindelige grafiske brugergrænseflade, er af forskellige grunde blevet forligt, og der tegner sig en stadigt stærkere opfattelse af, at ingen "ejer" disse almindelige principper for brugerkommunikation. I takt hermed er incitamentet til at søge domstolene om bistand til at håndhæve et "ejerskab" til sådanne systemer bortfaldet, og problematikken er dermed frataget en del af sin oprindelige, centrale betydning.

Disse betragtninger sætter også deres præg på vurderingen af, om markedsføring af en brugergrænseflade, der funktionelt er identisk med en anden producents brugergrænseflade, kan siges

at indebære en snyltning, der som sådan kan forbydes i medfør af generalklausulen i mfl. § 1. Når en sådan vurdering anlægges må der dog foretages en helhedsbedømmelse, hvor også hensynet til brugeren spiller ind. En grænseflade udgør en del af det "sprog", systemet taler til brugeren. Den skal læres af brugeren, og denne indlæring er ressourcekrævende. Samfundsøkonomisk er der en interesse i, at denne indlæring kan genbruges, ganske som billistens kendskab til, hvordan gearstangen flyttes og lyset tændes, kan genbruges af den enkelte bilproducent. Et sådant genbrug er også i den enkelte producents interesse og repræsenterer en samfundsøkonomisk optimering, som kun en monopolist kan have betænkeligheder ved.

Disse betragtninger fører til, at der i relation til brugergrænseflader skal ganske meget til, før man befinder sig i en snyltningssituation, der kan rammes af generalklausulen i mfl. § 1. Det rent funktionelle genbrug af virkemidler (f.eks. en særlig menuopsætning, eller brugen af bestemte funktionstaster) vil næppe være tilstrækkeligt. Er der foretaget en slavisk kopiering, hvorved ikke blot disse elementer, men også farve- og lydimpulser genskabes, nærmer man sig området for forbuddet i mfl. § 1.

I Norge har den tilsvarende regel om god markedsføringsskik været anvendt i forbindelse med programmel. Ved en dom afsagt af retten i Strømmen den 20. juni 1989 er det antaget, at brugergrænsefladen på et system til konvertering og formatering af data lignede et andet – eksisterende – system så meget i henseende til teknisk funktion og visuel fremtrædelse, at fremstilling og udnyttelse af dette andet system stred mod markedsføringslovens § 1.

7.3.d. Tekniske grænseflader

Karakteristik

Beskyttelsen af programmets tekniske grænseflader (dvs. de elementer af programmet der skaber interoperabilitet med andre programmer eller systemer) må til dels udledes af samme overvejelser som de, der omhandler brugergrænsefladen: Medmindre der er tale om en litterær beskrivelse af den tekniske grænseflade (som f.eks. er nedfældet i en programdokumentation el.lign.), nyder dette aspekt af programmet ikke selvstændig beskyttelse, hverken som edb-program eller som litterært værk af anden art. Den tekniske grænseflade kan sammenlignes med grundlaget for en roman i en føljeton: For at sidste bind i føljetonen skal kunne læses i sin sammenhæng med de andre, må forfatteren anvende de samme personer, steder og grundbegivenheder, ligesom han – alt efter konceptets fasthed – må sørge for, at handlingen indledes, hvor forrige roman sluttede. Men ingen af disse forhold

udgør i sig selv noget "værk" eller "delværk": De fremstår nærmest som faktuelle fikspunkter, som – i stil med andre faktiske forhold – kan begrænse det spillerum, som er til rådighed for den, der vil frembringe et selvstændigt værk (være sig romanen i føljetonen eller et program, der skal kommunikere med et eksisterende).

Closed source

De tekniske *specifikationer*, der – forud for programkodningen – tilsvarende fastslår, hvordan det nye program skal kommunikere med andre programmer mv. (herunder protokoller for kommunikation mv.) vil ikke være offentligt tilgængelige i såkaldt lukkede systemer. For at kunne udvikle et program, der skal kommunikere med et andet, må man erhverve en tilladelse (licens) til denne information, der ellers vil være hemmeligholdt som *erhvervshemmelighed* og beskyttet efter de regler herom, der i dansk ret findes i markedsføringslovens § 10. Opnår man ikke en sådan tilladelse, kan man i et vist omfang søge at stifte bekendtskab med dem ved at foretage såkaldt reverse engineering af programmer, der i forvejen er forberedt til denne kommunikation. Reglerne herom, der findes i ophl. §§ 36-37, gennemgås i afsnit 7.4.g.

Licensspørgsmål

Fordi tekniske grænseflader ikke er undergivet en selvstændig ophavsretlig beskyttelse, vil licenser til brugen af dem ofte knytte sig til den tekst, hvori de pågældende protokoller mv. er nedfældet. Som før nævnt vil denne optegnelse kunne beskyttes som litterært værk efter de almindelige regler, og når benyttelsen kombineres med en hemmeligholdelsesklausul vil rettighedshaveren både opnå en sikring mod kopiering, jf. ophl. § 2, og en tredjemandssikring mod videregivelse af oplysninger om selve protokollens indhold.

Nærmere om tekniske grænseflader, *Riis* (1998), s. 141 f. og (2001), s. 39 ff.

7.4. Licensspørgsmål

7.4.a. Licensbegrebet

Problemstilling

Den ydelse, der består i at "sælge" information, der beskyttes af en immaterialret, præsteres ofte i form af *licens* til under nærmere angivne vilkår at benytte denne information ved at foretage sig handlinger, der ellers ville falde inden for rettighedshaverens

eneret i henhold til en bestående immaterialret. Typisk vil licensen blive meddelt i form af en tilladelse, som rettighedshaveren eller en af denne udpeget mellemmand meddeler brugeren på en nærmere angiven måde og mod en nærmere fastsat betaling. Tilladelsen giver dermed brugeren ret til at gøre noget, som ellers ville være afskåret som følge af den pågældende eneret. Almindelige regler herom findes i ophl. § 36, stk. 1, nr. 1, der som fastsat i samme bestemmelses stk. 3, også finder anvendelse på rent digitale produkter (elektroniske bøger uden søgeprogrammel, clip-art samlinger, tabeller mv.).

Det ophavsretlige licensbegreb udspringer først og fremmest af rettighedshaverens eneret til at fremstille *eksemplarer* af programmet. Som en nærmest undtagelsesfri regel gælder det, at sådanne eksemplarer er en teknisk forudsætning for at kunne udføre de funktioner, programmet er konstrueret til at udføre: Når en programpakke købes, er første skridt brugerens kopiering af de nødvendige programfiler til systemets faste datalager (harddisk), hvor disse filer ligger klar til den løbende brug. Når dette er sket – eller hvis programmet er *præ-installeret* – sker næste serie af eksemplarfremstillinger, når programmet kaldes og enkelte moduler og dele bliver til eksemplarer i RAM-hukommelsen, jf. denne begrebsafgrænsning ovenfor i afsnit 3.1.c.

Retlig karakteristik

I en retlig karakteristik er licensen altså et *løfte*. Men løftet indgår i et tæt samspil med den eneret, der fremkalder behovet for den pågældende tilladelse. Derfor opstår de relevante licensspørgsmål i relation til hver enkelt eneret. I det følgende omtales alene de ophavsretlige licensspørgsmål, der gør sig gældende på programområdet. En tilsvarende gennemgang følger senere for så vidt angår de licenser, der knytter sig til databaseværnet og andre immaterialretlige eneretspositioner.

Sondringer

I en ophavsretlig sammenhæng må man skelne mellem to typer af licensspørgsmål:

- aftalt licens

Den ene type opstår i tilfælde, hvor brugerens ret til at benytte et edb-program udledes af en udtrykkelig (licens-)aftale med rettighedshaveren, hvori denne udnyttelsesadgang er normeret. Sådanne aftaler er hyppigere, jo "større" (og kostbare) programmer der er tale om, men forekommer sjældnere, jo "mindre" (og billige) programmer der er tale om. Foreligger en aftale gælder den, medmindre aftalen rammes af en ugyldighedsregel eller støder an mod en præceptiv barriere. Disse licensspørgsmål behandles i afsnit 7.4.d.

Begrebet licensaftale rummer dog andet og mere end sådanne overdragelsesspørgsmål. Ønsker erhververen f.eks. en mere eksklusiv

ret til at benytte den pågældende immaterialret, f.eks. med sigte på distribution, tager aftalen skikkelse af en distributionsaftale, jf. herom *PA* s. 656 og generelt om sådanne aftaler sst. s. 590 ff. I nær forbindelse hermed står de aftaler, der tildeler erhververen en fuldstændig ret til hele den ophavsret (eller anden immaterialret), der knytter sig til programmet, således at erhververen indtræder i *samtlige overdragelige rettigheder*. Disse aftaleforhold omtales ikke nærmere i det følgende. Sådanne aftaler indgås f.eks. i forbindelse med overdragelse af IT-virksomheder eller som led i programudgivelsesaftaler.

- legal licens

Den anden type licensspørgsmål opstår, når der ingen (udtrykkelig) aftale foreligger mellem rettighedshaveren og brugeren. Hvis ikke lovgivningen træder til med regulering i sådanne tilfælde, må man søge at præcisere en retsstilling gennem fortolkning af de tilkendegivelser, parterne har udvekslet, eller ved inddragelse af de typeforudsætninger og sædvaner, der er gældende på området. I dansk ophavsret findes en sådan hjemmel imidlertid på programområdet med reglerne i ophl. § 36, der etablerer, hvad man kan kalde en *legal programlicens*.

Almindelige bemærkninger

Hverken formålet med eller rammerne for denne fremstilling gør det muligt at redegøre mere detaljeret for licensaftalens retlige problemer. Foruden de særlige spørgsmål, der behandles i de følgende afsnit, henvises herom til speciallitteraturen, se f.eks. *ET* afsnit 7.4. De spørgsmål, der opstår i forbindelse med såkaldt *open source*-licensering, behandles særskilt i afsnit 9.5.b.

Generelt kan man sige, at enhver licensaftale nødvendigvis hviler på den immaterialretlige lovhjemmel, der definerer den beskyttede og dermed licenserede information, se hertil *ET* s. 423. Licensgivers præstationshandling er den tilladelse, han meddeler licenstageren til at udnytte den immaterialretlige retsposition, der hjemles gennem dette regelsæt. Denne licens indebærer ikke i sig selv, at der præsteres nogen garanti for, at eneretten består. Er dette ikke tilfældet, vil der typisk foreligge en retsmangel, jf. nærmere herom i afsnit 22.2.d. og *ET* s. 435 f.

I retssystematisk forstand må man sondre mellem en *licensret* i den førnævnte betydning af ordet (dvs. som en ret til at udnytte enkelte eneretspositioner) og en *rettighedsoverdragelse*. Indebærer aftalen en hel eller delvis overdragelse af *selve immaterialretten*, indtræder erhververen dermed i samtlige de rettigheder (og, for så vidt angår registrerede enerettigheder, også de pligter), der knytter sig hertil. I konsekvens heraf er det nu erhververen, der har kompetencen til at træffe bestemmelse om rettens opgivelse og senere videregivelse, retten til at forbyde tredjemænd at foretage sig handlinger, der er omfattet af eneretten samt – for de

registrerede enerettigheders vedkommende – pligten til at betale årsafgifter, se hertil *ET* s. 428. Undertiden kan det dog være vanskeligt at afgøre, om en eneretsaftale indebærer en licens eller en rettighedsoverdragelse. Er der tvivl herom, vil det fortolkningsprincip, der er indeholdt i ophl. § 53, stk. 3, ofte tale for at fortolke aftalen som en licensaftale.

7.4.b. Den legale programlicens

Ifølge ophl. § 36, stk. 1, nr. 1, har den, der har ret til at benytte et edb-program (i modsætning til den, der råder over en ulovlig kopi), ret til at fremstille sådanne eksemplarer af programmet og foretage sådanne ændringer i programmet, "som er nødvendige for, at erhververen kan benytte det efter dets formål, herunder foretage rettelse af fejl". Denne ret kan udvides og indskrænkes ved aftale, jf. stk. 3 modsætningsvis. Han må desuden fremstille et sikkerhedseksemplar af programmet, for så vidt det er nødvendigt for benyttelsen af det. Dette gælder uanset, hvad der er aftalt, jf. stk. 3. Bestemmelsen indfører en særlig afgrænsning af brugerens licensret. Retten til at bruge programmet *ved at fremstille eksemplarer af det* (jf. om denne sondring straks nedenfor) er nemlig en funktion af brugerens *formål*. Benytter brugeren programmet "efter dets formål", må han kopiere det, så frit han vil, jf. bestemmelsens stk. 1.

Det er en ganske særegen retstilstand, loven hermed indfører. Den indebærer nemlig, at den blotte tanke i sig selv kan gøre en handling mere eller mindre lovlig. Fremkalder jeg en kopi af et edb-program for at bruge det i overensstemmelse med manualens anvisninger, er jeg inden for den legale licens: Jeg benytter programmet efter dets formål. Men får jeg undervejs i processen den tanke, at jeg egentlig kunne eftergøre programmet, hvorefter jeg fortsætter min brug for at planlægge denne eftergørelse, bliver selvsamme kopi pludselig ulovlig, sml. dog stk. 1, nr. 3, og i det hele § 37, der under visse omstændigheder gør sådanne – i sig selv formålsstridige – eksemplarfremstillinger lovlige.

Forklaringen på denne regel ligger i bestemmelsens udspring i 1991-direktivet om retlig beskyttelse af edb-programmer. Under behandlingen af dette direktivforslag opstod en intens diskussion om *reverse engineering*. Reverse engineering forudsætter kopiering, men vidner til gengæld om en tydelig subjektiv hensigt. Ved at formulere loven som sket, giver man den rettighedshaver, der ønsker at modsætte sig reverse engineering, mulighed for at forfølge denne handling.

Eksemplar-begrebet

Som nævnt i afsnit 6.3.b. er grænsen mellem brug og *kopiering* af et program vanskelig at drage. Set fra et rent *ophavsretligt* synspunkt er den dog klar. *Eksemplarfremstilling* foreligger, hvis brugeren som led i sin anvendelse af programmet helt eller delvis knytter programmets informationsindhold til et medium (f.eks. i RAM eller på disk), hvorpå det ikke befandt sig før. *Brug* foreligger derimod, hvis programanvendelsen sker uden en sådan ny eksemplarfremstilling, f.eks. ved at brugeren blot foretager et kald til programmet, der rettes mod et eksemplar af det, der i forvejen er udført i systemets RAM eller i en ROM-kreds. Kan tredjemand udføre den handling, der giver programmet værdi (f.eks. konvertere indtastede data eller finde data i en database) ved en sådan brug, der ikke fører til frembringelse af nye eksemplarer af programmet, vil en sådan fremgangsmåde være uangribelig, hvis ellers det således anvendte eksemplar er dækket af en licens. I så fald er vi uden for anvendelsesområdet for §§ 36 og 37. Sådanne handlinger kan derimod være omfattet af særlige aftaler, der begrænser brugen i forskellige situationer, ligesom en aftale om *hemmeligholdelse* af informationer vedrørende det pågældende program almindeligvis lægger begrænsninger i adgangen til sådanne former for ikke-eksemplarfremstillende "brug".

Det lovlige formål

Hvad der nærmere ligger i det lovlige "formål" med at bruge et edb-program, er ikke fastlagt i forarbejderne til bestemmelsen. Af bestemmelsens forgænger (§ 11a, gældende fra juni 1989 og frem til december 1992, hvor § 36 fik sin nuværende affattelse), fremgik det udtrykkeligt, at den retmæssige bruger mistede sin ret til at udnytte sine kopier, når han videresolgte eksemplaret.

> Forarbejderne til § 11a berører licensproblemerne i FT 1988/89, till. A. sp. 3219, hvor det præciseres, at bestemmelsen er udformet med sigte på, at det ikke skal være lovligt under nogen form at videresprede de med hjemmel i § 11a fremstillede eksemplarer. Videre siges det, at "adgangen for ejeren til at fremstille eksemplarer efter § 11a bør være nøje begrænset til de formål, der angives i bestemmelsen. Der er således ikke ved § 11a åbnet mulighed for, at en person eller virksomhed fx kan fremstille kopier med henblik på samtidig kørsel af det erhvervede program på flere datamater. Dette har ikke mindst betydning for virksomhedsrelaterede programmer, som sælges gennem detailhandelen, fx til bogføring, lagerstyring og tekstbehandling."

Diskussion

Da der i øvrigt ikke foreligger domspraksis på området, giver formålskriteriet anledning til betydelig fortolkningstvivl – en tvivl, der må siges at udspringe af, at hverken baggrundsretten (§ 36) eller aftaleforholdet mellem parterne (sml. neden for afsnit 21.3.c. om de såkaldte shrink wrap-aftaler) tager udtrykkeligt

stilling. I sådanne tilfælde følger det af danske fortolkningsprincipper, at man bør lægge vægt på de *typeforudsætninger*, der almindeligvis vil være gældende på markedet for edb-programmel af den pågældende art. Problemet ved at anvende dette kriterium er imidlertid her – som på andre områder af IT-retten – at vi har at gøre med en branche, der ikke alene ændrer sig hastigt, men som tilmed henvender sig til et ubestemt, mangfoldigt og ofte konvergerende marked bestående af markedssegmenter med vidt forskellige forudsætninger og forventninger.

Alligevel lader det sig gøre at opstille visse nogenlunde faste udgangspunkter:

Enkeltbrugerlicenser

På det almindelige marked for standardprogrammel synes kontraktspraksis at have lagt sig fast på den betragtning, at anvendelsen af en programpakke betragtes som en "licens", hvorefter kopiering og brug enten tillades for en fysisk person (*personlig licens*) eller – navnlig for større installationer – en given virksomhed (*site-licens*), afgrænset efter geografiske (f.eks. en given lokalitet) eller tekniske (en given centralenhed) kriterier. Dette indebærer, at samme program aldrig må anvendes af flere brugere (henholdsvis på flere centralenheder) på samme tid. Licensbetragtningen knytter altså ikke an til, hvornår originaleksemplaret holder op med at eksistere, men til om det bliver anvendt (og dermed gjort til genstand for yderligere eksemplarfremstilling) i forbindelse med en brugskopiering. Den tidligere ophavsretslovs § 11a fastslog udtrykkeligt, at retten til at "udnytte" sikkerhedskopier mv. bortfalder, hvis originaleksemplaret spredes videre (§ 36).

Tankegangen er rammende formuleret i den såkaldte "No-Nonsense Licence Statement", som programproducenten Borland på et tidspunkt benyttede. Det hed bl.a. her, at "... you may treat this software just like a book ...". Videre hedder det: "By saying 'just like a book,' Borland means, for example, that this software may be used for any number of people and may be freely moved from one computer location to another, so long as there is no possibility of it's being used at one location while it's being used at another. Just like a book that can't be read by two different people in two different places at the same time, neither can the software be used by two different people in two different places at the same time". En tilsvarende holdning kan måske udledes af IT-Brancheforeningens pjece: "Undgå ulovlig kopiering – kend reglerne". Det hedder her: "Hvis ikke der er truffet speciel aftale, er et PC-program ... kun beregnet til én person på én PC. Det er ikke lovligt at bruge det på flere PC'er samtidig – hverken enkeltstående eller i et netværk."

Den legale programlicens giver derfor en bruger, der af praktiske grunde vælger at have det samme program liggende to forskellige steder på sin harddisk, adgang hertil. Det samme gælder, hvis et og samme program anvendes såvel på en bærbar PC som på en stationær, blot begge systemer ikke anvendes samtidig af to forskellige brugere. At skulle afkræve en bruger dobbelt betaling i disse tilfælde ville repræsentere en uforholdsmæssig fordyrelse af licensomkostningerne for programmel og indebære en berigelse af programindustrien med tvivlsomt realt grundlag.

Torvund (1997), s. 157, antager som utvivlsomt, at der ikke er ret til at fremstille eksemplarer af et program på flere maskiner. Udtalelsen, der ikke sondrer mellem selve fremstillingen af eksemplarer, henholdsvis anvendelsen af disse eksemplarer i en brugssituation, er efter min opfattelse diskutabel, og der kan ikke siges at have fæstnet sig nogen klar praksis i branchen om, hvad der er sædvanlig på dette område, jf. bemærkningerne herom ovenfor.

Tredjemandsbrug

§ 36 tager ikke stilling til, om tredjemand har ret til at benytte et program, som er licenseret til licenstagerens brug i dennes virksomhed. Som bestemmelsen er formuleret, retter den sig mod den, der har ret til at "benytte" et eksemplar af et edb-program. I mangel af særlig angivelse må dette begreb antages at knytte sig til den enkeltperson eller den type af brugere, der almindeligvis må forventes at benytte den eller de terminaler eller *klienter*, som programmet anvendes på. Hvilken personkreds, dette nærmere er, beror på det førnævnte formålskriterium, og der er ikke megen støtte for fortolkningen at hente i andre ophavsretlige regler. At ophl. § 19, stk. 3, forbyder "udlån" spiller i den forbindelse en mindre rolle, eftersom begrebet udlån her anvendes som et eksempel på spredning: Når programmet er udlånt, ophører "udlånerens" ret til at benytte det, ganske som hvis programmet var spredt videre ved salg.

Sikkerheds-kopiering

Foruden den form for eksemplarfremstilling, der er *nødvendig* af hensyn til programmets anvendelse (brug), tillader § 36, stk. 1, nr. 2, tillige fremstilling af et "reserve- og sikkerhedseksemplar", for så vidt det er nødvendigt for benyttelsen af det. Denne præceptive (jf. stk. 3) bestemmelse skal næppe forstås bogstaveligt. I den engelske tekst bruges præpositionen "a", og ikke tallet "one". Bortset fra dens præceptive indhold vil adgangen til denne nødvendige kopiering derfor svare til, hvad der allerede følger af ophl. § 36.

I sin redegørelse af 10. april 2000 (COM(00) 199 final) til Rådet, Parlamentet, og det Økonomiske & Sociale Udvalg om virkningerne af direktiv 91/250/EØF om retlig beskyttelse af edb-programmer, har Kommissionen angivet en anden holdning til dette spørgsmål. I afsnit VII vedrørende direktivets art. 5, stk. 2, slår Kommissionen fast som sin opfattelse, at retten til at frembringe "et" sikkerhedseksemplar skal forstås bogstaveligt, omend opfattelsen herom tilsyneladende er delt. Kommissionen har ingen særlig fortolkningskompetence, og dens opfattelse på dette punkt nyder ikke almen anerkendelse. Spørgsmålet må betragtes som uafklaret, indtil EF-domstolen har udtalt sig om det.

I reglen om, at brugeren alene må foretage de eksemplarfremstillinger, der er nødvendige for hans brug af programmet, ligger modsætningsvis, at en kopiering, der alene bæres af ønsket om at undersøge programmets tekniske struktur – såkaldt *reverse analysis* – med henblik på at fremstille et ligeartet produkt med samme basale tekniske funktioner, ikke er tilladt efter bestemmelsen. Se dog nedenfor i afsnit 7.4.f.

Rettens ophør

Ophl. § 36 giver ingen regler for, hvor længe det kopierede eksemplar må bestå. Hvis ejeren af eksemplaret spreder dette videre, mister han alene retten til at udnytte det. Ophavsretsloven forbyder ham ikke at beholde sine gamle sikkerhedskopier – blot må disse kopier ikke anvendes uden rettighedshaverens tilladelse, cf. *Wagle & Ødegaard* (1997), s. 314, der på ophavsretligt grundlag når til, at der gælder en egentlig sletningspligt. Resultatet kan ikke tiltrædes. At søge en sådan pligt gennemført mod en programbruger, der måske slet ingen forudsætninger har for at vide, hvor på hans system det nu bortsolgte program har frembragt ophavsretligt beskyttede eksemplarer af sig selv, må forekomme særdeles problematisk. I særlige tilfælde vil en sådan forpligtelse dernæst kunne gå ud over brugerens mulighed for – lovligt – at anvende den information, der er frembragt ved hjælp af det nu bortsolgte program. De bevishensyn, der kan tale for en sletningspligt, gør sig gældende i begge tilfælde: Det forekommer ligeså vanskeligt for rettighedshaveren at skulle bevise, at der fortsat *befinder sig* programkomponenter på brugerens udstyr, som det er at bevise, at han rent faktisk *bruger* dem.

Dermed har lovgiveren viselig undgået at tage stilling til, hvornår en programkopi kan siges at være ophørt med at eksistere. Dette problem dukker imidlertid op med modsat fortegn, nemlig ved overdragelser af (typisk brugte) medier. Hvis man "kun" har slettet programelementerne ved hjælp af de sædvanlige kommandoer hertil, og det ved brug af alment benyttede *utilities* er muligt at genskabe de slettede filer, må det pågældende me-

dium fortsat betragtes som bærer af et eksemplar, sml. dommen om advokatkontoret i *U 1996.1538 ØLK*. De fleste styresystemer giver brugeren let mulighed for at genskabe filer, som den uheldige bruger uforvarende har slettet. Man må derfor nå til, at der eksisterer et eksemplar, indtil det fysisk er *slettet*, f.eks. ved, at mediet reformateres eller overskrives, og at lagermedier med eksemplarer, der kan genskabes med de rette værktøjer, (fortsat) må betragtes som *eksemplarer* af de pågældende programmer.

Denne antagelse fører bl.a. til en regel om, at *overdrageren* af et digitalt medium, hvorpå der har været indlæst kopier af et beskyttet program, har en ophavsretlig pligt til at reformatere eller overskrive mediet, således at eksemplaret ikke uden videre kan bringes tilveje igen. Bryder han den, overdrager han et eksemplar af det pågældende værk og udsætter sig for de ophavsretlige sanktioner (herunder forbud, erstatning og straf), som dette implicerer.

Password-licenser

Undertiden leveres programmer eller data på lagermedier, som brugeren alene tillades adgang til efter betaling og efter udlevering af password. Dette gælder f.eks. for visse demo-disketter, der med eksemplets magt søger at overbevise kommende brugere om programmets kvaliteter, eller om visse CD-ROM-applikationer, hvor brugerne alene forventes at skulle råde over en del af de indlæste tekster. Den bruger, der ved hjælp af særlige teknikker skaffer sig adgang til sådanne filer, vil enten udføre en uautoriseret eksemplarfremstilling eller hidføre en uautoriseret *fremførelse* af programmet, jf. nærmere 6.3.f. Det forhold, at brugeren lovligt har mediet i sin rådighed, legitimerer med andre ord ikke sådanne handlinger.

7.4.c. Retten til fejlretning

Som nævnt ovenfor giver ophl. § 36, stk. 1, nr. 1, bl.a. brugeren ret til at rette fejl i programmet. En fejlretning vil altid indebære, at der sker en *eksemplarfremstilling* af det pågældende program, allerede fordi programmet må befinde sig i RAM, når fejlretningen udføres. Men udover denne nødvendige eksemplarfremstilling vil en fejlretning efter omstændighederne kunne indebære, at værket gøres tilgængeligt for almenheden i en *ændret* skikkelse, jf. bemærkningerne herom i afsnit 6.2.d. Af hensyn til denne særlige situation er der givet udtrykkelig hjemmel til brugerens fejlretning.

Den tidligere ophl. § 42a fastslog udtrykkeligt, at en aftale om ret til at udnytte et program medfører ret til at foretage sådanne ændringer i programmet, som er nødvendige for den aftalte udnyttelse. Denne adgang fremgår nu forudsætningsvis af ophl. § 36. Adgangen til at foretage ændringer kan fraviges ved aftale, sml. § 36, stk. 4.

Bestemmelsen tager ikke stilling til, hvilken karakter den fejl, der giver ret til at ændre programmet, skal have. I vurderingen af dette spørgsmål må der på den ene side lægges vægt på fejlens mere eller mindre graverende karakter og på den anden side på omfanget af den ændring, der kræves for at rette fejlen. Er der tale om en forholdsvis bagatelagtig fejl, der til gengæld kan rettes gennem en simpel fejlrettelse, må en sådan rettelse være berettiget. Kræves derimod mere omfattende indgreb må man formentlig kræve, at der er tale om mere gennemgribende fejl. Også kontrakts- og forudsætningssynspunkter må spille ind. Fejl, som brugeren har – eller burde have – kendt til inden erhvervelsen kan således ikke begrunde en fejlrettelse.

7.4.d. Aftalelicens

Begrebet "aftalelicens", som det benyttes i ophavsretsloven, dækker over den ordning, loven etablerer, når en repræsentativ organisation af rettighedshavere kan indgå aftale om ophavsretlig udnyttelse af visse værker på rettighedshavernes vegne efter nærmere fastsatte regler. Det særlige ved ordningen består i, at ophl. giver den pågældende organisation eksklusiv kompetence til at indgå sådanne licensaftaler. En enkelt rettighedshaver, der falder inden for den pågældende aftalelicensbestemmelse, kan altså ikke modsætte sig tilladelsen og kræve op på egne vegne. Da aftalelicensreglen for så vidt udgør et indgreb i den enkelte rettighedshavers ret til at disponere over egne værker, kræver regler herom udtrykkelig lovhjemmel. Af samme grund fortolkes de regler, der hjemler en aftalelicens, almindeligvis snævert. Er der hjemmel for aftalelicens til eksemplarfremstilling ved "fotokopiering", kan denne hjemmel ikke anvendes til at fremstille eksemplarer i digital form, selv om den funktionelle forskel kan fortone sig.

En sådan findes i lovens §§ 13-14 (om eksemplarfremstilling af *værker* inden for henholdsvis undervisnings- og erhvervsvirksomhed mv.), § 17, stk. 5 (om eksemplarfremstilling af *værker udsendt i radio eller fjernsyn* til syns- og høre-handicappede), § 23, stk. 2 (om gengivelse af *kunstværker* i visse antologier), § 30 (brug af *værker* i radio og tv) og § 35 (om kabelspredning).

Det har ved forskellige lejligheder været diskuteret, om der burde tilvejebringes aftalelicens for brug af visse værker i digital form. Ved den lovændring, der fandt sted i 1998, blev ophl. § 13 ændret således, at den aftalelicens, der i forvejen gjaldt efter denne bestemmelse til brug i undervisningsvirksomhed, nu også omfatter eksemplarfremstilling i digital form, herunder via Internet mv. En række forfatterorganisationer havde ellers, med støtte fra bl.a. Forskningsministeriet, lagt pres på Kulturministeriet for at opnå en tilsvarende digital aftalelicens på det erhvervsmæssige område. Men efter stærk modstand fra udgiverside blev denne adgang ikke givet. Derfor er der fortsat kun hjemmel til aftalelicens til eksemplarfremstilling på det erhvervsmæssige område, når det gælder eksemplarer frembragt ved fotokopiering "eller lignende", jf. ophl. § 14. Hvor denne regel på det erhvervsmæssige område vel afgiver hjemmel for aftalelicens til digitalt baseret *foto*kopieringsudstyr, er der altså ikke hjemmel til at give aftalelicens til digital eksemplarfremstilling i lokale datanet (LAN) eller på Internet. Ønsker brugeren en sådan anvendelse, må de nødvendige aftaler derfor indgås med rettighedshaverne selv.

7.4.e. Særligt klausulerede licenser

Overdragelse af mere kostbare programprodukter, hvad enten disse er standardiserede, tilpassede eller resultatet af en individuel programudvikling, ledsages ofte af licensklausuler, der på forskellig måde begrænser den ret, brugeren ellers ville have i henhold til ophl. § 36. Hvordan denne nærmere afgrænsning skal finde sted – og om dette tema overhovedet skal gøres til genstand for særskilt aftaleregulering – beror på en vanskelig forretningsmæssig afvejning. I denne afvejning indgår navnlig muligheden for at give kunden mest mulig nytte af produktet gennem en udstrakt frihed til at benytte som et hensyn, der står overfor risikoen for, at denne frihed underminerer det økonomiske udkomme af produktet.

Det er ikke ualmindeligt, at programleverandører sætter sig ud over denne afvejning ved at *ændre licenspolitik* ved næste opdatering af programproduktet. Kunden "lokkes" til at erhverve det pågældende program pga. de frihedsgrader, der gælder for dets første version; men når en senere version skal installeres, er frihedsgraderne snævret ind og betalingen sat i vejret. I denne situation vil en udskiftning koste dyrt i nyanskaffelse, implementering og uddannelse, og mange kunder vil derfor vælge at acceptere denne skærpelse, selv om den for så vidt var uforudset og måske – i bagklogskabens lys – ville have afholdt ham fra at have anskaffet førsteversionen. Risiko-

en for sådanne forretningsformer kan imødegås, hvis en programlicens er genstand for en forretningsmæssig forhandling, der resulterer i en aftaleregulering af licensvilkårene også for senere versioner.

Som udgangspunkt har parterne fri adgang til at klausulere en ophavsretlig licens. Også her kræver det særlig hjemmel at fravige det almindelige princip om aftalefrihed. En sådan hjemmel findes i de præceptive regler i ophl. § 36, stk. 1, nr. 2, om retten til fremstilling af et sikkerhedseksemplar og § 36, stk. 1, nr. 3, om retten til at besigtige med henblik på at opnå kendskab til bagvedliggende idéer og principper. Herudover kan licensvilkår tænkes at kollidere med den ugyldighedssanktionerede forbudsregel i konkurrencelovens § 6, stk. 2, nr. 5, der – blandt andre vilkår – forbyder sådanne, som stiller som betingelse for indgåelse af en aftale, "at medkontrahenten godkender tillægsydelser, som efter deres natur eller ifølge handelssædvane ikke har forbindelse med aftalens genstand."

Der har endnu ikke været afgørelser om den konkurrenceretlige gyldighed af sådanne klausuler herhjemme, selvom der i aftalepraksis utvivlsomt forekommer mange eksempler på vidtgående bindinger af denne art. Problemstillingen har givet anledning til en vis praksis i USA, jf. i det hele *Thomas Riis* i Jurlebog fra Juridisk Institut 1999, s. 33 ff. Kapitel 5 (s. 133-171) i Konkurrencestyrelsens *Konkurrenceredegørelse 2000* indeholder en oversigt over nogle af de konkurrenceretlige problemer, der gør sig gældende på det danske marked for softwarelicenser.

Enkeltbrugerlicenser

Ved overdragelse af standardprogrammer til enkelte brugere klausuleres den medfølgende licens ofte således, at brugeren opnår en tilladelse til at fremstille et enkelt eksemplar af programmet og med en begrænsning, der indebærer, at kun licenshaveren selv og dennes ansatte må bruge det pågældende produkt. Bestemmelser af sidstnævnte slags suppleres ofte med klausuler, der forpligter licenshaveren til at *hemmeligholde* de oplysninger, der opnås gennem denne brug. En sådan aftale rammes ikke af forbuddet i ophl. § 36, stk. 3, der alene knytter sig til brugerens ret til *selv* at opnå den pågældende viden. Det bemærkes i den forbindelse, at § 36 ikke har indbygget en bestemmelse svarende til § 37, stk. 2, nr. 2, om ret til videregivelse af oplysninger til tredjemand.

Flerbrugerlicens

I det omfang, vilkår af den førnævnte art klausuleres således, at flere end brugeren selv opnår ret til at betjene sig af programmet, taler man om en flerbrugerlicens. Sådanne licenser kan udformes på vidt forskellige måder, afhængigt af hvilken type program der er tale om (herunder hvor specielt, henholdsvis standar-

diseret, dette er), og hvilken licensafgift der forudsættes erlagt (som et engangsbeløb eller løbende).

Site-licens

En ofte anvendt variant er som nævnt den såkaldte *site-licens* (også kaldet virksomhedslicens eller *company license*), hvorefter programmer må anvendes på en hel virksomhed, uanset hvor mange medarbejdere eller IT-arbejdspladser, der befinder sig på denne. I sådanne aftaler bør der tages stilling til, hvilken ret medarbejdere har til at anvende programmer på bærbare terminaler, ligesom der bør tages stilling til licensforholdene ved opkobling til systemet udefra. For at sikre sig imod, at konkurrerende leverandører får kendskab til systemet, og måske ligefrem anvender dette kendskab til skade for rettighedshaveren (f.eks. ved at tilbyde programvedligeholdelse), vil rettighedshaveren ofte afskære brug af programmet, der ikke udvirkes af medarbejdere hos brugervirksomheden.

Platforms-licens

En anden type flerbrugerlicens er den såkaldte *platformslicens*, hvor der gives tilladelse til, at programmet anvendes på en CPU på en bestemt maskinkonfiguration, der f.eks. er præciseret i henseende til mærke, kapacitet og brugerantal mv. (jf. herom nedenfor). Sådanne licensvilkår indgås ofte vedrørende større operativsystemer til *mainframe* computere.

Bruger-begrænsning

Uanset licensstrukturen vil flerbrugerlicensen skulle tage stilling til, hvilke – og hvor mange – brugere, der må anvende programmet. En variant er den *numeriske begrænsning*, hvorefter kun et bestemt antal brugere må anvende programmet. Dette antal kan da enten beregnes som antallet af *samtidige brugere* (hvilket alt andet lige vil føre til en højere licensafgift pr. bruger) eller som et antal *mulige brugere* (hvorved licensbetalingen pr. bruger vil være lavere, men brugerintensiteten til gengæld også lavere). En række tekniske og økonomiske forhold vil være afgørende for valget mellem disse forskellige typer af udformninger.

- antal mulige brugere

For et program, som erfaringsmæssigt bruges fra morgen til aften (f.eks. styresystemer eller applikationsprogrammer til f.eks. regneark eller tekstbehandling), har leverandøren interesse i at knytte brugsretten til antallet af mulige brugere. En sådan klausulering er ligeledes lettere at håndtere for brugeren, idet risikoen for flaskehalsproblemer reduceres.

- samtidige brugere

Derimod vil programmer, der typisk anvendes under mere enkeltstående funktioner (f.eks. visse databaseprogrammer mv.), oftere være klausuleret ud fra, hvor mange samtidige brugere der kan kobles op på denne applikation. I sådanne tilfælde vil leverandøren typisk forsyne programmet med en anordning, der registrerer, hvor mange samtidige brugere der er koblet på, og lukker

ned, når grænsen er nået. Sådanne anordninger har til gengæld den for brugeren besværlige – men jo altså tilsigtede – virkning, at programmet ikke er tilgængeligt, når grænsen er nået.

Udfyldning

Typeforudsætningslæren har dog også gyldighed ved forståelsen af flerbrugerlicensens rækkevidde, for så vidt disse licenser ikke tager klart stilling til, om en bestemt udnyttelsesform (f.eks. ved aftaler om facility management eller outsourcing) er tilladt. Ifølge de i afsnit 7.4.b. citerede bemærkninger til 1989-lovforslaget ligger det således klart, at "nødvendig brug" ikke indebærer en ret til at kopiere programmet på en måde, så flere brugere (uden at have særskilt tilladelse) samtidigt kan betjene systemet fra flere arbejdspladser hos brugeren. Er der f.eks. givet en licens til to brugere, må dette betyde "to samtidige brugere", der betjener systemet fra hver sin terminal, jf. mine bemærkninger a.st.

Betaling

Aftaler om flerbrugerlicenser rejser et vanskeligt problem om, hvad der skal betales: Hvor det er forholdsvis enkelt for leverandøren at føre en fast prispolitik mht. enkeltbrugerlicenser, kan det volde større vanskelighed at fastslå betalingspligten for et program, som alle i en virksomhed i princippet gerne skulle kunne have adgang til, selvom det ligger klart, at de færreste medarbejdere vil få reelt brug for den i det daglige. Forhandlingerne om disse spørgsmål baseres undertiden på et princip om, at der skal erlægges et beløb, der giver rettighedshaveren en passende kompensation, f.eks. ud fra en vurdering af, hvor mange brugere der gennemsnitligt kan forventes at bruge programmet. En anden kilde til tvivl opstår for brugere, der driver virksomhed på tværs af landeskel, og som ønsker at installere programmet i flere lande samtidigt.

Andre licensformer

Udover de førnævnte typer af licenser, støder man på særlige licensklausuler i forbindelse med softwareudvikling. Et praktisk eksempel herpå er den såkaldte *run time*-licens, som giver brugeren ret til at indbygge et program i et andet program, som herefter under ét gives i licens til slutbrugeren.

7.4.f. Reverse analysis

Problemstillingen

Læser man ophl. § 36, stk. 1, nr. 1, isoleret, forbyder den brug af et program, der ikke tilsigter anvendelse af dets funktioner (tekstbehandling, regneark, e-post mv.), men som kun har til hensigt at aflure dets tekniske egenskaber med henblik på plagiering. Dette følger af, at § 36, stk. 1, nr. 1, henviser til brugerens subjektive formål. Og leverandørens tanke med at give brugeren licens til et

program er jo så åbenbart ikke at gøre brugeren til sin konkurrent!

Analyse

For at muliggøre den udveksling af almindelige oplysninger om programmers funktionalitet mv., der er nødvendig for at understøtte den teknologiske udvikling, kan det være nødvendigt at benytte programmet på en måde, der ikke er nødvendigt af hensyn til den praktiske brug, jf. ophl. § 36, stk. 1, nr. 1. Ifølge samme bestemmelses stk. 1, nr. 3, er det imidlertid tilladt den lovlige bruger af et program – uden rettighedshaverens tilladelse – at besigtige, undersøge eller afprøve programmet for at fastslå, hvilke idéer og principper der ligger til grund for de enkelte elementer af det. Det kræves blot, at disse undersøgelseshandlinger finder sted i forbindelse med en indlæsning, visning, kørsel, overførelse eller lagring af programmet, som licenstageren i øvrigt er berettiget til at foretage.

Black box-analyse

Med denne regel er der skabt grundlag for gennemførelse af en såkaldt *black box-analyse* af edb-programmer. Hermed sigtes til undersøgelseshandlinger, der udelukkende retter sig mod de data, programmet modtager og afgiver, men som ikke indebærer nogen kopiering eller transformering af selve programmet udover den, programmet er beregnet til selv at foretage. Sådanne former for analyse kendetegnes ved at kunne ske på grundlag af en kopiering svarende til den, en "almindelig" bruger vil være nødt til at udvirke.

Grænsen mellem de kopieringshandlinger, der har denne karakter, og den egentlige dekompilering, jf. herom nedenfor, kan være vanskelig at drage. I NIR 1992.79 antager *Thomas Vinje*, at brugeren f.eks. har ret til at udvirke hexadecimale skærmbilleder af objektkoden på skærmen. Dette resultat kan kun tiltrædes i det omfang, en "sædvanlig" bruger vil have anvendelse for den således frembragte kopi af objektkoden, hvilket nok vil høre til undtagelsen. *Plogell* (1996), s. 43, antager, at den ret, brugeren har til at ændre programmet i medfør af den legale programlicens, "teoretiskt sett" også giver ret til at dekompilere, f.eks. ved brug af såkaldte linetracers eller disassemblers, altså værktøjer, der giver indblik i, hvorledes bestemte elementer i programmet fungerer. Heller ikke denne antagelse kan tiltrædes. Var denne mulighed åben i medfør af ophl. § 36, stk. 1, nr. 3, ville den ganske opslue anvendelsesområdet for § 37 og gøre denne bestemmelses enkelte betingelser overflødige.

Informationstilegnelse

§ 36, stk. 1, 3. pkt., indebærer f.eks., at det er tilladt at anvende et program for at tilegne sig information om dets brugergrænseflade, også selv om dette sker med henblik på frembringelse af et andet program, der dækker samme marked. Betingelsen er blot, at brugeren af det pågældende program har "ret til at benytte" det,

og at de eksemplarfremstillinger mv., der udføres med henblik på at tilegne sig den pågældende information, i øvrigt ligger indenfor den gældende licens (sådan indlæsning, visning på skærm, kørsel, overførsel, lagring eller lign. af programmet, som vedkommende er berettiget til at udføre). I modsætning til lovens § 37 gælder der ingen begrænsninger i, hvorledes den pågældende information kan anvendes. Der er således intet til hinder for, at informationen spredes videre til almenheden, f.eks. i forbindelse med et offentligt udbud, jf. om disse regler afsnit 21.2.d.

7.4.g. Reverse engineering

Udtrykket reverse engineering stammer fra læren om erhvervshemmeligheder. Her er det almindeligt antaget, at almenheden (og konkurrenterne) har en ret til at trække tekniske oplysninger ud af produkter, der findes i den almindelige handel, ved at skille dem ad mv. En sådan ret gælder principielt også for *IT-produkter*. Problemet ved at udføre reverse engineering på *edb-programmel* er imidlertid, at det typisk kun er muligt at se "indmaden" i et program ved at frembringe eksemplarer af det, enten som forskellige stadier af arbejdskopier i en proces, der fører til en dekompilering af koden, eller som de teknisk nødvendige maskinkopier, der nødvendigvis skal ske til RAM, når processen udføres. Der er tale om en arbejdskrævende proces, der bl.a. indebærer en analyse af hver af de processor-instruktioner, programmets objektkode genererer. Opgaven består altså ikke i, populært sagt, at sætte program-oversætteren (*compileren*) i bakgear. En sådan mulighed findes ikke ved generering af objektkode, ligeså lidt som det lader sig gøre at frembringe det oprindelige stykke kød ved at køre kødhakkemaskinen baglæns.

Ophl. § 37, der har rod i art. 6 i direktiv 91/250/EØF, regulerer kun en del af den proces, der almindeligvis betegnes som reverse engineering. Bestemmelsen tillader visse former for kopiering – udført i forbindelse med såkaldt dekompilering – når denne sker med henblik på at skabe interoperabilitet mellem det kopierede program og et selvstændigt udviklet edb-program. Begrebet interoperabilitet beskriver det forhold, at to programmer kan fungere sammen, på samme måde som en CD kan afspilles på en CD-maskine og to Lego-klodser kan sættes sammen. Reglerne hviler på et udgangspunkt om, at dekompilering som hovedregel er forbudt. Men hvis den sker med henblik på interoperabilitet *kan* den være beføjet inden for de rammer, bestemmelsen sætter.

Bestemmelsen er meget vanskelig at læse. Vanskelighederne skyldes ikke alene det komplicerede tekniske problem, der ligger bag, men også den intense politiske kontrovers, der førte til dens indførelse. Denne kontrovers udspringer af et skisma mellem på den ene side hensynet til rettighedshaverens eneret, og på den anden side en konkurrenceretlig interesse i at undgå, at eneretten til et enkelt værk de facto forvandler sig til en eneret også til forskellige typer af omkringliggende værker i form af tilbehør mv. Se hertil *Jens Schovsbo* i NIR 1997.29 f.

"Dekompilering"

Selv om ordet "dekompilering" sprogligt udgør en modsætning til "kompilering", er der tale om to principielt forskellige begreber. Hvor kompilering (eller oversættelse) sker i en automatiseret proces, der styres af en *compiler*, og som kun kan udføres på én måde, er dekompilering en principielt anderledes proces. Udgangspunktet er et kendskab til de funktioner, programmet udfører under anvendelsen, f.eks. en måde at kommunikere med en hardware-enhed på. Med dette udgangspunkt udføres en arbejdskrævende proces, der ved at udsætte programmet for en række påvirkninger søger at rekonstruere centrale dele af den bagvedliggende kildetekst. Opgaven består så at sige i at arbejde sig baglæns fra den digitale objektkode til det instruktionssæt, der ligger bag. Kompleksiteten af denne proces beror på det anvendte programmeringssprog: Ganske få linjer kildekode kan i kompileret stand resultere i et antal programlinjer, der er hundrede eller tusinde gange større. Se generelt til problemstillingen *Bjerke* i Complex 9/1994.

Hvor vanskeligt det er at gennemføre en dekompilering beror på programmets karakter. Java-programmer er f.eks. følsomme overfor dekompilering, fordi programmet kompileres til et mellemkodestadium, inden det omdannes til maskinkode. Fra dette stadium er det forholdsvis enkelt at gennemføre dekompileringen: De enkelte instruktioner er relativt enkle at identificere, omend programmørens bemærkninger og kommentarer ikke er. Trods den lethed, hvormed man kan nå dette mellemkodestadium, gælder de almindelige regler om dekompilering. Reglerne må i den forbindelse ses i sammenhæng med den almindelige legale programlicens med dens formålsbeskrivelse – ikke som et udtryk for, at den, der dekompilerer et program, må belønnes for sin indsats herved.

Hvem må dekompilere?

Ifølge ophl. § 37, stk. 1, nr. 1, må dekompilering for det første kun udføres *af licenshaveren* eller af en anden person, der har *ret til at benytte* et eksemplar af et edb-program, eller på disses vegne af en person, der har tilladelse hertil. Dette sidste led i bestemmelsen synes at forudsætte, at retten til at dekompilere kan delegeres til andre end licenshaveren. Denne situation vil da

også være den praktisk forekommende, eftersom de færreste edb-brugere vil have ekspertise til selv at forestå disse handlinger.

Hemmeligholdelse

Bestemmelsen har ikke taget stilling til, om reverse engineering er tilladt, hvis licensaftalen indeholder en hemmeligholdelsesaftale. På den ene side kan man argumentere for, at en sådan aftale ikke kan være bindende, da retten til reverse engineering er præceptiv, jf. ophl. § 37, stk. 3. Heroverfor står det synspunkt, at en hemmeligholdelsesaftale etablerer et særskilt immaterialretligt retsværn, jf. mfl. § 10, der går på tværs af reglerne i ophavsretsloven, jf. nærmere afsnit 10.5.b., og som principielt er ligeværdigt med andre industrielle rettighedsformer (som f.eks. patentretten og brugsmodelbeskyttelsen).

Efter min opfattelse har det sidstnævnte synspunkt mest for sig. Ifølge art. 9, stk. 1, i direktiv 91/250/EØF viger direktivet for andre retsforskrifter, herunder vedrørende patenter og forretningshemmeligheder. Den begrænsning i adgangen til at udføre reverse engineering, der følger af at anerkende aftaler om hemmeligholdelse, adskiller sig ikke mærkbart fra den, der følger af at skulle anerkende patentretlige begrænsninger. Hemmeligholdelsesvilkår er almindeligt forekommende i licensaftaler om mere kostbare standardprogrammer, hvor de også søges håndhævet efter deres indhold.

Denne antagelse fører dog ikke til, at man blot ved at indbygge en "hemmeligholdelsesaftale" i en licensaftale – f.eks. i en *shrink wrap*-licens – kan bringe sig uden om det præceptive forbud i ophl. § 37, stk. 3. Der skal være tale om et aftalemæssigt arrangement, som reelt sigter til at bevare de hemmeligheder, programmet indeholder, og som også søges håndhævet med dette formål. Har aftalen alene til formål at undgå brugerens ret til reverse engineering, rammes den af præceptiviteten. Dette vil i praksis altid ske for shrink wrap-aftaler, der jo kendetegnes ved, at rettighedshaveren end ikke kender sin licenstager og derfor heller ikke ved, hvem han deler sin "hemmelighed" med.

Tredjemandsbistand

Man kan diskutere, under hvilke rammer tredjemand kan udøve reverse engineering på programmet. Af det førnævnte følger, at en licenstager – hvor der ikke er aftalt hemmeligholdelse – kan lade tredjemand udføre reverse engineering på licenstagerens egen installation og under anvendelse af den licens, der er erhvervet for den pågældende installation, se § 37, stk. 1, nr. 1, in fine. Disse spørgsmål må løses på grundlag af en fortolkning af ophl. § 36. Som tidligere anført kan § 36 næppe give grundlag for en regel om, at der kun må sidde en enkelt person ved den terminal, hvorfra programmet afvikles. Brugeren må som udgangspunkt

godt lade en rådgiver eller kollega "sidde med" ved skærmen. Lægges dette resultat til grund, må det også antages, at brugeren kan lade en rådgiver betjene sig af programmet, hvis blot brugeren ikke gør det. Licensen genbruges jo i så fald ikke. Denne frihed kan dog være afskåret i kontrakten, jf. ophl. § 36, stk. 3, modsætningsvis. Af denne regel følger, at reglerne om den legale programlicens netop ikke er præceptive.

Derimod kan licenstageren ikke overdrage et eksemplar af programmet til tredjemand med henblik på, at denne på eget udstyr skal foretage de nødvendige analyser for derefter at levere programmet tilbage til den egentlige bruger. En sådan handling vil blive betragtet som "udlån" uden for den private sfære, der må anses for afskåret gennem reglen i ophl. § 19, stk. 3. Derimod er det tvivlsomt, om en udefra kommende rådgiver har ret til at benytte en enkelt brugers licens til programmet gennem en opkobling udefra, der foretages på brugerens vegne (således at denne ikke samtidig gør brug af programmet). Spørgsmålet bør løses med udgangspunkt i en fortolkning af den pågældende licensaftale.

Plagiering

Ifølge ophl. § 37 er der ikke ret til at udføre reverse engineering, hvis formålet er at frembringe et program, der plagierer det oprindelige program, se herved § 37, stk. 2, nr. 1) – 2). Det fremgår heraf, at formålet med handlingen skal være at gøre et *selvstændigt udviklet* edb-program interoperabelt. At det program, reverse-ingeniøren forbereder, vil konkurrere med det eksisterende program, er ikke til hinder for reverse engineering, uanset om konkurrencen retter sig mod givne IT-funktioner. Netop denne konkurrencemæssige problemstilling var en af hovedårsagerne til den så intense debat, der gik forud for reglernes vedtagelse i 1991. Indenfor de ovennævnte rammer er der imidlertid intet til hinder for, at licenstageren lader en potentiel budgiver udføre den dekompilering, der er nødvendig for at kunne specificere grænsefladen. Betingelserne for at overlade en sådan opgave til tredjemand er de samme, hvad enten tredjemand opererer som konsulent eller som potentiel leverandør til licenstageren.

Offentliggørelse

Ifølge § 37, stk. 1, nr. 2, er dekompilering ikke tilladt, såfremt de oplysninger, der er nødvendige for at tilvejebringe interoperabilitet, tidligere har været og er let og hurtigt tilgængelige for den personkreds, der har ret til at udføre dekompileringshandlingerne. Denne regel, der har historisk udspring i de konkurrenceregulerende vilkår, Kommissionen havde pålagt en større IT-virksomhed (IBM), indebærer, at rettighedshaveren har mulighed for helt

at afskære dekompileringshandlingen ved blot at offentliggøre de pågældende grænseflade-specifikationer. Bestemmelsen tager ikke stilling til, om rettighedshaveren kan forlange nogen betaling for at stille disse oplysninger til rådighed. I det omfang, rettighedshaveren kan siges at have egentlige udgifter i forbindelse hermed, må det formentlig være berettiget at opkræve en betaling, der nogenlunde modsvarer disse udgifter. I den forbindelse kan man skele til den praksis, der er fastlagt ved visse standardiserings-organisationer (herunder ETSI), og som tillader en ikke-diskriminerende betalingsopkrævning, såfremt en standard er omfattet af immaterielle rettigheder, jf. herom afsnit 5.3.g.

Afgrænsning

§ 37, stk. 1, nr. 3, fastslår for det tredje, at dekompileringshandlingerne skal være begrænsede til "de dele af det oprindelige edb-program, der er nødvendige for at opnå interoperabilitet". På grund af denne bestemmelse vil det være i rettighedshaverens interesse at strukturere et program således, at de dele af det, der rummer grænseflade-specifikationerne, findes i klart afgrænsede elementer af programmet. Er der, som det ofte forekommer i dag, tale om objektorienteret programmering, hvor de forskellige dele af programmets funktioner er henlagt til forskellige moduler, vil det være muligt at lægge oplysningerne om interoperabilitet i en "object class", som i så fald kan dekompileres efter de i øvrigt gældende regler herfor.

Erhvervshemmeligheder

Ifølge § 37, stk. 2, gælder der særlige begrænsninger i, hvorledes den dekompilerende part kan råde over den herved indvundne information. For det første må vedkommende ikke benytte de indhentede oplysninger til andre formål end at gøre det selvstændigt udviklede edb-program interoperabelt. Oplysningerne må med andre ord betragtes på samme måde som erhvervshemmeligheder, jf. mfl. § 10, altså uden ret til at videregive oplysningerne til andre. Dette forbud gælder formentlig uanset, om modtageren af de pågældende oplysninger underkaster sig en erhvervshemmeligholdelsespligt, for hvor skulle grænsen i givet fald gå? En åbning for muligheden af at indføre sådanne forpligtelser ville dernæst skabe usikkerhed om, hvilke formål der kunne begrunde en overførsel til tredjemand. Visse formål ville f.eks. falde lige for (herunder konsulentpræget bistand ved programudviklingen) hvorimod andre ville falde klart uden for (f.eks. visse handlinger, der kunne *forberede* frembringelsen af et plagiatprodukt).

I USA er spørgsmålet om reverse engineering ikke reguleret af *Copyright Act*; men i praksis tegner der sig gradvis en retsopfattelse, der harmonerer med europæisk ret efter 1991-direktivet, baseret på principperne om "fair use". I sagen *Atari Games Corp. v. Nintendo of America Inc.*, 975 F.2d 832 (1992) antog CAFC, at midlertidig kopie-

ring med henblik på reverse engineering indebar "fair use", der som sådan ikke kolliderede med den ophavsretlige eneret. Et tilsvarende resultat nåede appelretten for 9. circuit til i et tilfælde, hvor reverse engineering var den eneste måde at skabe et konkurrerende værk, se *Sega Enterprises, Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (1992) og *Sony Computer Entertainment v. Connectix Corp*, 203 F.3d 596 (9th Cir., 2000). Afgørelsen i *Aymes v. Bonnelli*, 47 F.3d 23 (1995) antog tilsvarende, at den lovlige bruger af et eksemplar af et program havde ret til at ændre det med henblik på at opdatere dets funktioner til det forudsatte formål. I *Sony Computer Entertainment v. Connectrix Corp.*, 203 F 3rd 596 (9th Cir., 2000) fandtes det berettiget at foretage *reverse engineering* af en Playstation-maskine med henblik på at frembringe en maskine med tilsvarende grænseflader.

Clean room-teknik

For at imødegå indsigelser om, at det udviklede program plagierer kildetekst fra det program, der har været genstand for reverse engineering fra udviklerens side, anvender man ofte såkaldte *clean room*-teknikker. Teknikken går i korthed ud på, at de programudviklere, der skal frembringe det nye program, afsondres fuldstændigt fra de medarbejdere, der forestod arbejdet med at dekompilere. Teknikken er bl.a. omtalt hos *Schmidt* (1989), s. 238 f. og af *Bing* NIR 1999.290 f.

7.4.h. Programdistribution

Karakteristik

En aftale om distribution af programmel involverer to typer af transaktioner. Dels rummer aftalen et *licenselement*, idet rettighedshaveren giver tilladelse til, at det distribuerede program gøres til genstand for en eksemplarfremstilling og spredning, som ellers ville falde inden for hans eneret, jf. ophl. § 2, stk. 1 og 3. Dels – og i logisk forlængelse heraf – rummer aftalen et element af *distribution*, idet den tilladelse (licens), som rettighedshaveren giver hertil, tilsigter at nå et marked, der normalt vil være afgrænset som ved anden distribution, jf. herom i det hele *ET* s. 352 ff.

Øjemeddet tilsiger ikke, at der på dette sted gives en mere udtømmende gennemgang af de reguleringstemaer, der bør indgå i en sådan distributionsaftale. I overskriftsform kan det dog fremhæves, at parterne i det mindste bør aftale, hvad det nærmere er for *produkter*, der er omfattet af distributionsretten, *vederlaget* herfor, om distributionsretten er *eksklusiv* eller ikke (samt i givet fald, hvilket *territorium* distributionsretten gælder for), *prissætningen* i slutbrugerleddet, samt hvilken *rollefordeling* parterne ønsker i henseende til praktiske anliggender som f.eks. *retshåndhævelse* mv.

Distributionsformer

IT-retten kender mange eksempler på programdistribution, der er formet efter de særlige behov på IT-området.

- OEM/VAR

En hyppigt forekommende distributionsform er den såkaldte OEM-aftale (OEM = *Original Equipment Manufacturer*), der indebærer, at distributøren får ret til at distribuere det nævnte produkt, som om det var hans eget. Sådanne aftaler benævnes ofte også som *Value Added Reseller* Agreements (eller blot VAR-aftaler), fordi distributøren ofte forædler produktet med yderligere funktionalitet mv. eller ved at levere det i samspil med andre produkter. Producenten vil som regel kun have interesse i at indgå en sådan aftale, hvis han ikke selv planlægger at konkurrere inden for det nævnte område. Dette spørgsmål kan dog give anledning til særlig regulering (grænsedragning) af den art, der er velkendt inden for læren om distribution.

Som nævnt i *ET* s. 359 f. rejser aftalen bl.a. spørgsmål om, hvorledes distributøren skal forholde sig overfor krav, som han ifølge produktansvarslovens § 4, stk. 1, hæfter for, men som må tilskrives producentens forhold. Det er imidlertid tvivlsomt, om den danske mellemhandlerhæftelse kan opretholdes, efter at EF-domstolen ved sin dom af 25. april 2002 (C52/00) har underkendt en lignende lovbestemmelse i fransk ret. Spørgsmålet er for tiden genstand for en sag ved EF-domstolen, der forventes afgjort senere i 2005. Se nærmere *Jesper Lett* U 2002B.398 ff., *Vibe Ulfbeck* i U 2003B.1 ff. og *Martin Habersaat* i 2003B.122 ff.Andre problemer opstår omkring retten til de forbedringer, OEM-forhandleren indbygger i produktet.

- Tredjeparts-programmel

Som led i nutidens IT-implementering er det den praktiske regel, at der indgår et større eller mindre element af såkaldt tredjepartsprogrammel. Herved forstås programmel, som leverandøren leverer på licens fra en underleverandør (tredjepartsleverandøren) med henblik på indbygning som ingrediens i leverandørens endelige produkt. Indbygningen kan *enten* ske i fuldt integreret form, hvor slutbrugeren ikke ser, at det leverede system er opbygget gennem komponenter fra forskellige tredjepartsleverandører, *eller* som en kombineret komponentleverance, hvorved der leveres en flerhed af applikationer (f.eks. en Windows-baseret kontorpakke med Wordperfect-tekstbehandlingsprogrammel) i en samlet leverance.

Det definitoriske krav om, at produktet – for at blive betragtet som tredjepartsprogrammel – skal indgå som *ingrediens* i det færdige produkt indebærer bl.a., at et oversætter-program ikke betragtes som sådant: Når et program oversættes fra kildetekst til objektkode ved hjælp af et oversætterprogram, får man en ny version (objektkodeversionen) af det gamle program, men oversætterprogrammet har dermed udtømt sin rolle og følger ikke med som ingrediens. En omfattende undersøgelse af de juridiske, tekniske og kommercielle pro-

blemstillinger ved indkøb og brug af programmel fra underleverandører foreligger med *Jan Villumsen & Mads Bryde Andersen*: Indkøb og brug af programmel fra underleverandører (november 1993). Rapporten er udgivet af DELTA – Dansk Elektronik, Lys & Akustik for Datateknisk Forum.

Aftaler om integreret tredjepartsprogrammel giver anledning til vanskeligheder ved fastlæggelsen af de driftsmæssige krav til programmet: Hvad kan slutbrugeren forvente, og hvem hæfter for, at disse krav ikke er opfyldte? Man vil ofte stå overfor den velkendte problemstilling, at systemet ikke fungerer, men at ingen med sikkerhed kan sige, hvorfor. De spørgsmål, der her opstår i relation til slutbrugeren, drøftes nærmere i kapitel 22. Problemstillingen giver ofte anledning til vanskelige forhandlinger med slutbrugeren under aftaleforhandlingen. Brugeren vil ofte forvente, at leverandøren hæfter for tredjepartsprogrammets funktionalitet på samme måde som han hæfter for egne ydelsers funktionalitet, men leverandøren vil ofte værge sig herimod, da hans muligheder for at påvirke denne funktionalitet – uden rådighed over kildeteksten – vil være begrænsede.

Gennemgående temaer

Blandt de spørgsmål, der ofte indgår i aftaler vedrørende tredjepartsprogrammel, kan peges på følgende:

- rettigheder

Et af de mest centrale reguleringstemaer drejer sig om karakteren af de immaterielle retspositioner, der går over fra tredjepartsleverandøren til leverandøren (og derfra til slutbrugeren): Er meningen, at tredjepartsprogrammet integreres i den færdige løsning, vil aftalen mellem parterne almindeligvis forme sig som en almindelig *licensaftale*, der må fortolkes i overensstemmelse med det almindelige ophavsretlige specialitetsprincip, jf. ophl. § 53, stk. 3: Retten til at forhandle tredjepartsprogrammet vil f.eks. være begrænset til en bestemt type af applikationer, med virkning for et bestemt territorium og med bestemte mængdemæssige begrænsninger mv. – sidstnævnte bl.a. for at imødegå risikoen for, at der produceres et stort antal (hver for sig lovlige) eksemplarer, som i forbindelse med en senere tvangsfuldbyrdelse, jf. herom afsnit 12.2.b., afsættes til lav pris i konkurrence med de eksemplarer, rettighedshaveren selv har på markedet. Er der derimod indsat en mængdebegrænsning i licensaftalen, vil eksemplarer, der fremstilles på den forkerte side af denne grænse, kunne inddrages som retsstridige, jf. nærmere afsnit 12.3.b. .

Leveres tredjepartsprogrammet derimod som en *komponentleverance* (f.eks. som et tekstbehandlingssystem, der leveres sammen med et system til drift af lokalnet) er reguleringsbehovet begrænset: Slutbrugerens ret til at benytte programmet vil her

skulle udledes af ophl. § 36 på ganske samme måde, som hvis programmet var erhvervet i den almindelige handel. Af samme grund tager de følgende bemærkninger primært sigte på ingredienstilfælde.

- slutbruger-relationen

Visse leverandører stiller krav om, at der skal indgås særskilte licensaftaler med slutbrugerne, eventuelt effektueret i et direkte aftaleforhold mellem tredjepartsleverandøren og slutbrugeren. En sådan ordning anses dog generelt for at være upraktisk, da den ofte – konsekvent udført – vil resultere i ganske komplekse aftalerelationer mellem slutbrugeren og de ofte mange tredjepartsleverandører, der har leveret software-ingredienser til den endelige løsning. Det praktiske udgangspunkt er derfor, at aftaleforholdet med tredjepartsleverandøren reguleres i aftalen mellem slutbrugeren og leverandøren gennem en *inkorporering* af de licensvilkår, tredjepartsleverandøren har fastsat.

- kontrolforanstaltninger

For at styre leverandørens eksemplarfremstillinger vil tredjepartsleverandøren ofte indbygge anordninger, der indbygger et serienummer i hvert kopieret program eller udstyre dette med en nøgle, som skal tilvejebringes ad anden vej. Sådanne ordninger følges ofte op med procedurer, hvorefter leverandøren skal udarbejde produktionslister med serienumre for de produkter, tredjeparts-programmet indgår i. Kontrollen med disse lister kan variere, jf. generelt herom *PA* s. 347 ff.

- hemmeligholdelse

Som i andre distributionsaftaler vil det ofte forekomme, at producenten (leverandøren af tredjepartsprogrammet) i tillæg til selve licensen til programmet yder distributøren nogle tjenester, som udspringer af den *knowhow*, producenten har opbygget til sit program. Denne knowhow kan bl.a. dreje sig om, hvorledes programmet implementeres under forskellige tekniske eller driftsmæssige omstændigheder, eller om hvordan forskellige typer af kundeproblemer løses. Da information af denne art ofte vil have stor kommerciel værdi for producenten (bl.a. fordi den vil muliggøre en intens konkurrence med dennes produkter), vil producenten typisk ønske at belægge den med en pligt til hemmeligholdelse.

- kildetekstlicens

Hemmeligholdelsesforpligtelser vil i sagens natur også være aktuelle, hvis aftalen indebærer, at distributøren får rådighed over kildetekst. En adgang hertil kan f.eks. tænkes, når leverandøren har påtaget sig en pligt til at vedligeholde, tilpasse eller videreudvikle programmet. På grund af kildetekstens ekstremt følsomme karakter vil sådanne forpligtelser ofte være tæt klausuleret, f.eks. således at licensen alene gælder for særligt udpegede personer og under en løbende kontrol fra tredjepartsleverandørens side.

Support

Som nævnt vil leverandøren ofte påtage sig at supportere det samlede system, der leveres til slutbrugeren, dvs. også den del, der indeholder tredjepartsprogrammel. Uanset om en sådan vedligeholdelsespligt sker på grundlag af en kildetekstlicens eller ikke, vil mulighederne for at løse konkrete problemstillinger typisk lettes, hvis man har adgang til "intern" viden om systemet og dets opbygning. For at gøre denne viden tilgængelig, indbygger man ofte en forpligtelse for tredjepartsleverandøren til at yde særlige tjenesteydelser herom, både med sigte på den praktiske *implementering* i den enkelte transaktion og til brug for den efterfølgende *vedligeholdelse*.

- særlige spørgsmål

Foruden de førnævnte mere almene spørgsmål vil aftaler om programdistribution efter omstændighederne berøre en række specifikke spørgsmål. Et eksempel herpå er den aftaleretlige håndtering af de begrænsninger, der kan være forbundet med eksport af software, der kan indeholde komponenter af militærstrategisk betydning, til præsumptivt fjendtlige tredjelande, jf. nærmere herom afsnit 21.2.e.

Retsgrundlag

Aftaler om distribution af edb-programmel er som udgangspunkt ikke undergivet særlig lovregulering. Med handelsagentloven, lov nr. lov nr. 272 af 2. maj 1990 (herefter HAL) er der imidlertid indført særlige regler om distribution gennem handelsagentur, der efter omstændighederne kan få betydning også for programdistribution. Loven bygger på rådsdirektivet af 18. december 1986 om samordning af medlemsstaternes lovgivning om selvstændige handelsagenter (86/653/EØF), EFT 1986 L382/17, og er således EU-harmoniseret lovgivning. Da en del af lovens regler er præceptive (herunder navnlig reglerne i §§ 25-29, der hjemler handelsagenten ret til godtgørelse ved ophør), knytter der sig en betydelig interesse til at få fastslået lovens rækkevidde.

I U1995B.169 ff. har jeg gjort dette spørgsmål til genstand for en mere dybtgående analyse. De følgende bemærkninger bygger delvis herpå.

HAL regulerer visse typer af aftaler mellem en producent og en distributør, nemlig, jf. lovens § 2, aftaler, der involverer, at handelsagenten for agenturgiverens regning påtager sig "selvstændigt og vedvarende at virke for salg eller køb af varer ved at indhente tilbud (ordre) til agenturgiveren eller ved i dennes navn at indgå aftale herom". Enkeltstående dispositioner eller dispositioner, der indebærer, at distributøren indgår i et ansættelsesforhold for agenturgiveren, er ikke omfattet af loven.

Lovens varebegreb

Det springende punkt for, om HAL regulerer en softwaredistribution, er afgrænsningen af begrebet "varer". Anvendelsen af dette begreb skyldes, at loven oprindelig tog sigte på den egentlige varedistribution. Der er i den forbindelse enighed om, at fast ejendom, skibe, immaterialrettigheder, værdipapirer samt egentlige tjenesteydelser falder uden for begrebet. I grænsetilfælde – hvor der såvel formidles salg af varer som tjenesteydelser – er det ifølge lovens forarbejder afgørende, om varesalget er et dominerende element i aftalen. Således vil salg af fotokopieringsmaskiner med tilhørende service være omfattet af loven, hvorimod leverandører af rengøringssystemer, hvori også indgår salg af rengøringssystemer og -produkter, næppe vil være det.

Standardprogrammel

Om edb-programmel udtaler betænkningen om handelsagenter, nr. 1151/1988, s. 43: "Standard-edb-programmel, som markedsføres i mange eksemplarer, må anses som »varer«, hvorimod individuelt udviklede programmer snarere må opfattes som tjenesteydelser, hvis aftalen i overvejende grad vedrører levering heraf". Sædvanligvis defineres standardprogrammel som programmer, der er udviklet med henblik på massedistribution til vidt forskellige brugere med samme databehandlingsbehov. Denne begrebsafgrænsning peger på et velkendt marked af programmer, der typisk overdrages i »pakker« og under velkendte varemærker (»WordPerfect«, »Lotus 1-2-3«, »Windows« osv.). Det må antages, at hyldevareprogrammel, der ikke distribueres med tillægsydelser i form af implementering og tilpasning, falder *inden for* HAL, jf. mine bemærkninger i U1995B.172 f. Dette har f.eks. betydning i relation til de såkaldte standardramme-systemer. Sådanne systemer vil være *omfattet* af HAL, hvis de distribueres i ubearbejdet form. Ledsages distributionen derimod af et væsentligt element af tilpasning, vil transaktionen falde *uden for*. I denne afgrænsning spiller det også ind, hvilke ophavsretlige beføjelser, brugeren indtræder i. Opnår brugeren alene de ophavsretlige beføjelser, der er nødvendige for sin brug, taler dette for en vareanalogi. Udstyres han derimod med beføjelser til f.eks. at videresælge programmet taler dette for, at man er uden for loven. Grænsedragningen kan volde vanskeligheder i tilfælde, hvor brugeren udstyres med en licens til at foretage forandringer eller videreudviklinger af programmet.

Mellemformer

Grænsen kan også volde tvivl på markedet for de lidt mere kostbare systemer, hvor det indgår som en indarbejdet del af leverandørens ydelse at foretage den nødvendige tilpasning af programvaren, eller hvor overdragelsen kun kan ske, hvis leverandøren forinden har foretaget en teknisk afklaring af brugerens

driftsmæssige forudsætninger mv. Her må formodningen være for, at HAL ikke gælder, hvorved udgangspunktet om aftalefrihed slår igennem fuldt ud.

Kapitel 8. DATABASER MV.

8.1. Begrebsafgrænsning

8.1.a. Den tekniske terminologi

Udgangspunktet

Efter gængs teknisk terminologi er en database en organiseret datamængde, der er bygget op således, at data kan fremkaldes på en måde, der bestemmes af brugeren. Det centrale i begrebet er altså, at brugeren af en database har mulighed for at lokalisere og hente de informationer i basen, han har brug for efter *individuelle* kriterier. En informationssamling, som brugeren er nødt til at tilegne sig ved gennemlæsning fra start til slut, falder uden for begrebet. Da en sådan individuel søgemulighed almindeligvis (om end ikke begrebsmæssigt nødvendigvis) vil være styret af et program, har begrebet grænseflader mod såvel programbeskyttelsen (jf. generelt kapitel 7), mod beskyttelsen af almindelige litterære værker (afsnit 8.2.) og mod beskyttelsen af samleværker (afsnit 8.3.).

Direktivet

I direktivet af 11. marts 1996 om retlig beskyttelse af databaser, 96/9/EØF (EFT 1996 L 77/2), defineres databaser som "en samling af værker, data eller andet selvstændigt materiale, der er struktureret systematisk eller metodisk og kan konsulteres individuelt ved brug af elektronisk udstyr eller på anden måde", art. 1, stk. 2. En database behøver altså ikke være styret elektronisk. Også en trykt telefonbog vil således falde inden for begrebet pga. sit alfabetiske princip. Når det gælder elektroniske databaser præciserer bestemmelsens stk. 3, at beskyttelsen efter dette direktiv ikke gælder for de edb-programmer, der anvendes til fremstilling og drift af elektroniske databaser.

Denne afgrænsning mellem de to loves anvendelsesområder burde almindeligvis være uproblematisk og følger i øvrigt de principper, der er skitseret i kapitel 7, jf. navnlig afsnit 7.3: At give søgefaciliterne eller de bagved liggende redaktionelt prægede valg ophavsretlig beskyttelse som edb-programmer ville være ensbetydende med en grænsefladebeskyttelse, som er fremmed for dette lovsystem. I al-

mindelighed må det antages, at en sådan redaktionelt præget innovation kan udtrykkes på mangfoldige måder i et edb-program, og at der derfor er plads for den nødvendige individualitet i hvert enkelt program.

Hovedgrupper

For den efterfølgende oversigt over databasens retsbeskyttelse kan det være hensigtsmæssigt at foretage en opdeling af forskellige typer af databaser:

- infrastrukturdatabaser

I en første gruppe kan man udskille de baser, hvis informationsindhold udgør en del af samfundets almindelige *infrastruktur*: Sådanne baser opbygges typisk i naturlig konsekvens af de aktiviteter, der er tale om. Eksempler herpå er den statslige lovdatabase "Retsinformation", se <www.retsinfo.dk>, og baserne med kursdata fra Københavns Fondsbørs (se <www.xcse.dk> og tilknyttede abonnementssystemer). På grund af disse systemers vitale betydning knytter der sig en særlig politisk interesse til vilkårene for almenhedens brug. Denne interesse indebærer ofte, at reglerne om brug af disse baser lovreguleres. Et eksempel herpå er lov nr. 419 af 31. maj 2000 om Statstidende, der underlægger dette informationssystem en almindelig lovregulering, jf. nærmere lovens §§ 5-8 om offentliggørelse, der bl.a. sikrer almenheden en almindelig og fri adgang til oplysningerne i denne base. Ved lov nr. 596 af 24. juni 2005 om videreanvendelse af den offentlige sektors informationer er der givet nærmere regler om, hvilke principper, der skal gælde i forbindelse med adgang til kommerciel og ikke-kommerciel videreanvendelse af de dokumenter og datasamlinger, som offentlige myndigheder er i besiddelse af. Lovens regler omtales nærmere i afsnit 8.4.f.

- kommercielle databaser

I en anden gruppe finder man de databaser, der bliver til som en målrettet investering i informationsindsamling, og som udbydes kommercielt på et marked. Eksempler herpå er de store baser, der findes med juridisk, medicinsk, markedsmæssig, økonomisk eller teknisk information, og som markedsføres af en egentlig informationsindustri. Det kendetegner disse baser, at de ikke nødvendigvis "findes i forvejen", men at de bliver til som en målrettet investering med henblik på at dække et markedsbehov. Af samme grund vil der i praksis aldrig være tvivl om, hvorvidt betingelserne for at beskytte disse baser efter *sui generis*-reglerne i ophl. § 71 er tilstede, hvorimod det kan give anledning til tvivl, om der også er grundlag for ophavsretlig beskyttelse.

- databaseapplikationer

I en tredje gruppe kan man herefter udpege de databaser, der i praksis opbygges i tilknytning til applikationer, der i øvrigt ikke fremstår som egentlige "databaser", f.eks. for at muliggøre praktisk betonede søgninger el.lign. Da den slags faciliteter netop

indebærer en individuel konsultation efter data, rummes de uden videre af databasebegrebet. Derfor vil talrige søgefaciliteter i edb-programmel kunne tænkes beskyttet efter reglerne om databaser, for så vidt som de giver mulighed for en sådan individuel informationssøgning. Dette kan f.eks. være aktuelt for talrige hjemmesider og andre hypertekst-applikationer, for indholdsfortegnelser til dokumentationsmateriale, samt for ordbogsfaciliteter til tekstbehandlingsprogrammel.

Præambelen til direktivet omtaler en række eksempler på beskyttelse. I 19. betragtning hedder det f.eks., at en kompilation af flere musikoptagelser på en CD "normalt" ikke falder inden for databasebegrebet. Da den standard, der anvendes på nutidens CD'er, giver plads for op til 99 indspilninger, kan man fristes til at indfortolke en slags nedre grænse i denne betragtning. Derimod siges det i 20. betragtning, at beskyttelsen kan tænkes at omfatte Thesaurus og index-systemer, jf. om disse begreber straks nedenfor. Efter det angivne vil der i almindelighed ikke være tvivl om, at en Internet-portal vil falde inden for beskyttelsen, uanset om den er generel (se f.eks. <www.jubii.dk> eller afgrænset til et bestemt fagområde (se f.eks. den børsorienterede <www.aktienyt.dk>. Se i øvrigt *Thomas Riis* i Juridisk Instituts Julebog (1996), s. 176.

Nogle sidebegreber

Når en database konstrueres, fastlægger frembringeren visse principper for, hvordan brugeren skal kunne søge i basen. Disse principper finder udtryk i et såkaldt index (dvs. stikordsliste) eller Thesaurus. Herudover foretages der en række valg af, hvilke informationer der skal kunne søges i. Disse funktioner understøttes af programmel, såkaldte database management systemer (forkortet DBMS). Allerede efter gældende ophavsretlige regler kan databaser altså tænkes beskyttede såvel som edb-programmer (DBMS-systemet), efter reglerne om samleværker (sammenstillingen) som efter de almindelige ophavsretlige regler (selve strukturen i den informationsopbygning, databasen repræsenterer). Hertil kommer beskyttelsen af de enkelte værker mv., som måtte være indeholdt i databasen.

8.1.b. Nogle udgangspunkter

Informations-frihed

Information, der – uden at udgøre ophavsretlige værker eller andre beskyttede frembringelser – befinder sig i en bog, en database eller i andre sammenhænge, hvorfra de kan hentes, er som udgangspunkt i *public domain*. Dette fundamentale udgangspunkt er bl.a. fastslået ved højesteretsdommen om On-line avisen, *U 1987.882 H*, der antog, at en elektronisk database med korte ekstrakter af dagbladenes nyheder, som kun i begrænset omfang

indeholdt egentlige citater, ikke krænkede ophavsretten til dagbladsartiklerne.

> Ligeså klart er det, at de værker, der er lagret i basen (f.eks. artikler eller tabeller), beskyttes som andre eksemplarer af de pågældende værker, altså som litterære værker der ikke er programmer. I sig selv rummer sammenstillingen nemlig ingen "instruktioner til processoren". Omvendt vil de programværktøjer, der benyttes i DBMS'et, beskyttes som andre programmer.

Sui generis-beskyttelse

Udgangspunktet om, at information er i public domain, må imidlertid modificeres i relation til sådan information, som det – trods sin principielt "frie" natur – almindeligvis vil være umuligt at lokalisere, fordi den befinder sig i en uoverskuelig mangfoldighed af anden information. Når nogen herefter præsterer den investering, der gør det muligt at finde vej rundt i et sådant "informationshav", brydes udgangspunktet om informationsfrihed med et andet grundlæggende princip i immaterialretten, nemlig at den, der gør en væsentlig investering i frembringelse af ny information (eller her: nye informationsstrukturer) bør kunne nyde en vis beskyttelse for sin investering i form af en eneret. Dette modhensyn begrunder den særlige *sui generis*-regel i § 71, stk. 2, om databaser. Herom i afsnit 8.4.

Værket i basen

Dansk ret hjemler som udgangspunkt ingen litterær *findeløn* el.lign. til den, der lokaliserer et eller flere ophavsretlige værker, som andre har skabt. At indsatsen med at finde et værk er nok så kvalitetsfuld, og at den ofte vil repræsentere værdifuld historisk eller humanistisk forskning (i kraft af kildestudier el.lign.) fører ikke til ophavsretlig beskyttelse. Den eneste beskyttelsesform, der står til rådighed, når det gælder sådanne frembringelser, er beskyttelsen som *samleværk*, jf. nærmere i afsnit 8.3. Men når det gælder sådanne frembringelser er det udgangspunktet, at det enkelte *værk* i samleværket bevarer sin ophavsretlige retsstilling. Dette udgangspunkt har to konsekvenser: For *redaktøren* af samleværket betyder det, at ophavsretten til samleværket ingen indskrænkning gør i ophavsretten til de enkelte værker, jf. udtrykkeligt § 5. For *brugeren*, at de retlige bånd (eller fraværet af samme) til de enkelte værker, består uantastet. Hvis sammenstillingen består af værker, for hvilke ophavstiden er udløbet, vil brugeren tilsvarende have ret til at disponere over de enkelte værker, men ikke over samleværket (som sådant). Denne ret kan dog være modificeret ved udtrykkelig aftale. For en gennemgang af disse ophavsretlige spørgsmål henvises til den almindelige fremstilling i kapitel 6.

Basen som værk

Vi så i gennemgangen af den ophavsretlige beskyttelse af programkoden, jf. afsnit 6.2.c., at der her ofte vil være overlappende værkselementer. Fordi der ingen klar begrebsmæssig grænse er for, hvornår noget er et "edb-program", vil dette begreb både kunne omfatte helheden og en ubestemt mængde, delvis overlappende, dele. Samme forhold gør sig gældende ved beskyttelse af databaser. Som "database" vil man både kunne karakterisere et samlet produkt og en række bestanddele heri. Tilsvarende kan det være vanskeligt at drage nogen klar grænse mellem de værker, der indgår i en database, og selve databasen, jf. til illustration dommen om vejviseren i *U 1985.389 H*. Hvor sådanne uklare grænsedragninger gør sig gældende, vil det ofte være berettiget at overveje, om ikke selve databasen kan kvalificere til den stærkeste beskyttelse som et litterært værk. Herom i det følgende.

8.2. Ophavsretlig værksbeskyttelse

8.2.a. Det beskyttede værk

For at en ophavsretlig beskyttelse af en database som *selvstændigt litterært værk* kan komme på tale, må det for det første kræves, at databasen som litterært værk besidder den fornødne originalitet: Det må med andre ord kunne konstateres, at resultatet af frembringerens indsats – med en vis sandsynlighed – vil tage sig anderledes ud, end hvis en anden frembringer var sat til opgaven med at frembringe den pågældende database. En person (eller for den sags skyld, en kreds af personer), der sætter sig for at skrive en ordbog eller et leksikon frembringer dermed såvel en database som et litterært værk, der beskyttes efter den almindelige regel i ophl. § 1, forudsat deres udvalg af ord og hertil hørende oversættelser og forklaringer mv. er anderledes, end hvis et andet forfatterkollegium havde sat sig denne opgave for. Ligeledes får den person, der udarbejder en guide til de gode restauranter i en by – med graduerede kvalitetsmærker for den enkelte osv. – ophavsret til denne samlede frembringelse som litterært værk.

Et ofte forekommende problem i afgrænsningen af den litterære værksbeskyttelse drejer sig om de dataansamlinger, der beskriver, hvilke produkter en virksomhed har til salg eller på lager. Hvor kedsommelige den slags tekster umiddelbart må forekomme den almindelige læser, kan de have stor kommerciel betydning for den virksomhed, der ønsker at kontrollere sin markedsføring fuldt ud, og som navnlig ønsker at undgå konkurrerende

virksomheders præsentation af deres varesortimenter mv. Selv om der kan være et berettiget ønske om at varetage dette hensyn, bør det dog ikke slå igennem i form af en ophavsretlig beskyttelse, jf. således *U 1983.981 Ø*, der nægtede ophavsretlig beskyttelse for en prisliste med planteskoleprodukter. Går man frem efter dobbeltfrembringelseslæren, vil der som regel kun være én måde at opstille et produktsortiment på og derfor ikke spillerum for originalitet. En beskyttelse af sådanne frembringelser må i stedet søges opnået gennem *sui generis*-reglerne om databasebeskyttelse. En sådan beskyttelse blev da også givet i den førnævnte sag, efter den daværende katalogbeskyttelse.

Er der derimod tale om, at frembringeren efter egne kriterier giver sig i kast med at indsamle oplysninger om forskellige virksomheders produkter mv., vil der være spillerum for en ophavsret. Dette er bl.a. antaget ved dommen i *U 1962.254 H* om "Ingeniørens indkøbsbog", der lod en samling af tekniske annoncer og firmabeskrivelser fra ca. 1.000 virksomheder være beskyttet ophavsretligt. Se tilsvarende den amerikanske afgørelse i *CCC Information Services, Inc. v. Maclean Hunter Market Reports et al.*, 44 F.3d 61 (2nd Cir., 1994), der fandt en database over brugte biler med angivelse af den enkelte bils værdi i forskellige geografiske områder beskyttet som litterært værk.

8.2.b. Originalitetskravet

For at opnå *ophavsretlig* beskyttelse til en database må frembringeren kunne godtgøre, at basen besidder den fornødne originalitet. Denne originalitet må enten reflekteres ved databasens *opbygning og struktur* eller ved indholdet af dens enkelte elementer (som i givet fald må optræde som originale del-værker). I forarbejderne til 1995-ophavsretslovens § 1 (FT 1994-95, tillæg A, s. 1332) siges det således, at "... samlinger af ubeskyttede data kan ... være omfattet af beskyttelsen efter stk. 1, under forudsætning af, at frembringelsen har karakter af et værk, dvs. at den er resultatet af en egen selvstændigt skabende intellektuel indsats fra ophavsmandens side."

En sådan ophavsret er i øvrigt forudsat ved art. 3, stk. 1, i direktivet om retlig beskyttelse af databaser, der fastslår, at databaser "... som på grund af udvælgelsen eller strukturering af indholdet udgør ophavsmandens egen intellektuelle frembringelse" beskyttes ophavsretligt, idet der "... ikke [gælder] andre kriterier for, om de er berettiget til denne beskyttelse." Præambelens 16. betragtning bemærker

som i programdirektivet, at der ikke må foretages en vurdering af databasens *kvalitet* eller dens *æstetiske værdi* som led i bedømmelsen af basens originalitet.

Når kravet om originalitet fastlægges for en § 1-database, skal der ikke skeles til databasens tekniske funktionalitet. Ligesom en teknisk raffineret database ikke øger sandsynligheden for en § 1-beskyttelse vil det forhold, at dataene gøres tilgængelige fra et lagermedium på en måde, der ikke effektivt udnytter mediets egenskaber, heller ikke svække den.

8.2.c. Retsvirkninger

Selv om det i praksis kan fortone sig, om man har at gøre med samleværks-databasen (§ 5-database) eller en database, der beskyttes som selvstændigt litterært værk (§ 1-database) er grænsedragningen i princippet klar: En § 1-database er i hovedsagen frembragt i sin helhed, medens en § 5-database er blevet til i kraft af en sammenstilling af værker, der fandtes uafhængigt af sammenstillingen.

Indrubriceringen har betydning i enkelte relationer:

I relation til *eksemplarfremstilling* vil kopiering fra en § 5-database, der alene vedrører et enkelt værk eller en enkelt informationsmængde, som udgangspunkt kunne ske uafhængigt af retten til sammenstillingen. Et modsat resultat ville være ensbetydende med, at man tildelte frembringeren (sammenstilleren) en slags "findeløn". Om en sådan kopiering er tilladt vil da bero på, om der i øvrigt knytter sig ophavsretlige bånd til det pågældende værkselement: Er ophavstiden udløbet? Og hvis ikke: Foreligger den nødvendige tilladelse?

I konsekvens heraf må det antages, at reglerne om den ophavsretlige *citatret* beror på de forestillinger om god skik mv., der knytter sig til de enkelte værker. En citatret i relation til samleværket har kun betydning, hvis så store dele af databasen kopieres, at det kopierede reflekterer skaberens originale *sammenstilling*.

I det omfang en database indeholder programværker, må man sondre mellem beskyttelsen af selve sammenstillingen, der som sådan kan tænkes at være et samleværk, og beskyttelsen af de enkelte programværker, der måtte indgå i en sådan sammenstilling. Det forhold, at der indgår programmer i en sådan samleværksdatabase, jf. ophl. § 5, forvandler ikke denne til et edb-program med det resultat, at reglerne om edb-programmer finder anvendelse. Se tilsvarende om programantologier, afsnit 6.2.e.

Omvendt indebærer det forhold, at et program indgår i en samleværksdatabase, at de særlige regler for edb-programmer fortsat gælder for det enkelte program. Dette har bl.a. betydning i relation til reverse analysis og reverse engineering, jf. ophl. §§ 36-37. Denne indrubricering får ingen betydning for betingelserne for at opnå ophavsretlig beskyttelse. De originalitetskrav, ophavsretsloven opstiller, er således i hovedsagen sammenfaldende, uanset om databasen er et samleværk, jf. § 5, eller en database, der beskyttes som selvstændigt litterært værk, jf. § 1.

8.3. Samleværksbeskyttelse

8.3.a. Samleværksbegrebet

Som nævnt i afsnit 6.2.e. kan reglerne om samleværker tænkes at beskytte en database, der består af værker eller værkselementer (og muligvis også litterære elementer, der ikke har værkshøjde), når sammenstillingen er udtryk for ophavsmandens ("sammenstillerens") originalitet. Denne beskyttelsesform vil ikke alene være relevant i relation til databaser, der tjener samme litterære funktion som den klassiske antologi (f.eks. databaser over avis- eller tidsskriftsartikler), men også på områder, hvor der ingen direkte parallel findes til den klassiske ophavsrets værker. Et praktisk eksempel herpå er hjemmesider, der gennem *kreative links* til andre hjemmesider med værker, samler disse på en måde, der reflekterer databasefrembringerens originale tanke.

Multimedia

Under kategorien samleværk kan man også henføre mange af de frembringelser, der med en moderne, omend stadigt sjældnere anvendt, term omtales som "multimedia", dvs. frembringelser, der integrerer tekst, grafik, lyd, billede og video, til brug for undervisnings- eller underholdningsformål.

Begrebet er ikke velvalgt, eftersom det peger på den stik modsatte egenskab end den begrebsmæssigt interessante, nemlig at der på ét – digitalt – medium (og ikke mange, "multi") kan lagres en mangfoldighed af forskellige informationstyper. Hvor den "klassiske" database typisk vil indeholde informationselementer af en bestemt art, kendetegnes multimediaværket ved at sammenstille disse vidt forskellige informationstyper. Se i øvrigt *Peter Mahrt og Per Mejer* i U1997B.31 ff. og om filmbeskyttelsen afsnit 9.2.

8.3.b. Originalitetskravet

Ligesom det gælder i øvrigt, beskytter den ophavsretlige samleværksbeskyttelse af databaser frembringerens personlige udtryk. Det er principielt uden betydning for denne beskyttelse, om databasen/samleværket besidder en funktionel kvalitet. Det er ved at *strukturere* databasen på en bestemt måde, dvs. udvælge de forskellige bidrag til den og placere disse bidrag i forhold til hinanden på selvstændig vis, at beskyttelsen nås. Ikke ved at gøre antologien så omfattende som muligt. Tværtimod vil en datamængde, der bliver så omfattende, at den inden for den afgrænsede ramme nærmer sig det komplette, kunne bringe databasen uden for det ophavsretlige værn. Den komplette samling af information inden for et på forhånd afgrænset tema vil pr. definition være uoriginal.

Se nærmere betænkning 1064/1986, s. 20 og Supreme Court's skelsættende dom i *Feist Publications, Inc., v. Rural Telephone Service Company, Inc.* 499 U.S. 340 (1991), der nægtede ophavsret til en telefonbog, fordi denne – trods det ubestridelige arbejde, der lå i sammenstillingen af de enkelte telefonnumre mv. – ikke var udtryk for originalitet. At en tilsvarende uensartet praksis vedrørende den ophavsretlige originalitetsvurdering også gjorde sig gældende i visse europæiske lande, se herved *Wagle & Ødegaard* (1997), s. 91, om den hollandske højesteretsdom af 4. januar 1991 i sagen *Van Dale Lexicografie B.V. v. Rudolf Jan Romme*, trykt i engelsk oversættelse hos *Dommering & Hugenholtz* (ed.): Protecting Works of Fact (1991), s. 93 ff.

Med den udbredte anvendelse af Internet-hjemmesider som led i elektronisk handel har spørgsmålet om datasammenstillingers ophavsretlige beskyttelse fået fornyet aktualitet. Typisk vil en hjemmeside indeholde flere typer af information. Når denne information fremtræder som *litterære værker* (f.eks. avisartikler), værker af *billedkunst*, *musikværker* o.lign., vil der som udgangspunkt være ophavsretlig beskyttelse til disse værker – hvis ellers ikke beskyttelsestiden er udløbet, eller der er andre formelle hindringer mod beskyttelsen. Hvis sammenstillingen af disse elementer er original, vil der knytte sig ophavsret til selve hjemmesiden som *samleværk* eller som selvstændigt *litterært eller kunstnerisk værk*.

8.4. Sui generis-beskyttelse

8.4.a. Beskyttede frembringelser

Hvis ikke kravene til at beskytte en database som et ophavsretligt værk er opfyldte, kan det tænkes, at databasen beskyttes efter de særlige regler, der er indført i ophl. § 71 på grundlag af EU's databasedirektiv 96/9/EF af 11. marts 1996. Reglerne herom hører systematisk til i de ophavsretlige "naboregler", fordi de netop ikke forudsætter, at der er tale om et ophavsretligt værk.

Ifølge ophl. § 71 har den, som fremstiller et katalog, en tabel, en database eller lignende, hvori *et større antal oplysninger er sammenstillet*, eller som er resultatet af *en væsentlig investering*, en særlig eneret til at råde over det pågældende arbejde på forskellig vis, jf. nærmere i det følgende. Er arbejder af den nævnte art eller dele deraf genstand for ophavsret eller anden beskyttelse, kan også denne beskyttelse gøres gældende, jf. § 71, stk. 3. Den ene beskyttelse udelukker altså ikke den anden. § 71, stk. 6, erklærer aftalevilkår, der udvider fremstillerens ret efter stk. 1 til et offentliggjort arbejde, for ugyldige.

"Kataloghøjde"

Før gennemførelsen af databasedirektivet var det den almindelige opfattelse i dansk ret, at et katalog ikke skulle opfylde særlige *kvalitetskrav* for at opnå beskyttelse, hvis blot kataloget sammenstillede et "større antal oplysninger". Var dette tilfældet, forelå "kataloghøjde" (en pendant til det tidligere anvendte begreb "værkshøjde"). Formålet med bestemmelsen var at yde beskyttelse af den betydelige indsats af *arbejde og kapital*, der kan ligge til grund for sådanne frembringelser, se herved FT 1959-60, till. A, sp. 2770 f. En tilsvarende beskyttelse har været gældende i de øvrige nordiske lande. Se hertil diskussionen i NIR 1972.248, NIR 1972.393 og NIR 1973.51. Kurslister, regnetabeller, kalendere, bogfortegnelser og fartplaner udgør eksempler på "kataloger", jf. f.eks. henvisningerne til tidligere praksis hos *Schønning* (1998), s. 557.

Investeringskravet

Ifølge databasedirektivet er beskyttelsen betinget af, at den pågældende database er "resultatet af en væsentlig investering": Hvad har frembringeren investeret af penge eller kreativitet i udviklingen? I direktivets art. 7, stk. 1, er dette krav præciseret med en bemærkning om, at investeringskravet skal måles enten *kvantitativt* eller *kvalitativt*, jf. nærmere herom *Henrik A. Jensen* i NIR 1999.64 ff. Det er på nuværende tidspunkt, hvor der ingen retspraksis foreligger, vanskeligt at udtale sig herom. Men i mangel af en sådan praksis er det nærliggende at skele til den praksis,

der foreligger i relation til den ligeartede "katalogregel", jf. ovenfor.

Kravet om "væsentlig investering" anlægges på bedømmelsestidspunktet: Ville det her kræve væsentlige investeringer at skulle indsamle, kontrollere eller præsentere databasens indhold, opnås beskyttelsen, jf. *Riis* i Juridisk Instituts Julebog (1996), s. 178. Betragtningen indebærer, at en database, der på frembringelsestidspunktet ikke er genstand for beskyttelse, kan blive det på et senere tidspunkt, hvor den forgangne periodes indsats nu foreligger i kumuleret skikkelse.

Undergrænsen

Som eksempel på en "database", der herefter ikke vil kunne beskyttes, nævner lovbemærkningerne (pkt. 3.1) i overensstemmelse med direktivets 19. præambelbetragtning ".. en sammenstilling af optagne musikværker på fx en CD-plade". Eksemplet vil formentlig kun være dækkende for sådanne musik-CD'er, som almindeligvis udbydes i handelen, hvorimod en samling af værker eller værkselementer, som det har krævet store investeringer at finde frem, formentlig vil kunne beskyttes efter sui generis-reglerne eller – hvis udvælgelsen tilmed besidder originalitet – efter reglerne om samleværker.

Også tidligere praksis om § 71 lægger vægt på, om der er lagt en vis investering i udarbejdelsen af kataloget, se således *U 1975.258 V*, der nægtede katalogværn for en præmieliste udarbejdet af to journalister på et fællesdyrskue. Listen indgik som en integreret del af en pressereportage fra skuet og var frembragt således, at de to journalister indsamlede de bedømmelser, der forelå fra dyrskuedommerne. Bedømmelserne blev pr. bud bragt hen til presselokalet, efterhånden som de blev færdige. Journalisterne samlede og sammenstillede dem herefter i en præmieliste, der i formen opfyldte kravene til et avismanuskript. Ved byrettens dom fik journalisterne medhold i, at præmielisten måtte anses som et katalog, jf. ophl. § 71. Retten tilkendte herefter journalisterne erstatning for tab. Vestre Landsret bedømte sagen anderledes. Landsretten lagde vægt på, at præmielisten havde kunnet tilendebringes på få timer "hvilket formentlig er noget mindre end af lovgiveren ved bestemmelsens anvendelse på kataloger, tabeller og lignende forudsat". En del af den domspraksis, der nægter ophavsretlig værksbeskyttelse, beskytter i stedet de pågældende frembringelser efter katalogreglen. Det gør f.eks. dommen i *U 1983.981 Ø* om prislisten over planteskoleprodukter, der uden videre fandt listen omfattet af ophl. § 71. Se ligeledes *U 1985.389 H*, der anså realregisteret til den kommunale vejviser som et katalog. Den sidstnævnte dom er kommenteret af *Else Mols* i U1985B.253. Kommentaren henviser til, at der i den juridiske litteratur er enighed om, at der må stilles et kvalitetskrav og krav om en vis systematisering, idet en tilfældig sammenstilling af de pågældende oplysninger ikke er tilstrækkelig. Se ligeledes bemærkningen

sammesteds s. 254 f., hvorefter "en bestemt systematik ofte vil være den eneste mulighed ved sammenstillingen (kompilationen) af bestemte oplysninger." Om beskyttelsen af databaser efter tidligere ret, se nærmere *Stensaasen* (1987), s. 193 ff., *Blume* (1989), s. 37 ff. og betænkning 1064/1986. s. 19 ff.

Den nærmere afgrænsning af, hvilke krav der skal være opfyldt for at opnå beskyttelse som database, har givet anledning til fire afgørelser fra EF-domstolen, der alle er truffet den 9. november 2004 i sagerne C-46/02: *Fixtures Marketing Ltd. mod O.Y. Veikhaus AB*, C-203/02: *British Horseracing Board Ltd. mod William Hill Organization Ltd.*, C-338/02: *Fixtures Marketing Ltd. mod Svenska Spel AB* og C-444/02: *Fixtures Marketing Ltd. mod OPAP*. Alle sagerne tager stilling til, hvordan begrebet "beskyttet database" skal forstås i relation til resultater af forskellige kampe og hestevæddeløb mv., som alle kendetegnes ved at udgøre en sekundær frembringelse i forhold til frembringerens primære virksomhed (den pågældende sportsaktivitet). Sagen om British Horseracing (C-203/02) tager dernæst også stilling til afgrænsningen af begrebet "udtræk og genanvendelse".

I alle dommene antages det, at begrebet "investering" i databasedirektivets artikel 7, stk. 1, skal forstås således, at det betegner "de midler, der anvendes til fremskaffelsen af eksisterende materiale og til samlingen heraf", men ikke "midler, der anvendes til frembringelsen af de bestanddele, der udgør databasens indhold". I forbindelse med udarbejdelsen af et program vedrørende de pågældende sportsaktiviteter blev det derfor antaget, at databasebegrebet ikke omfatter de midler, der anvendes til fastsættelse af datoer, klokkeslæt og kombinationerne af de hold, der skal spille mod hinanden to og to, med hensyn til de forskellige kampe i disse mesterskaber (*Fixtures*-sagerne) henholdsvis de midler, der anvendes til at oprette en liste over heste, der deltager i løb (*British Horseracing*). Derimod skal begrebet investering forstås således, at det omfatter "de midler, der med henblik på at sikre troværdigheden af den information, der er indeholdt i den nævnte database, anvendes til at kontrollere det fremskaffede materiales nøjagtighed ved oprettelsen af databasen, og mens den er i drift." Disse midler kan bestå i anvendelse af menneskelige, finansielle eller tekniske ressourcer men skal være væsentlige ud fra et kvantitativt eller kvalitativt synspunkt.

EF-domstolen har hermed sendt et klart signal om, at det investeringskrav, der skal være opfyldt for at opnå databasebeskyttelse efter *sui generis*-reglerne, ikke er opfyldt alene i og med, at databasen er kommet til verden som en afledet følge af en hoved-

aktivitet, selv om en udefra kommende virksomhed ville have skullet foretage en væsentlig investering for at bringe en sådan database til verden *uden* også at drive denne hovedaktivitet. Denne konklusion indebærer, at en virksomhed, der uden særlige foranstaltninger blot lægger sit salgskatalog ud på nettet, ikke dermed tilvejebringer en database, der opfylder direktivets krav. Selv om dommene i Fixtures-sagerne retter sig mod de nævnte sekundære databaser, siges det dog udtrykkeligt (præmis 39 i sag C-46/02, præmis 35 i sag C-203/02, præmis 29 i sag C-338/02 og præmis 45 i sag C-444/02), at det forhold, at databasen er forbundet med en hovedvirksomhed ikke som sådan *udelukker*, at den kan nyde *sui generis*-beskyttelse. Men i så fald må der stilles yderligere investeringskrav, f.eks. i forbindelse med den løbende fremskaffelse og kvalitetssikring mv., og beskyttelsen rækker da kun til de aspekter af databasen, der reflekterer denne investering.

I dommen om British Horseracing (C-203/02) var der bl.a. rejst spørgsmål om, hvorvidt det påvirker retten til genudtræk mv., at de pågældende informationer skal benyttes i en anden database, der *konkurrerer* med den beskyttede. Spørgsmålet blev besvaret benægtende (præmis 47). Dermed har domstolen taget afstand fra den opfattelse, at der i afgrænsningen af databasebegrebet skal anlægges et integreret skøn under inddragelse af konkurrenceretlige synspunkter.

Den legale databaselicens

I det omfang en database er omfattet af de særlige sui generis-regler, er rettighedshaveren beskyttet mod to former for udnyttelse, jf. § 71, stk. 1 (afsnit 8.4.b.) og stk. 2 (afsnit 8.4.c.). Begge disse bestemmelser tager primært sigte på parter, der ikke i kraft af aftale eller overdragelse har ret til at benytte basen. I relation til sådanne autoriserede brugere henviser § 71, stk. 5, til den *legale databaselicens* i ophl. § 36, stk. 2, der i overensstemmelse med den legale programlicens (i § 36, stk. 1, nr. 1) fastslår, at den, der har ret til at benytte en database – ganske som brugeren af et program eller et litterært værk i digital form – "må foretage sådanne handlinger, som er nødvendige for, at den pågældende kan få adgang til databasens indhold og gøre normal brug af dette". Har ejeren købt databasen på CD-ROM med en forudsat tilladelse til at installere den på harddisk, er denne installation altså ikke retsstridig. Bestemmelsen er præceptiv, jf. samme bestemmelses stk. 4.

8.4.b. Stk. 1-beskyttelsen

Ifølge stk. 1 har fremstilleren af (bl.a.) en database eneret til at råde over databasen *som helhed* eller en *væsentlig del* deraf, ved at fremstille eksemplarer af den og ved at gøre den tilgængelig for almenheden. Bestemmelsen rammer først og fremmest kopieringshandlinger, der har til hovedformål at genskabe den funktionalitet, databasen tilbyder ved efterfølgende at kunne rette søgninger mod de pågældende dele: Fra en landsdækkende telefonbog uddrages f.eks. de telefonabonnenter, der befinder sig i et udvalgt byområde, eller de abonnenter, der korresponderer med visse stillingsbeskrivelser.

Bestemmelsen gennemfører databasedirektivets art. 7, stk. 1, der sikrer databasens fremstiller en ret til at forbyde udtræk og/eller genanvendelse af hele basens indhold eller en væsentlig del deraf, vurderet kvalitativt eller kvantitativt. Med "*udtræk*" forstås ifølge stk. 2, litra a, en permanent eller midlertidig overførsel af hele en databases indhold eller en væsentlig del deraf til et andet medium på en hvilken som helst måde eller i en hvilken som helst form. Begrebet "*genanvendelse*" defineres i henhold til litra b som enhver form for tilgængeliggørelse for almenheden af hele databasens indhold eller en væsentlig del deraf ved spredning af eksemplarer, udlejning, online-transmission eller på anden måde. Se hertil diskussionen hos *Thomas Riis* (2002), s. 112 f., med kritik af den danske gennemførelse af disse to begreber. Ifølge Riis har direktivets nye og selvstændige begreber den fordel, at de mere præcist beskriver de relevante brugshandlinger vedrørende databaser og endvidere klargør, at beskyttelsesgenstanden efter henholdsvis ophavsretten og *sui generis*-retten er forskellig.

Man kan overveje, om bestemmelsen kan bruges i forbindelse med den *indexering*, der almindeligvis foretages i forbindelse med *robottering* af hjemmesider med henblik på at tilvejebringe Internet-søgefaciliteter. Klart er det således, at den linkede hjemmeside må kopieres i det omfang linket aktiveres af en bruger. Men som nærmere forklaret i afsnit 6.3.a. sker der forud herfor en indexering af den pågældende hjemmeside, hvorved samtlige data heri lægges i et "stikordsregister" i den server, der betjener den søgerobot, der frembringer den pågældende link. Det kan dog næppe antages, at en sådan indexering i sig selv skulle være retsstridig. Skulle man antage et sådant resultat, ville dette være ensbetydende med, at enhver brug af generelle søgerobotter på nettet uden videre ville være retsstridig. Den relevante håndtering

af problematikken må foretages gennem den legale databaselicens, jf. ophl. § 36, stk. 2. I det omfang der er tale om en normal og loyal robottering må det således antages, at den nødvendige indexering udgør "normal brug". Se nærmere herom min afhandling i U2000B.311 ff. og neden for afsnit 8.5.d.

8.4.c. Stk. 2-beskyttelsen

Ifølge stk. 2 er der derudover beskyttelse for så vidt udnyttelsen består i "... en eksemplarfremstilling eller tilgængeliggørelse for almenheden af uvæsentlige dele af indholdet ... som foretages gentagne gange og systematisk, såfremt de nævnte handlinger kan sidestilles med handlinger, der strider mod en normal udnyttelse af de pågældende arbejder, eller som skader fremstillerens legitime interesser urimeligt".

Med denne formulering lægges op til en skønspræget afvejning, der minder om den, der indgår i generalklausulen i mfl. § 1, og som bl.a. henser til, om den nævnte udnyttelse må betragtes som illoyal. Også her er det primært praksis for linking og robottering på nettet, der giver anledning til afgrænsningsproblemer. I denne afvejning er det nødvendigt at sondre mellem forskellige typer af formål med en robottering eller linking. Groft sagt kan man på den ene side udskille den linking og robottering, der søger at understøtte en konkurrerende virksomhed og dermed søger at fjerne omsætning fra informationsleverandøren, og på den anden side den, der understøtter virksomhed af anden art, f.eks. ved at skabe trafik på egne hjemmesider for dermed at kunne opnå indtjening ved salg af banner-annoncering eller anden afledt forretning. Problemstillingen drøftes nærmere i afsnit 11.4.c.

8.4.d. Begrænsninger

En række af ophavsretslovens almindelige regler gælder også for denne særlige sui generis-beskyttelse. Det gælder – foruden den allerede nævnte § 36 – bl.a. undtagelsesbestemmelserne vedrørende offentlige myndigheders "aktstykker" (§ 9), forbuddet mod digital privatkopiering (§ 12, stk. 2, nr. 4) og citatretten (§ 22). På grund af mulighederne for at udnytte et citat på en måde, der gør indgreb i databaseindehaverens økonomiske interesser, må det antages, at retten til at citere fra en database er noget snævrere end adgangen til at citere fra en informationsmængde af anden art, jf. *Thomas Riis* i Juridisk Instituts Julebog (1996), s. 185.

8.4.e. Varighed

Sui generis-beskyttelsen varer indtil 15 år er forløbet efter udgangen af det år, hvor arbejdet blev fremstillet, § 71, stk. 4. Hvis et arbejde af den nævnte art gøres tilgængeligt for almenheden inden for dette tidsrum, varer beskyttelsen dog indtil 15 år er forløbet efter udgangen af det år, hvor arbejdet første gang blev gjort tilgængeligt for almenheden, altså – jf. § 2, stk. 3 – ved spredning, offentlig visning eller fremførelse. I relation til databaser, der er undergivet løbende opdatering (f.eks. tidsskriftsdatabaser) indebærer dette, at beskyttelsen kommer til at vare ligeså længe som opdateringen + 15 år.

8.5. Linking, framing og robottering

8.5.a. Problemstilling

Redegørelsen i det følgende er for en betydelig dels vedkommende baseret på dele af min afhandling i U 2000B.311 ff., idet omtale af nyere litteratur og praksis dog er føjet til.

Særlige problemer knytter sig til benyttelsen af de links, der typisk befinder sig på en hjemmeside, og som gør det muligt for brugeren at "surfe" videre til andre hjemmesider. Et væsentligt spørgsmål er her, hvem der er ansvarlig for det retsbrud, der realiseres på den hjemmeside, brugeren når hen til, hvis denne indeholder retsstridig information. Dette spørgsmål berøres i kapitel 17.1.d. som led i den almindelige strafferetlige medvirkenslære. Men herudover opstår spørgsmålet, om man ved at linke til andre hjemmesider, som i sig selv indeholder *retmæssig* information (nemlig ejerens egen), kan siges at krænke de rettigheder, der knytter sig til denne information. Ofte vil informationsleverandørens forudsætninger for at stille disse værker mv. til rådighed for almenheden nemlig adskille sig afgørende fra de forudsætninger, informationsbrugeren har – f.eks. når informationen linkes i bestemte sammenhænge, eller når hjemmesidens informationsindhold ekstraheres for at understøtte en efterfølgende søgning. Disse spørgsmål berøres i det følgende.

Anvendelsesformer

En retlig behandling af disse spørgsmål må tage udgangspunkt i de forskellige handlinger, der udfolder sig ved brug af hjemmesiden og forud herfor.

- referencelinking

Når en bruger får kontakt med en hjemmeside ved at indtaste en *request* i browserens navigationsfelt direkte mod informationsleverandørens hjemmeside, taler man undertiden om *referencelinking*, hvad enten der sigtes mod startsiden, en underside eller en fil, der er placeret herpå. At brugeren kender adressen for sin request har bl.a. betydning for vurderingen af, om han har et lovligt formål med at benytte værket, jf. ophl. § 36, stk. 1, nr. 1, jf. stk. 3, jf. nærmere herom i afsnit 7.4.b.

- indirekte brug

Heroverfor står den brug af en hjemmeside, som indledes ved, at brugeren hjælpes på vej mod den anden side uden – nødvendigvis – at kende den korrekte URL på startsiden. Dette kan forekomme på flere måder. Ved såkaldt *linking* afgives en request, når brugeren klikker på et felt, der enten kan fremtræde som en ikon (f.eks. et varemærke), som et billede eller – måske mest hyppigt – som en tekst, der repræsenterer en del af den information, der linkes til (f.eks. en overskrift). Det kan også forekomme, at brugeren ved hjælp af såkaldt *push-teknologi* oplever, at www-browseren selv åbner nye vinduer, når brugeren gør forsøg på at afslutte de vinduer, der allerede er åbnet. Disse sidste situationer, der ofte vil kunne rammes efter reglerne i mfl. § 1 om god markedsføringsskik, omtales ikke yderligere her, jf. således nærmere afsnit 15.2 og 15.3.

- framing

En tredje metode til at fremkalde information på en anden hjemmeside sker ved såkaldt *framing* (eller mere korrekt: *frame linking*). Herved frembringer den hjemmeside, brugeren befinder sig på, automatisk en request mod *en del* af en anden hjemmeside, f.eks. et billede, som hermed fremtræder i en ramme *("frame")* på den hjemmeside, brugeren befinder sig på. Framing indebærer altså en slags skjult linking, idet den rekvirerede information hentes automatisk ind på hjemmesiden og umiddelbart fremtræder som en del af denne.

Almindelig linking

Linking kan ske på to måder. Såkaldt *almindelig linking* retter sig – ligesom referencelinking – mod den Internet-adresse, informationsleverandøren selv anvender over for omverdenen, f.eks. <www.firma.dk>, altså hjemmesidens første skærmbillede.

Denne gruppe omfatter også tilfælde, hvor A søger at gennemføre sit ønske om at henvise B til en særlig hjemmeside ved at sende B en e-mail, der indeholder en link til den pågældende hjemmeside. En sådan praksis vil man typisk se i forbindelse med en privat kommunikation eller i lukkede nyhedsgrupper. Uden for de tilfælde, hvor der herigennem søges udfoldet en kriminel adfærd, giver sådanne former for linking ikke anledning til retlige problemer. Det samme kan siges om den linking, der undertiden omtales som *mail links*, hvor en hjemmeside under brug giver brugeren mulighed for at indtaste

en elektronisk meddelelse, der herefter afsendes til en anden part eller til hjemmesidens udbyder. Se om disse former for linking *Karl Svanström* i NÅR 2000.143 ff., s. 159 f.

Deep linking

Heroverfor står såkaldt *deep linking*, hvor der linkes til efterfølgende sider eller filer under øverste niveau. Ved deep linking når brugeren altså ikke sit mål fra hjemmesidens øverste niveau.

Robottering

En teknik, der spiller en særlig rolle ved deep linking, og som giver anledning til særlig tvivl, er den såkaldte *robottering*, der kan defineres som maskinel udvælgelse af links til andre hjemmesider. Ved at robottere et udvalg af de hjemmesider, der findes på nettet, gør man det muligt for robottens bruger at søge efter information på disse hjemmesider efter bestemte kriterier. Sådanne søgerobotter kan have forskellige funktioner indbygget i sig og herunder være baseret på mere eller mindre generelle søgekriterier. De generelle søgerobotter retter sig mod hjemmesider af enhver art. Derimod er andre søgerobotter, de såkaldte *intelligente agenter*, på forhånd indrettet til at eftersøge information af en bestemt karakter, f.eks. ydelser, som restaurationer, hoteller, udbudte faste ejendomme og ferierejser.

8.5.b. Ophavsretlige spørgsmål

Når det gælder den ophavsretlige eneret til eksemplarfremstilling, opstår flere spørgsmål under den proces, der fører til robottering og heraf følgende indirekte brug af en hjemmeside.

Indledende analyse

Det *første* angår den indledende brug af de pågældende hjemmesider, der sker, når robotfunktionen skal konstrueres med det formål at afdække, hvad der skal linkes til. Dette problem har primært betydning ved intelligente agenter. Problemet er nærmere bestemt, om den, der udbyder en hjemmeside til almenheden, dermed kan siges at have accepteret, at andre uden tilladelse gør hjemmesiden tilgængelig for en sådan automatiseret brug med henblik på i givet fald at kunne udvirke links til hjemmesiden.

- eksemplar?

For at kunne besvare dette spørgsmål må det afklares, om resultatet af en request (altså den modtagne information fra den efterspurgte hjemmeside) frembringer et "eksemplar" hos brugeren, selv om den kun modtages i den såkaldte RAM-hukommelse. Om sådanne RAM-kopier udgør eksemplarer i ophavsretlig forstand, er omdiskuteret, jf. nærmere afsnit 6.3.b, hvor det antages, at en sådan fiksering udgør et eksemplar.

Antages denne (del-)konklusion, er konsekvensen heraf, at den eksemplarfremstilling af hjemmesidens indhold, der er tale om i den forberedende undersøgelsesfase, ikke kan støttes på

reglerne om privatkopiering i ophl. § 12: For det første er der typisk tale om en *erhvervsmæssig* eksemplarfremstilling; men selv om man skulle falde inden for det private område, rammes forholdet af det særlige forbud mod *digital privatkopiering* i § 12, stk. 3, nr. 4 og 5.

- tilladelse?

Frem til den gennemførelse af Infosoc-direktivet, der fandt sted i december 2002, gav ophl. § 36 stk. 1, nr. 1, hjemmel til brug af værker i digital form, "hvis anvendelse styres af et edb-program". Med denne bestemmelse var der skabt hjemmel for, at Internet-brugere kunne fremstille de eksemplarer, der var nødvendige for f.eks. at benytte en hjemmeside efter dens formål. Bestemmelsen er nu afløst af den langt snævrere bestemmelse i ophl. 11a, der ikke giver adgang til en sådan brugsorienteret eksemplarfremstilling af værker. I mangel af en sådan lovhjemmel må man udlede brugerens ret til at benytte ophavsretligt beskyttede værker på en hjemmeside af aftaleretlige konstruktioner.

Dermed bliver det for det første afgørende, hvilke *klausuler*, rettighedshaveren har knyttet til benyttelsen af det pågældende værk. Disse klausuler kan enten fremtræde på selve hjemmesiden eller de kan fremgå af det enkelte værk, f.eks. i form af en *Creative Commons*-licens, se hertil afsnit 9.5.c.

I mangel af en sådan klausulering må man se på, om rettighedshaveren må formodes at have givet almenheden en stiltiende tilladelse til at foretage den brug af værkerne på hjemmesiden, der sker i forbindelse med en robottering. En sådan analyse ligger til grund for den tyske forbundshøjesterets dom af 17. juli 2003 i den såkaldte Paperboy-sag, der statuerede, at etablering af et link til en hjemmeside med ophavsretligt beskyttede værker ikke indebar noget indgreb i ophavsmandens eneret til eksemplarfremstilling. Dommen fastslår ligeledes, at en rettighedshaver, som gør et ophavsretligt beskyttet værk offentligt tilgængeligt på nettet uden tekniske beskyttelsesforanstaltninger, dermed gør det muligt at foretage de handlinger vedrørende værket, som internetbrugere kan foretage. Derfor sker der ikke nogen ophavsretlig krænkelse, når adgangen til sådanne værker lettes gennem oprettelse af links, herunder også dybe links. Sagen blev rejst i forbindelse med søgetjenesten "Paperboy", som via links formidlede forskellige former for informationstilbud herunder artikler fra pressen.

I en fortolkning af ophavsmandens formodede hensigt med at stille et værk til rådighed fra en hjemmeside spiller i hvert fald følgende synspunkter en rolle: Formålet med at gå på nettet er, at offentligheden skal læse den information, man lægger på sin

hjemmeside – ikke at brugeren skal udvikle konkurrerende hjemmesider. Men anlægger man en bredere betragtning, kan der omvendt argumenteres for, at interessen ved at være på nettet netop knytter sig til almenhedens adgang til at søge bredt efter information – en adgang, som netop forudsætter, at der findes søgeværktøjer og hertil hørende indekseringsteknikker. Hertil skal lægges det retstekniske argument, at et forbud mod at undersøge hjemmesider med henblik på målrettet robottering vil være vanskeligt at afgrænse over for den frihed, som utvivlsomt gælder til at anmelde og omtale forskellige typer af hjemmesider.

Sammenfattende må man derfor nå til den konklusion, at man i mangel af modstående klausulering har adgang til at undersøge en hjemmeside – og i den forbindelse foretage de eksemplarfremstillinger, der er nødvendige – med henblik på i givet fald at robottere den målrettet.

Indexering

Det *andet* spørgsmål opstår ved den løbende indeksering af siderne. Man kan her spørge, om disse udgør en *hjemlet* eksemplarfremstilling.

På den ene side kan det være vanskeligt at hævde, at et stikordsregister, der indeholder alle ord i en bog, udgør en kopi af bogen, eftersom de fleste af ordene optræder flere gange i bogen, uanset de kun står én gang i stikordsregisteret. Men det særlige for et hypertekst-baseret indeks er, i modsætning til et traditionelt stikordsregister, at hvert ord er forsynet med information om, hvilke andre ord det hører til. Derfor kan man argumentere for, at indekset må betragtes som en overførelse af "bogen" (og her hjemmesiden) til en indretning, der er egnet til at gengive denne, jf. ophl. § 2, stk. 2. Selv om denne betragtning har meget for sig, er resultatet ikke utvivlsomt. Der kan således også argumenteres for, at indekset som "indretning" slet ikke tager sigte på gengivelse, og at det kun med betydeligt besvær vil kunne udvirke en gengivelse af de pågældende værker.

Spørgsmålet spiller dog næppe nogen større praktisk rolle, hvis det antages, at aftaleretlige overvejelser også her fører til, at det eksemplar, man måtte konkludere, at der forelå, må anses for lovligt, fordi der er tale om en anvendelse af nettet i overensstemmelse med god skik. Nærmere herom under 8.5.d.

Brug

Tredje spørgsmål angår den delvise eksemplarfremstilling, der sker fra linkerens hjemmeside, når de udvalgte hjemmesider udsættes for indirekte brug. Det må her antages som forholdsvis utvivlsomt, at det link, der frembringes, når man anvender en robot (eller i øvrigt placerer et link på en side), ikke i sig selv udgør et eksemplar af det pågældende værk. For at kunne antage,

at et sådant eksemplar er kommet til eksistens, måtte det kunne konstateres, at eksemplaret var skabt, før linket var aktiveret. Det må imidlertid høre til undtagelsen, at de overskrifter, der kan tænkes at indgå i et sådant link, udgør et selvstændigt værk.

I visse tilfælde har man dog set eksempler på, at et link forsynes med uddrag af den tekstmængde, der linkes til, f.eks. de første linjer af en artikel fra en elektronisk avis. Her kan der opstå et spørgsmål om, hvorvidt citatretten er overskredet. Om dette er tilfældet vil bero på den sammenhæng, hvori "citatet" indgår, herunder om der er tale om loyale henvisninger, der vil bringe brugeren hen i en almindelig og forudsat anvendelse af den pågældende hjemmeside, eller om en snyltningspræget handling, der omvendt har til formål at undgå, at brugeren bevæger sig hen til den anden hjemmeside med henblik på en selvstændig søgning her.

Tilgængeliggørelse?

Tilbage står derfor spørgsmålet, om man ved at linke til et værk kan siges at have gjort det til genstand for en ophavsretlig udnyttelse i form af tilgængeliggørelse for almenheden, jf. ophl. § 2, stk. 3. Som nævnt oven for i afsnit 6.3.f. må dette spørgsmål besvares benægtende.

8.5.c. Databasespørgsmål

Man kan herudover overveje, om robottering er i strid med ophl. § 71.

Stk. 1-beskyttelsen

Som nævnt i afsnit 8.4.a. har fremstilleren af (bl.a.) en database (og herunder en hjemmeside, der beskyttes efter § 71) eneret til at råde over databasen som helhed eller en væsentlig del deraf ved at fremstille eksemplarer af den og ved at gøre den tilgængelig for almenheden. Igen opstår de tre spørgsmål, som gav anledning til tvivl i relation til reglerne om eksemplarfremstilling, nemlig i relation til undersøgelseshandlinger, indeksering og den løbende tilvejebringelse af søgemuligheder i robotten.

Når det gælder det redaktionelle forberedelsesarbejde er man klart uden for § 71. De eksemplarer, der fremstilles i den forbindelse, vil alene udgøre repræsentative udpluk af basen og altså ikke hele basen eller "en væsentlig del deraf".

- indexering

Med hensyn til den efterfølgende indexering ledes man tilbage til de overvejelser, der tidligere er gjort om retmæssigheden af sådanne eksemplarfremstillinger. Dette skyldes, at § 71, stk. 5, udtrykkeligt henviser til § 36, stk. 2, der fastslår, at den, der har ret til at benytte en database – ganske som brugeren af et program eller et litterært værk i digital form – "må foretage sådanne hand-

linger, som er nødvendige for, at den pågældende kan få adgang til databasens indhold og gøre normal brug af dette". En ophavsretlig eneret til en sådan undersøgelse og indexering ville være ensbetydende med, at enhver brug af generelle søgerobotter på nettet ville være retsstridig, hvilket på afgørende vis ville ændre de almindelige forudsætninger, der utvivlsomt hersker for adfærd på nettet.

- søgeadgang

Derimod ligger det nogenlunde fast, at man ved at stille søgemuligheder til rådighed for almenheden gennem en søgerobot ikke bevæger sig inden for området af stk. 1. Søgerobottens funktion er jo netop ikke at kopiere hele basen, men derimod at give brugeren en enklere adgang til selv at finde frem til og kopiere udvalgte dele af den. Dermed samler opmærksomheden sig om bestemmelsens andet stykke.

Stk. 2-beskyttelsen

Ifølge stk. 2 er der derudover beskyttelse, for så vidt udnyttelsen består i "... en eksemplarfremstilling eller tilgængeliggørelse for almenheden af uvæsentlige dele af indholdet ... som foretages gentagne gange og systematisk, såfremt de nævnte handlinger kan sidestilles med handlinger, der strider mod en normal udnyttelse af de pågældende arbejder, eller som skader fremstillerens legitime interesser urimeligt".

Objektivt set må det antages, at den linking, der foretages fra en søgerobot (uanset om denne er generel eller målrettet som en intelligent agent), falder inden for den del af beskrivelsen, der taler om en gentagen og systematisk brug af uvæsentlige dele af den linkede database (nemlig de enkelte oplysninger). Det er netop søgerobottens hovedfunktion at foretage en sådan systematisk gennemsøgning af de sider, hvortil der robotteres. Det springende punkt er derfor, om denne anvendelse kan siges at udgøre en "normal udnyttelse" eller "skade fremstillerens legitime interesser urimeligt", jf. § 71, stk. 2, 2. pkt. Vurderingen af dette spørgsmål falder i hovedsagen sammen med den god skik-vurdering, der f.eks. anlægges efter mfl. § 1. Herom i det følgende.

8.5.d. God skik-betragninger

Som nævnt flere gange i det foregående beror svaret på de centrale spørgsmål om retten til at linke og robottere hjemmesider på betragtninger om god skik, der i større eller mindre omfang korresponderer med generalklausulen i mfl. § 1. Det er almindeligt antaget, at begrebet "god markedsføringsskik" bl.a. kan ramme efterligning, snyltning og anden udnyttelse af andres indsats, jf. *Koktvedgaard* (2003), s. 341 ff.

I denne afvejning er det nødvendigt at sondre mellem forskellige typer af formål med en robottering eller linking. Groft sagt kan man på den ene side udskille den linking og robottering, der søger at trække kunder med over til en konkurrerende virksomhed og dermed søger at fjerne omsætning fra informationsleverandøren, og på den anden side den, der understøtter virksomhed af anden art, f.eks. ved at skabe trafik på egne hjemmesider for dermed at kunne opnå indtjening ved salg af banner-annoncering eller anden afledt forretning.

Formidlingsvirksomhed

Til illustration af første gruppe kan nævnes de meget besøgte hjemmesider, der efter forskellige forretningsmæssige principper formidler en forretningsmæssig kontakt, f.eks. stillingsannoncer eller billetsalg, uden selv at markedsføre ydelser af den pågældende art, eller således at der kun linkes i det omfang linkeren ikke selv har ydelser inden for sortimentet, som kunden måtte efterspørge.

Når en sådan tjeneste finansieres ved banner-annoncering, vil dens levedygtighed stå og falde med, at brugerne rent faktisk lægger deres søgninger på hjemmesiden og dér eksponeres for de forskellige reklamer: Man sælger jo ikke andre ydelser. Med nutidens intense fokus på reklameeksponering må der i dag antages en vis retsbeskyttelse af denne eksponering. En robottering mod en sådan side, der i væsentligt omfang reducerer denne eksponering, må derfor anses for at være en snyltningshandling, der strider mod mfl. § 1. Forholdet kan nærmest beskrives således, at robotten tilegner sig den modydelse (i form af annonceeksponeringen), som indehaveren af den robotterede hjemmeside med rimelighed kunne forvente til gengæld for sin investering med hjemmesidens opbygning og markedsføring.

Hjemmesider med salg af egne ydelser

Problemet er omvendt, når hjemmesidens formål er at sælge ydelser, som dens indehaver selv markedsfører, f.eks. fast ejendom. Her er det forholdsvis klart, at der ikke foreligger nogen snyltning: Resultatet af en søgning på den intelligente agent er jo netop, at brugeren ledes hen til den, der har varen til salg, hvilket i givet fald kan resultere i en handel til fordel for denne. Som udgangspunkt må det antages, at en sådan linking og robottering ikke er i strid med god Internet-skik (som praksis synes at tegne sig i dag) i almindelighed og god markedsføringsskik i særdeleshed. Problemet med bannerannoncering har her en begrænset betydning. En hjemmeside, der alene anvendes til at markedsføre ydelser, sidens indehaver udbyder alene, vil ofte ikke indeholde bannerannoncer for andre udbydere. Derfor opstår der ikke noget problem om beskyttelse af bannerannonceringerne.

Tidsfaktoren

Man kan overveje, om dette udgangspunkt bør fraviges i relation til intelligente agenter, ud fra den betragtning, at der kan opstå risiko for vildledning i det tidsrum, der går mellem sidens opdatering og robottens seneste indeksering. Når dette argument vurderes, må det tages i betragtning, at en sådan tidsforskydning er sædvanligt forekommende for alle søgerobotter på nettet. Søgerobotter fungerer ved på forhånd at have indekseret en række oplysninger, som herefter trækkes ned, og der vil derfor altid forekomme en tidsforskydning. Hvis man i øvrigt antager, at søgerobotter tjener en nyttig funktion til understøttelse af søgninger på Internet – og denne opfattelse er vistnok den almindelige – får problemet karakter af et spørgsmål om forbrugeroplysning: I det omfang denne viden ikke er almindeligt kendt blandt den typiske bruger af den intelligente agent, bør udbyderen af en sådan tjeneste sørge for, at den meddeles tydeligt, og helst på det skærmbillede, hvorfra søgningen gennemføres.

Nyheds-virksomhed

I modsætning til de netop nævnte tilfælde står salg af information, f.eks. i form af nyheder. Disse tilfælde kendetegnes ved på den ene side at udgøre et produkt, der sælges af virksomheden (f.eks. et dagblad), men ved på den anden side at have flygtig karakter, idet informationen konsumeres i og med søgningen.

Vurderingen af tilladeligheden af et informationsmæssigt genbrug påvirkes her af visse almene hensyn til den almindelige informationsstrøm i samfundet. Synspunktet er vel nærmest, at den, der vælger at lægge en nyhed ud på nettet, til en vis grad må acceptere, at nyheden fatter andres interesse; men at nyhedens ophavsmand på den anden side også må have en berettiget interesse i at andre nyhedsformidlere ikke giver nyheden videre som sin egen.

U 1987.882 H

I retspraksis har spørgsmålet om lovligheden af elektroniske søgetjenester været prøvet ved en enkelt lejlighed. Ved Højesterets dom om *On-line avisen*, *U 1987.882 H*, blev det fastslået, at en elektronisk database med korte ekstrakter af dagbladenes nyheder, som kun i begrænset omfang indeholdt egentlige citater, hverken krænkede ophavsretten til dagbladsartiklerne eller indebar en uberettiget snyltning, jf. mfl. § 1. Højesteret tilslutter sig her de præmisser, Sø- og Handelsretten havde lagt til grund for sin afgørelse. I denne rets præmisser siges det således, at tjenesten "... ikke kan antages at have tilsigtet konkurrence med dagbladene og findes i hvert fald ikke at have kunnet påføre dagbladene konkurrence af nogen betydning. En orientering om, hvad der findes af stof om forskellige emner i dagens aviser, kan utvivlsomt være af interesse og dermed have et rimeligt formål."

Diskussion

Man kan nok have sine tvivl om, hvorvidt afgørelsen foregriber den hensynsafvejning, der vil gøre sig gældende i det moderne netværkssamfund. Modsat forholdene i midten af 1980'erne, hvor On-line avisen blev skabt, er de større aviser nu selv gået på nettet, hvor de står i direkte konkurrence med sådanne tjenester. Denne del af Højesterets begrundelse er derfor ikke længere dækkende. Omvendt ligger det også klart, at den konkurrence, der således udøves, i vid udstrækning accepterer, at der linkes og robotteres: Man kan jo også linke til det øverste niveau af den elektroniske avis, hvilket som udgangspunkt ikke kan være retsstridigt. I nogle tilfælde sker en linking til mere målrettede informationsmængder efter aftale (uden at der tegner sig noget klart billede af, hvorfra og -til pengestrømmene i givet fald går), i andre tilfælde foreligger sådanne aftaler ikke.

Praksis er formentlig i bevægelse. Det eneste, man formentlig kan sige i dag, er, at man ved dyb linking i almindelighed må respektere den bannerannoncering, der fremtræder på den konkurrerende informationsleverandørs side, eller – hvor en sådan ikke findes – sikre sig, at det gøres klart over for den indirekte bruger, hvordan den autentiske informationsmængde ser ud, og hvem der er den autentiske nyhedsformidler.

Illustrerende for denne bevægelse er *U 2003.1063 SH*, der ved en udeblivelsesdom stadfæster Københavns Byrets fogedkendelse af 7. juli 2002 i sagen vedrørende nyhedstjenesten "NewsBooster". Danske Dagblades Forening havde som mandatar for en række dagblade nedlagt påstand om, at NewsBooster skulle forbydes at drive sin nyhedstjeneste med dybe links til de pågældende dagblades hjemmesider med tilgængeliggørelse af overskrifter herfra, ved distribution af elektroniske nyhedsbreve med dybe links hertil og ved distribution af overskrifter fra Internet-udgaverne af de pågældende dagblades Internet-udgaver. Sagen var alene rejst på grundlag af databasebeskyttelsen i ophl. § 71. Ved fogedrettens kendelse fik rekvirenterne medhold i, at der skulle nedlægges forbud mod de nævnte aktiviteter. Det hedder bl.a., at NewsBoosters brug af dybe links betyder, at brugerne af NewsBooster føres direkte til Internet-mediernes artikler på Internet-aviserne og uden om disse mediers indledende Internet-sider. En almindelig søgning eller gennemgang af Internet-aviserne overflødiggøres derved i nogen grad, hvilket må antages at kunne påvirke disse mediers bannerannoncer. Der forelå således en aktivitet, der var i direkte konkurrence med dagbladenes Internet-virksomheder, og som forringede annonceværdien af de pågældende hjemmesider. Derfor fandtes den anvendte brug af

overskrifter og dybe links at være i strid med ophl. § 71, stk. 2, og ikke legitimeret ved den citatret, der gælder efter ophl. § 22, jf. § 71, stk. 5. Samme grunde førte retten til at antage, at den pågældende virksomhed var i strid med mfl. § 1.

Spørgsmålet om dyb linking til boligportaler berøres i øvrigt ved Trondhjems Tingsrets kendelse af 27. januar 2004, trykt i Lov & Data nr. 77, s. 4 ff. Ej heller ved denne afgørelse fandt retten, at et link fra boligportal til en ejendomsmæglers hjemmeside indebar en krænkelse af databaseværnet. I overensstemmelse med den tyske afgørelse fremhæver byretten, at linking er en væsentlig funktionalitet ved nettet, og at man må gå ud fra, at den som gør ophavsretligt beskyttet materiale tilgængeligt på nettet, også accepterer en loyal linking til materialet. Retten fandt heller ikke, at en sådan linking indebar illoyal konkurrence. For anden europæisk praksis henvises til *Perttu Virtanens* afhandling fra 2005.

Den amerikanske udvikling tegnes indtil videre af to afgørelser. I sagen *Ticketmaster v. Tickets.com* (CD Calif, 27. marts 2000), havde den markedsdominerende leverandør af web-baserede billetbestillinger, Ticketmaster Corp., begæret fogedforbud nedlagt mod en tilsvarende billet-tjeneste drevet i noget mindre målestok, Tickets.com. Fra sin tjeneste linkede Tickets.com til Ticketmasters hjemmeside i det omfang man ikke selv kunne levere efterspurgte billetter. Tickets. com blev frifundet, men det er værd at studere præmisserne herfor: Der var ikke tale om kopiering af ophavsretlige værker (i relation til den betragtning, at linkingen i sig selv indebar en eksemplarfremstilling af hele hjemmesiden, sammenlignede retten forholdet med "taking historical facts from a work of reference and printing them in different expressions"), og amerikansk ret hjemler ingen særskilt beskyttelse af databaser. Retten undlod i øvrigt at tage materiel stilling til, om de amerikanske regler om "tortious interference with prospective business advantage" var tilsidesat i kraft af den mulige tilegnelse af de indtægter fra banner-annoncer, som vil indtræde, hvis brugerne generelt vælger at søge billetter fra Tickets.com. Den anden afgørelse faldt i sagen *eBay Inc. v. Bidders Edge* 100 F.supp., 2d 1058 (NDCA, 24. maj 2000). Her blev resultatet, at der ikke kunne ske linking til en auktionssite. Resultatet var bl.a. begrundet med, at den *indeksering* af den pågældende site, der skete i forbindelse med robotteringen, trak så meget kapacitet ud af serveren, at dette gik ud over hastigheden. Resultatet er begrundet med, at der forelå *trespass* (altså en betragtning om, at Bidders Edge herigennem foretog en uberettiget teknisk brug af eBay's servere). Retten tog derimod *ikke* stilling til, om forholdet var omfattet af andre af de søgsmålsgrunde, eBay gjorde gældende, herunder false advertising, trademark dilution, unfair competition, unjust enrichment og interference with prospective economic advantage. *Kelly v. Arriba Soft Corporation* 280 F.3D 934 (2002, U.S. App.), 61 U.S.P.Q.

2nd, 1564 drejede sig om en søgemaskine, der var i stand til at fremfinde fotografier fra hjemmesider på nettet. Når brugeren foretog en sådan søgning, modtog han et antal små billeder (kaldet *thumb nails*), der afsluttede hans søgning, hvorefter han gennem et klik på et sådant thumb nail-billede kunne bevæge sig hen på den autentiske side. Den søgning, der fremskaffede de nævnte *thumb nails*, forudsatte en forudgående indeksering, hvorefter de pågældende billeder i fuld størrelse blev kopieret til tjenestens server. Afgørelsen, der er truffet i medfør af generalklausulen om "fair use" i den amerikanske Copyright Act, konkluderede, at den eksemplarfremstilling, der skete i konsekvens af den nævnte søgefunktion, indebar "fair use". Se i øvrigt *Henrik Spang-Hanssens* omtale af amerikansk retspraksis i Lov & Data, nr. 68, december 2001, s. 1 ff.

Framing

Med denne konklusion er det også forudsat, at det ikke er lovligt at linke dybt til en side således, at det kun er enkelte informationselementer herfra, der trækkes over i en anden side. Har B således placeret et fotografisk billede på sin hjemmeside, må A ikke foretage en link isoleret hertil, hvorved billedet trækkes ind som sådant, uden at brugeren af A's hjemmeside er i stand til at se, at billedet reelt er udvirket ved en framet request mod billedet på B's side. En sådan handling må reelt sidestilles med en eksemplarfremstilling af billedet udvirket af A til et formål, der ikke har hjemmel i ophl. § 36, stk. 1, nr. 1, og ikke A's bruger, jf. bemærkningerne ovenfor om framing. Betragtningen er her, at det er linkeren, der i det hele kontrollerer den pågældende eksemplarfremstilling, jf. *Svanström* i NÅR 2000.151.

Disclaimere

At en informationsleverandør indsætter disclaimere, der forbyder linking eller formidling af oplysninger, som i øvrigt er frit tilgængelige, kan som udgangspunkt ikke tillægges betydning. En sådan, ensidig, meddelelse er ikke i sig selv aftaleskabende og vil således alene – i mangel af en immaterialretlig beskyttelse – kunne tillægges retsvirkning, i det omfang den pågældende anvendelse er retsstridig på andet grundlag (f.eks. som stridende mod reglerne om god markedsføringsskik).

Der er i øvrigt næppe grund til at antage, at denne praksis for indgåelse af aftaler om linking vil blive særligt udbredt. I kraft af det kontraktsforhold, linkeren derved bringes i over for den part, der linkes til, vil retten til at linke stå og falde med kontraktsforholdet. Bringer den linkede part kontraktsforholdet til ophør, vil det være vanskeligt for linkeren at gøre gældende, at retten til at linke bestod uafhængigt af aftaleforholdet.

8.6. Den offentlige sektors informationer

8.6.a. Formål og baggrund

Ved lov nr. 596 af 24. juni 2005 om videreanvendelse af den offentlige sektors informationer er der givet særlige regler om, hvorledes det offentlige kan give licens til brug af informationer og databaser, der udspringer af myndighedernes arbejde mv. Loven har som sit formål at fremme investeringer og innovation i informationsindustrien ved at opstille gennemsigtige regler for, hvilke vilkår og betingelser myndigheden kan stille for videreanvendelse. Disse regler findes i lovens § 3 (§§ 4-12).

Loven er vedtaget på grundlag af direktiv 2003/98/EF om videreanvendelse af den offentlige sektors informationer. Formålet er "at etablere ensartede minimumsregler i forbindelse med adgang til kommerciel og ikke-kommerciel videregivelse af eksisterende dokumenter og datasamlinger, som offentlige myndigheder er i besiddelse af", jf. § 1 og den nærmere afgrænsning i §§ 2-3. De informationer, der dækkes af loven, angår f.eks. sociale forhold, økonomi, geografi, vejrforhold, turisme, erhvervsforhold, patentrettigheder og uddannelse. Det fremgår af bemærkningerne til loven, at denne kun finder anvendelse, når en offentlig myndighed har gjort de pågældende dokumenter mv. *tilgængelige*. Dermed ændrer loven ikke ved de regler, der findes om aktindsigt i offentligheds- og forvaltningsloven. Ej heller ændrer loven reglerne om retsbeskyttelse af de pågældende oplysninger.

8.6.b. Licensering

Ansøgninger om licenser og fastsættelse af andre vilkår for videreanvendelse af eksisterende dokumenter og datasamlinger skal ifølge lovens § 4 indgives til den myndighed, der er i besiddelse af dokumentet mv., eller som i henhold til anden lovgivning administrerer den pågældende datasamling. Det kræves ikke, at informationerne er offentliggjort ved en særlig formel procedure. Alene det forhold, at oplysningerne er tilgængelige på en hjemmeside, kan give grundlag for en ansøgning, jf. § 4. En sådan ansøgning er dog ufornøden, såfremt oplysningerne er undtaget ophavsretlig beskyttelse efter reglerne om offentlige aktstykker (ophl. § 9) eller efter reglerne om offentlige forhandlinger og aktindsigt mv. (ophl. §§ 26-28).

Almindelige principper

I lovens §§ 9-11 er der fastsat en række principper om gennemsigtighed og ikke-diskrimination, der har til formål at forhindre, at det offentlige benytter sine informationsenerettigheder til at fordreje konkurrencen til fordel for enkelte, private informationsleverandører. Ifølge § 10, stk. 1, må offentlige myndigheder i de betingelser, der sættes for videreanvendelse af dokumenter og datasamlinger ikke "begrænse mulighederne for videreanvendelsen". Sådanne betingelser må dernæst ikke benyttes til at "begrænse konkurrencen". I det omfang myndighederne anvender standardlicenser, skal disse gøres tilgængelige i elektronisk form. En klausulering (og en licenspraksis), som for eksempel tillader videreanvendelse mod kildeangivelse og ansvarsfraskrivelse, vil både være sædvanlig og tilstrækkelig til at opfylde kravet i § 10.

Ingen enelicenser

Lovens § 11 forbyder offentlige myndigheder at indgå aftaler om eneret til videreanvendelse af dokumenter og datasamlinger. Sådanne aftaler må alene indgås, hvis en eneret må anses for "nødvendig" for levering af en tjenesteydelse i offentlighedens interesse. Bemærkningerne til lovforslaget nævner som eksempel herpå tilfælde, hvor etableringen af de nødvendige tjenester vil være kostbare, og hvor den nødvendige investering i givet fald må hentes hjem over tid. Det fremgår af § 11, stk. 2, at begrundelsen for i disse tilfælde at tildele en eneret må revurderes med jævne mellemrum og under alle omstændigheder hvert tredje år. Heri ligger, at den periode, inden for hvilken investeringen er forrentet, må ligge ud over tre år. Bestemmelsen forbyder således myndighederne at gennemføre udbud under tilsagn om eksklusivitet alene med det formål at opnå en højere betaling.

8.6.c. Formkrav mv.

Lovens § 4 opstiller en række formelle regler, som gælder for de i stk. 1 nævnte ansøgninger. Ifølge stk. 2 er der en svarfrist på 10 dage efter ansøgningens modtagelse. Er en videregivelse forbundet med særlige omkostninger, kan myndigheden betinge tilladelsen af, at ansøgeren afholder disse omkostninger, jf. § 4, stk. 4. Videregivelse skal i givet fald ske i overensstemmelse med tilgængelige formater, jf. § 7, der blandt andet (stk. 3) indeholder en hjemmel for fastsættelse af nærmere regler herom ved bekendtgørelse.

Litteratur

Reglerne om beskyttelse af databaser efter EU-direktivet af 1996 er bl.a. gennemgået af *Thomas Riis* i Juridisk Instituts Julebog 1996, s. 169 ff. og i Blume m.fl.: IT-retlige emner (1998), s. 185 ff. Herudover henvises til den almindelige ophavsretlige litteratur, navnlig *Koktvedgaard* (2005) og *Peter Schønning* (2003).

I Lov & Data, 2001, s. 1-6, gennemgår *Bernt Hugenholtz* den retspraksis, der på tidspunktet for udarbejdelsen af artiklen (april 2001) foreligger om databasedirektivet. I en doktorafhandling fra 2005, "Database Rights in Safe European Home: The Path to More Rigorous Protection of Information" (Acta Universitatis Lappeenrantaensis 202) har *Perttu Virtanen* samlet en lang række af de afgørelser, der er truffet på grundlag af databasedirektivet i de enkelte EU-lande.

Kapitel 9. TILGRÆNSENDE PROBLEMSTILLINGER

9.1. Frembringelser skabt med IT

9.1.a. Problemstillingen

Udgangspunktet

I afsnit 6.2.c. så vi, at den ophavsretlige beskyttelse kræver, at nogen – altså et menneske – har udvist originalitet. For en række frembringelser gælder det, at den opståede værdi udspringer af processer mv., som har rent maskinel karakter, og hvor processen altså er blevet gennemført uden samtidig menneskelig påvirkning. Den forandring af en informationsmængde, som f.eks. en processor kan udvirke, kan være nok så kompleks og omfattende men i bund og grund kendetegnes den ved at være forudbestemt af et program, der samvirker med de kommandoer, brugeren retter til systemet. Derfor – kan man hævde – er det ikke muligt at tale om, at noget ophavsretligt "værk" opstår, som skabt af computeren: Hvad enten der er tale om en originær frembringelse (når programværket skabes fra grunden) eller om en bearbejdning, er selve systemet ganske enkelt ikke i stand til at udføre de "originale" bidrag, der frembringer den nødvendige originalitet.

Skulle man anerkende en maskine som "ophavsmand", ville man underminere hele den juridiske pligt- og rettighedslære, jf. nærmere *E&A*, s. 165 ff. Alle IT-systemer er prædisponerede, uanset hvor komplekse de er, og uanset om de gør brug af den ene eller anden type programmering – det være sig via neurale net, parallelprocessing eller andet. En maskine kan aldrig medvirke kreativt ved frembringelsen af et værk og vil endnu mindre kunne udtrykke den "personlighed" i værket, som er en forudsætning for at opnå ophavsret. Det er derfor misvisende – som det ofte ses – at tale om "*værker* skabt ved edb" el.lign. Se tilsvarende WIPO: Committee of experts on model provisions for legislation in the field of copyright – Draft Model Law on Copyright (WIPO doc.no. CE/MPC/III/2) af 30. marts 1990, pkt. 122, der om værker skabt ved edb antager, at "the results of such "creation" would hardly be covered by the Berne Convention". Problemstillingen er berørt i den engelske *Copyright, Designs and Patents Act* fra 1988, som i section 178 definerer "computer-generated" som dette, at "the work is generated by computer in circumstan-

ces such that there is no human author of the work". Lovens section 9 (3) fastslår, at ophavsmanden til et litterært, dramatisk, musikalsk eller kunstnerisk værk, som er "computer-generated", skal anses som "the person by whom the arrangements necessary for the creation of the work are undertaken". Det interessante ved loven er, at den anser computer-generated works som en særskilt værkskategori, sml. herved section 12(3), der beskytter disse værker i 50 år fra det kalenderår, hvori de blev skabt. Dette fører til en delikat sondring mellem værker, der er henholdsvis "computer aided" og "computer generated", sml. *Dworkin & Taylor* a.st. s. 185 f. Problemet behandles af *Michael Plogell* i NIR 1999.4 ff., der sondrer mellem den "skabende" og den "indirekte skabende" indsats, idet han påpeger de særlige problemer, der i det sidstnævnte tilfælde kan opstå i henseende til, hvordan den enkelte indsats finder kreativt udtryk i det færdige værk (a.st. s. 10).

Knoph

Problemet er i og for sig ikke nyt. Allerede i 1936 afviste *Knoph* (Åndsretten, s. 70), at man skulle tale om et kunstværk, hvis dette var hidført ved, at mekaniske hjælpemidler har arbejdet helt på egen hånd, eller ophavsmandens medvirken har været rent underordnet. Han påpegede herved, at fotografiernes udelukkelse fra ophavsbeskyttelse markerer et klart udtryk for lovens syn i så henseende. Men samtidig betonede han, at en kunstner godt kan tilføre et værk så meget af sin personlighed, at det opnår fornøden værkshøjde, selv om han tager mekaniske hjælpemidler i anvendelse. Man må med andre ord se på, hvem der *disponerer kreativt* i den pågældende sammenhæng.

Den moderne digitale ophavsret har imidlertid frembragt en række tilfælde, hvor en frembringelse på den ene side kan konstateres at være udvirket ved et kompliceret samspil mellem en række tænkende medvirkere; men at man på den anden side er ude af stand til at konstatere, *hvem* blandt disse medvirkere der kan karakterises som "ophavsmand". At man er det skyldes, at den endelige udformning af værket beror på et komplekst teknisk samspil mellem disse medvirkere. Eksempler herpå kan være fantastiske grafiske figurer, der er skabt gennem kompliceret matematik (*Mandelbroot*-fraktaler) eller tredimensionelle geometriske figurer.

Analyse

For at nærme sig denne problematik kan man først tænke sig, at en sådan frembringelse fra ende til anden er skabt af *en og samme person*. Den pågældende har altså såvel konstrueret hele den automatiserede procedure, der ligger bag frembringelsen, som de enkelte påvirkninger af denne procedure, der bevirker, at konstruktionen til sidst udskrives af printeren. I et sådant eksempel vil der ikke kunne rejses tvivl om, at værket er beskyttet, og at den pågældende konstruktør er ophavsmand. Problemet må

derfor være at udskille de elementer af den kreative frembringelsesproces, hvor den for ophavsbeskyttelsen nødvendige *originalitet* udvises. Svaret på dette spørgsmål må beror på, hvilken type frembringelse man har at gøre med. Herom i det følgende.

9.1.b. Litterære fremstillinger

I relation til almindelige litterære værker kan man spørge, hvordan rettighedsforholdene tager sig ud, hvis ophavsmand A på forhånd har etableret rammerne for en litterær fremstilling – f.eks. en fortælling eller beskrivelse – som ophavsmand B herefter kan fylde ud med variable oplysninger. Har forfatter A udviklet et program, der tilbyder brugeren at skrive en novelle på 5 minutter, må det antages at A har den fulde ophavsret til de noveller, bruger B skriver, når brugerens kreative spillerum har begrænset karakter (f.eks. udmøntet i valg af navn, lokalitet, tid, handlingstype, fravalg af bandeord etc.). Men dette udgangspunkt viger, jo mere brugeren sættes i stand til at fylde handlingselementer på. Tilsvarende må det antages, at bruger B af et handlingsbaseret computerspil udviklet af programmør A ikke opnår nogen "medophavsret" over det hændelsesforløb, spillet gennemløber, når B sætter sig i den enkelte rolles sted og træffer beslutninger inden for spillets rammer. Problemet kan f.eks. få praktisk betydning ved TV-transmission af brugerens udførelse af et computerspil.

9.1.c. Programoptimering mv.

Objektkodegenerering

Vender man sig til programsiden kan man i spektrets ene ende tage udgangspunkt i den frembringelse af programmets objektkode, der sker ved oversættelse af kildetekst. Selv om objektkoden fremtræder anderledes end kildeteksten – og for så vidt kan siges at udgøre en "bearbejdning" af denne – må den udelukkende betragtes som en *eksemplarfremstilling* af kildeteksten. Dette skyldes, at der ingen kreative valg er udfoldet i det forløb, hvor kildetekst bliver til objektkode. At *objektkoden* ophavsbeskyttes, skyldes netop programmørens kreative udfoldelse i *kildeteksten* før oversættelsen.

CASE-programmering

Visse programværktøjer inden for fjerdegenerationssprogene og den såkaldte CASE-programmering er i stand til at frembringe programstof af en karakter, der tidligere nødvendiggjorde programmørarbejde. Programmøren angiver blot nogle mål for programmeringen, hvorefter den nødvendige kode automatisk frem-

bringes. Har CASE-udvikleren kunnet udvikle sit program med et fåtal af instruktioner og må det antages, at disse instruktioner ikke vil afspejle udviklerens personlighed (f.eks. fordi en hvilken som helst anden udvikler ville gøre brug af de samme for at opnå en given funktion), vil den færdige applikation næppe give CASE-udvikleren ophavsret. Dette implicerer dog ikke, at sådanne programmer er beskyttet dårligere. Ophavsretten vil i stedet tilfalde rettighedshaveren til CASE-værktøjet.

9.1.d. Digital bearbejdning

Digitalisering

Den "bearbejdning" af en manifestation, der resulterer i en digitalisering, indebærer ikke i sig selv, at der er skabt et litterært værk, medmindre der i forbindelse med digitaliseringen er sket en sådan forædling af informationsmængden, at der foreligger en bearbejdning, jf. ophl. § 4. Problemet kan f.eks. opstå, når et litterært værk, som ophavstiden er udløbet for, digitaliseres og lægges frem for almenheden på en hjemmeside. I denne digitaliseringsproces er der i almindelighed ikke mulighed for at udvise den fornødne originalitet: Den ene skulle jo gerne blive identisk med den anden! Enkeltstående tilfælde af fejlretning kan ikke opfylde dette krav. Sådanne indslag vil som udgangspunkt have karakter af "teknisk medhjælp", for hvilken der ikke opnås (med)ophavsret.

Derimod kan det tænkes, at den samling af data, som digitaliseringen udvirker, kan beskyttes som database, jf. nærmere afsnit 8.4., hvis kravene om "væsentlig investering" samt muligheden for metodisk struktur og individuel konsultationsmulighed er opfyldte. Begge disse betingelser vil ofte kunne give anledning til tvivl.

Virtual reality

I nær forbindelse med ovennævnte spørgsmål er beskyttelsen af *virtual reality*-information, dvs. information, der præsenteres grafisk for at gengive en del af virkeligheden, f.eks. et brobyggeri, der er under opførelse, eller en situation, som deltageren i et spil befinder sig i. I modsætning til den rene digitalisering vil frembringeren af et VR-produkt typisk tilføje værket en værdi, der i et eller andet omfang er udtryk for hans originalitet. I det omfang, en sådan originalitet er udvist, kan VR-frembringelsen give grundlag for ophavsretlig beskyttelse som selvstændigt værk eller – såfremt grundlaget er retsbeskyttet (f.eks. et arkitektonisk værk) – som bearbejdning, jf. ophl. § 4, stk. 1.

En principielt anden problemstilling er det, at den digitaliserede frembringelse må betragtes som et *eksemplar* af det pågældende værk, f.eks. i relation til spørgsmål om konsumption, privatkopiering

og lignende. Ved at digitalisere et kunstværk kan man altså ikke påberåbe sig de regler, der gælder for konsumption af litterære værker, jf. om disse regler nedenfor under 6.4.d. Digitalisering af kunstværker og andre værker anvendes hyppigt i multimedia-produkter og ved design af hjemmesider mv. Når en hjemmeside f.eks. afbilder et beskyttet eksemplar af brugskunst, skal sidens indehaver følgelig sikre sig samtykke fra designeren. Derimod er det tilladt at afbilde bygningsværker uden samtykke fra arkitekten, jf. ophl. § 24, stk. 3. Se i øvrigt om disse spørgsmål, *Pernille Kallehave*: "Hvad må jeg? – ophavsret i teknologistøttet uddannelse", udsendt af Center for Teknologistøttet Uddannelse under Dansk Teknologisk Institut (1997).

Tekstkonvertering

Det må ligeledes antages, at en virksomhed (f.eks. indenfor det stigende område for såkaldt digital publishing), der *forædler* et datamateriale ved at *konvertere* det fra ét format til et andet, ikke dermed opnår nogen medophavsret til det færdige produkt. Produktet er nemlig ikke udtryk for nogen særlig kreativitet; ligger standarderne klart – hvilket typisk er hele forudsætningen for bearbejdningsopgaven – vil og skal to programmører, der stilles overfor den samme opgave, frembringe fuldstændigt det samme datamateriale. Ønsker den virksomhed, der yder en sådan bistand, en form for medandel i det færdige resultat, må dette altså ske ved aftale. Ophavsretten skaber ikke nogen medophavsret i dette tilfælde.

9.1.e. Ekspertsystemer

Et ekspertsystem er et IT-system, der ved hjælp af programmel udfører beslutninger eller danner grundlag for at udføre beslutninger ved at simulere de overvejelser og handlingsvalg, som en ekspert ville træffe i en given situation. Grundlaget for ekspertsystemets beslutninger mv. er en vis viden, hvorfor man ofte taler om "videnbaserede systemer". Sådanne systemer er typisk opbygget af flere moduler, der ophavsretligt må håndteres forskelligt. De konklusioner, systemet f.eks. udskriver på skærmen, er beskyttet på samme måde, som hvis de var nedfældet i en bog, ligesom det programmateriale, der er inkorporeret i det programmodul (kaldet "inferensmaskinen"), der drager slutninger, beskyttes som andre programværker.

Ekspertsystemets centrale komponent er den videnbase, der inkorporerer informationerne fra "eksperten" gennem et antal teknisk indicerede valg af typen "hvis ..., så ...". Indbegrebet af disse valg udgør næppe i sig selv noget værk; nogen sammenstilling af værker er der heller ikke tale om, og ophavsretsloven giver

ikke beskyttelse for den ekspertise, der herved kommer til udtryk. Dette element af ekspertsystem-teknologien må derfor i givet fald beskyttes på grundlag af konkurrenceretlige regler og/eller efter reglerne om databaser, jf. ophl. § 71.

Neurale net

Et særligt vacuum i den ophavsretlige beskyttelse opstår for ekspertsystemer, der er baseret på såkaldt *neurale net*. Et neuralt net virker således, at det ud fra en angivelse af visse bestemte aspekter indlæser et antal eksempler og på grundlag heraf konkluderer noget om, hvilke mønstre eller lovmæssigheder der er gældende for disse eksempler. Som grundlag for udviklingen af et neuralt net anvender man et særligt programværktøj, der selvfølgelig kan beskyttes som ethvert andet program. Problemet om beskyttelse af neurale net har at gøre med det aspekt af applikationen – den investering – der består i optræningen.

Som ophavsretsloven er formuleret, er dette aspekt ikke beskyttet. Optræningen af det neurale net skaber ikke noget "litterært værk", medmindre der er tale om litterære bearbejdninger af det anvendte programværktøj. Hertil kommer, at den, der optræner et neuralt net, ikke har kontrol over den funktion, som det kommer til at varetage. Meningen er netop, at nettet skal udlede en logisk struktur ud af de eksempler, der indlæses. En beskyttelse af optrænede neurale net må derfor praktiseres ved, at brugeren efter nærmere aftale indtræder i den ophavsret, programværktøjet er belagt med. Ellers må man nøjes med den konkurrenceretlige beskyttelse i medfør af markedsføringsloven. Der findes endnu ingen praksis på området – hverken herhjemme eller i USA. Se for amerikansk ret *Gerald H. Robinson* i 7 The Computer Lawyer (March 1990), s. 17 ff. Selve listen over de eksempler, der er indlæst i det neurale net, kan beskyttes som *database* (katalog), jf. ophl. § 71.

9.2. Fonte og skrifttyper

9.2.a. Problemstillingen

Til nutidens IT-anvendelse hører muligheden for at printe dokumenter ud i avanceret grafik med høj opløsning og med muligheden for at bibringe det færdige produkt æstetiske kvaliteter, som kan aktualisere en retsbeskyttelse. Behovet for en sådan retsbeskyttelse kendes allerede fra forlagsverdenen, hvor det diskuteres, om den grafiske tilrettelæggelse af en bog (herunder i henseende til valget af skrifttype, skriftstørrelse, overskriftsangivelse,

sideopsætning, forside, registre mv.) bør kunne beskyttes ophavsretligt, se hertil *Koktvedgaard* (2005), s. 189.

En sådan beskyttelse ville i givet fald. kunne indebære, at den forlægger, der selvstændigt tilrettelægger og udgiver et værk i *public domain*, indtil 70 år efter udløbet af tilrettelæggerens dødsår kunne modsætte sig en gengivelse af værket, der genskaber denne tilrettelæggelse (f.eks. i forbindelse med en fotokopiering). En sådan retstilstand, der ikke har sikker hjemmel i ophl. eller i anden lovgivning, er der næppe belæg for og støttes i øvrigt ikke af nyere dansk eller anden sammenlignelig retspraksis. Nærgående efterligninger må derfor i givet fald håndteres gennem reglerne om god markedsføringsskik, jf. mfl. § 1.

I en IT-retlig sammenhæng er det navnlig beskyttelsen af den enkelte skrifttype – eller font – der giver anledning til interesse. Denne beskyttelse har primært betydning for den kommercielle udnyttelse af de løsninger, der indbygger de nødvendige fonte mv. i IT-udstyret, f.eks. i computerens printerdrivere eller i den enkelte printer. Som grundlag for disse anvendelsesformer indgås der typisk licensaftaler med relevante rettighedshavere på det globale marked for disse frembringelser. I relation til den private og erhvervsmæssige bruger af dette udstyr har beskyttelsen stort set ingen praktisk betydning. Det retlige og praktiske udgangspunkt er her, at retten til at benytte de nævnte fonte mv. må antages videreført til slutbrugeren i kraft af den licens, der gives til at installere skrifttypen på det udstyr, der er beregnet til at skulle benyttes af denne.

Restbeskyttelsen af en font mv., kan støtte sig på to regelsæt, ophavsretten og designretten, se hertil afsnit 9.2.b. og 9.2.c. I tillæg hertil kan det – som anført i petit-afsnittet ovenfor – tænkes, at en nærliggende efterligning kan rammes efter reglerne herom i mfl. § 1. På grund af styrken i den ophavs- og designretlige beskyttelse er denne beskyttelse dog sjældent aktuel og den omtales derfor ikke videre i det følgende.

9.2.b. Ophavsretlig beskyttelse

Værksbeskyttelse

Når man overvejer, om fonte og skrifttyper skal kunne beskyttes ophavsretligt, er det nødvendigt at knytte dette spørgsmål til det enkelte bogstav mv. Som anført af *Koktvedgaard* a.st. kan arbejdet med at udarbejde en ny skrifttype være krævende. Omvendt ligger det klart, at udformningen af et bestemt bogstav er begrænset af, hvorledes man forventer, at bogstavet skal se ud. Bogstaverne F og E adskiller sig nu engang ved at have henholdsvis to

og tre vandrette streger etc. I henseende til denne kreativitet er frembringerens handlefrihed dog ikke mere begrænset end handlefriheden er det for den, der i brugskunstens verden designer en stol. Derfor kan fonte og skrifttyper beskyttes som brugskunst under samme (skrappe) krav til originalitet, som i øvrigt gælder for brugskunsten, hvor funktionelle formål lægger begrænsninger i kreativiteten. Fordi kravene til originalitet sættes så højt finder man derfor også en betydelig mængde bogstaver mv., der *ikke* er beskyttet ophavsretligt.

Ækvivalensvurderingen

Fordi originalitetsvurderingen tager udgangspunkt i det enkelte bogstav mv. er der ingen ophavsret til hele alfabeter *som sådanne*. Under almindelig tekstskrivning mv., der involverer hovedparten af alfabetets bogstaver, vil den praktiske konsekvens af denne begrænsning være beskeden: Beskyttes kun 5 af de mest benyttede bogstaver, vil denne beskyttelse være tilstrækkelig til at sikre frembringerens interesser.

9.2.c. Designbeskyttelse

Med bestemmelsen i designlovens § 2, stk. 1, nr. 2, er ordet "produkt" i designloven defineret som "en industrielt eller håndværksmæssigt fremstillet artikel, herunder bl.a. dele, der er bestemt til at blive samlet til et sammensat produkt, samt emballage, udstyr, grafiske symboler og typografiske skrifttyper, men ikke edb-programmer." Bestemmelsen indebærer en udvidelse af den retlige beskyttelse af disse indretninger i forhold til den tidligere mønsterlov. Et produkt behøver heller ikke at være en fysisk genstand. Også den grafiske fremtrædelse af en opsætning (f.eks. i form af et skema eller lignende) kan beskyttes, selv om det alene vises på et display eller som skærmbillede på en computer. Se nærmere om denne beskyttelse i afsnit 10.3.

9.3. Naborettigheder

9.3.a. Kunstneriske præstationer

Ifølge ophl. § 65 beskyttes en udøvende kunstners fremførelse af et litterært og kunstnerisk værk. Bestemmelsen forudsætter, at der foreligger en kunstnerisk fremførelse. Den animation, der f.eks. finder sted ved IT-baseret automatiseret tegnefilmproduktion, fører ikke til en sådan beskyttelse af animatoren. En sådan beskyttelse er da heller ikke påkrævet, da animatoren som ud-

gangspunkt opnår beskyttelse af værket som kunstnerisk værk (eller i det mindste som en del af et kunstnerisk fællesværk, der også indbefatter ophavsmanden til det litterære eller filmiske forlæg).

VActing

En omvendt problemstilling foreligger, når en skuespiller eller danser lader information om sine bevægelser "optage" ved hjælp af registrerende sensorer. Selve optagelsen må i så fald betragtes som en "optagelse på bånd, film eller anden indretning", jf. § 65, stk. 1, nr. 1. Men spørgsmålet er, om den heraf følgende ret til at modsætte sig tilgængeliggørelse for almenheden, jf. samme bestemmelses nr. 2, også gælder for de digitale frembringelser, der udnytter disse bevægelser i andre sammenhænge, f.eks. som grundlag for tegnefilm-animation, undertiden kaldet VActing (Visual Acting).

Identitetsskift

Problemerne opstår navnlig, hvis man digitalt fjerner eller ændrer skuespillerens identitet, således at seeren oplever en anden end skuespilleren. Denne problemstilling har to sider. Hvis det gennemførte identitetsskift indebærer, at en ikke kendt skuespiller nu fremtræder som en kendt, er vi uden for området af § 65, men inde i de dommerskabte regler, der gælder om personbeskyttelse, se således dommene i *U 1965.126 H* (Buster Larsen – "Cirkus Buster"), *U 1974.952 Ø* (multi-kunstneren Otto Sigvaldi), *U 1986.272 SH* (Per Pallesen: "Lige på en studs"), *U 1986.428 Ø* (fremtrædende erhvervsledere i politisk reklame), *U 1989.1146 SH* (erhvervsleder i reklame for dagblad) og *Henrik Udsen* i U1997B.261 ff. Er der derimod tale om, at skuespillerens præstation "genbruges" i en form, der ikke gør det muligt at genkende den skuespiller, der har frembragt bevægelserne, må forholdet betragtes som omfattet af § 65, hvilket betyder, at det indlæste ikke må gøres tilgængeligt for almenheden. Anvendelsen af denne regel udelukker dog ikke en samtidig påberåbelse af de førnævnte dommerskabte regler om brug af personidentiteter.

MIDI-afspilning

Tilsvarende problemer opstår i forbindelse med beskyttelsen af såkaldte MIDI-filer. MIDI (Musical Instrument Digital Interface) er en standard, der definerer det sprog, som elektroniske musikinstrumenter baseret på digital teknik anvender, og dermed sammenkobles efter. En MIDI-fil vil således kunne indeholde den udførelse af den enkelte tonestemme i en indspilning, der f.eks. registreres ved pianistens berøring af de enkelte tangenter på klaviaturet. Filen kan herefter indspilles med andre instrumentlyde, f.eks. således at klaverstemmen afspilles som guitarlyd. Tek-

nikken tillader næsten enhver form for manipulation af disse lyde, f.eks. klange, rytmer og toner på de tilkoblede instrumenter.

Isoleret set må en MIDI-fil rubriceres under forskellige regelsæt. Den udgør for det første et *eksemplar* af det pågældende musikværk. Dernæst kan den betragtes som en lydfæstning på "anden indretning" af den kunstneriske fremførelse, pianisten udfører ved "indspilningen" til filen, jf. ophl. § 65, stk. 1.

I relation til efterfølgende ændringer i filen kan der opstå tvivl om, hvorvidt ændringen angår den *kunstneriske udførelse*, om der er tale om rent *teknisk redigering*, eller om ændringen indebærer en ændring i den pågældende *komposition*. Disse spørgsmål er dog nogenlunde sammenfaldende med dem, der knytter sig til afgrænsningen mellem improvisation og udførelse, se hertil *Schønning* (2003), s. 97 og 198.

9.3.b. Mekaniske rettigheder

Ophl. § 66 yder fremstilleren af en "lydoptagelse" en 50-årig beskyttelse mod "eftergørelse", hvilket ifølge bestemmelsen også omfatter det forhold, at en lydoptagelse (lydfæstning) overføres fra én optagelse til en anden. Beskyttelsen gælder ikke alene det store område for *musikalske* CD-produktioner, men giver bl.a. også en fonogramproducent beskyttelse mod eftergørelse af andre lydlige frembringelser. Det er således uden betydning for beskyttelsen efter § 66, hvilken type lyd der er tale om. Også metalliske lyde, kanonskud og naturens lydlige indtryk vil være beskyttet i denne mekaniserede form, hvad enten de foreligger i særskilt form (f.eks. en CD med dyrestemmer) eller som led i en større helhed. I konsekvens af denne bestemmelse er det den praktiske hovedregel, at CD-produkter med lydfæstninger ikke kan lægges på en hjemmeside uden producentens samtykke, medmindre det drejer sig om enkelte småbidder, der uddrages som citater, jf. ophl. § 22.

Med hjemmel i § 66 kan producenten af et multimedia-produkt med lydeffekter (f.eks. et computerspil med lyd og animation eller et kursusprogram med tilsvarende effekter) modsætte sig eftergørelse af disse lydeffekter. Det kræves dog, at den lydfæstning, han har foretaget til dette formål, er den første lydoptagelse og ikke blot en kopi, jf. nærmere *Schønning* (2003), s. 562 f.

9.3.c. Film

I overensstemmelse med det almindelige ophavsretlige udgangspunkt må det antages, at de digitaliserede filmsekvenser, der kan

optræde i digitale samleværker mv., må behandles på samme måde som andre filmsekvenser. Navnlig underholdningsprægede oplevelsesspil til børn har stor funktionel lighed med tegnefilm (som utvivlsomt falder inden for filmreglerne). Sådanne produkter fortæller gerne en historie ved hjælp af stort set samme virkemidler som anvendt inden for tegnefilm. Den eneste forskel ligger i, at brugeren (barnet) selv "klikker" sig rundt i historien gennem en række interaktive valg; men dette interaktive aspekt må være uden ophavsretlig betydning: Gjaldt et sådant krav i relation til celluidfilm, ville man jo heller ikke nå til, at der så ikke længere var retsbeskyttelse. At "tegningerne" i en sådan filmsekvens udelukkende er baseret på digitalteknik spiller heller ingen afgørende rolle, da beskyttelsen som filmværk indtræder uanset det medium, hvorpå filmværket distribueres. Afgørende må være, om der på forhånd er indbygget et kunstnerisk handlingsforløb i produktet, som hermed fortæller en historie, eller flere. Et computerspil, der udfolder sig ved, at to fodboldhold spiller mod hinanden, vil ikke opfylde dette krav.

Spørgsmålet blev pådømt i den tyske afgørelse om edb-spillet "Donkey Kong Junior", GRUR 1983.757, der nægtede beskyttelse som filmværk u.h.t., at spillets handlingsudfald ikke var givet på forhånd. En tilsvarende opfattelse er lagt til grund af den svenske højesteret i *NJA 2000.580* (2000:87), se hertil – kritisk – *Daniel Westman* i L&D no. 65, s. 10 ff. (marts 2001). Men den herved udtrykte retsopfattelse beror formentlig på, at der var store iøjnefaldende forskelle mellem grafikken i dette første generations computerspil og nutidens produkter med deres høje opløsning og intensive brug af levende billeder.

Derimod kan det næppe antages, at multimedia-værker i ophavsretlig terminologi skal betragtes som filmværker. Virkningen af en sådan indrubricering ville være, at lovens særregler om filmværker fandt anvendelse, herunder ophl. § 58, der bl.a. indeholder en formodningsregel om, at de medvirkende ikke kan modsætte sig, at der fremstilles eksemplarer af filmen, at denne spredes til almenheden, fremføres offentligt eller at den forsynes med tekster eller tale på et andet sprog.

Andre særregler findes bl.a. i § 12, stk. 3, nr. 2), om forbud mod benyttelse af fremmed medhjælp ved eksemplarfremstilling, § 12, stk. 4, om forbud mod at stille teknisk kopieringsudstyr til rådighed på biblioteker og andre offentligt tilgængelige steder mv., § 19, stk. 3, om forbud mod spredning af filmværker gennem udlån, § 20, der forbyder visning af eksemplarer af kunstværker, som ophavsmanden har overdraget til andre, i fjernsyn eller på film, § 21, hvis stk. 1 forbyder offentlig fremførelse af filmværker, dog med mulighed for gen-

nemsyn på biblioteker mv., jf. stk. 3 samt § 25 om fremførelse af værker som led i dagsbegivenheder på film. Derimod kan man næppe anvende reglerne i § 13, stk. 2, der udelukker filmværker i biografernes almindelige repertoire fra aftalelicensen på undervisningsområdet, samt andre af de aftalelicensregler, der tager særligt sigte på den klassiske spille- og dokumentarfilm.

9.4. Tekniske beskyttelsesforanstaltninger

9.4.a. Problemstillingen

Formål og funktion

Det er ikke ualmindeligt, at programrettighedshavere søger at *understøtte* en licensregulering eller at *håndhæve* ophavsretten gennem tekniske foranstaltninger af forskellig art. Sådanne anordninger kan enten tilsigte at gøre det helt umuligt at foretage en sådan kopiering (ofte kaldet *copy protection*) eller dog at vanskeliggøre denne kopiering (ofte kaldet *copy discouragement*). Nogle af disse anordninger er indbygget uden særskilt aftale, som en slags "ophavsretlig selvhjælpshandling" (jf. terminologien hos *Thomas Riis* i Festskrift til Koktvedgaard (2003), s. 425 ff.), medens andre fremstår som et dertil indrettet program, som brugeren skal anvende i overensstemmelse med en aftale, der begrænser kopieringen til et bestemt antal kopier etc. Nogle anordninger udfører deres funktioner uden at involvere brugeren aktivt, medens andre virker ved en gang eller løbende at afkræve brugeren en dokumentation (f.eks. et password eller andet identifikationsbevis). Hertil kommer de systemer, der har til formål at registrere omfanget af en tilladt brug.

Den tekniske udformning af disse foranstaltninger kan variere. Nogle foreligger som rene softwareløsninger, medens andre er indbygget i hardwareenheder. En hardwareenhed kan f.eks. fremtræde som en USB-nøgle, som brugeren må tilslutte sin computer, når programmet benyttes. På tv-området er det almindeligt at benytte såkaldte dekoderkort, der f.eks. placeres i en satellitmodtager med henblik på at omforme det krypterede tv-signal.

De kopibeskyttelsesanordninger, der beskyttes af reglerne i kapitel 6a, falder i flere kategorier. I en kategori kan man rubricere de *hardwarebaserede* anordninger, der f.eks. bygges ind i såkaldte "dongles" (f.eks. et kort, der placeres i computerens parallelle eller serielle port) eller på en diskette. Når programmet kaldes, kontrolleres det, at smart card eller dongle er installeret. Ved at overdrage, hen-

holdsvis tilbagegive den anvendte hardwareenhed, kan man gennemføre transaktionen på samme måde som almindelige løsørekøb. En anden form for hardwarebeskyttelse, der primært kendes inden for elektronikindustrien, benævnes på engelsk *Serial Copy Management System* (SCMS). Denne løsning, der f.eks. er indbygget i visse DAT-afspillere, kommunikerer med de særlige digitale hoveder, som er indbygget i visse fonogrammer (med henblik på at afskære piratkopier heraf). Mange brugere anser også denne form for kopibeskyttelse for at være besværlig, og dette forhold tjener måske til at forklare DAT-teknologiens forholdsvis ringe udbredelse. Blandt de *softwarebaserede* beskyttelsesanordninger kan først og fremmest nævnes password og serienummerbeskyttelse. Løsningen kan her enten være, at brugeren løbende afkræves indtastning af et password (som f.eks. hentes fra den mere kopieringstunge manual), eller at programmet henter denne værdi fra en original diskette (som permanent eller med mellemrum fordres indlæst i systemet). En anden softwarebaseret beskyttelsesform er de såkaldte ERMS-systemer (*Electronic Rights' Management Systems*), der med henblik på en individuel udlodning af ophavsretlige vederlag identificerer rettighedshaverne til de enkelte værker.

Det har erfaringsmæssigt altid vist sig muligt for personer med de rette forudsætninger at *bryde* sådanne kopispærreanordninger og at *distribuere* kendskabet til disse omgåelsesmetoder effektivt (f.eks. via Internet), så forsøget på at begrænse den ulovlige brug er bragt til en videre kreds. Motivet hertil kan være et ønske om at kunne profitere af en ulovlig kopiering og omsætning af de pågældende programmer. I visse kredse er der ligefrem gået sport i at være den første, der "cracker" en ny kopibeskyttelse, hvorved der nærmest er opstået en slags våbenkapløb mellem rettighedshavere og crackere.

Retsudvikling

I dette kapløb har lovgiveren bl.a. søgt at komme rettighedshaverne til undsætning ved selvstændigt at kriminalisere visse former for besiddelse og omsætning af programmer mv., der gør det muligt at bryde sådanne kopispærreanordninger. De regler, der findes herom i lovgivningen, har alle været resultatet af – forståelige – retspolitiske ønsker fremsat af de forskellige industrier, der har været særligt ramt. Det første eksempel på en sådan lovgivning er ophl. § 75b (tidligere § 78), der forbyder omsætning eller besiddelse i kommercielt øjemed af midler, hvis eneste formål er at lette ulovlig fjernelse eller omgåelse af tekniske indretninger, som måtte være anvendt for at beskytte et *edb-program*. Bestemmelsen har udspring i direktiv 91/250/EØF art. 7, stk. 1, litra c). Ved lov nr. 1095 af 29. december 1997 blev en lignende regel indsat om tv-dekodere, jf. herom senere. Reglen blev ændret ved lov nr. 446 af 31. maj 2000, hvorved forbuddet blev udvidet fra

erhvervsmæssig fremstilling etc. til også at omfatte privat besiddelse af piratdekodere mv.

Efter at USA med vedtagelsen af *the Digital Millennium Copyright Act* i 1999 indførte en lignende kriminalisering i relation til *andre værker* kom der et pres på EU for at vedtage lignende regler. Disse regler blev indført i Infosoc-direktivets art. 6 og 7 og ved den implementering af direktivet, der fandt sted ved lov nr. 1051 af 17. 12. 2002, blev der indføjet et nyt kapitel 6a til ophavsretsloven, der med overskriften "Tekniske foranstaltninger mv." omfatter §§ 75b-75e. Hvor § 75b svarer til den tidligere lovs § 78, er reglerne om beskyttelse af tekniske indretninger til beskyttelse af *andre* værker og frembringelser i digital form end edb-programmer (lovens §§ 75c-75d), nye i forhold til i den tidligere lov. Reglerne herom er omtalt af *Kim Frost* i U 2004B.142 ff. og i det førnævnte indlæg af *Thomas Riis*.

Retsområdet

Hele denne lovgivning indtager en egenartet placering i den ophavsretlige struktur. I en forstand befinder den sig uden for ophavsretsloven, idet den ikke har at gøre med den nærmere afgrænsning af den eneret, der tilkommer rettighedshaveren til den beskyttede frembringelse (værket, tv-udsendelsen etc.). Med sin fokus på den retsstridige omgåelse ligger reglerne nærmere den strafferetlige regulering af medvirkenshandlinger. Og navnlig efter indførelsen af reglerne i strfl. § 263a (der straffer den, der udbreder en kode eller andet adgangsmiddel til et *ikke offentligt tilgængeligt* informationssystem, hvortil adgangen er beskyttet med kode eller anden særlig adgangsbegrænsning), har reglerne fundet en strafferetlig pendant, hvor en række af de vanskeligheder, der er forbundet med deres anvendelse, træder frem. Da reglerne samtidig søger at ramme den erhvervsmæssige distribution og markedsføring af de nævnte værktøjer mv., rummer de også en væsentlig markedsføringsretlig regulering.

Systematisk indplacering

Disse mange facetter af reguleringen kan i en tværgående fremstilling vanskeliggøre en placering i én systematisk ramme. I overensstemmelse med den afgrænsning, der er gjort i strfl. § 263a mellem offentlige og ikke-offentlige informationssystemer, er afgrænsningen her gjort således, at der i dette kapitel, der knytter sig til beskyttelsen efter ophavsretsloven, sættes fokus på de regler, der findes i denne lov. Reglerne om beskyttelse af adgangsmidler til ikke-offentlige informationssystemer i strfl. og i radio- og fjernsynslovens § 91 behandles derimod i den strafferetlige fremstilling, se herved afsnit 17.5. De almene problemstillinger, der knytter sig til begge regelværk, behandles dog mest hensigtsmæssigt ét sted, nemlig i det følgende.

9.4.b. Almene problemstillinger

Indhold og kompleksitet

Såvel Infosoc-direktivet som de implementerede regler var genstand for indgående diskussion og kritik inden vedtagelsen – såvel nationalt som internationalt. En del af kritikken gik på, at reglerne er svære at håndhæve, da de er formuleret meget bredt og derfor kan give anledning til en del fortolkningstvivl. Der er ikke megen fortolkningshjælp at hente i forarbejderne til direktivet, der begrænser sig til at udtale, at formålet er at beskytte ophavsret, beslægtede rettigheder og *sui generis* rettigheder i databaser, se betragtning nr. 48. I erkendelse af, at de nye regler på en række centrale punkter giver anledning til afgrænsningsproblemer, og for at imødekomme fremtidige vanskeligheder med at anvende bestemmelserne, er der tilføjet en revisionsbestemmelse til den danske gennemførelseslov, se ophl. § 89, stk. 3. Heri er det fastsat, at forslag til revision af §§ 75c og § 75d fremsættes i Folketinget senest i folketingsåret 2005-06. Dermed har Danmark implementeret direktivet rettidigt, men samtidig sikret sig adgangen til at tilpasse sin regulering på dette komplicerede og kontroversielle område.

Forholdet til licensen

Det er vigtigt at slå fast, at en teknisk foranstaltning ikke i sig selv påvirker omfanget af de *licensrettigheder*, en bruger har. Når man skal fastslå, hvilke beføjelser slutbrugeren har til at benytte et værk eller en anden frembringelse, må man derfor sondre mellem hvilken frembringelse, der er tale om, og afgrænse den lovlige brug efter de regler herom, der fremgår af ophavsretten eller af den indgåede aftale. At rettighedshaveren har indbygget en teknisk anordning i sit digitale produkt, der forhindrer en brug, der efter disse regler må anses for tilladt, vil som hovedregel tilføje produktet en mangel, som vil give brugeren misligholdelsesbeføjelser.

Strafansvar

Bestemmelserne er gjort strafbare ved ophl. § 78, som hjemler bødestraf for den, som *forsætligt eller groft* uagtsomt overtræder §§ 75b eller 75c. Bestemmelsen hjemler ligeledes bødestraf for overtrædelse af § 75e, men hertil kræves *forsæt*.

9.4.c. Edb-programmer

Ifølge ophl. § 75b er det ikke tilladt at omsætte eller i kommercielt øjemed besidde midler, hvis eneste *formål* er at lette ulovlig fjernelse eller omgåelse af tekniske indretninger, som er anvendt til at beskytte et edb-program. Bestemmelsen er indført på grundlag af art. 7, stk. 1, litra c, i direktivet om retlig beskyttelse af

edb-programmer (91/250). Den giver anledning til flere tvivlsspørgsmål.

Formålskriteriet

Det første angår det anvendte formålskriterium. Da tekniske indretninger ikke har noget formål (forstået som et subjektivt *motiv* bag bestemte handlinger mv.), må kravet herom antages at vise hen til den *sædvanlige funktion*, brugeren må forvente, at producenten har haft med indretningen. For at et "middel" skal være omfattet af bestemmelsen kræves det, at denne funktion er den "eneste". Derfor er bestemmelsens praktiske anvendelsesområde snævert. Selv om et indlæg i en nyhedsgruppe, der forklarer hvordan en kopibeskyttelse omgås, isoleret set udgør et "middel" til at omgå denne kopibeskyttelse, jf. *Schønning* i NIR 1992.71 f., er man uden for bestemmelsens anvendelsesområde, når dette formål ikke er det eneste med indlægget. F.eks. kan indlægget jo også tænkes at have til formål at advare rettighedshaveren om denne risiko. Tilsvarende vil generelle *utility*-programmer, der blandt andre funktioner kan anvendes til at omgå en kopibeskyttelse, være uden for forbuddet i § 75b.

§ 75b gælder kun, hvis det pågældende middel har som "eneste formål" at omgå kopibeskyttelsen. Kan indehaveren af en sådan anordning dokumentere, at hans formål med at besidde midlet er at sikre muligheden for en lovlig sikkerhedskopiering, må det være udelukket at anvende bestemmelsen. Generelle *utility*-programmer mv., der blandt mange andre funktioner kan anvendes til sådanne formål, vil altså ikke være omfattet af forbuddet.

Område

Også systemer til såkaldt *copy discouragement* er omfattet af bestemmelsen. Sådanne systemer gør det særligt besværligt at udføre ekstra kopier. Brugerens navn fremgår f.eks. af kopien, så enhver uautoriseret og distribueret kopi vil signalere, hvem der havde den lovlige ret til at bruge programmet (en faktor, der også understøtter retshåndhævelsen), eller systemet kan kun initieres ved hjælp af passwords, som brugeren må finde i programmets manual. Den, der vil kopiere programmet, må derfor også kopiere manualen for at have tilgang til de nødvendige passwords, og det vil ofte være så besværligt, at man afstår. Se herom *Andersen & Græbe* (1991), s. 42 ff. og generelt om "software locks" *Edward C. Saltzberg* i 5 C/LJ 163 (1984), s. 163 ff.

"Midler"

Med "midler" tænkes først og fremmest på programmer, hvad enten disse foreligger som ren kode eller indbygget i særlige kort el.lign. Men begrebet omfatter også rent numeriske værdier, f.eks. til indtastning med henblik på dekryptering af en informationsmængde. Det afgørende er, at der er tale om en "indretning",

der – underforstået – kan "besiddes". Hvor kendskab til et password ikke som sådan besiddes (for så vidt som det kan huskes), er et program, der er bygget til at kunne "knække" et password i forbindelse med en kopibeskyttelse, omfattet af bestemmelsen. Grænsetilfælde kan opstå, når et større antal passwords "besiddes" på særlige lister. Visse former for erhvervsmæssigt salg og spredning af sådanne koder kan derimod straffes efter strfl. § 263a, se hertil afsnit 17.5.a.

De beskyttede frembringelser

Dernæst kræves, at den pågældende kopibeskyttelse tilsigter at beskytte et "edb-program" eller "andre værker i digitaliseret form" mod det nævnte angreb. En anordning til omgåelse af kopibeskyttelse, der alene tilsigter at reservere et tv-signal for dekodere af en bestemt slags med henblik på betaling, rammes altså ikke af ophl. § 75b, allerede fordi det, anordningen beskytter imod, ikke indebærer nogen "kopiering". Sådanne omgåelsesforanstaltninger kan derimod efter omstændighederne rammes af 91 i lov om radio og fjernsynsvirksomhed.

- Retsstridighedskravet

Det kræves endelig, at den kopibeskyttelse, der er tale om at omgå, er lovlig. En kopibeskyttelse, der ikke tillader brugeren at udføre en sikkerhedskopi, jf. ophl. § 36, stk. 1, nr. 2, rammes følgelig ikke af forbuddet. Kravet får primært betydning, når bestemmelsen tænkes anvendt i relation til gerningsmandens besiddelse af omgåelsesmidlet. Mange midler til omgåelse af kopibeskyttelsesanordninger knytter sig ikke til kendte produkter, men derimod til generelt definerede metoder til kopibeskyttelse. Derfor vil *frembringeren* af sådanne, generelle, omgåelsesmidler ofte kunne godtgøre en række lovlige anvendelsesformer (nemlig i relation til de programprodukter, der hindrer lovlig sikkerhedskopiering mv.). Dette betyder, at *besidderen* i givet fald må godtgøre, at hans besiddelse af midlet tog sigte på en kopispærreanordning, der udelukkede en lovlig kopiering, for ikke at blive ramt af bestemmelsen.

9.4.d. Andre værker og frembringelser

Brugsforbuddet

Ophl. § 75c, stk. 1, forbyder *omgåelse* af effektive tekniske *beskyttelsesforanstaltninger* i andre værker og frembringelser end edb-programmer (jf. stk. 5) uden samtykke fra rettighedshaveren. Bestemmelsen har brugeren som sin adressat. I de tilfælde, hvor den finder anvendelse, vil der ofte allerede foreligge et ulovligt eksemplar. Men da den version af det ulovlige eksemplar, der frembringes uden en kopibeskyttelse, er langt farligere for ophavsmanden end selve det ulovlige eksemplar med beskyttelse

(fordi en yderligere kopiering og spredning dermed er langt enklere at foretage), er der et beskyttelsesbehov, som følgelig varetages af stk. 1.

- omgåelse

Det er ikke klart defineret, hvilke omgåelseshandlinger forbuddet retter sig mod. Men læser man stk. 1 i sammenhæng med ophl. § 75d (tvangslicensreglen) ligger det klart, at reglen må omfatte de foranstaltninger, der rammer den lovlige såvel som den ulovlige eksemplarfremstilling mv. Selv om brugeren ifølge sin aftale med rettighedshaveren har adgang til at udføre en eksemplarfremstilling, og selv om en eksemplarfremstilling er lovlig, f.eks. efter reglerne i ophl. kapitel 2, retfærdiggør dette tekniske forhold, der måtte forhindre brugeren heri, altså ikke, at brugeren udfører en omgåelseshandling. Baggrunden herfor er igen, at selve denne handling vil efterlade et eksemplar uden kopibeskyttelse mv., der – hvis det spredes videre – er mere farligt for rettighedshaveren end den manglende koperingsmulighed (som følge af anordningen) er generende for brugeren.

- foranstaltningerne

Ved "effektive tekniske foranstaltninger" forstås ifølge stk. 4 enhver form for effektive tekniske foranstaltninger, der under deres *normale funktion* har til formål at beskytte de retsbeskyttede værker og andre frembringelser mv. Med denne begrebsafgrænsning har man løst det logiske problem, bestemmelsen ellers ville indebære, læst efter ordlyden: Det er jo netop kun de foranstaltninger, der rent faktisk kan omgås (og som derfor ikke viser sig fuldt "effektive"), som det er relevant at regulere. Med afgrænsningen i stk. 4 sigter effektivitetsbegrebet mod den funktion, foranstaltningen tjener overfor brugeren.

Forsøg og medvirken

Ophl. § 75c, stk. 1, har karakter af et selvstændigt strafferetligt delikt. Heraf følger, at reglerne om forsøg og medvirken, jf. strfl. §§ 21 og 23, finder anvendelse i relation til denne bestemmelse. Denne iagttagelse er væsentlig for forståelsen af de øvrige led i § 75c. Formålet med disse led er nemlig ikke at ramme de handlinger, hvorved nogen *medvirker* til en omgåelseshandling, som omtalt i stk. 1, eller gennem markedsføring el.lign. *forsøger* at udføre en sådan handling. Formålet med de øvrige regler i § 75c er derimod at ramme handlinger, der uden at indebære forsøg eller omgåelse kan rumme forberedelsen til de handlinger, der er omtalt i stk. 1. Herved har lovgiveren gennem et *yderligere* led fremrykket fuldbyrdelsesmomentet i forhold til det centrale forhold – den ulovlige værksbenyttelse eller eksemplarfremstilling.

Notoritetstanken

Ophl. § 75c, stk. 2, forbyder fremstilling, import, spredning, salg, udledning, reklame eller besiddelse i kommercielt øjemed af tre forskellige indretninger, produkter eller komponenter, der

har til formål at omgå effektive tekniske foranstaltninger. De tre typer af produkter kendetegnes alle ved at fremtræde i situationer, hvor det er *notorisk*, at produktet rent faktisk er udviklet med henblik på at tjene de nævnte omgåelsesfunktioner.

Ifølge ophl. § 75c, stk. 2, stk. 1, retter forbuddet sig for det første mod produkter, der er genstand for *salgsfremme*, reklame eller markedsføring *med henblik på omgåelse* af effektive tekniske foranstaltninger. Tankegangen er den, at når nogen har taget skridt til at markedsføre en teknisk løsning under fremhævelse af dens evne til at omgå en teknisk anordning, vil det normalt være klart, hvad man har at gøre med. Notoriteten fremtræder i og med markedsføringshandlingen. Gerningsmandens forsæt skal derfor knytte sig til det forhold, at indretningen markedsføres som en sådan løsning.

Ifølge ophl. § 75c, stk. 2, nr. 2, retter forbuddet sig for det andet mod at fremstille, importere, sprede, sælge, udleje, reklamere for salg eller udlejning af eller i kommercielt øjemed besidde indretninger, produkter eller komponenter, der kun i begrænset omfang har *andet* kommercielt formål eller anden kommerciel anvendelse end omgåelse af effektive tekniske foranstaltninger. Dermed indfører bestemmelsen en form for *teknisk notoritet*, der modsvarer den markedsføringsmæssige notoritet, der fremgår af stk. 2, nr. 1.

Endelig forbyder § 75c, stk. 2, nr. 3, fremstilling mv. af indretninger, produkter eller komponenter, der primært er udviklet, produceret, tilpasset eller ydet med henblik på at muliggøre eller befordre omgåelse af effektive tekniske foranstaltninger, jf. nr. 3. Bestemmelsen må antages at have et snævert anvendelsesområde ved siden af de to foregående bestemmelser: Hvor de to foregående bestemmelser retter sig mod en notoritet, der kan konstateres på selve produktet – enten gennem dets markedsføring eller ved dets funktioner – er tankegangen her, at man skal afklare, hvilke formål *udvikleren* havde med at udvikle produktet. I en situation, hvor kravene i medfør af nr. 1-2 ikke er opfyldt, må det antages, at dette bevis vil være endog særdeles vanskeligt at føre.

Tjenesteydelser

Ifølge ophl. § 75c, stk. 3, finder de tre tilfældegrupper, der er omtalt i stk. 2, tillige anvendelse på tjenesteydelser. Gennem denne udvidelse af bestemmelsen har man undgået at skulle tage stilling til det undertiden vanskelige beskrivelsesproblem om grænsen mellem produkter/løsøre og tjenesteydelser, se f.eks. fremstillingen i afsnit 18.3.b og 20.2.b. Bestemmelsen vil i praksis omfatte personer, der tilbyder hjælp ved udførelsen af de handlinger mv., der fører til en handling som nævnt i stk. 1.

9.4.e. Tvangslicens

Ifølge ophl. § 75d kan Ophavsretslicensnævnet pålægge en rettighedshaver at stille nødvendige midler til rådighed for en bruger med lovlig adkomst til et værk, således at brugeren kan drage fordel af nogle af de bestemmelser i ophavsretsloven, som hjemler en specifik udnyttelse af værket. De bestemmelser, der herved er henvist til, er §§ 15 og 16, § 17, stk. 1-3, § 18, stk. 1 og 2, § 21, stk. 1, nr. 2, § 23, stk. 1, og §§ 26-28, 31 og 68. For at kunne gøre brug af denne særlige form for tvangslicens skal rettighedshaveren have undladt "ved frivillige foranstaltninger, herunder aftaler med andre involverede parter" at have sikret, at brugeren uanset anvendelsen af de effektive tekniske foranstaltninger har kunnet drage fordel af de nævnte bestemmelser, jf. stk. 2.

Bestemmelsen i stk. 1 finder ikke anvendelse på værker og andre frembringelser mv., der efter aftale stilles til rådighed for almenheden *on demand*, jf. § 2, stk. 4, nr. 1, 2. led. I disse tilfælde – der typisk vil udfolde sig via Internet-anvendelse under en løbende brug – vil brugerens interesser almindeligvis være tilstrækkeligt værnet gennem aftaleretlige sanktionsmuligheder.

9.4.f. Sikring af rettighedsoplysninger

Ophl. §75e indeholder en bestemmelse, der beskytter de såkaldte ERMS-systemer (*Electronic Rights Management Systems*). Uden tilladelse fra rettighedshaveren er det ikke tilladt at (1) fjerne eller ændre elektroniske oplysninger om rettighedsforvaltning eller (2) foretage eksemplarspredning, import med henblik på eksemplarspredning eller overføring til almenheden af værker og andre frembringelser mv., hvor de elektroniske oplysninger om rettighedsforvaltning er blevet fjernet eller ændret uden samtykke. At man har reguleret disse oplysninger om rettighedsforvaltning skyldes, at oplysningerne er nøglen til den lovlige (herunder *betalte*) brug. Det er uden betydning, hvad det er for viden, der er indeholdt i disse oplysninger, herunder om de identificerer det beskyttede materiale og/eller rettighedshaverne. Der kan også være tale om oplysninger om betingelserne for anvendelse af det beskyttede materiale, numre og koder.

Ifølge bestemmelsens stk. 2 er der indbygget en culpabetingelse i gerningsindholdet. Det er kun den gerningsmand, som *ved eller burde vide*, at de pågældende oplysninger er fjernet med den virkning, at der foranlediges, muliggøres, lettes eller skjules en

krænkelse af retten til et værk eller en anden frembringelse, der er omfattet. I modsætning til andre af de bestemmelser, der findes i kapitel 6a, er det tilstrækkeligt, at gerningsmanden viser uagtsomhed. For at ifalde bødestraf for overtrædelse af bestemmelsen kræves dog forsæt, jf. strfl. § 78, 2. pkt.

9.5. Public domain og open source

9.5.a. Public domain

Det forekommer ofte, at et programværk kan udnyttes helt eller delvis uden ophavsretlige bånd. Med en amerikansk betegnelse hører programmet da til "the public domain" (almenhedens rådesfære). Årsagen hertil kan enten være, at der efter ophavsretlige regler slet ingen ophavsret gælder på det pågældende område, eller at rettighedshaveren af forskellige grunde har valgt ikke at gøre sine rettigheder gældende.

Retlige årsager

Det vil høre til sjældenhederne, at et programværk af retstekniske grunde befinder sig i public domain. Programmer vil ikke falde inden for den særlige undtagelse for offentlige aktstykker, der fremgår af ophl. § 9. Og med den almindelige globale tilslutning til Bernerkonventionen (der forbyder formkrav som betingelse for at opnå ophavsret) er det den praktiske regel, at alle programværker med den fornødne originalitet også beskyttes ophavsretligt. Men en undtagelse kan netop tænkes, hvis et programværk ikke opfylder kravene til originalitet. Dernæst kan det – teoretisk – forekomme, at et programværk er skabt i et land, som ikke beskytter ophavsretten, og som Danmark derfor ikke har indgået gensidighedsoverenskomst med efter den almindelige regel i ophl. § 88. Med den nugældende beskyttelsestid på 70 år efter ophavsmandens dødsår kommer det derimod til at vare en rum tid, før public domain-programmel vil forekomme pga. udløb af ophavstiden. I relation til disse regler har reglerne om public domain dog stor praktisk betydning for så vidt angår den brug af litterære og kunstneriske værker (f.eks. af billedkunst og musik), som ofte inkorporeres i nutidens programværker.

I det omfang en anden immaterialret til programmet (f.eks. et patent eller en brugsmodelret) udspringer af en registrering eller offentlig godkendelse, kan det tænkes, at rettigheden overgår til public domain, hvis den nødvendige registrering ikke opretholdes, f.eks. når et patent eller en halvlederret udløber, eller når det formelle

grundlag for at opretholde denne ret (afgiftsbetaling mv.) ophører. Disse public domain-tilfælde har primært betydning i relationen mellem professionelle program-udviklere – ikke i relation til den enkelte bruger.

Afståelsestilfælde

I det følgende sættes fokus på de mest praktiske tilfælde, hvor der er tale om, at rettighedshaveren helt eller delvis opgiver sin ret til en ophavsretlig retsposition. Situationen kan enten foreligge ved, at rettighedshaveren vælger – nu eller senere – at undlade at opkræve betaling for udnyttelseshandlinger, der ellers falder inden for hans eneret, eller ved at han uden at forbeholde sig betalingskrav stiller krav om, hvorledes programmet skal anvendes.

Udgangspunktet er her, at immaterialrettens regler giver rettighedshaveren fuld frihed til at klausulere sit krav om vederlag, som han vil. I betragtning af dispositionens rækkevidde kræves dog et *utvetydigt* tilsagn om rettens opgivelse fra den beføjede indehaver af de rettigheder, der er tale om at opgive. Det er ikke tilstrækkeligt, at rettighedshaveren blot undlader at opkræve licensafgift, at han gør værket tilgængelig for download på en hjemmeside eller at han undlader at forfølge pirateri. Stilles programmet til rådighed fra en hjemmeside med opfordring for almenheden til at hente det her, er udgangspunktet, at der kun er givet en licens til den enkelte bruger, sml. princippet i ophl. § 53, stk. 2, der udtrykkeligt fastslår, at overdragelse af eksemplarer af et værk ikke indbefatter overdragelse af ophavsretten. Et løfte om overgang til public domain må udtrykkeligt angive denne retsvirkning, eventuelt ved klausuler om, at samtlige rettigheder til et program er opgivet, at programmet ved ophavsmandens beslutning er overgået til public domain eller ved en lignende sprogbrug. Ved at afgive en sådan melding ændrer programmet populært sagt karakter fra at være "payware" (betalingspligtigt) til i en eller anden forstand at være "freeware" (gratis).

Fortolkning

Selv om der foreligger et tilsagn af denne karakter vil rettighedshaveren typisk ikke opgive samtlige rettigheder til sit program, og selv om han skulle ønske dette, følger det af ophl. § 3, at de personlige rettigheder ikke kan opgives, medmindre det gælder en efter art og omfang afgrænset brug af værket. Ligeledes rummer ophl. § 53 en regel om tilbageholdende fortolkning af ophavsretlige overdragelsesdispositioner.

Praktiske tilfælde

I praksis opgives de ophavsretlige retspositioner i visse typiske tilfældegrupper:

- markedsføring

Den ene er, at programmet foreligger i sin første version og endnu ikke er markedsført bredt. Formålet med at give det frit er at skabe almindelig interesse for det. Ved på denne måde at opnå

en bred brugerskare håber producenten at berede markedet for næste version af programmet, som så markedsføres mod betaling. Denne praksis ses hyppigt på markedet for Internet-applikationer. Den web-browser, der fik sit første kommercielle gennembrud, fra firmaet Netscape, blev markedsført på denne vis. I denne situation er det åbenbart, at de rettigheder, der opgives, er snævert afgrænsede til denne første version af programmet, og at brugeren f.eks. ikke opnår en almindelig ret til – hvis dette ellers er praktisk muligt – at videreudvikle det til nye versioner.

- idealisme

Det andet yderpunkt foreligger, når afståelsen af retten til et program bæres af idealistiske motiver. Sådanne motiver kan være mere nærliggende at anlægge, jo mindre kommercielle hensyn, ophavsmanden er motiveret af: Det er lettere at vise uegennytte, når markedet for det værk, der er tale om, er tabt til konkurrerende producenter, eller når man i tillæg til det værk, man nu lægger i public domain, har et bedre værk at tilbyde mod betaling. Det kan dog også tænkes, at beslutningen herom er truffet efter mere rendyrkede idealistiske motiver, jf. herom i afsnit 9.4.b. om *open source*-bevægelsen. I begge disse situationer vil der være en større sandsynlighed for, at brugeren har frie hænder med hensyn til sin anvendelse af programmet.

I tilknytning til public domain-problematikken – men adskilt fra den licensering, der sker i relation til såkaldt open source-programmel (jf. herom straks nedenfor) – er det vigtigt at kende to yderligere begreber:

"Freeware"

Betegnelsen "freeware" anvendes ofte, når programmet er gratis at anskaffe og bruge, idet rettighedshaveren dog fastholder sine grundlæggende rettigheder til det. Brugeren er altså fortsat begrænset i sine udfoldelsesmuligheder vedrørende produktet. Han kan f.eks. ikke videredistribuere det, hverken gratis eller mod betaling, medmindre han opnår licens hertil. Ligeledes forbyder rettighedshaveren ofte, at der sker ændringer i programmet. Ofte har rettighedshaveren fastsat en række betingelser for denne benyttelse, som brugeren forpligter sig til at acceptere i forbindelse med downloadning. Den meget benyttede *Adobe Acrobat*-løsning, der gør det muligt at frembringe dokumentfiler i det meget udbredte grafiske pdf-format, er et eksempel herpå.

Shareware

Et begreb, som navnlig var udbredt i 1980'erne, er shareware. Betegnelsen er ikke retvisende, eftersom shareware-programmel ikke specielt retter sig mod applikationer, der deles mellem flere brugere el.lign. Idéen er derimod, at programmet kan benyttes og distribueres frit og uden betaling i umodificeret form i en periode (f.eks. inden for en prøveperiode af 90 dage), indtil brugeren

bestemmer sig for at bruge det. Når dette sker, skal programmet registreres, og denne registrering vil normalt være forbundet med en betalingspligt. Formålet med den indledende betalingsfrihed er typisk at give brugeren mulighed for en indledende aftestning mv. Udover at rettighedshaveren altså principielt ikke kræver betaling for denne indledende brug, har shareware-konceptet den praktiske side, at rettighedshaveren typisk ikke retsforfølger dem, der – mod intentionerne – undlader at betale for den fortsatte brug.

Betalingskrav

Ved brugen af shareware-programmel opstår spørgsmålet, om brugeren er forpligtet til at erlægge den licensafgift, rettighedshaveren forlanger erlagt, når prøveperioden for programmet er udløbet. Spørgsmålet må besvares med udgangspunkt i den legale programlicens i ophl. § 36, stk. 1, nr. 1, og er for så vidt enkelt: Da det angivne formålskriterium er afgørende, må man se på, hvilke krav brugeren blev præsenteret for ved aftaleindgåelsen. Dette fører utvetydigt til, at der opstår en retlig pligt til enten at ophøre med brugen eller erlægge en betaling som den opkrævede. Den retlige konstruktion, der ligger bag denne pligt, kan rettest beskrives som en kvasiaftale. Se modsat *Wagle & Ødegaard* (1997), s. 258 f., der dog tilføjer, at problemet næppe har den store interesse, da rettighedshaveren ofte vil have sikret sit betalingskrav med en kopispærrefunktion, der træder i funktion, hvis ikke der sker betaling (og efter betaling indtastes en kode el.lign., der tillader fortsat brug).

Bevisspørgsmål

Hvor der, som nærmere anført i afsnit 9.4.b., er ved at udvikle sig en global sædvane for licensering af *open source*-programmel, kan der bestå en høj grad af uklarhed om, hvilket rettighedsmæssigt spillerum der gælder for brugen af programmel, der enten er opgivet som *public domain*, eller som er knyttet til en shareware-licens. Et af problemerne er, at man ikke har kildeteksten (som typisk vil være lukket, dvs. distribueret i objektkode), til at angive de licensvilkår, der skal være gældende. Uden fuld sikkerhed for, at rettighederne er opgivet, kan det være særligt risikabelt at indbygge *public domain*-programmer i programløsninger, der ønskes markedsført på et almindeligt marked. Skulle der opstå en konflikt med en påstået rettighedshaver (som ad teknisk vej typisk vil have let ved at identificere de programkomponenter i det nu "nye" programværk, han gør retskrav gældende for), vil det være udvikleren af det nye program, der har bevisbyrden for, at der er meddelt det fornødne samtykke til denne anvendelse. Men har udvikleren ingen aftale med den part, som påstås at have opgivet sin ophavsret, kan det være vanskeligt at

bevise, hvad det egentlig var for et samtykke, der blev meddelt. Kan dette bevis ikke føres, vil en dokumenteret rettighedshaver tænkes at kunne nedlægge forbud mod brugen af det færdigudviklede program, jf. den almindelige regel om bearbejdninger i ophl. § 4, stk. 1. I praksis har der formet sig forskellige variationer af opgivelsesdispositioner, der beror på, hvilke enerettigheder der opgives, se herom *Andersen & Græbe* (1990), s. 34 ff.

9.5.b. Open source

Begrebsafgrænsning

"*Open source*" betyder åben kildetekst. I daglig tale anvendes udtrykket om programmer, der udbydes således, at brugeren (licenstageren) ikke alene får adgang til den objektkode, der eksekverer programmet, men også til den kildetekst, der skal bruges til at foretage eventuelle tilretninger mv., se hertil redegørelsen i afsnit 3.2.c. Gennem de seneste år har der udviklet sig et fintmasket og effektivt system til distribution af open source-programmel. Denne distribution bygger på en række grundlæggende principper, som i forskellige variationer finder vej til de licensaftaler, der holder systemet sammen.

Historik

Interessen for *open source*-programmel kan føres tilbage til en række enkeltpersoner, der enten har fundet det *uetisk* at arbejde med programmel i *closed source*, eller som har set en mulighed for *effektivisering* af arbejdet med at udvikle software ved at lade kildeteksten være frit tilgængelig. Der findes ikke én samlet *open source*-bevægelse, men forskellige initiativer, der hver fra sit udgangspunkt har medvirket til at skabe den interesse for området og den praktiske udbredelse af open source-programmel, der findes i dag.

- Free Software Foundation

Et første skridt i denne retning var etableringen af den amerikansk baserede organisation Free Software Foundation. Initiativtageren var *Richard Stallman*, der under sin forskning på MIT's AI Laboratory havde fundet det uetisk at medvirke til hemmeligholdelsen af den kreativitet, der udfolder sig under programudvikling, ved kun at distribuere programmel i objektkode. Han valgte derfor at forlade tjenesten ved MIT for i stedet at hellige sig arbejdet med at udvikle disse nye programmer. De principper, der ligger til grund for arbejdet i Free Software Foundation, har siden fundet vej til de licenser, der i dag ligger til grund for distribution af *open source*-programmel, jf. herom senere.

- Linux

Det var imidlertid først, da *Linus Torvalds* valgte at underlægge den Linux-kerne, han havde medvirket til at udvikle, under en GNU General Public License (GPL), at open source-bevægelsen

for alvor fik vind i sejlene, se nærmere herom *Mikael Pawlo* i L&D no. 65, marts 2001, s. 13 ff. I kraft af denne disposition gjorde Torvalds ikke alene sin kerne til genstand for fri anvendelighed; han opdaterede den med korte mellemrum og indarbejdede i den forbindelse de kommentarer, der var indkommet i mellemtiden. Derfor spiller open source-distribution navnlig en rolle inden for de applikationer, der knytter sig til styresystemet Linux. I dag har Linux-kernen i kraft af den tilknyttede GPL-licens opnået stor udbredelse, ligesom der findes et væld af særdeles velkørende applikationer inden for de væsentligste områder af den moderne IT-anvendelse, der bygger på *open source*.

Flere forhold i de seneste års IT-udvikling har medvirket til at understøtte brugen af sådanne løsninger. For det første har Internettets udbredelse gjort det praktisk muligt at gennemføre det intense, globale samarbejde om programudvikling og -vedligeholdelse, som har været en drivende kraft bag udviklingen af nutidens *open source*-applikationer. En anden væsentlig faktor er den dominans, den amerikanske programleverandør *Microsoft* har haft på markedet for standardprogrammel og styresystemer – en dominans, der som nævnt s. 154, har vanskeliggjort konkurrencen på disse markeder, men som trues af en forretningsmodel, der slet ikke bygger på licensbetaling. Ønsket om at opnå et alternativ til Microsofts løsninger har fået yderligere næring ved de vanskeligheder, der ofte har været omkring disse programmers driftssikkerhed. Alternative programløsninger, der gør det muligt for brugerne – eller for aktive inden for det open source-miljø, der findes for den pågældende løsning – at rette opståede fejl, vil ofte føre til langt sikrere, og i tillæg hertil også billigere, programløsninger. Hertil kommer den fleksibilitet, der ofte vil følge af muligheden for selv at kunne tilpasse kildeteksten.

- the Open Source Initiative

Et andet væsentligt skridt i udviklingen af den moderne open source-bevægelse er etableringen i 1998 af The Open Source Initiative (OSI). Initiativtageren var *Eric Raymond*, der bl.a. i sin bog "The Cathedral and the Bazaar" (se <www.catb.org>) havde argumenteret for, at *open source*-bevægelsen burde orientere sig bort fra sine følelsesladede og ideologiske begrundelser. Raymond fremhævede den effektiviseringsgevinst, der ligger i den "bazar"-prægede programudvikling, der kan betragtes som en form for *agil* programudvikling, se hertil s. 152: Hver enkelt deltager med sin lille bod til at løse de behov, markedet efterspørger, som modsætning til den tankegang, der ligger til grund for kommercielle *closed source*-løsninger, hvor programmet bygges op som en stor "katedral", hvor hver programmør står under

samme tag, og hvor det færdige resultat lægges frem for markedet som en enhed. OSI blev skabt som en platform til markedsføring af denne tankegang, bl.a. ved fremlæggelse af et antal "officielle" open source-definitioner mv. OSI forestår i den forbindelse en vis certificeringsvirksomhed, idet et program kan markedsføres som "OSI Certified Open Source Software", hvis det opfylder de hovedkrav, OSI stiller herfor, se hertil <www.opensource.org>.

Talrige andre open source-licenser end de her anførte kan nævnes, f.eks. the Berkely Software Distribution License, the MIT Public License, the Mozilla Public License, og the Apache License. Se herved *Välimäki* (2005), s. 152 ff. For en nærmere redegørelse over det udviklingsforløb, der har ført til den moderne open source-bevægelse, henvises til *Mikko Välimäki*: The Rise of Open Source Licensing – A Challenge to the Use of Intellectual Property in the Software Industry (Turre Publishing, 2005)

- Monetized Open Source

I dag er det de store kommercielle virksomheder, der udgør de stærkeste kræfter inden for open source-bevægelsen. Som nærmere uddybet hos *Ieuan G. Mahony & Edward J. Naughton* i 19 CLAB 87 ff. (2004), har en række af de store IT-virksomheder i dag valgt at markedsføre open source-løsninger inden for områder, hvor en sådan (licensfri) dækning af brugernes behov må anses for mest generende for konkurrerende virksomheder, der tilbyder betalbare closed source-applikationer.

Forretningsgrundlaget

Det grundlæggende princip i en *open source*-licens er, at rettighedshaveren tillader sine licenstagere at benytte programmet frit til gengæld for at licenstageren lover også at lade *sine* efterfølgende licenstagere opnå tilsvarende rettigheder over deres bearbejdninger af det licenserede programmel. Man kan med en vis ret spørge, hvordan open source-udviklere da overhovedet er i stand til at finansiere deres udviklingsfaciliteter, når de dermed giver afkald på vederlag ved eksemplarfremstilling mv. Svaret på dette spørgsmål rummer flere forklaringer.

For det første er det en kendsgerning, at en række af de personer, der har deltaget i udviklingen af open source-programmel, har været motiveret af uegennytte, f.eks. ønsket om at bidrage til et fællesskab, at sætte sig sine spor eller at glædes ved samarbejdet med andre kyndige. Mange open source-udviklere er særdeles kyndige programmører, der deltager i disse communities i fritiden og udvikler deres personlige netværk herom. Bl.a. derfor spiller det også en stor rolle for licenseringen af open source-programmel, at den enkelte udvikler krediteres behørigt i kildeteksten.

For det andet indebærer fravalget af en licensbetaling ikke et fravalg af andre former for betaling. Ved overdragelse af *monetized open source*-programmel vil leverandøren typisk også overdrage betalbare ydelser i form af closed source-programmel eller hardwarekomponenter. Hertil kommer den rent konkurrencemæssige fordel ved at ramme konkurrenter, der befinder sig på markedet med betalbare løsninger. Også den mindre programudvikler vil kunne sælge tilgrænsende tjenester, f.eks. i forbindelse med vedligeholdelse, tilpasning, installation og undervisning, ligesom virksomheden – alt efter løsningens karakter – vil kunne skabe en forretning ved at indestå for bestemte funktioners tilstedeværelse i det leverede programmel.

Et spørgsmål, der i en forbindelse kan give anledning til betydelig tvivl, angår forholdet mellem den brug af et *open source*-program, der er tilladt, fordi licenstageren undlader at kræve betaling for brugen, og den brug, der er forbudt, fordi licenstageren kræver betaling for en brug af et tilgrænsende program, der under driften kalder *open source*-programmet. Se hertil *Emil Paldam Folker* i NIR 2005.165 ff. (s. 175 ff.). Spørgsmålet diskuteres indgående i de nyhedsgrupper, der beskæftiger sig med open source-licensering.

At distribuere programmel under en open source-licens indebærer *ikke*, at programmet lægges i *public domain*, selv om begrundelsen herfor (hvad enten denne er etisk eller strategisk) *kan* være sammenfaldende med den, der leder rettighedshaveren til at opgive samtlige rettigheder til sit program. Licenstagerens ret til at benytte *open source*-programmet knytter sig netop til en licensaftale. I den såkaldte GNU General Public License (GPL) pointeres det, at "free" skal forstås i betydningen "ubundet af retlige bånd", og ikke i betydningen "gratis": Vilkårene giver brugeren ret til fri anvendelse af programmet til selvvalgte formål, fri ret til at undersøge programmet, frihed til at kopiere programmet samt sprede kopier af det til tredjeparter – med eller uden betaling – samt frihed til at forbedre programmet og kopiere og sprede eksemplarer af det forbedrede program.

GNU General Public License

En af de mest udbredte licenser for distribution af open source-programmel er den af Free Software Foundation fastsatte GNU General Public License, ofte forkortet GPL, se <www.gnu.org/copyleft/gpl.html>. Som før nævnt bygger denne licens på et princip om, at brugeren sikres ret til frit at kopiere og redistribuere programmet: Til gengæld for at opnå ret til at benytte den åbne software, underlægger han sig en pligt til at lade sine forbedrin-

ger til softwaren underlægge en tilsvarende fri benyttelse. Man har ligeledes pligt til at sikre den oprindelige ophavspersons integritet: Udvikles der et afledet værk, må dette således navngives anderledes end det oprindelige værk. Ligeledes er der forbud mod diskriminerende markedsopdelinger, hvorefter en softwarebearbejdning alene kan benyttes inden for bestemte brancher eller vidensområder.

- selve licensen

I overensstemmelse med almindelig praksis inden for programlicensering er GNU-GPL inddelt efter de forskellige udnyttelsesformer, der tilstås brugeren. I pkt. 1 gives der licens til kopiering af programmet i den licenserede form. Pkt. 2 giver ret til bearbejdning og videreudvikling. Og pkt. 3 giver ret til at kopiere og distribuere det videreudviklede program. Er en handling ikke legitimeret gennem en af disse licenser, følger det af pkt. 4, at den er forbudt. Sanktioner i anledning af en sådan krænkelse kan dog ikke gøres gældende mod en slutbruger, der selv efterkommer licenskravene.

- kreditering

Som betingelse for de licenser, der tilstås i henhold GNU-GPL, skal licenstageren sikre navngivning af den oprindelige rettighedshaver (udvikler). Navngivningen tjener dels til at sikre udvikleren den anerkendelse, som er en væsentlig motiverende kraft for udviklingen af *open source*-programmel, dels giver den brugeren mulighed for at rette henvendelse til den pågældende, hvis der skulle opstå ønske om at opnå en videregående licensret, herunder licens til at opkræve anden betaling end den, der er hjemlet ved vilkårene.

- betaling, sanktioner

Efter GNU-GPL kan den, der distribuerer programmel, alene oppebære betaling til dækning for "the physical act of transferring a copy" eller for løftet om "warranty protection". Krænkes denne pligt, eller andre af de pligter, der følger af GNU-GPL, mistes licensen og de eksemplarer mv., der udføres over programmet må derfor anses for uhjemlede.

9.5.c. Creative Commons

Begrebet

Creative Commons er en organisation, der er stiftet af en række universitetsfolk, bl.a. den amerikanske juraprofessor *Lawrence Lessig* i 2001 med det formål at skabe en standard for, hvilke licenser rettighedshavere, der ønsker at lægge værker ud på nettet, giver andre til at benytte disse værker. Creative Commonsfortalerne hævder, at de aftaleordninger, som opnås gennem CC-licenser, reducerer den uforholdsmæssigt langvarige ophavsbe-

skyttelse, der følger af gældende lovgivning. Sådanne spørgsmål opstår navnlig ved brugen af nyhedsgrupper og weblogs, og når videnskabelige artikler og undervisningsmateriale stilles til rådighed fra hjemmesider. I mangel af klart fastsatte vilkår kan der her opstå tvivl om, hvilke rettigheder, ophavsmanden har overdraget, henholdsvis opgivet, sml. herved for dansk ret *Lars Stoltze*: Internet Ret (2001), s. 43 ff. Se nærmere om fænomenet, *Välimäki* (2005), s. 154 ff. samt hjemmesiden <www.creativecommons.org>.

Varianter

Første version af CC-licenserne blev udgivet den 16. december 2002. Siden er der sket ændringer, og fænomenet må formodes at udvikle sig fremover. CC-licenserne foreligger i forskellige formater, henholdsvis henvendt til ikke-jurister (med fokus på almindelig, brugervenlig oplysning), til jurister og til maskinlæsbar registrering. Hver enkelt licens har forskellige retsvirkninger og er forsynet med et grafisk symbol, som ledsager licensen. Symbolet fremtræder i en cirkel, der svarer til den, der anvendes til markering af en copyright-notits (©). Organisationen *Creative Commons* arbejder dels med vedligeholdelsen af disse licenser, dels danner den rammerne for særlige delforeninger, der arbejder med disse licensløsninger inden for bestemte samfundsområder (f.eks. science, se http://sciencecommons.org).

De brugervenlige versioner af licenserne lyder som følger: *Attribution:* You let others copy, distribute, display, and perform your copyrighted work – and derivative works based upon it – but only if they give you credit. *Noncommercial:* You let others copy, distribute, display, and perform your work – and derivative works based upon it – but for non-commercial purposes only. *No Derivative Works:* You let others copy, distribute, display, and perform only verbatim copies of your work, not derivative works based upon it. *Share alike:* You allow others to distribute derivative works only under a license identical to the license that governs your work.

Selv om CC-licenserne er konciperet på baggrund af amerikansk ret og amerikansk juridisk terminologi, har bevægelsen oplevet en betydelig international bevågenhed, også i Danmark. Medvirkende hertil er dels den sympati, der ofte hersker om den rettighedshaver, der på forhånd er indstillet på at fravige velerhvervede retspositioner. En anden faktor er det rent tekniske forhold, at visse søgemaskiner kan begrænse søgninger efter information (og værker), der på forhånd er genstand for en CC-licens.

Hvor sympatisk Creative Commons kan forekomme inden for områder, hvor der i forvejen hersker en almindelig forventning om, at værker genbruges og kopieres uden betaling til ophavs-

manden, kan en CC-løsning vise sig problematisk på områder, hvor der normalt hersker betalingsforventninger, f.eks. på musikområdet. Den kunstner, der vælger at lade sine musikindspilninger stille til rådighed på nettet på grundlag af en (uigenkaldelig) cc-licens, kan efter omstændighederne miste det vederlag for benyttelsen, som f.eks. ville tilfalde ham i medfør af kollektive licensordninger, der dækker Internet-benyttelse. Derfor har bevægelsen givet anledning til forståelig skepsis blandt rettighedshaverrepræsentanter, der frygter, at den vil underminere respekten for den ophavsretlige beskyttelse.

9.6. Pligtaflevering

9.6.a. Oversigt

Formål

Ved lov nr. 1439 af 22. december 2004 er der pålagt pligtaflevering af en række forskellige værker, der udgives i Danmark. Loven suppleres med en bekendtgørelse om pligtaflevering af udgivne værker, nr. 636 af 13. juni 2005. Yderligere vejledning om det ikke helt ukomplicerede regelsæt kan i øvrigt hentes fra <www.pligtaflevering.dk>.

Som det gælder for den tidligere lovgivning herom (der går helt tilbage til 1697) er lovens formål at sikre, at den litterære arv kan føres videre til kommende generationer. Loven afløser en lignende lov fra 1997, der blev fremsat på grundlag af forslaget fra Udvalget om Bibliotekerne i Informationssamfundet i Betænkning om Pligtaflevering (juni 1995). Den nye lov har grundlag i et udvalgsarbejde, der i 2003 førte til en Udredning om bevaring af Kulturarven. Med de to seneste love sikres det, at også materiale, der udgives på digitale medier mv., indsamles. Derfor knytter der sig en betydelig interesse til at få fastslået lovens rækkevidde i relation til digitale frembringelser. Med den nye lov er der taget yderligere højde for den tekniske udvikling, bl.a. ved indførelse af et særligt kapitel 3 om materiale, der offentliggøres i elektroniske kommunikationsnet.

9.6.b. Almindelige regler

Udgangspunktet

Ifølge lovens § 1 omfatter loven såvel ophavsretlige værker som andre frembringelser, nemlig nærmere bestemt følgende:

1) værker, som offentliggøres ved udgivelse i eksemplarform, jf. kapitel 2,
2) materiale, som offentliggøres i elektroniske kommunikationsnet, jf. kapitel 3,
3) radio- og fjernsynsprogrammer, jf. kapitel 4, og
4) film, som er produceret med henblik på offentlig forevisning, jf. kapitel 5.

Loven indfører dermed en sondring mellem "værker" og andet afleveringspligtigt materiale.

Om værker bestemmer § 2, at der *ved udgivelse* skal afleveres to eksemplarer til en pligtafleveringsinstitution, som udpeges af kulturministeren, jf. lovens § 20 (i praksis Det Kongelige Bibliotek i København og Statsbiblioteket i Århus). Loven opererer med et udgivelsesbegreb, der svarer til det ophavsretlige, jf. § 2, stk. 2. Værker anses dog for udgivne, når der med ophavsmandens samtykke tilgår almenheden meddelelse om, at eksemplarer af værket fremstilles og distribueres på bestilling. Dermed er også *print on demand*-udgivelser omfattet af afleveringspligten.

Pligtens opfyldelse

Afleveringspligten påhviler den, der fremstiller færdige eksemplarer til udgivelse, jf. § 4, stk. 1. Kan fremstilleren ikke entydigt identificeres, påhviler afleveringspligten efter påkrav fra pligtafleveringsinstitutionen udgiveren, jf. stk. 2. Udgifterne til eksemplarfremstilling af de pligtafleverede eksemplarer afholdes af udgiveren, jf. § 7, stk. 1. Når det gælder eksemplarer, der er fremstillet i udlandet, afholdes de tilsvarende udgifter af den afleveringspligtige efter § 4, stk. 3.

Som udgangspunkt efterkommes afleveringspligten ved, at værket afleveres i den form, hvori det udgives, jf. lovens § 3, stk. 1. Dette giver ikke anledning til problemer, når værket udgives i klassisk form, f.eks. som bog eller musik-CD. Men hvis tilegnelsen af værkets informationsindhold kræver brug af særligt udstyr, må der tages særlige skridt for at give afleveringspligten reelt indhold. Kan et værk kun anvendes ved brug af teknisk udstyr, skal de afleverede værker efter påkrav fra pligtafleveringsinstitutionen ledsages af adgangskoder og andre oplysninger mv., der er nødvendige for at få adgang til værket, fremstille eksemplarer af værket og gøre værket tilgængeligt for almenheden, jf. § 3, stk. 2.

Den afleveringspligtige kan kræve, at adgangskoder og lign. ikke meddeles udenforstående. På tv-området skal Statens Mediesamling have adgang til de nødvendige dekoderkort for at kunne modtage og optage programmer, som udsendes i krypteret form, og som mediesamlingen skal optage i henhold til de regler, der er fastsat i medfør af § 13, stk. 3, jf. nærmere pligtafleveringsbekendtgørelsens §§ 13-16

Høstning

En væsentlig del af pligtafleveringsinstitutionernes arbejde med at sikre materiale fra den danske del af internettet består af såkaldt høstning. Herved forstås en delvis automatiseret proces, hvorved materiale nedtages fra hjemmesider på internettet, se herved bekendtgørelsens § 9, stk. 3. Selve indsamlingen sker efter et såkaldt "høsterprogram", som arbejder på grundlag af en liste over internetadresser, der anses for at være danske. For hver adresse i denne liste henter programmet den første side og gemmer den. Høsteren undersøger dernæst, om der på siden er links til andre sider. Linkes der hen på andre "danske" internetadresser, hentes disse også af programmet. Dermed simulerer programmet en bruger, der med sin browser klikker på alle danske links og gemmer de valgte sider. De pågældende – betydelige – datamængder gemmes både på Det Kongelige Bibliotek og i Statsbiblioteket, idet det løbende kontrolleres, at data de to steder er identiske. Registranten af internetdomænet kan sikre ikke-offentliggjort materiale mod automatisk høstning ved brug af adgangskoder, jf. bekendtgørelsens § 9, stk. 3. Pligtafleveringsinstitutionerne må ikke videregive oplysninger om adgangskoder og lignende til uvedkommende, jf. stk. 4.

Der anvendes flere former for høstning og gerne i kombinationer. Pligtafleveringsinstitutionerne har på forhånd udvalgt et antal hjemmesider, hvorfra der målrettet høstes materiale, f.eks. hjemmesider for større danske medier. I forbindelse med udvalgte begivenheder foretages dernæst en *begivenhedsorienteret høstning*, hvorved også udenlandske mediers dækning af en dansk begivenhed hentes ned. Dette sker typisk 3 gange årligt, for eksempel i forbindelse med et valg eller et kongeligt bryllup. *Selektiv høstning* indebærer, at der hentes materiale fra en række væsentlige web-steder, hvis informationsindhold ændres dagligt.

9.6.c. Edb-programmer

Edb-programmer skal ikke afleveres, medmindre programmet udgør en del af et værk af en anden art og udgives sammen med dette, jf. § 2, stk. 4. Dermed lægger pligtafleveringsloven sig op

af samme definition som den, der er afgørende for, om der indtræder ophavsretlig konsumption vedrørende eneretten til udlån af et edb-program, jf. ophl. § 19, stk. 3, andet pkt.

9.6.d. Materiale i elektroniske kommunikationsnet

Med § 8 i pligtafleveringsloven er det bestemt, at også dansk materiale, som offentliggøres i elektroniske kommunikationsnet, er afleveringspligtigt. Materiale, som offentliggøres i elektroniske kommunikationsnet, anses som dansk, når det offentliggøres fra internetdomæner og lign., der særligt er tildelt Danmark (i praksis .dk-domænet) eller det offentliggøres fra andre internetdomæner og lign. og er rettet mod et publikum i Danmark, f.eks. fordi der anvendes dansk sprog. Ifølge lovens § 8, stk. 3, kan kulturministeren fastsætte nærmere bestemmelser om afgrænsningen af afleveringspligten efter stk. 1 og 2.

Afleveringspligten af dette elektroniske materiale opfyldes ved, at pligtafleveringsinstitutionen har adgang til at rekvirere eller fremstille eksemplarer af materialet. Modsat tidligere lovgivning er der således ikke længere pligt til at give pligtafleveringsinstitutionen (som vil være et netarkiv etableret i samarbejde mellem Det Kongelige Bibliotek og Statsbiblioteket i Aarhus) meddelelse om hjemmesider. I stedet indfører loven en række regler, der sikrer, at kulturbærende elektroniske udgivelser sikres for eftertiden.

For så vidt angår materiale, der offentliggøres fra internetdomæner og lign., der særligt er tildelt Danmark, er den afleveringspligtige *registranten* af det domænenavn, hvorunder materialet offentliggøres, jf. § 9, stk. 1. For så vidt angår materiale, der offentliggøres fra andre internetdomæner og lign., er den afleveringspligtige udgiveren af materialet, dvs. den for hvis regning materialet udgives, jf. lovens § 17. Ligesom det gælder for fysiske værker skal den afleveringspligtige efter påkrav give pligtafleveringsinstitutionen meddelelse om de adgangskoder og andre oplysninger mv., der er nødvendige for at få adgang til materialet, fremstille eksemplarer af materialet og gøre materialet tilgængeligt for almenheden, jf. § 10. Den afleveringspligtige kan kræve, at adgangskoder og lignende ikke meddeles udenforstående. Udgifter i forbindelse med at rekvirere eller fremstille eksemplarer af materialet afholdes af pligtafleveringsinstitutionen, jf. § 12.

Supplerende litteratur

For henvisninger til litteraturens behandling af den ophavsretlige beskyttelse af edb-programmel henvises til litteraturlisten i slutningen af kapitel 6.

Reglerne om den ophavsretlige regulering af brugerens rettigheder med henblik på at sikre programmers interoperabilitet mv. er behandlet af *Thomas C. Vinje* i NIR 1992.74 ff. og at *Thomas Riis* (2001), s. 55 ff.

En god gennemgang af de problemer, der opstår i forbindelse med brugen af *open source*, findes hos *Emil Paldam Folker* i NIR 2005.165 ff. Spørgsmålet er i øvrigt genstand for en finsk doktorafhandling, se *Mikko Välimäki*: The Rise of Open Source Licensing – A Challenge to the Use of Intellectual Property in the Software Industry (Turre Publishing, 2005).

Kapitel 10. INDUSTRIEL RETSBESKYTTELSE

10.1. Patentbeskyttelse

10.1.a. Oversigt

Retsfaktum

Et patent er en industriel tidsbegrænset eneret til en opfindelse, der opnås på grundlag af en ansøgningsprocedure. Denne procedure indebærer en prøvelse af, om de i patentloven angivne patentbetingelser er opfyldte. Grundbetingelsen er, at ansøgeren – eller en part, fra hvem han erhverver sin ret – har gjort en *opfindelse*, som kan udnyttes industrielt, f.eks. som et produkt, der frembringes med henblik på markedsføring eller som en procedure, der indbygges i en produktionsproces. Herudover kræves, at opfindelsen adskiller sig væsentligt fra, hvad der tidligere har været kendt (såkaldt *opfindelseshøjde*). Endelig kræves det, at kendskabet til opfindelsen ikke allerede er udbredt (såkaldt *nyhed*), se nærmere PL § 2.

Foruden disse materielle patentbetingelser prøves det under ansøgningsproceduren, om opfindelsen opfylder visse krav af formel karakter. Beslutter patentmyndigheden, at dette er tilfældet, offentliggøres ansøgningen, og efter en bestemt indsigelsesperiode udstedes patentet. Også udstedelsen er forbundet med en offentliggørelse. Offentliggørelsen giver tredjemand mulighed for at gøre indsigelse mod patentet, hvorved kampen herom kan – men ikke nødvendigvis skal – udkæmpes, før retten skal stå sin prøve i en håndhævelsessag. Samtidig kan offentliggørelsen ses som den "pris", patenthaveren betaler for sin tidsbegrænsede eneret: Han afgiver den viden, patentet repræsenterer, men som han alternativt kunne have beholdt som erhvervshemmelighed, til samfundet. Når patentet udløber – eller hvis ansøgeren senere frafalder patentafgiften eller undlader at betale årsafgifter – kan alle frit udnytte opfindelsen. Indtil da etablerer patentretten et tidsbegrænset monopol.

Patentretten anses som retssystemets stærkeste eneret på grund af dens høje abstraktionsniveau: Alt efter patentkravenes

udformning beskyttes den pågældende teknologi, uanset hvordan den konkret implementeres. Til forskel herfra beskytter ophavsretsloven kun edb-programmet i dets *konkrete* udformning. Den bagvedliggende idé mv. må i givet fald beskyttes ad anden vej.

Patentproceduren

Den ansøgningsprocedure (patentproceduren), der ligger forud for patentudstedelsen, tager udgangspunkt i, at der indleveres en ansøgning, der beskriver den opfindelse, patentet dækker, se PL § 8, stk. 2, og §§ 19 ff. og i det hele bekendtgørelse nr. 6 af 6. januar 2003 om patenter og supplerende beskyttelsescertifikater. Ansøgningens beskrivelse af den opfindelse, der ønskes patenteret, skal være så tydelig, at en fagmand på grundlag deraf kan udøve opfindelsen.

Om patentproceduren henvises i øvrigt til de almindelige fremstillinger, se navnlig *Koktvedgaard*: Lærebog i immaterialret (2005), s. 199 ff.

Nyhedskravet

For at en opfindelse skal kunne patenteres, kræves det efter PL § 2, stk. 1, at opfindelsen er ny i forhold til, hvad der var kendt før patentansøgningens indleveringsdag, og at den tillige adskiller sig væsentligt derfra. Som kendt anses alt, hvad der er blevet almindelig tilgængeligt gennem skrift, foredrag, udnyttelse eller på anden måde, § 2, stk. 2. Nyhedskravet er absolut og globalt. Uanset hvor i verden opfindelsen er publiceret, uanset det anvendte sprog og uanset publiceringsformen vil den være "nyhedsskadelig" i relation til et dansk patent, hvis publikationen har fundet sted inden ansøgningstidspunktet.

Nyhedskravet giver anledning til praktiske problemer i relation til de nyheder, der måtte være indeholdt i kildeteksten til et edb-program, der er skrevet og offentliggjort, før en opfindelse gøres. Er en sådan kildetekst ikke stillet til markedets benyttelse (f.eks. fordi den foreligger i *closed source*), opstår spørgsmålet om nyhed ikke, eftersom en sådan kode netop ikke er læsbar for andre. Men er kildeteksten givet ud til almenheden, f.eks. fordi programmet er markedsført som *open source*-programmel, kan man overveje, om der hermed er offentliggjort "nyhedsskadelig" viden i relation til senere opfindelser.

Spørgsmålet berøres i EPO's Guidelines for Examination in the European Patent Office fra 2003 (tilgængelige fra <www.european-patent-office.org>), Part C, afsnit 4.14a. Ifølge denne bestemmelse er det et krav, at den beskrivelse, der i givet fald fremholdes som nyhedsskadelig, er "written substantially in normal language, possibly accompanied by flow diagrams or other aids to understanding". Ifølge denne fortolkning – hvis holdbarhed ikke ses prøvet i retspraksis – vil end ikke offentliggjort kildetekst, der

ikke ledsages med en tilsvarende forklaring, kunne være nyhedsskadelig. Holdbarheden af denne antagelse må anses for tvivlsom. I praksis vil konstateringen af, om der foreligger *nyhed*, i disse tilfælde umærkeligt glide over i vurderingen af, om opfindelsen har opfindelseshøjde. Således vil en indsigelse om, at en opfindelse savner *opfindelseshøjde*, ofte kunne underbygges med henvisning til, at den allerede har været praktiseret i eksisterende, kendt kildetekst.

Industriel anvendelse

En anden betingelse for patentering er, at opfindelsen kan udnyttes industrielt, jf. PL § 1, stk. 1. Dette krav volder ikke praktiske vanskeligheder på IT-området. Tekniske løsninger mv. til spil anses f.eks. for at besidde den fornødne industrielle anvendelighed.

Opfindelseshøjde

For det tredje stilles der et krav om opfindelseshøjde, § 2, stk. 1, der kræver, at opfindelsen "adskiller sig væsentligt" fra, hvad der hidtil har været kendt. I praksis håndteres dette krav gennem en sammenligning med en hypotetisk opfinder udstyret med en gennemsnitlig faglig viden, jf. nærmere *Koktvedgaard* (2005), s. 250 ff. Der er forbløffende få domme om dette krav, som med udvidelsen af det patenterbares område (herunder i relation til edb-programmer) må formodes at få stadigt større selvstændig retlig betydning. I EPO's Guidelines knyttes kravet om opfindelseshøjde til, om opfindelsen er "*not obvious*" for fagmanden. Dette krav uddybes i pkt. 9.4 som en viden, "which does not go beyond the normal progress of technology but merely follows plainly or logically from the prior art, i.e. something which does not involve the exercise of any skill or ability beyond that to be expected of the person skilled in the art." Der angives herved ganske beskedne krav, der i mange tilfælde vil kunne gøre enhver fagmand, der blot gør sig en lille smule umage for at optimere en løsning på f.eks. et programmeringsproblem, til opfinder i patentlovens forstand.

I konsekvens af den retsudvikling, der er beskrevet i afsnit 10.1.d., har der gennem de seneste år udviklet sig en praksis i IT-branchen, hvorefter man – hvis man har økonomisk mulighed derfor – søger patenter på programrelaterede opfindelser. Forklaringen herpå er enkel: I ethvert udviklingsprojekt består der en risiko for, at der foreligger et for udvikleren ukendt patent, som er til hinder for at udnytte det udviklede program kommercielt. Denne risiko kan minimeres, hvis man dækker sig af med egne patenter, dels fordi man herigennem vil være tvunget til at foretage en nyhedsundersøgelse, dels fordi der med patentet i hånden er noget at "handle med", hvis et patentkrav gøres gældende

udefra. I konsekvens heraf er den samlede patenteringsaktivitet eksploderet. At man søger så mange patenter på IT-området er navnlig forståeligt, når ansøgeren er en virksomhed med eksterne investorer, for hvem det er afgørende, at de fornødne immaterialrettigheder er sikret. Men udviklingen har gjort patentsystemet til en problematisk og omkostningskrævende faktor i moderne IT, som man vanskeligt kan sige bidrager til den innovative udvikling – snarere det modsatte.

På nuværende tidspunkt er der ingen sikkerhed for, om de mange patenter, der udstedes på programrelaterede opfindelser, overhovedet opfylder kravet om opfindelseshøjde. Spørgsmål herom, og om adgangen til i almindelighed på at patentere programrelaterede opfindelser, har ikke for nylig været påkendt ved øverste retsinstanser i jurisdiktioner som f.eks. UK, Frankrig, Tyskland og USA. Den voldsomme debat, der har udfoldet sig om Kommissionens 2002-forslag til et direktiv om computer-implementerede opfindelsers patenterbarhed antyder, at en retlig stillingtagen hertil på grundlag af gældende ret bliver tilsvarende problematisk givet det forbud mod patentering af edb-programmer, der fortsat står indskrevet i den Europæiske Patentkonvention, jf. nærmere afsnit 10.1.d. Retsstillingen netop i henseende til dette aspekt af patentbeskyttelsen må derfor i enhver henseende siges at være uafklaret.

Undtagelser?

På IT-området har det herudover stor praktisk betydning, at PL § 1, stk. 2-4, fastslår en række tilfælde, hvor der ikke kan meddeles patent, selv om de øvrige betingelser i loven er opfyldte. Bestemmelsen indebærer bl.a., at der ikke kan meddeles patent på "opdagelser, videnskabelige teorier og matematiske metoder" (nr. 1), "planer, regler eller metoder for intellektuel virksomhed, for spil eller for erhvervsvirksomhed og programmer for datamaskiner" (nr. 3) samt "fremlæggelse af information" (nr. 4).

Baggrunden for disse undtagelsesregler må søges i den historiske udvikling i amerikansk patentpraksis, der er beskrevet i afsnit 10.1.b. Når man anskuer dem i en kommunikationsteoretisk ramme kan man imidlertid fremhæve, at de alle drejer sig om tilfælde, hvor en frembringelse alene består i benyttelse af *information* som sådan, f.eks. i forbindelse med almindelig åndelig kundskabserhvervelse eller i forbindelse med tilrettelæggelsen af sociale aktiviteter eller handleformer. Ved patentlovens givelse fremstod alle disse undtagelser som relativt ukontroversielle. For det første var de almindeligvis knyttet til ikke-teknologiske og ikke-industrielle aktiviteter. For det andet var der ingen industri, der gjorde sig gældende med krav om en eneretsbekyttelse. Men

den efterfølgende samfundsudvikling på IT-området har sat flere af dem under pres, herunder – i historisk-kronologisk rækkefølge – udelukkelsen af matematiske metoder (algoritmer), programmer for datamaskiner og senest planer eller metoder for erhvervsvirksomhed.

Retsfølge

Patenter udtrykkes i patentskrifter. I patentskriftet udtrykkes omfanget af selve eneretten i et eller flere patentkrav. De enkelte patentkrav vil hver for sig kunne tænkes at dække henholdsvis produkter, fremgangsmåder, anvendelser eller kombinationer heraf. Da patentkravene læses meget bogstaveligt, er sprogbrugen ofte ganske kompliceret og "firkantet". Med patentskriftet i hånden kan patenthaveren forbyde andre at udnytte opfindelsen. Indholdet af denne forbudsret beror på, om patentet dækker et produkt, en fremgangsmåde eller en anvendelse.

Produktpatent

Produktpatentet giver indehaveren eneret til at fremstille, udbyde, bringe i omsætning eller anvende et produkt, der er genstand for patent, eller importere eller besidde produkter med sådant formål, se PL § 3, stk. 1, nr. 1. Sådanne patenter kan først og fremmest tænkes i relation til enkelte teknologiske komponenter, f.eks. processorer, lagerenheder, halvlederteknologi, bus-teknologier o.m.a.

Procespatenter

Procespatenter, også kaldet fremgangsmådepatenter, giver eneret til "at anvende en fremgangsmåde, der er genstand for patent, eller udbyde den til anvendelse her i landet, såfremt den, der udbyder fremgangsmåden, ved, eller omstændighederne gør det åbenbart, at fremgangsmåden ikke må anvendes uden patenthaverens samtykke". Sådanne patenter kan navnlig tænkes i relation til den procedure, der implementeres ved en softwareløsning. Et fremgangsmådepatent vil ikke alene kunne dække en industriel produktionsmetode, der understøttes af IT, men også særlige matematiske fremgangsmåder (algoritmer), der f.eks. kan anvendes som grundlag for kryptering eller komprimering i en IT-applikation. Beskyttelsen for fremgangsmådepatenter omfatter også en eneret til at "udbyde, bringe i omsætning eller anvende et produkt, som er fremstillet ved en fremgangsmåde, der er genstand for patent, eller importere eller besidde produktet med sådant formål", såkaldt indirekte produktbeskyttelse.

Et eksempel på, hvor betydningsfuldt et fremgangsmådepatent kan være på IT-området, er sagen mellem *Stac Electronics v. Microsoft Corp.*, 38 F.3d 1222 (CAFC, 1994). Stac var indehaver af et patent til komprimering af data, som Microsoft på et tidspunkt havde udvist interesse for at erhverve. Nogen licensaftale kom ikke i stand. Allige-

vel indførte Microsoft i DOS 6.0 en lignende kompressionsordning under navnet "DoubleSpace", der for brugeren betød en fordobling af lagerarealet på en harddisk. Retten fandt, at Microsoft havde krænket retten til Stacs patent og tilkendte Stac en erstatning på 120 mio. USD, svarende til ca. 5,2 USD pr. solgt eksemplar af DOS 6.0 og 6.2.

Anvendelsespatent

En tredje type patent er anvendelsespatentet. Dette patent beskytter den måde, hvorpå et produkt eller en fremgangsmåde – uanset om dette eller denne er patenteret eller ikke – anvendes i en konkret sammenhæng. Også anvendelsespatenter har stor praktisk betydning på IT-området. Anvendelsespatentet anvendes navnlig for at undgå patentbeskrivelser, der anderledes formuleret ville være omfattet af en særlig patentudelukkelse, f.eks. den, der gælder for edb-programmer, jf. nedenfor.

Varighed

Patentretten vedvarer i 20 år fra datoen for indgivelsen af patentansøgningen, PL § 40, forudsat at patentansøgeren betaler en årsafgift. Årsafgiften beregnes efter en progressiv skala, der tilskynder patenthavere til at frafalde gamle og ubenyttede patentrettigheder. Når man læser ældre amerikanske patenter, bør det haves for øje, at patenttiden tidligere løb i 17 år fra patentets *udstedelse*. Dette er nu ændret, jf. *Koktvedgaard* (2005), s. 284.

Geografisk område

Et dansk patent har som udgangspunkt alene gyldighed i Danmark. Dette udgangspunkt er dog undergivet to væsentlige modifikationer. For det første kan patentansøgeren efter reglerne i PL kap. 3 iværksætte en international patentansøgning. I det omfang, denne procedure fører til patent, etableres der herved en vifte af nationale patenter i de pågældende lande. For det andet kan der søges om europæisk patent, jf. lovens kapitel 10A. Opnås patent gennem en sådan procedure, får ét og samme patent gyldighed i de designerede lande.

Europapatent

Da Danmark har ratificeret Europapatentkonventionen fra 1973 (EPK), jf. nedenfor, kan ansøgeren vælge mellem en dansk eller en europæisk patentprocedure. Europa-patenter udstedes af et centralt europæisk patentkontor i München (European Patent Office, EPO) med retsvirkning for de medlemsstater, der designeres i ansøgningen. Reglerne om sidstnævnte findes i PL kap. 10A. Kompetencen til at fortolke og eventuelt underkende et europæisk patent, f.eks. i en sag om krænkelse, ligger hos medlemsstaternes myndigheder, dvs. de domstole, hvor sagen kommer for.

Konventionen har ikke alene proceduremæssig interesse, men også materiel betydning for praksis vedrørende IT-patentering, se hertil *Meijboom* i 16 Rutgers 407 (1989), s. 417 ff. og samme i *Kaspersen & Oskamp* (1991), s. 47 f. Se også *Robert J. Hart* i ICLA, (august 1989), s. 7 ff. I sin afgrænsning af, hvad der kan patenteres,

har EPK overført de centrale bestemmelser fra Europarådets lovkonvention af 1963 om harmonisering af visse dele af den materielle patentret, der dog ikke gav regler om software-patentering.

Som det gælder for andre lande, der har tilsluttet sig EPK, indeholder den danske patentlov et udtrykkeligt forbud mod patentering af "programmer for datamaskiner", se lovens § 1, stk. 2, nr. 3. Forbuddet har rod i EPK art. 52, stk. 2, litra c, der udelukker patent på "schemes, rules, and methods for performing mental acts, playing games or doing business, and programs for computers". Rækkevidden af dette patentforbud er dog uklar, og retsopfattelsen på området er – som det vil fremgå (afsnit 10.1.d.) – genstand for en stadig bevægelse. Som det gælder for de ophavsretlige problemer må vurderingen af disse tvivlsspørgsmål dels inddrage nogle af de internationale erfaringer, dels tage højde for de interessemodsætninger, patentretten søger at afbalancere. Programudelukkelsen

10.1.b. Den internationale dimension

Dansk patentret er opbygget i nøje overensstemmelse med et veletableret internationalt konventionssystem. For patentadgangen på IT-området spiller det internationale samarbejde inden for EPK en særlig rolle. Ikke alene er det fra EPK, at det danske patentforbud for programmer hidrører. Den praksis, EPO følger om udelukkelsen af patent på "programmer til datamaskiner", og som bl.a. har udmøntet sig i en række retningslinjer for patentproceduren ved EPO, har stor indflydelse på forståelsen af dansk patentret. Patentudelukkelsen var oprindelig begrundet med, at dette svarede til retstilstanden i USA, se *Meijboom* i 16 Rutgers 407 (1989), s. 412, men denne praksis blev efterfølgende ændret, således at man i højere grad tillod patentering af software-relaterede opfindelser. Ifølge forarbejderne blev den – paradoksalt nok – indsat for at skabe klarhed på området, se *Hanneman* (1985), s. 242. EPO

I opfølgning af Kommissionens meddelelse af 5. februar 1999, KOM(1999) 42, endelig udg., som allerede var varslet i grønbogen af 24. juni 1977 om EF-patentet og det europæiske patentsystem (KOM97) 314 endelig udg., fremsatte Kommissionen den 20. februar 2002 forslag til "Direktiv om computer-implementerede opfindelsers patenterbarhed", (KOM(02) 92 endelig udg.) af. Ifølge forslagets art. 4 skal medlemsstaterne sikre, at en "computer-implementeret opfindelse" kan patenteres, såfremt den opfylder de eksisterende krav (stk. 1) og herudover "yder et teknisk bidrag" (stk. 2). Det tekniske bidrag skal vurderes som forskellen mellem patentkravets genstand som helhed, hvoraf Direktivforslaget

nogle dele kan omfatte både tekniske og ikke-tekniske karakteristika, og det aktuelle tekniske niveau (stk. 3). Begrebet "computer-implementeret opfindelse" defineres i forslagets art. 2, litra a, som "enhver opfindelse, hvis implementering indebærer anvendelse af en computer, et computernet eller en anden programmerbar maskine, og som omfatter ét eller flere *prima facie* nye karakteristika, som helt eller delvis implementeres ved hjælp af ét eller flere edb-programmer". Forslagets art. 2, litra b, definerer "et teknisk bidrag" som "et bidrag til det aktuelle tekniske niveau, som ikke er indlysende for en fagmand".

Forslaget har givet anledning til en voldsom debat, der ikke blot har drejet sig om det hensigtsmæssige i de foreslåede bestemmelser, men nok så meget om hensigtsmæssigheden af selve patentsystemet (således som det praktiseres nu) på it-området. I løbet af de år, direktivforslaget har været under behandling, har der været fremsat en række kompromisforslag om de centrale bestemmelser. Blandt andet har Rådet den 7. marts 2005 vedtaget en Fælles Holdning om spørgsmålet. Hvordan den endelige tekst vil se ud, er dog fortsat uklart. En god oversigt over disse spørgsmål findes på hjemmesiden <www.softwarepatenter.dk>.

Et af de problemer, der herved er blevet aktualiseret, angår kravet til opfindelseshøjde. Når dette krav praktiseres således, at det omfatter enhver løsning på et teknisk problem – selv de mest beskedne – som en fagmand ikke har fundet indlysende, se herved bemærkningerne s. 473 f., kan der opstå en ubalance: Den finansielt stærke IT-virksomhed vil her få mulighed for at dække ganske betydelige dele af sin IT-udvikling med patentpositioner, som kan vise sig uventet problematiske for den lille virksomhed, som ikke har tilsvarende ressourcer til patentering og patentovervågning, som derfor ikke kender de beskedne tekniske bidrag, der er dækket af med patenter, men som i en open source-løsning måske ligefrem vil blotlægge sin teknologi for omverdenen. Den heri liggende mulighed for, at pengestærke patenthavere møder succesfulde små *open source*-virksomheder med patentkrav, når konkurrencen herfra bliver for hård, har nærmest skabt en religionskrig mellem den patentanvendende IT-industri og *open source*-bevægelsen, som har vanskeliggjort den politiske proces om vedtagelsen af direktivet.

USA

Gennem de seneste år har man i USA set et stigende pres på patentsystemet. Der er flere forklaringer herpå. Generelt set er amerikanske virksomheder mere opmærksomme på værdien af en stærk patentbeskyttelse, end mange europæiske virksomheder er det. Hertil kommer, at usikkerheden om rækkevidden af den

ophavsretlige beskyttelse på programområdet, navnlig i henseende til de tekniske grænseflader mv., har ført til et pres på patentsystemet.

Verdens tre førende patentmyndigheder (USPTO, EPO og JPO) gennemfører med jævne mellemrum komparative ("trilaterale") undersøgelser af deres patenteringspraksis (det såkaldte trilaterale projekt). Det seneste studium vedrørende patenteringen af edb-programmel blev gennemført i november 1995. På grundlag af et antal udvalgte patentansøgninger konkluderes det bl.a., at der er "clear differences in the methods of interpretation and evaluation of claims for statutory subject matter among the three Offices". Den seneste praksis fra EPO's tekniske appelkammer, jf. f.eks. *T 1173/97* om implementering af en "commit procedure" (dvs. fremgangsmåde til at etablere juridiske forpligtelser), tyder dog på, at kammeret følger den amerikanske praksis for at udvide patenteringsområdet for software-relaterede patenter. Det forhold, at TRIPS-aftalen under WTO (art. 27) fastslår, at der skal sikres patenteringsadgang for "any inventions, whether products or processes, in all fields of technology", har formentlig påvirket denne opfattelse. Et trilateralt studium vedrørende patentering af forretningsmetoder er udført i juni 2000. Undersøgelsen konkluderer bl.a., at europæiske forretningsmetodepatenter kun kan udstedes, hvis de omfatter et teknisk aspekt.

En tredje forklaring ligger i, at amerikansk patentret ikke – som dansk og europæisk – indeholder noget eksplicit forbud mod patent på edb-software. Ikke desto mindre udviklede der sig gennem 1950'erne en praksis, hvorefter patentkrav, der alene var rettet mod anvisninger til den menneskelige ånd ("*mental steps*"), ikke kunne patenteres, se herom min Lærebog i edb-ret (1991), s. 227 ff. Denne tidlige praksis førte til en amerikansk retsopfattelse, hvorefter algoritmer ikke i sig selv kunne patenteres; en praksis, der dog siden ændrede sig således, at dette i dag kan ske, hvis ikke opfindelsen kan siges at udtømme algoritmen, hvilket ikke vil være tilfældet, hvis den blot er implementeret på en specifik måde, der opfylder patentkravene.

Testen stod sin afgørende prøve ved Supreme Court's – hidtil seneste – patentafgørelse på programområdet: *Diamond v. Diehr*, 450 U.S. 175 (1981). Diehr havde opfundet en fremgangsmåde til gummibehandling, der bl.a. anvendte en IT-styret anordning til temperaturregistrering. Det amerikanske patentkontor, USPTO, afviste patentansøgningen under henvisning til, at de temperatur-beregninger, anordningen foretog, ikke kunne patenteres, og at opfindelsen i øvrigt ikke besad den fornødne nyhed. Ved Supreme Court blev dette afslag omgjort. I sin begrundelse anførte flertallet (5-4), at et krav, der omfatter en matematisk algoritme, kan patenteres, hvis det implementerer eller anvender denne algoritme "in a structure or process which, when considered as a whole, is performing a function which

the patent laws were designed to protect (e.g., transforming or reducing an article to a different state or thing)". Se i øvrigt for en oversigt over den amerikanske praksis *Kristian E. Beyer* i Justitia 1999, nr. 4, s. 52 ff.

In re Alappat

Den nuværende amerikanske retstilstand vedrørende programpatentering er fastlagt gennem en række afgørelser, der faldt igennem 1990'erne, og som repræsenterer et klart skridt i retning mod generelt at tillade patent på *computer-related inventions*. Et markant nyere udtryk for denne tendens er CAFC's dom i *In re Alappat* 33 F.3d 1526 (CAFC, 1994). Sagen angik et program til nuancering af billedet i et oscilloscop (et apparat, der viser en elektrisk værdi – f.eks. de elektriske udladninger fra et hjerte – i en løbende grafisk repræsentation). CAFC fandt, at programmer beregnet for general purpose computere "creates a new machine, because a general purpose machine in effect becomes a special purpose computer once it is programmed to perform particular functions pursuant to instructions from program software" (s. 1545). Betragtningen førte retten frem til generelt at anerkende, at en computer, der opnår en bestemt funktion i overensstemmelse med det indlæste program, dermed kan være patenterbar. Tilsvarende blev resultatet i *In re Warmerdam*, 33 F.3d 1354 (1994).

USPTO Guidelines

På grundlag af Alappat-sagen udsendte USPTO den 18. januar 1996 et nyt sæt retningslinjer for patentering af "computer-implemented inventions", se 61 Fed.Reg. 7478. Vejledningen indeholder den hidtil mest detaljerede autoritative oversigt over forskellige typer af program-relaterede opfindelser, systematiseret under overskrifterne "Claims that encompass any machine or manufacture embodiment of a process", "Product claims directed to specific machines and manufacturers" og "Hypothetical machine claims which illustrate claims of the [aforementioned] types".

Forretningsmetoder

Den imødekommende linje, domstolene har anlagt i sager om program-relaterede opfindelser, er på det seneste videreført på det tilgrænsende (men ikke sammenfaldende) område for patenter på forretningsmetoder – et område, der som tidligere nævnt også er omfattet af patentudelukkelsen i PL § 1, stk. 2, nr. 3. Se hertil neden for i afsnit 10.1.e.

10.1.c. Hensynsafvejning

Innovationshensynet

Det grundlæggende hensyn bag patentretten er innovationshensynet: Ved at stille innovative personer og virksomheder de fordele i udsigt, som patentretten indebærer, giver man dem et inci-

tament til at investere de fornødne ressourcer til innovativ aktivitet. Dette synspunkt ligger ligeledes bag andre regler i immaterialretten.

Konkurrence-synspunktet

Heroverfor står – ikke overraskende – hensynet til det marked, der berøres af patentretten, og for hvem patentet bliver ensbetydende med, at de patenterede varer og tjenester nu kun kan udbydes af patenthaveren eller personer, som denne – typisk mod betaling – har givet tilladelse (licens). De argumenter mod softwarepatentering, der har været ført frem i den tidligere amerikanske praksis, fokuserede navnlig på dette synspunkt, bl.a. fordi patentretten – modsat ophavsretten – beskytter mod dobbeltfrembringelser, sml. diskussionen i EU's Grønbog om ophavsret, pkt. 5.5.3. Blandt visse Internet-entusiaster har man i nyere tid dertil føjet den ideelle betragtning, at information som udgangspunkt bør være fri.

Omkostnings-synspunktet

Et andet argument mod patentsystemet er, at det "vender sin tunge ende nedad". Omkostningerne ved at udtage et patent i form af honorarer til patentrådgiveren, oversættelse af ansøgninger, registreringsgebyr mv., samt omkostningerne ved at vedligeholde det (årsafgifter samt løbende honorar til den lovkrævede lokale patentrepræsentant) vil ofte løbe op i millionbeløb. Hertil kommer omkostningerne ved i givet fald at skulle gennemtvinge et udstedt patent (advokatomkostninger). Omfanget af disse omkostninger kan være prohibitive for IT-branchens små og mellemstore aktører. Denne byrde må ikke mindst sættes i forhold til, at det jo er gratis at opnå ophavsrettens beskyttelse. Historien viser dog mange eksempler på succesfulde IT-produkter, der er frembragt af enkeltpersoner, og som markedsføres af små og mellemstore virksomheder.

Heller ikke denne betydning er nødvendigvis rammende. Et patent som det, *Gilbert P. Hyatt* i august 1990 fik på basal mikroprocessorteknologi (U.S. pat.no. 4.942.516), kan placere et stærkt våben hos en lille aktør. Hyatt indgik siden en licensaftale med Philips Electronics, og patentet har såvidt vides ikke siden været søgt håndhævet. Netop denne effekt kan måske ligefrem føre til en balance i den praktiske patenthåndtering. En tilsvarende situation foreligger med det såkaldte "Bellboy"-patent, se fremlæggelsesskrift EP 0 738 446B1, som med sin patenterede metode til modtagelse af ordre ved hjælp af et datanetværk må formodes at dække store dele af moderne Internet-handel.

10.1.d. Undtagelsen for programmer

Det nugældende forbud mod patentering af "programmer for datamaskiner" i PL § 1, stk. 2, nr. 3, må fortolkes i lyset af dets udspring i EPK. Selv om der ikke gælder nogen umiddelbar pligt for danske patentmyndigheder til at lægge sig ind under praksis fra EPO's appelkammer – eftersom de to systemer fungerer sideløbende – vil det være naturligt at søge den videst mulige harmonisering, så ansøgerne ikke tvinges til at gøre brug af begge procedurer med virkning for samme territorier. Patent- og Varemærkestyrelsen har ved forskellige lejligheder markeret, at man vil søge en sådan koordinering opnået gennem sin praksis, og et sådant resultat må der i almindelighed være sagligt belæg for, sml. for så vidt angår svensk patentret *Marianne Levin* i NIR 1991.197 ff.

Indtil 1985 fortolkedes patentforbuddet som en absolut grænse, der kun gav mulighed for patent på rene hardware-opfindelser (f.eks. et lagermedium) eller på opfindelser, der integrerer hardware og software på en sådan måde, at programmet er et nødvendigt led i en mekanisk eller elektromekanisk mekanisme. Men flere omstændigheder har sat denne fortolkning under pres. *Internationalt* bevirkede den patentretlige udvikling i USA efter afgørelsen i *Diehr*-sagen en ny synsvinkel, der smittede af i Europa med EPO's første guidelines om spørgsmålet af 6. marts 1985. I *teknisk* henseende blev sondringen mellem hardware- og softwareimplementering af forskellige tekniske løsningsmetoder stadigt mere uklar, bl.a. pga. udviklingen i halvlederteknologien, der gjorde det muligt forholdsvis ubesværet at indlejre software-løsninger i hardware-produkter. Hertil kom, som bl.a. fremhævet af *Riis* (1998), s. 169, at en stigende del af den innovative virksomhed i IT-branchen knytter sig til softwarefrembringelser, som det ville føles forkert ikke at tilbyde den beskyttelse, der anerkendes for hardware.

Vicom-sagen

EPO's retningslinjer fra 1985 udmøntede sig i flere afgørelser. Den første faldt den 15. juli 1986 i sag *T 208/84* om *Vicom Systems* (OJ EPO 1987.14). Her tillod EPO's tekniske appelkammer patentering af et digitalt billedbehandlingssystem beregnet til satellitbilleder. Opfindelsen indbefattede bl.a. en matematisk algoritme, der nedsatte antallet af de beregninger, der efter tidligere teknikker var nødvendige for at opnå billedoverførelsen. Da algoritmen imidlertid hidførte en ændring i den fysiske tilstand som opfindelsen angik – billedet – forelå den nødvendige tekniske effekt.

Koch & Sterzel

Den næste patentafgørelse for EPO's tekniske appelkammer faldt mindre end et år efter, nemlig den 21. maj 1987 med sagen *Koch & Sterzel* (*T 26/86*), OJ EPO 1988.19. Opfindelsen angik et røntgenapparat, der var styret af en programalgoritme. Denne kombination af tekniske og ikke-tekniske elementer udelukkede ikke patentering.

Disse to afgørelser udgør hovedhjørnestenen i den europæiske patentmyndigheds praksis. Siden har patentmyndigheden truffet en række afgørelser, der på forskellig vis har belyst kriteriet om teknisk effekt i relation til de forskellige informations-relaterede patentudelukkelser. *T 22/85* (OJ EPO 1990.12), som blev afgjort den 5. oktober 1988, angik en metode til at ekstrahere informationsindholdet i et dokument kombineret med funktioner til lagring og søgning. EPO havde den 30. august 1984 (altså før de nye retningslinjer var trådt i kraft) afvist ansøgningen med den begrundelse, at opfindelsen angik et program, der som sådant var udelukket fra patentering. Under klagesagen gjorde ansøgeren (IBM) gældende, at der forelå en teknisk løsning på et teknisk problem, ganske som i Vicom-sagen, men heri fik man ikke medhold. Opfindelsen ansås at falde under EPK's undtagelse for "schemes, rules and methods of performing mental acts" – den var med andre ord ikke teknisk.

Af yderligere patentpraksis fra EPO henvises til *T 6/83* (OJ EPO 1990.5, 21 IIC 358 (1990)), hvor en metode til parallelprocessing i et netværk til telekommunikation blev patenteret. Den pågældende kontrol og koordination var ikke karakteriseret ved de pågældende data eller ved den måde, hvorpå et konkret program anvendte disse data. Sagsbehandleren havde afvist patentet pga. manglende nyhed. *T 52/85* (utrykt) Technical Board of Appeal, 16. marts 1989 angik et system til automatisk behandling af en liste af semantisk relaterede udtryk på grundlag af data hidrørende fra en hukommelsesenhed. Patentbeskyttelse blev afvist. *T 115/85* (OJ EPO 1990.30, 21 IIC 354 (1990) angik en fremgangsmåde til at dekode tekst med henblik på udlæsning af forløb i et tekstbehandlingssystem. Sagsbehandleren havde afvist ansøgningen under henvisning til, at dens nyhed og opfindelseshøjde bestod af et program; den hardware, der indgik i opfindelsen, svarede til, hvad der indgik i et klassisk tekstbehandlingssystem. Appelkammeret hjemviste sagen på grundlag af den antagelse, at den mekanisme til visuel visning af data, som opfindelsen gik ud på, indebar en teknisk løsning. I *T 163/85* (OJ EPO 1990.379) fik BBC patent på et farve-TV signal, der transmitterer information på en anden – og mere effektiv – måde end vanligt. Resultatet i *T 38/86* (OJ EPO 1990.384) forekommer umiddelbart overraskende. Her blev patent nægtet på en metode til tekstbehandling, der muliggjorde automatisk udfindelse og erstatning af lingvistiske udtryk. Teknikken indebar en kombination af valg, som

brugeren skulle træffe, og forløb, som systemet havde kontrol over. Appelkammeret lagde vægt på, at brugeren uden brug af IT ville kunne foretage en tilsvarende teksttilretning som den, programmet udførte, og at programmet derfor ikke indebar en teknisk løsningsmodel. Afgørelsen, der er truffet den 14. februar 1989, kunne måske læses som udtryk for en ændring i EPO's praksis, se nærmere *Meijboom* i Kaspersen & Oskamp (1991), s. 55 ff. Efterfølgende praksis synes dog igen at være på linje med sagerne i *Vicom* og *Koch & Sterzel*. *T 42/87* (utrykt), der er afgjort den 5. oktober s.å. (1989), giver således patent for en "Method and apparatus for multilingual communications of computer-specified control messages". I præmisserne hævdes det, at der ingen inkonsistens er mellem denne afgørelse og T 38/86, da opfindelsen i T 38/86 tog sigte på at understøtte brugerens tekstformulering. *T 216/89* (utrykt), afgjort den 10. oktober 1990, gav patent på et "Data communication system with capabilities to analyse an error or problem condition". Her var der også tale om, at brugeren skulle træffe beslutning på grundlag af systemets data, men appelkammeret fandt – efter at patentkravene var blevet tilpasset – at "the system itself ... does not involve a mental act". Som begrundelse for, at patentet ikke hermed udgjorde et program, henviste kammeret til, at det pågældende signal undergik "various technical transformations in which the represented text per se remains unchanged". *T 109/90* angik et program, der konverterede én slags information til en anden. Appelretten fandt, at der hverken forelå en anvisning til den menneskelige ånd ("mental act") eller et program. *T 110/90* omhandlede en metode til transformering af tekst og printerkommandoer. Appelretten fandt også her, at transformering af printerkommandoer fra ét format til et andet, hvorved en tekst kunne konverteres fra ét tekstbehandlingssystem til et andet, indebar en teknisk effekt. Ansøgningen drejede sig derfor hverken om at udføre en "mental act" eller om et program. *T 236/91* angik et menu-baseret input-system i naturligt sprog. Igen fandt Appelretten, at ansøgningen hverken angik information, en "mental act" eller et program. Se senest *T 1173/97*, der anerkendte to patentkrav vedrørende indlæsning af programmel i en RAM-enhed til brug for gennemførelse af en procedure til etablering af en aftaleforpligtelse (afgørelsen indeholder i øvrigt en god oversigt over appelkammerets praksis). Afgørelsen markerer en bevægelse bort fra kriteriet om "teknisk effekt", idet den tillader andre nyttige virkninger af opfindelsen end de rent "tekniske". Se i samme retning *T 935/97* og *T 1194/97* (om et billedsøgningssystem) og om den nævnte praksis *Kristian E. Beyer* i Justitia, 1999, nr. 4, s. 63 ff.

EPO's praksis om patentering af "computer-related inventions" er i dag indeholdt i EPO's Guidelines part C, Chapter IV, afsnit 2.3.6. Retningslinierne tager udgangspunkt i begrebet "computer-implemented inventions", som omfatter patentkrav, der involverer computere, computernetværk eller programmerbare indretninger, hvor opfindelsen viser sin nyhed og opfindelseshøjde ved

hjælp af programmel. Retningslinjerne fremhæver, at sådanne opfindelser altid vil rumme visse fysiske effekter (for eksempel forløbet af et elektrisk kredsløb), men at det forhold, at programmet udvirker en sådan effekt, ikke i sig selv åbner patentvejen. Hertil kræves en teknisk effekt, som går "beyond these normal physical effects". En sådan, patenterbar, teknisk effekt kan for eksempel foreligge i forbindelse med overvågning af en industriel proces, i behandlingen af data vedrørende fysiske enheder eller i computeres interne funktioner: "As a consequence, a computer program claimed by itself or as a record on a carrier or in the form of a signal may be considered as an invention within the meaning of art. 52(1) if the program has the potential to bring about, when running on a computer, a further technical effect which goes beyond the normal physical interactions between the program and the computer."

Retningslinjerne udtaler dernæst: "When considering whether a claimed computer-implemented invention is patentable, the following is to be borne in mind. In the case of a method, specifying technical means for a purely non-technical purpose and/or for processing purely non-technical information does not necessarily confer technical character on any such individual step of use or on the method as a whole. On the other hand, a computer system suitably programmed for use in a particular field, even if that is, for example, the field of business and economy, has the character of a concrete apparatus, in the sense of a physical entity, and thus is an invention within the meaning of Art. 52(1) (see T 931/95, OJ 10/2001, 441)."

Konklusion

Det essentielle i kravet om "technical effect" ligger formentlig i, at dette krav kan anses som en negation af selve de instruktioner, et program sender til processoren. Man kan for så vidt betragte den ophavsretlige programbeskyttelse som rettet mod "input"-siden (instruktionerne til processoren), og patentbeskyttelsen som rettet mod "output" (den tekniske effekt). Anlægges kravet på denne måde vil patentsystemet fungere komplementært til det ophavsretlige system. Dermed vil de to beskyttelsessystemer kunne eksistere side om side. Den, der skriver et edb-program, kan herved komme til at krænke en patentret (nemlig, hvis programmet dækker en fremgangsmåde eller anvendelse, som er beskyttet af et patent). Derimod vil indehaveren af et patent som altovervejende hovedregel være i stand til at implementere sit program-relaterede patent via en mangfoldighed af forskellige programløsninger, hver med sin ophavsretlige programbeskyttelse.

10.1.e. Anden patentudelukkelse

PL § 1, stk. 2, nr. 3, forbyder ligeledes patent på planer, regler eller metoder for intellektuel virksomhed, for spil eller for erhvervsvirksomhed. At en opfindelse rummer en "plan" for noget, eller i øvrigt angiver metoder eller regler, er i sig selv ikke til hinder for, at den kan patenteres, jf. herved den norske patentstyreafgørelse i *NIR 1995.674*. Patentudelukkelsen knytter sig til planens *genstand*: Intellektuel virksomhed, spil eller erhvervsvirksomhed.

Forretningsmetoder

Navnlig i relation til erhvervsvirksomhed har bestemmelsen givet anledning til afgrænsningsvanskeligheder, eftersom stadigt flere forretningsmæssige idéer alene kan nyttiggøres ved hjælp af IT og for så vidt står i samme forhold til denne teknologi som edb-programmerne (som jo også efter ordlyden er patentudelukkede). Domspraksis i USA samt patentpraksis i EPO tyder da også på, at man – indtil videre – tenderer mod at anlægge samme linje som gjort på programsiden og altså ikke gøre brug af denne undtagelse.

State Street-sagen

En toneangivende amerikansk dom på dette område foreligger i *State Street Bank v. Signature Financial Group*, 149 F.3rd 1368 (CAFC 1998). Her antog CAFC, at et patent udstedt i 1994, der dækkede et program til håndtering af aktieinvesteringer (løbende beregninger af tab og gevinster mv.) var gyldigt. Dommen udtaler bl.a., at det forhold at "a claimed invention involves inputting numbers, calculating numbers, outputting numbers and storing numbers, in and of itself, would not render it nonstatutory subject-matter, unless, of course, its operation does not produce a 'useful, concrete and tangible result'."

Afgørelsen i denne sag gav anledning til en del uro, selv om opfindelsen kun havde betydning på et forholdsvis snævert afgrænset markedssegment, og selv om dens "tekniske effekt" trods alt *kunne* beskrives som en serie avancerede matematiske løsninger. Afgørelsen er efterfølgende fulgt op med anden praksis fra CAFC, se således *AT&T Corp. v. Excel Communication*, 175 F.3rd. 1352 (CAFC 1999). Siden er et stort antal amerikanske patenter på forretningsmetoder udstedt, og der er opstået en generel diskussion om det hensigtsmæssige i disse – ofte bredt formulerede – patenter, der i mange tilfælde blot udstedes ud fra defensive formål.

Som eksempler på andre forretningsmetodepatenter kan henvises til U.S. Patent 5.794.207 (Priceline: Metode for kryptografisk baseret kommercielt net-system, der understøtter køber-styret betinget

ordreafgivelse), U.S. Patent 5.960.411 (*Amazon.com*: Metode og system til at placere en købsordre via et kommunikationsnet – patentet er nu genstand for retssag), U.S. Patent 5.963.916 (*Intouch*: Netforbundet apparat og metode til forhåndgennemsyn af musikprodukter og til indsamling af markedsføringsoplysninger) og U.S. Patent 5.809.242 (*Juno*: E-mailsystem, der viser reklamemateriale, mens klienten er i off-line tilstand). De nævnte patenter er tilgængelige fra <www.uspto.gov>).

Diskussion

Når spørgsmålet om hensigtsmæssigheden af patenter på almindelige forretningsmetoder drøftes kan det være nødvendigt at overveje, om det er samfundsmæssigt ønskeligt at lade forretningsmæssige løsninger, hvis værdi udelukkende står og falder med skiftende tiders psykologiske vaner og kulturfaktorer, omfatte af en industriel ejendomsret. Betænkeligheden herved stiger, jo bredere de pågældende patenter dækker, og jo mere tvivlsomt det er, om den fornødne opfindelseshøjde er tilstede.

Sådanne indvendinger kan således rejses mod det amerikanske patent 5.960.411 (udstedt 28. september 1999). Patentet dækker den form for hypertekst-linking, der sker ved hjælp af banner-annoncer. En tilsvarende uro har det såkaldte "Bellboy"-patent skabt, se fremlæggelsesskrift EP 0 738 446 B1, som omfatter en metode til modtagelse af ordrer ved hjælp af et datanetværk (og dermed centrale dele af den elektroniske handel, der foregår via World Wide Web). Hvis de pågældende patenter opretholdes, vil dette medføre en ganske betydelig økonomisk kontrol hos de pågældende patenthavere over den almindelige Internet-handel. Findes det fra politisk hold ønskeligt at etablere sådanne industrielle enerettigheder, burde en sådan løsning måske ledsages af en mulighed for at etablere tvangslicenssystemer, der går videre (bl.a. i henseende til de tidsmæssige betingelser for at gøre en tvangslicens gældende) end de eksisterende regler, jf. herom straks nedenfor.

Det retspolitiske problem ligger dog nok ikke så meget i, at den legale patentudelukkelse reelt er bortfortolket i praksis, men i at man inden for dette område ikke synes at stille iøjnefaldende store krav til karakteren af den opfindelseshøjde, der kan begrunde et patent. Hvis kravene hertil sættes så lavt, at enhver blot nogenlunde kreativ idé kan begrunde et patent, vil man på et innovativt område som f.eks. e-handelsområdet skabe tilfældige magtpositioner, som blot bliver til fordel for den, der (tilfældigvis?) får idéen først og søger patent, i stedet for – som det oprindeligt er formålet – at belønne den, der investerer i innovativ udvikling og lægger resultatet af denne innovation frem for almenheden. En opfindelse, der blot udspringer af opfinderens spontane, lyse idé kan selvsagt også beskyttes med et patent. Dette er der adskillige eksempler på inden for den klassiske pa-

tentret. Men i den retspolitiske drøftelse er det måske navnlig påkrævet at stille krav til opfindelseshøjde, når der er tale om sådanne "spontane" opfindelser, der ikke angår klassisk tekniske løsningsmodeller, og som vil kunne føre til brede eneretspositioner.

I et forsøg på at imødegå kritikken mod de amerikanske patenter på forretningsmetoder indførte USA i november 1999 en lovændring (se § 273(b) i Title 35), hvorefter forretningsmetoder, der er udviklet uafhængigt af det meddelte patent og faktisk anvendt før dettes udstedelse, ikke skal rammes af patentet. En sådan forbenyttelsesret er dog allerede hjemlet ved den danske patentlovs § 4, stk. 1.

EPO-praksis

I europæisk patentpraksis har man endnu ikke taget skridtet fuldt ud mod en patentering af patenter på forretningsmetoder "som sådanne". Det kræves således, at den pågældende forretningsmetode rummer en teknisk effekt. Det er ikke tilstrækkeligt for at opfylde dette krav, at metoden rummer et element, der kan udnyttes ad teknisk vej, hvis selve formålet er ikke-teknisk, jf. således udtalelsen i *T 0931/95*, der er afgjort af det tekniske appelkammer den 8. september 2000. Der var tale om en opfindelse, der indebar en metode til beregning af pensionsfordele i private pensionsordninger.

10.1.f. Udnyttelse og håndhævelse

En patentret udnyttes på samme måde som en hvilken som helst anden eneret. I modsætning til udnyttelse af ophavsrettigheder beror patentudnyttelsen dog på, hvilken type patent der er tale om: fremgangsmåde, produkt eller anvendelse. Denne sondring vil derfor afspejle sig i den pågældende licens.

Licens

PL giver enkelte regler om patentlicenser i §§ 43-44. Har patenthaveren givet en anden ret til erhvervsmæssigt at udnytte opfindelsen, kan denne ikke overdrage denne ret til andre, medmindre andet måtte være aftalt. PL § 44 bestemmer endvidere, at et patent, der er overgået til en anden eller er givet i licens, på begæring skal indføres i patentregisteret. Godtgøres det, at en registreret licens er ophørt, skal licensen slettes af registeret. Registreringen har i hvert fald to formål. For det første indebærer den, at søgsmål vedrørende et patent altid kan anlægges mod den, som i registret er indført som patenthaver. Dernæst er registeradressen den adresse, til hvilken patentmyndigheden kan tilskrive patenthaveren – et formelt forhold, der bl.a. har betydning, fordi det er hertil advarslen om patentets bortfald ved manglende betaling af årsafgifter sendes.

Efter reglerne i PL §§ 45 – 50 kan der under forskellige omstændigheder gives tvangslicens til anvendelse af et patent, dvs. en tilladelse til at udnytte patentet i nærmere bestemt omfang, der ikke baseres på patenthaverens viljeserklæring. Muligheden for tvangslicens står for det første åben, hvis et patent ikke udøves i rimeligt omfang, jf. nærmere § 45 (3 år fra patentets meddelelse og 4 år fra patentansøgningens indlevering). Der kan dog ikke gives tvangslicens, hvis der foreligger skellig grund til undladelsen. Bevisbyrden herfor påhviler patenthaveren. Hvis udøvelsen af et patent beror på et andet patent (såkaldt afhængighedspatent), kan der pålægges indehaveren af dette andet patent tvangslicens, "hvis den førstnævnte opfindelse udgør et vigtigt teknisk fremskridt af væsentlig økonomisk betydning", PL § 46. Meddeles en sådan tvangslicens, kan patenthaveren tilsvarende opnå tvangslicens hos den tvangslicensberettigede for de opfindelser, han har gjort, og som begrunder tvangslicensen, jf. § 46, stk. 2. Endelig indeholder PL § 47 en generalklausul, der giver hjemmel til tvangslicens med henblik på erhvervsmæssig udnyttelse af en opfindelse, "når vigtige interesser gør det påkrævet". Bestemmelsen anvendes sjældent. Generelt gælder det, at tvangslicens kun må meddeles den, som kan antages at være i stand til at udnytte opfindelsen på en rimelig og forsvarlig måde og i overensstemmelse med licensen, PL § 49. Sø- og Handelsretten i København er kompetent til som første instans at tage stilling til krav om tvangslicens.

Håndhævelse

Reglerne om håndhævelse af patent fremgår af PL kap. 9, der hjemler straf (§ 57), vederlag og erstatning (§ 58) samt forebyggelse (§ 59). Der henvises herom i det hele til *Koktvedgaard* (2005), kapitel VIII.

10.1.g. Patent i ansættelsesforhold

For så vidt angår retten til patenter gælder 1955-loven om arbejdstageres opfindelser, se herom min lovkommentar fra 1995. Loven bygger på det udgangspunkt, at arbejdstageren har retten til de af ham gjorte opfindelser, se § 3. Har en arbejdstager gjort en opfindelse, som han må anses for at være nået til gennem sin tjeneste, er arbejdsgiveren dog berettiget til at kræve retten til opfindelsen overdraget til sig for et eller flere lande, jf. lovens § 5. Samme ret har arbejdsgiveren i tilfælde, hvor udnyttelsen af opfindelsen ikke falder inden for virksomhedens arbejdsområde, såfremt opfindelsen angår en nærmere angiven opgave, som er stillet den ansatte af virksomheden. Den ansatte er i begge tilfælde berettiget til en "rimelig godtgørelse" til gengæld for at skulle afstå retten, jf. nærmere lovens § 8, der er præceptiv. Godtgørelse kan dog ikke kræves, hvis værdien af opfindelsen ikke overstiger,

hvad arbejdstageren under hensyn til sine arbejdsforhold i det hele med rimelighed kan forudsættes at skulle præstere.

Opfinderloven er begrænset i forskellige henseender. Efter § 1 gælder den kun for opfindelser, der "kan patenteres her i riget". Dette krav, der er båret af praktiske grunde (vanskeligheden ved at overskue en mulig patenterbarhed udenfor Danmark), indebærer, at det er patenterbarheden efter dansk ret, der er afgørende for lovens anvendelse; ikke den faktiske patentering. Som udgangspunkt vil loven derfor gælde, hvis en opfindelse efter at være patenteret i Danmark senere patenteres i udlandet. Det samme gælder, hvis den alene patenteres i udlandet under omstændigheder, hvor den kunne patenteres i Danmark. På områder, hvor der af særlige grunde skulle være uoverensstemmelser mellem dansk ret og retstilstanden ved de større patentkontorer, taler meget for at se bort fra denne betingelse, jf. min lovkommentar, s. 31.

Opfinderloven begrænses i relation til lærere og andet videnskabeligt personale ved universiteter og andre højere læreanstalter, jf. § 1, stk. 3, hvorefter denne personalegruppe ikke anses som arbejdstagere. De har følgelig den fulde ret til de af dem gjorte opfindelser, medmindre andet måtte være bestemt ved anden lov eller følge af aftale, jf. nærmere min lovkommentar (1995), s. 37 ff.

Universitetsforskere

Som anført i afsnit 6.5.c. giver lov nr. 347 af 2. juni 1999 om opfindelser ved universiteter og sektorforskningsinstitutioner disse institutioner råderet over opfindelser gjort på stedet. Inden for bestemmelsens anvendelsesområde fraviges reglerne i lov om arbejdstageres opfindelser, og den pågældende offentlige forskningsinstitution kan inden for lovens regler overtage kontrollen med den pågældende opfindelse.

Beskyttelsen

10.2. Brugsmodelbeskyttelse

Ved loven om brugsmodeller, jf. lovbekendtgørelse nr. 367 af 9. juni 1998, er der gennemført en særlig beskyttelse af "enhver frembringelse, som kan udnyttes industrielt, og som indebærer en løsning på et teknisk problem". I forhold til patentbeskyttelsen nedtoner loven beskyttelseskravene. Hvor patentloven stiller krav om, at en opfindelse adskiller sig "væsentligt" fra det kendte (PL § 2, stk. 1), kræver brugsmodellovens § 3, stk. 1, blot, at den brugsmodelbeskyttede frembringelse adskiller sig "tydeligt" derfra.

Proceduren

Brugsmodelregistrering er ikke forbundet med samme prøvelse som den, der gælder ifølge patentloven. Efter lovens § 12 skal Patent- og Varemærkestyrelsen – der er den instans, der modtager registreringen – alene påse, at ansøgningen opfylder betingelserne i lovens § 1 ("frembringelse som kan udnyttes industrielt, og som indebærer en løsning på et teknisk problem"), § 2 (særlige udelukkede områder), § 9 (flere af hinanden uafhængige frembringelser) og § 11 (ændringer ud over den oprindelige ansøgning). Derimod skal direktoratet ikke foretage nogen prøvelse af, om frembringelsen – som krævet i brugsmodellovens § 3 – er ny i forhold til, hvad der var kendt før ansøgningens indleveringsdag. De formelle regler vedrørende overdragelse af brugsmodelrettigheder svarer til de patentretlige.

Udelukkelse

Brugsmodelloven undtager de forhold, der er nævnt i PL § 1, stk. 2-4. Dette indebærer, at de programrelaterede opfindelser, der efter patentretlig praksis er udelukket fra at opnå patent, heller ikke kan opnå brugsmodelregistrering. Derimod kan brugsmodelregistreringen efter omstændighederne beskytte en række af de aspekter, der hidtil har været vanskelige at få passet ind under eksisterende eneretssystemer – herunder printkort og andre dele af den indmad, der findes i elektroniske produkter.

Som anført af *Koktvedgaard* i NIR 2000.540 indebærer brugsmodelbeskyttelsen svaret på en række af de problemer, patentsystemet giver anledning til på programområdet (behovet for en hurtig retsstiftelse med efterfølgende domstolskontrol mv.). Brugsmodelbeskyttelsen nyder dog ikke samme internationale udbredelse, som patentsystemet, og kan derfor ikke på kort sigt ventes at udgøre et reelt alternativ for den, der ønsker en sådan international retsbeskyttelse. Kommissionen fremlagde i 1997 et forslag til direktiv om brugsmodelbeskyttelse, se KOM(97) 691 endelig udg. Direktivet skulle have til formål at introducere dette særlige beskyttelsessystem i de medlemsstater, der ikke allerede har indført det, og at harmonisere lovgivningen herom i de stater, der har. I sin foreslåede form indeholdt det samme undtagelser som de, der for tiden gælder for patenter, herunder vedrørende "planer, regler og metoder for samt fremgangsmåder til intellektuel virksomhed, spil eller erhvervsvirksomhed samt edb-programmel", se herved art. 3, stk. 3, litra c). Der viste sig dog ikke politisk vilje til at gennemføre dette forslag.

Retssubjektet

I relation til spørgsmålet om rettighedens subjekt følger brugsmodelloven samme regler som patentloven. Denne tilpasning er gennemført ved, at opfinderloven udtrykkeligt præciserer, at lovens udtryk "opfindelser" også omfatter "frembringelser, der kan registreres som brugsmodel her i riget".

10.3. Designbeskyttelse

10.3.a. Designloven

Efter § 1 i designloven (tidligere mønsterloven) kan den, der har frembragt et design (designeren) eller den, til hvem hans ret hertil er overgået, erhverve *eneret* til erhvervsmæssigt at udnytte designet. Beskyttelsen forudsætter, at designet er nyt og har individuel karakter, jf. § 3, stk. 1. Reglerne har grundlag i direktiv 98/71/EF af 13. oktober 1998 om retlig beskyttelse af mønstre (EFT 1998 L 289/28).

Eneretten opnås ved registrering, jf. nærmere lovens kapitel 2. Ansøgning om registrering af et design indgives til Patent- og Varemærkestyrelsen.

Designretten erhverves for en gyldighedstid på op til 25 år, jf. DL § 23. Fordi denne beskyttelsestid er kortere end den, der kan opnås i medfør af de ophavsretlige beskyttelsesregler for brugskunst, spiller designretten ofte ikke nogen stor rolle for beskyttelsen af brugskunst. Denne begrænsning er væsentlig at mærke sig, eftersom der ikke kan opnås designret til de dele af et produkts udseende, der udelukkende er bestemt af produktets tekniske funktion eller som kræver nøjagtig reproduktion af hensyn til samspillet med andre produkter, jf. nærmere lovens § 9, stk. 1.

Begrebet "design" defineres i lovens § 2, nr. 1, som "et produkts eller en del af et produkts udseende, som er bestemt af de særlige træk ved selve produktet eller dets udsmykning, navnlig for så vidt angår linjer, konturer, farver, form, struktur eller materiale". Et "produkt" er ifølge samme bestemmelses nr. 2) "en industrielt eller håndværksmæssigt fremstillet artikel, herunder bl.a. dele, der er bestemt til at blive samlet til et sammensat produkt, samt emballage, udstyr, grafiske symboler og typografiske skrifttyper, men ikke edb-programmer". Designretten kan herved først og fremmest give en eneretsbeskyttelse til de visuelle aspekter af IT-systemet, der træder frem i terminalens *design*, formgivning mv. Væsentlig er i den forbindelse den beskyttelse af typografien (fonte), som kan opnås gennem reglerne om designbeskyttelse, sml. herved bemærkningerne i afsnit 9.2.

Printplader

Designretten kan efter omstændighederne benyttes som grundlag for at beskytte de *printplader*, hvori IT-systemets komponenter (halvlederprodukter, modstande, spoler mv.) fastgøres ved lodning. En sådan beskyttelse er dog af beskeden rækkevidde, da den ikke giver eneret til nogen teknisk funktion. Den funktion, der udføres ved en given sammensætning af komponenter,

beror som udgangspunkt på, hvilke komponenter der indgår i printkortet og på, hvorledes disse er forbundet. Da den visuelle fremtoning af forbindelseslinjerne som udgangspunkt er underordnet for systemets funktion, kan printkortets funktion kopieres, uden at selve printkortet kopieres, og uden at designretten derved krænkes.

Brugergrænseflader

Et andet område, hvor designretten kan tænkes at supplere de mere veletablerede beskyttelsesformer, er beskyttelsen af visse dele af programmets brugergrænseflader (ikoner, skærm-mønstre mv.). Mange af disse frembringelser kan dog beskyttes som ophavsretlige værker, jf. afsnit 7.3.b.

Edb-programmer

Et edb-program som sådan kan efter loven ikke være et produkt og kan derfor ikke som sådan beskyttes efter loven. Men efter forarbejderne til loven, men dog ikke til direktivet, kan webdesigns, skærmbilleder og ikoner beskyttet som designs i medfør af lovens § 2, stk. 2.

10.3.b. Designforordningen

Ved rådets forordning (EF) 6/2002 er der indført umiddelbart anvendelige regler om et nyt EF-design. Forordningen, som blev vedtaget den 12. december 2001, og som trådte i kraft den 7. marts 2002, etablerer således en ny immaterialretstype i Danmark, nemlig det *uregistrerede* EF-design. På grund af sin formløshed fremstår denne beskyttelse som en særegen kombination af markedsføringslovens og ophavsretslovens regler. Et EF design har retsvirkning allerede fra det tidspunkt, hvor det er offentligt tilgængeligt, jf. art. 1, stk. 1 litra a, hvorefter det er beskyttet i 3 år, jf. art. 11. Det registrerede EF design skal registreres senest 12 måneder efter offentliggørelse. Den maksimale beskyttelsestid for det registrerede design er 25 år, jr. art. 12.

Det er forudsat, at denne beskyttelse primært vil få praktisk betydning i relation til modeprægede produkter. Dermed kan det ikke udelukkes, at beskyttelsen også vil få betydning for grænsefladerne i edb-programmer og andre digitale frembringelser. Se for en nærmere oversigt over reglerne om det europæiske design, *Koktvedgaard* (2005), s. 303 ff., samme i U 2002B.101 ff. samt *Jens Schovsbo* og *Niels Holm Svendsen*: Designret (2002).

Heller ikke forordningen beskytter edb-programmer som sådanne, men om udelukkelsen af edb-programmer udtales det i de indledende bemærkninger til forordningsforslaget fra juni 1993 at "this does not exclude the protection of specific graphic de-

signs as applied for example to icons or menus provided the normal requirements are met".

10.4. Halvlederbeskyttelse

10.4.a. Teknisk baggrund

Problemet

Lov nr. 778 af 9. december 1987 om beskyttelse af halvlederes udformning (topografi) – halvlederloven, eller HLL – etablerer en særlig *sui generis* retsbeskyttelse for edb-teknologiens byggesten, de såkaldte halvlederchips (i loven kaldet "halvlederprodukter"). Der er tale om en særegen beskyttelse, der specifikt omhandler den teknologi, der ligger til grund for opbygningen af halvlederprodukter. Indholdet af beskyttelsen forstås derfor kun, hvis man har kendskab til disse teknikker.

Halvleder-materialet

Den tekniske indmad i en halvlederchip er opbygget på grundlag af et halvledermateriale (f.eks. silicium). Dette materiale stanses ud i skiver (skive hedder på engelsk: "chip"), der først påføres et lag oxid og dernæst et fotoresistent materiale. Herefter placeres der en maske bestående af en tynd film oven på den forarbejdede chip. På denne maske er tegnet et bestemt mønster, der angiver de mikroskopiske områder, hvor det er meningen, at siliciumskiven skal lede strøm, hæmme for strøm og henholdsvis virke som halvleder. Når masken er placeret på siliciumskiven, eksponeres den for en kraftig stråling. Det ueksponerede materiale ætses herefter bort, og tilbage står et kredsmønster. Oven på dette placeres der et lag bestående af ledende materiale, typisk metal. Herved fremkommer en "sandwich" af silicium, oxid og metal, der i kombination kan udgøre en såkaldt bipolær transistor, der er karakteriseret ved enten at kunne lagre et over- eller underskud af elektroner. Gennem passende elektriske påvirkninger kan der opnås enten en forstærkning af et signal (hvilket kendes fra transistorradioer mv.), eller transistoren kan bringes i én blandt flere mulige fysiske tilstande (hvilket giver transistoren sit potentiale som medium for eller forarbejder af digital information). Teknikken kan dog også anvendes til at frembringe andre former for komponenter. Foruden de føromtalte såkaldt aktive komponenter – også kaldet diskreter (dvs. transistorer) – anvendes teknologien til at frembringe passive komponenter (f.eks. spoler, kondensatorer og modstande).

Topografien

Den tredimensionelle sandwich bestående af ledende og halvledende områder, som det således forarbejdede siliciumstykke

udgør, betegnes som chippens topografi, og det er den, HLL beskytter. Ordet kan være svært at associere til det, man ser, når man holder en "chip" (et halvleder*produkt*) i hånden; men det sigter nærmest på det forhold, at chip'en på sit mikroskopiske plan fremtræder med samme tredimensionelle struktur som et landskab. I den amerikanske lov anvendes ordet *mask-work*, hvorved antydes den pointe, at halvlederproduktet i hovedsagen er et produkt af den maske, der bestemmer dets topografi. WIPO's – ikke ikrafttrådte – konvention fra 1989 taler stedse om *layout-design* som synonymt med *topography*.

Indbygningen

Når den nævnte proces er gennemført, placeres det færdige siliciumstykke i en lille plastkasse, hvor det er forsynet med ben, der transmitterer de elektriske impulser til og fra den. Denne sidste del af arbejdet, der efterfølges med aftestning mv., er arbejdsintensiv og udføres ofte adskilt fra arbejdet med at producere selve siliciumskiven.

Masken

Den væsentligste investering i udviklingen af nye halvlederprodukter ligger i at konstruere masken. Hertil anvendes idag avancerede CAD/CAM-systemer kombineret med ekspertsystemteknologi. Den gode chip komprimerer et maksimalt antal aktive komponenter på et minimalt areal, med et minimalt strømforbrug og med optimal funktion. Hertil kræves dels, at de enkelte diskreter er konstrueret, så de giver en optimalt ledende eller halvledende funktion, dels at diskreterne effektivt udnytter den afmålte plads.

Retspolitiske krav

Den maske, der altså optimerer halvlederproduktet, indebærer et innovativt element, som har central betydning for produktets funktion, men som samtidig kan eftergøres for en brøkdel af den omkostning, det har kostet at konstruere det. Op gennem 1970'erne beklagede store dele af den amerikanske chip-industri sig over, at disse værdifulde dele af chipteknologien – således som de først og fremmest blev anvendt i mikroprocessorer – blev plagieret. Efter 8 års forarbejde i nært samarbejde med halvlederindustrien gennemførte USA i 1984 en sui generis beskyttelse for chip-teknologien: *the Semiconductor Chip Protection Act* (SCPA), der i overensstemmelse med industriens ønsker beskyttede maskens design: "A mask-work fixed in a semiconductor chip product". Tanken var ikke at skabe et nyt slags patent, men blot at værne mod den føromtalte totale plagiering af masken. Derfor forbød loven f.eks. ikke reverse engineering.

SCPA

SCPA beskytter kun amerikanske chips. For at tilskynde andre lande til at indføre tilsvarende beskyttelsesformer tilbød USA frivilligt en *midlertidig* beskyttelse af udenlandske chips, jf. nær-

mere *Jukka Liedes* i NIR 1989.401 ff. Tilbuddet var i første omgang tidsbegrænset til 8. november 1987, hvilket i stor hast fremtvang vedtagelsen af EU's rådsdirektiv af 16. december 1986 (87/54/EØF) om retlig beskyttelse af halvlederprodukters topografi – det direktiv, der er grundlaget for den danske lov. Direktivet pålagde medlemsstaterne at indføre beskyttelse for halvlederes topografier senest den 7. november 1987. Forslaget til den danske lov blev fremsat den 14. oktober 1987, og den færdige lov vedtoges allerede den 3. december med ikrafttræden dagen efter bekendtgørelsen, den 10. december 1987. Tilsvarende lovgivning er indført i de øvrige EU-lande samt i de fleste industrialiserede nationer verden over.

Bilateral løsning

Den internationale beskyttelse af halvlederchips er dermed blevet løst på bilateralt plan. Om den beskyttelse, man har opnået i ét land (i hvilken forbindelse EU regnes som ét), også opnås i et andet, beror derfor på lovgivningen i dette andet land. Denne procedure var mulig – og nødvendig – fordi halvledertopografier ikke er rubriceret under et eksisterende internationalt konventionssystem, sml. afsnit 6.1.c. om den ophavsretlige konventionsregulering. Omvendt har ordningen ikke løst verdenssamfundets behov for en global beskyttelse. Et sådant initiativ forelå i 1985, da WIPO fremlagde udkast til en international konvention om beskyttelse af chips. Denne konvention blev dog først færdigbehandlet under et ekspertkomité-møde i Washington D.C. i slutningen af maj 1989, hvor den blev vedtaget *imod* de to væsentligste chip-producenters, USA og Japans, stemmer. Dermed vil konventionen næppe få nogen reel gennemslagskraft. Konventionen er optrykt i *Bryde Andersen* (1991) s. 158 ff. Se for en nærmere redegørelse for de politiske motiver bag denne aparte regulering, *Jon Bing* sst. s. 63 ff. og *Ralph Oman* i NIR 1989.422 ff.

Inden vedtagelsen af EU's halvlederdirektiv i 1986 var spørgsmålet om beskyttelse af halvlederprodukter til drøftelse i Kulturministeriets udvalg til revision af ophavsretslovgivningen. I betænkning 1064/1986, s. 70 ff. anbefalede udvalget, at "mønsteret for et integreret halvlederkredsløb" blev beskyttet som en særlig ophavsretlig værkstype, se forslaget til en ny § 49 a, sst. s. 86. Da rådsdirektivet senere blev vedtaget, var det fortsat genstand for diskussion, om beskyttelsen skulle fremtræde i tilknytning til det ophavsretlige system eller fremstå som en selvstændig lov på linje med de industrielle enerettigheder (patent, varemærke, mønster mv.). Resultatet blev det sidste.

10.4.b. Beskyttelsesobjektet

Efter HLL § 2, stk. 1, kan den, der frembringer en topografi til et halvlederprodukt – eller den, til hvem frembringerens ret er overgået – erhverve eneret til at råde over topografien. Loven indsnævrer dermed sit beskyttelsesområde til at gælde *topografier* i *halvlederprodukter*. Disse to begreber er defineret i HLL § 1, stk. 1 og 2.

Halvleder-produktet

Efter stk. 1 afgrænses et halvlederprodukt som et materiale*legeme* (hele det hus, i hvilken halvlederchippen er indbygget), der indbefatter et lag af halvleder*materiale* (den førnævnte skive af silicium). Dernæst kræves det, at halvlederproduktet fremtræder som den førnævnte sandwich af et eller flere lag af ledende (f.eks. metal), isolerende (f.eks. oxid) eller halvledende (f.eks. silicium) materiale placeret i et forud fastlagt tredimensionelt mønster. Endelig stiller loven det – hverken overraskende eller vel egentlig strengt nødvendige – krav, at halvlederproduktet er beregnet til at udføre en elektronisk *funktion* – udelukkende eller sammen med andre funktioner. Modsat den sædvanlige forståelse af ordet "produkt" (i.e. noget færdigt) omfatter indledningsordene til § 1 også halvlederproduktets slut- og mellemtrin, se tilsvarende SCPA § 901 (a)(1).

Hermed er rammen sat. Halvleder-produktet er det, de fleste vil kalde "chippen" eller "halvlederchippen". Men selv om loven knytter visse retsvirkninger til den – f.eks. i relation til konsumptionsreglerne – er det som nævnt kun et enkelt aspekt af den, der beskyttes: topografien.

Efter lovens § 1, stk. 2, menes hermed den "række sammenhørende *billeder*, der, uanset hvordan de måtte være fikseret eller kodet, *repræsenterer* det tredimensionale mønster af de lag, som halvlederproduktet består af, og i hvilken række hvert enkelt billede repræsenterer en del af eller hele mønstret af en overflade af halvlederproduktet på et hvilket som helst forarbejdningstrin". Der er ikke tale om noget læsevenligt sprog. Definitionen er vanskeligt forståelig uden forudgående kendskab til teknologien i en chip. Meningen er imidlertid klar nok. Det er i kraft af den tredimensionelle struktur, at de enkelte diskreter dannes, og at halvlederproduktet kan udføre sin funktion.

Definitionen stammer fra direktivet, se dettes artikel 1, der dog fremtræder klarere. Ordet bør ikke forveksles med "topologi", der betegner punktstrukturen i et edb-net. I betænkning 1064/1986 havde Kulturministeriets revisionsudvalg som nævnt foreslået det mere

læsevenlige "mønster for et integreret halvlederkredsløb". Som loven definerer begrebet *topografi* dækker dette nogenlunde det samme som SCPA's *mask-work*. Der er dog den forskel, at SCPA alene beskytter det endelige, tredimensionelle mask-*work*, medens halvlederloven også beskytter dele af topografien samt mellemprodukter frembragt i forbindelse med dens konstruktion, se § 1, stk. 2: "på et hvilket som helst forarbejdningstrin".

Som før nævnt giver loven ingen beskyttelse for halvleder-*produktet* som sådant, endsige for den funktion, det udfører. Beskyttelsen gælder kun for det tredimensionelle aspekt, som topografien udgør. Det *tekniske formål* med en halvlederchip er dermed uden betydning for beskyttelsen. Programmerbare chips (PROM's, EPROM's og EEPROM's) har hverken bedre eller ringere beskyttelse end andre. En funktionsbeskyttelse kan i det højeste opnås gennem de patentretlige regler. Selve topografien i en halvlederchip kan ikke beskyttes af ophavsret, jf. ophl. § 10, stk. 2.

Den tredimensionelle struktur er ikke den eneste immaterialretlige form for teknologi, der kan manifestere sig i en halvlederchip. Halvlederchips kan fungere som medium for programmel beskyttet af *ophavsretten*, de kan – og vil ofte – bygge på *patenterbare* teknikker, og de kan rumme den faktiske foranstaltning, der sikrer en *erhvervshemmelighed*, f.eks. ved at etablere en faktisk sikring mod kopiering af den indlæste information.

Navnlig muligheden for at patentere de teknikker, der anvendes ved produktion og anvendelse af halvlederchips, har interesse. Talrige patenter tager sigte på den måde, hvorpå de enkelte diskreter fungerer i chippen. Et meget bredt patent på den basale mikroprocessorteknologi er i august 1990 – efter et 20-årigt tovtrækkeri – udstedt til en privat forsker ved navn *Gilbert P. Hyatt* (U.S. pat.no. 4.942.516). Patentet ville ikke få gyldighed for Danmark, hvor patenttiden (20 år fra ansøgningens indgivelse) for længst er udløbet.

10.4.c. Betingelser for retsbeskyttelsen

Originalitetskrav

Hovedbetingelsen for at opnå halvlederbeskyttelse er, at topografien er "resultatet af frembringerens egen intellektuelle indsats", jf. § 2, stk. 2, og direktivets art. 2, stk. 2. Derudover opstilles et krav om, at topografien ikke må være "almindelig" inden for halvlederindustrien. Består topografien af elementer, der ikke opfylder dette krav, er den kun omfattet, hvis kombinationen af dem opfylder det. Ordene må først og fremmest dække del-elementer, der befinder sig under kravet til halvledertopografiens originalitet, eller overordnede strukturer heraf, der ikke manifesterer no-

gen sådan originalitet. Tanken med halvlederbeskyttelsen er netop ikke at beskytte den "idé", der kommer til udtryk i et halvlederprodukt, jf. herved lovens § 2, stk. 2, 2. pkt., og SCPA § 902(b), men at sikre de omfattende investeringer, der er nødvendige for at producere et unikt halvlederprodukt. Af sammenhængen med lovens § 1, stk. 2, følger tillige, at beskyttelsen kun omfatter topografien i dens konkrete udformning, dvs. rækken af sammenhørende billeder.

At disse krav minder om ophavsrettens originalitetskrav er ikke overraskende, når man ser på lovens rødder i den amerikanske SCPA. Selv om beskyttelsen i formen fremtræder som sui generis, er der ingen tvivl om, at SCPA har flest træk til fælles med ophavsretten, jf. udtrykkeligt Congressional Record, Senate, October 3, 1984, S. 12923 f. I USA er administrationen af SCPA da også henlagt til Copyright Office – ikke (som herhjemme) til patentmyndigheden.

At kravene til halvlederproduktets værkshøjde snarere må læses i de ophavsretlige krav om originalitet, end i patentrettens krav om opfindelseshøjde, harmonerer med, at lovens § 7 udelukker de begreber, fremgangsmåder, systemer, teknikker eller kodede informationer, som er indeholdt i topografien, fra beskyttelse, samt med adgangen til at udføre reverse analysis og reverse engineering, jf. nærmere § 6, stk. 2, nr. 2 og 3. Også det forhold, at man ved direktivets afgrænsning af beskyttelsesobjektet tog højde for den komplementære beskyttelse af forarbejderne til et *mask-work*, der ydes af amerikansk copyright-lovgivning, indicerer, at der må være en grundlæggende strukturlighed mellem de to systemer.

Det afgørende kriterium er derfor, at en topografi kan opnå beskyttelse, hvis den rummer en manifestation, der er så unik, at den i almindelighed ikke kan forventes at få samme indhold, hvis en anden end den oprindelige frembringer (eller – mere praktisk: den pågældende gruppe af frembringere) skulle sætte sig for at gøre noget "lignende". Med den mangfoldighed af valgmuligheder der står åbne for den, der konstruerer en halvledertopografi, skulle det uden for de helt tydelige krænkelsestilfælde i almindelighed ikke give vanskeligheder at opfylde dette originalitetskrav. Er der omvendt tale om, at topografiens udformning dikteres af en speciel elektronisk funktion eller rummer én ud af ganske få foreliggende muligheder for at opfylde denne funktion, vil der ikke være beskyttelse. Et tilsvarende resultat antages i USA, jf. notits fra U.S. Copyright Office (Cirular R 100, Federal Protection for Mask Works).

Praktisk betydning

Da SCPA blev til, regnede man med, at der inden for et par år ville danne sig en praksis, der nærmere afgrænsede lovens betin-

gelser. Men sådan forløb udviklingen ikke. Den plagiering, som industrien havde fremholdt som begrundelse for at få halvlederbeskyttelsen, viste sig ikke at være så aktuel, som man havde overbevist Kongressen om. Den reelle konkurrence mod den amerikanske industri kom fra Japan. Nok analyserede og lærte de japanske konkurrenter af den amerikanske teknik; men så længe de anvendte denne viden til at markedsføre nye halvlederprodukter, der ikke krænkede nogen amerikanske rettigheder, var halvlederbeskyttelsen uanvendelig. Antallet af egentlige chip-pirater var og er derfor begrænset. De grundlæggende nyudviklinger blev søgt patenteret, og ophavsretten dækkede jo under alle omstændigheder det indlæste programmateriale. Dette førte dels til, at kun et fåtal af chip-producenterne valgte at registrere deres topografier, dels til at der ikke udviklede sig nogen praksis om loven.

I Wisconsin Law Review 1990. 241 ff.: "Five years without infringement litigation under the semiconductor chip protection act: unmasking the spectre of chip piracy in an era of diverse and incompatible process technologies", har *Robert L. Risberg, Jr.* en indgående analyse af disse faktorer. Risberg konkluderer, at de mere sofistikerede halvlederprodukter er for dyre at plagiere, og at andre faktorer – bl.a. det forbedrede klima for patentering af IT-relaterede opfindelser – har fjernet behovet for beskyttelse. En artikel (Note) i Utah Law Review 1986.417 betegner SCPA som noget, der måske ikke er andet end "a white elephant", og påpeger, at grundlæggende chips (f.eks. INTEL 8088 og 8086, der udgjorde CPU'en i de på daværende tidspunkt mindste IBM PC'er) ikke er dækket af denne beskyttelse.

Brooktree-sagen

Dette har bl.a. betydet, at der hersker betydelig usikkerhed om lovens rækkevidde. Til dato foreligger der kun en enkelt amerikansk afgørelse herom: *Brooktree Corporation v. Advanced Micro Devices, Inc.,* 705 F.Supp. 491 (1988). Sagen angik topografien til et halvlederprodukt udviklet af den lille chip-producent Brooktree. Produktet styrer farvegrafikken på en IBM PS/2-skærm. I halvlederproduktet – som beklageligvis ikke er nærmere dokumenteret i sagen – indgik en serie celler blandt talrige andre, der besad et særligt mønster. Dette mønster havde sagsøgte, AMD (der er en af verdens største chip-producenter), udviklet ved bl.a. at foretage reverse engineering på Brooktree's topografi. Mønsteret i AMD-cellen, der fremtrådte som nogle kant- og pyramideformede strukturer, var imidlertid blevet raffineret for bl.a. at forbedre strømstyrken, og selv om de pågældende celler gik igen i hele serier og dermed for en ydre betragtning kunne synes at dominere topografien (i følge dommen "approximately

27-35 % of the chip area"), repræsenterede de i sig selv kun en begrænset del af topografiens teknologi.

Under forbudssagen fandt retten det ikke bevist, at AMD's topografi dermed var identisk med Brooktree's. Retten lagde til grund, at den lighed, der bestod mellem kanter og pyramideformer mv. i AMD's topografi, vel ikke var identisk med den, der kunne påvises i Brooktree's, men at en yderligere bearbejdning af cellen formentlig ville have givet den yderligere lighed med Brooktree's topografi, fordi denne repræsenterede en bedre teknisk løsning. Sammenfattende fandt retten ikke, at betingelserne for en injunction var opfyldt. Inden den endelige afgørelse kom for, havde Brooktree fået udstedt to patenter, der dækkede de pågældende teknikker. Den endelige afgørelse er derfor ikke sammenfaldende med afgørelsen i forbudssagen. Den endelige afgørelse blev truffet under medvirken af en jury og faldt ud til fordel for Brooktree, der blev tilkendt en erstatning på 25,6 mio. $.

Selv om der kan være grund til at antage, at forbudsafgørelsen i Brooktree-sagen er korrekt, vil den amerikanske praksis ikke nødvendigvis være udslagsgivende for europæisk ret. Rådsdirektivet om retlig beskyttelse af halvlederprodukters topografi beskytter som tidligere anført ikke helt de samme aspekter af halvlederproduktet. I en europæisk sag vil den endelige afgørelse af spørgsmålet om "originalitet" hhv. "individualitet" henhøre under EF-domstolens jurisdiktion og i givet fald føre til forelæggelse af nationale sager efter EØFT art. 177.

Ansøgningsproceduren

For at opnå beskyttelse efter halvlederloven må rettighedshaveren indgive ansøgning om registrering til Patent- og Varemærkestyrelsen. Denne regel er ikke fremtvunget af Rådsdirektivet om retlig beskyttelse af halvlederprodukters topografi, sml. herved dettes artikel 4, men er indført efter dansk ønske, og det kan i det hele taget diskuteres, om denne lovtekniske løsning er hensigtsmæssig, jf. *Schmidt* i NIR 1989.429 f. og 458 f. Efter HLL § 5, stk. 1, skal ansøgning om registrering indsendes senest 2 år efter den dag, topografien første gang blev "udnyttet erhvervsmæssigt", jf. definitionen heraf i § 3. Udnyttelse i "fortrolig sammenhæng" undtages, for så vidt der ikke sker nogen yderligere distribution til tredjemand. De formelle regler for registreringssagens behandling fremgår af bekendtgørelse nr. 482 af 10. juni 2003 angående ansøgninger om beskyttelse af halvlederprodukters udformning (topografi).

Hemmeligholdelse?

Når man skal vurdere det hensigtsmæssige i at tage skridt til halvlederregistrering, må risikoen for at afgive forretningshemmeligheder til omverdenen gennem registreringsproceduren tages i betragtning. I patentretten er denne risiko afbalanceret med

den stærke (og længerevarende) eneret til selve idégrundlaget, som patentet indebærer. Men med halvlederrettens mere begrænsede rækkevidde får hensynet aktualitet.

Problemstillingen er udførligt reguleret i bekendtgørelsens §§ 6, 8 og 9. Efter § 8 skal det materiale, der ledsager registreringsansøgningen til identifikation eller anskueliggørelse af topografien, jf. § 6, holdes utilgængeligt for offentligheden, hvis ansøgeren *erklærer* det som en forretningshemmelighed. Man kan dog højst erklære halvdelen af det samlede antal lag som forretningshemmelighed. Men da ansøgeren selv har kontrol med, hvilke lag der erklæres hemmelige, rummer dette en faktisk sikring. Dernæst kan Patent- og Varemærkestyrelsen iflg. § 9 på begæring bestemme, at et dokument eller andet indleveret materiale, som indeholder forretningshemmeligheder, som ikke er nødvendige til identifikation eller anskueliggørelse af topografien eller til fastlæggelse af tidspunktet for den første erhvervsmæssige udnyttelse, helt eller delvis skal være utilgængeligt for offentligheden.

Prøvelse?

Som det herved vil være antydet, er ansøgningssagen begrænset til en undersøgelse af, om lovens formelle krav for erhvervelse af eneretten til en topografi er opfyldt. Registreringen er i hovedsagen ordensmæssig. Styrelsen skal navnlig ikke foretage nogen nærmere undersøgelse af topografien. Udfaldet af registreringen indicerer for så vidt alene, at retten gøres gældende, og af hvem. En materiel prøvelse kommer først på tale, hvis der senere rejses indsigelse mod en registrering.

Ophævelse

Efter lovens § 10 skal styrelsen (på begæring) ophæve registreringen af en topografi, hvis det godtgøres, at lovens materielle og formelle betingelser ikke er opfyldt, eller hvis nogen gør gældende, at en stedfunden registrering strider mod hans ret. Lovens § 11 forudsætter, at den sidstnævnte situation kan foreligge så klart, at det må anses "godtgjort", at der består en bedre ret. Er dette tilfældet, skal Direktoratet efter anmodning overføre registreringsansøgningen til den berettigede. Efter bestemmelsens andet stk. kan direktoratet dog også henskyde spørgsmålet til afgørelse ved dom. Direktoratets afgørelser kan påklages efter reglerne i lovens kapitel 5.

10.4.d. Beskyttelsens indhold

Efter HLL § 6, stk. 1, nr. 1, indebærer eneretten til en topografi først og fremmest beskyttelse mod eftergørelse af *topografien*. Her og i de efterfølgende bestemmelser anses eftergørelse af to-

pografien – naturligt nok – også at foreligge ved fremstilling af halvlederprodukter ved hjælp af den. HLL § 6, stk. 1, nr. 2, forbyder dernæst erhvervsmæssig udnyttelse af topografien. Herved forstås ifølge § 3 udbud, salg, leje, leasing eller anden erhvervsmæssig distribution af topografien eller af et halvlederprodukt, der er fremstillet ved hjælp af den. Udnyttelse, der sker i fortrolig sammenhæng (f.eks. efter indgået hemmeligholdelsesaftale), anses ikke som erhvervsmæssig udnyttelse, for så vidt der ikke sker nogen yderligere distribution til tredjemand, se nærmere § 3, stk. 2. Endelig forbyder HLL § 6, stk. 1, nr. 3, erhvervsmæssig import (men derimod ikke privat).

Efter HLL § 6, stk. 2, begrænses eneretten i tre forskellige relationer.

Konsumption

For det første undtages den erhvervsmæssige udnyttelse, der sker, når topografien eller et halvlederprodukt, der er fremstillet ved hjælp af den, er bragt i omsætning i et EU-land. Denne regel om enerettens konsumption svarer i sin struktur til, hvad der gælder i relation til ophavs- og patentrettigheder: Den rettighedshaver, der lægger sit produkt ud i den almindelige omsætning, må leve med, at senere erhververe i omsætningen gør med det, hvad de vil, blot de ikke genskaber produktet. Til forskel fra vore nationale konsumptionsregler gælder konsumptionen for samtlige EU-lande. Et halvlederprodukt, der bringes på markedet i Tyskland, kan således opkøbes og distribueres videre i Danmark.

Reverse analysis

Efter lovens § 6, stk. 2, 2. pkt., er "eftergørelse, som sker med henblik på analyse og vurdering af eller undervisning i selve topografien eller de begreber, processer, systemer eller teknikker, der er indeholdt i topografien" undtaget fra eneretten. Når bestemmelsen bruger ordet "eftergørelse", tænkes alene på den genskabelse af topografien, der finder sted ved undersøgelseshandlingen. Ganske som edb-programmer kun kan "læses" ved at blive kopieret til en RAM, kan en halvleders topografi kun undersøges, hvis den kopieres op i et format, som man kan håndtere. Det er den heri liggende eftergørelse, den såkaldte *reverse analysis*, der hjemles ved bestemmelsen. Halvlederbeskyttelsen giver her et svagere værn end den ophavsretlige beskyttelse af edb-programmer, jf. nærmere reglerne om dekompilering i ophl. § 37. I bemærkningerne til lovforslaget, der også her bygger på de amerikanske lovforarbejder, begrundes dette med den praksis, branchen allerede havde affundet sig med.

Reverse engineering

Den tredje undtagelse fra eneretten angår bearbejdelser af en topografi, lovens § 6, stk. 2, 3. pkt. Bestemmelsen er vanskeligt forståelig. Den undtager fra eneretten "handlinger i forbindelse

med frembringelse af en topografi, der opfylder betingelsen i § 2, stk. 2, og som er frembragt på grundlag af en analyse og vurdering af en anden topografi". Der er tale om en omskrivning af artikel 5, stk. 4, i EU-direktivet om retlig beskyttelse af halvlederprodukters topografi. Men hvor direktivet rettede sig mod "handlinger i forbindelse med en topografi", hvilket sigtede mod den nye topografi, har man formuleret lovteksten som "handlinger i forbindelse med *frembringelse* af en topografi", underforstået den gamle. Dermed er nr. 3) blevet sammenfaldende med nr. 2). Meningen må være at hidføre et resultat svarende til SCPA § 906(a)(2), hvorefter en person, der har udført lovlig reverse analysis, har ret til at "incorporate the result of such conduct in an original *mask-work* which is made to be distributed". Det er med andre ord *reverse engineering*, der hermed – som det også angives i bestemmelsens forarbejder – gives hjemmel for.

Med denne forståelse kan man se, at halvlederloven også på dette punkt har overført en problemstilling, der er velkendt fra ophavsretten; sondringen mellem bearbejdelser af ophavsretligt beskyttede værker (ophl. § 4, stk. 1) og fri benyttelse (samme bestemmelses stk. 2). HLL § 6, stk. 2, nr. 3) må naturligt læses i sammenhæng med nr. 2) om reverse analysis; har man ved studiet af en eksisterende og retsbeskyttet topografi opdaget et hensigtsmæssigt teknisk princip, da har man ret til at anvende dette princip i forbindelse med frembringelsen af et værk, som man efter de herfor gældende regler kan demonstrere værkshøjde til.

Varighed

Halvlederbeskyttelsen er gældende i en periode på 10 år regnet fra udgangen af det kalenderår, hvor ansøgning blev indgivet eller produktet første gang markedsførtes, HLL § 5, stk. 3, jf. stk. 2. Samme regel gælder ifølge SCPA, jf. dennes § 904. Dog rummer halvlederloven en absolut tidsgrænse på 15 år fra det tidspunkt, topografien første gang blev fikseret eller kodet, uden at registreringsansøgning er indleveret. Denne regel genfindes ikke i den amerikanske lov.

Område

Som følge af halvlederlovens EU-retlige udspring er halvlederrettens geografiske beskyttelse afgrænset i relation til EU. Ifølge lovens § 4 kan retten erhverves af en fysisk eller juridisk person, der er statsborger eller har bopæl i en medlemsstat, når den pågældende har frembragt topografien eller ladet den frembringe i kraft af et ansættelsesforhold, se nærmere stk. 1, nr. 1-2. Bopælskravet forudsætter en vis tættere tilknytning til EU. Bemærkningerne til lovforslaget advarer mod omgåelsesforsøg gennem "pro forma tilknytning til EU". Ligeledes kan eneretten erhverves ved aftale eller succession (f.eks. arv eller virksomhedsoverdragelse), se herom stk. 1, nr. 3-4. Efter samme bestem-

melses andet stk. kan Erhvervsministeren udvide denne beskyttelse ved at etablere bilaterale aftaler om gensidig beskyttelse.

Ved bekendtgørelse nr. 1274 af 18. december 1996 er denne regel knyttet til overenskomsten om oprettelse af WTO, således at beskyttelsen gælder for *fysiske personer*, som er statsborgere i en WTO-medlemsstat eller som har bopæl på dettes område, eller *juridiske personer* (eller fysiske personer), der har et reelt og fungerende anlæg til frembringelse af topografier eller fremstilling af integrerede kredsløb på det område, som hører ind under et medlem af overenskomsten om oprettelse af WTO. Det samme gælder for juridiske og fysiske personer, der er statsborgere i, eller (for så vidt angår juridiske personer) har en regulær industri- eller erhvervsvirksomhed i, et af de særlige lande og territorier, der er angivet i det til bekendtgørelsen hørende bilag.

10.4.e. Udnyttelse og håndhævelse

Licens

Som andre immaterielle enerettigheder kan eneretten til en topografi overdrages til andre. Halvlederloven forudsætter, at dette enten sker fuldstændigt, jf. reglerne i § 4, eller delvis, jf. § 6. Adgangen til at give licens er i loven formuleret som en mulighed for rettighedshaveren til at give "samtykke" til udnyttelse, jf. § 6. Et sådant – begrænset – samtykke (licens) kan fastsættes efter parternes ønsker, men med respekt af EU's konkurrenceregler. Det kan f.eks. begrænses i henseende til tid og rum og, hvad der nok vil være mest praktisk, i relation til specifikke teknologiformer.

Retsoverdragelse

Den fuldstændige rettighedsoverdragelse er i § 4, stk. 1, nr. 3, formuleret således, at rettighedserhververen opnår "eneret til at udnytte topografien erhvervsmæssigt overalt i Fællesskaberne". For at en sådan eneret kan indtræde, må den første erhvervsmæssige udnyttelse være sket i en medlemsstat. Dette umiddelbart vanskeligt forståelige krav skyldes ifølge bemærkningerne til lovforslaget et ønske om at "understrege" tilknytningen til EU. Kravet får den praktiske konsekvens, at halvlederprodukter, der er udviklet i et EU-land, og som ønskes beskyttet af EU's eneretsregler, også markedsmæssigt må "fødes" i et EU-land. Dette modvirker, at en tysk chip-producent overdrager eneretten til en topografi med henblik på første-udgivelse i USA. Også reglen i HLL § 4, stk. 1, nr. 2, implicerer realt en fuldstændig rettighedsoverdragelse. Herefter overgår den ansatte topografi-udviklers rettigheder over topografien til arbejdsgiveren, medmindre andet må anses for aftalt.

Tvangslicens

Ifølge HLL § 13, der har hjemmel i § 6 i direktivet, kan Sø- og Handelsretten efter begæring meddele tredjemand tvangslicens til at udføre de handlinger, der er nævnt i lovens § 6, stk. 1. Dermed kan den, der som følge af halvleder-rettigheder ellers var forhindret heri, få ret til at eftergøre, udnytte og importere en i øvrigt retsbeskyttet topografi. De nærmere vilkår herfor, herunder størrelsen af det beløb, der skal betales, fastslås af retten. For at udstede en sådan tvangslicens kræver bestemmelsen, at det halvlederprodukt, hvori topografien findes, ikke udbydes "i rimeligt omfang" af rettighedshaveren "trods tilbud om passende vederlag".

På grund af adgangen til at foretage reverse engineering og med halvlederlovens manglende beskyttelse af idégrundlaget i en topografi kan det ikke ventes, at disse regler får nogen praktisk betydning. Ifølge lovbemærkningerne er de begrundet med, at visse halvlederprodukter er så specialiserede og har en så central rolle i gennemførelsen af væsentlige samfundsinteresser, at rettighedshaverens interesse i eventuelt at kunne forbyde anvendelsen af det pågældende halvlederprodukt langt fra kan opveje de samfundsmæssige konsekvenser heraf. Tilsvarende regler om tvangslicens har man allerede i patentloven. Heller ikke disse regler hverken påberåbes eller anvendes særligt ofte. Tvangslicensreglen sættes i øvrigt først i kraft ved industriministerens bestemmelse.

Når halvlederretten overgår til en anden – herunder ved tvangslicens, indføres der meddelelse herom i registeret, se HLL § 8.

Erstatning

HLL kapitel 4 giver særlige regler om erstatning og strafansvar for krænkelse af de rettigheder, loven hjemler. Efter lovens § 14, stk. 1, udmåles erstatningskrav dels som vederlagskrav, dels som skadeserstatning. Dernæst kan det ved dom bestemmes, at eksemplarer af en topografi eller et halvlederprodukt skal ændres på nærmere angivet måde, tilintetgøres eller udleveres til den forurettede. Beslutningen herom kan eventuelt kombineres med pligt til at betale vederlag. Når ganske særlige grunde foreligger, kan retten efter påstand meddele krænkeren tilladelse til fortsat at råde over sådanne eksemplarer eller produkter i resten af eneretens gyldighedstid.

Straf

Strafansvaret for overtrædelse af lovens § 6 (eneretten til topografien) er fastsat til bøde, medmindre højere straf er forskyldt efter anden lovgivning, hvorved navnlig sigtes til strafansvaret i andre immaterialretlige love, f.eks. ophavsretsloven, brugsmodelloven, patentloven og markedsføringsloven. Som det gælder for andre lignende eneretsregler, er der gjort undtagelse for visse tilfælde, hvor en krænkelse sker i *god tro*. For det første fastslår lovens § 11, stk. 4, at udnyttelsen af en topografi, der viser sig

uretmæssig, fordi "rettighedshaveren" får frakendt registreringen, kan fortsætte, hvis der svares rimeligt vederlag til rettighedshaveren. Herudover undtager HLL § 6, stk. 3, den person, der har erhvervet et halvlederprodukt uden at vide eller have grund til at formode, at det indeholder en beskyttet topografi. Denne ret omfatter også den godtroende *erhvervsmæsssige* brug. Til gengæld bestemmer § 6 – ligesom § 11 – at den fortsatte udnyttelse skal finde sted "på rimelige vilkår, der aftales mellem parterne".

10.4.f. Rettighedssubjektet

HLL § 4 indeholder en bestemmelse om medarbejderes rettigheder til en topografi, hvoraf det fremgår, at en erhvervsvirksomhed opnår eneretten til en topografi, "når topografien er frembragt af en person, der er ansat hos den pågældende [virksomhed] eller frembragt på bestilling af denne, medmindre det er eller må anses for aftalt, at eneretten tilkommer frembringeren". Bestemmelsen fører til, at topografi-rettigheden opstår *originært* hos arbejdsgiveren. Den "overgår" med andre ord ikke, som efter ophl. § 59.

Reglen har baggrund i direktivet, der giver medlemsstaterne ret – men ikke pligt – til at fastsætte sådanne regler. Den svarer til SCPA § 903 (b), jf. § 901 (6), der bygger på den amerikanske work for hire-doktrin. Da industriministeren valgte at gøre brug af denne mulighed i den danske lov, skete det på den baggrund, at topografier, der udvikles i en virksomhed af virksomhedens ansatte, almindeligvis frembringes på virksomhedens foranledning og bekostning og som led i dennes virksomhedsområde. Som det gælder efter ophl. § 59, kan lovens udgangspunkt fraviges ved aftale.

10.5. Erhvervshemmelighedsbeskyttelse

10.5.a. Problemstillingen

Den mest omfattende eneret til en informationsmængde får man ved at holde sin hemmelighed tæt på kroppen. Total hemmeligholdelse er et sjældent set fænomen, men findes. I de fleste tilfælde er man nødt til at dele sin hemmelighed med andre, det være sig ansatte, forretningsparter eller rådgivere. Hver gang dette sker, udvides kredsen af personer, der potentielt kan røbe hemmeligheden.

Begreb

En erhvervshemmelighed er en oplysning om en erhvervsvirksomheds driftsmæssige (herunder teknologiske og økonomiske) forhold, som virksomheden effektivt søger at hemmeligholde overfor omverdenen. Retssystemet beskytter på forskellige måder den part, der vælger at hemmeligholde en erhvervshemmelighed for kun at dele den med aftaleparter, som på forhånd påtager sig en forpligtelse til at gøre det samme.

- Mfl. § 10

Den bredeste beskyttelse heraf findes i mfl. § 10. Bestemmelsen omtales straks nedenfor. Bestemmelsen ledsages af en strafferetlig hjemmel, jf. mfl. § 22, stk. 4, der hjemler straf med bøde, hæfte eller fængsel indtil 1 år og 6 måneder, medmindre højere straf er forskyldt efter strfl. § 299 a. Påtale finder kun sted efter den forurettedes begæring. Strfl. § 299a, der er indsat efter forslaget i betænkning 1417/2002 om IT-kriminalitet, giver hjemmel for straf med fængsel indtil 6 år til den, der under særligt skærpende omstændigheder gør sig skyldig i overtrædelse af mfl. § 10. Som særligt skærpende omstændigheder anses navnlig tilfælde, hvor handlingen har medført betydelig skade eller der er fremkaldt nærliggende fare herfor.

- PL § 2, stk. 5

En vis yderligere regulering af aftaleretlige forpligtelser til at hemmeligholde erhvervshemmeligheder følger af PL § 2, stk. 5, nr. 1: Sker der i en periode på 6 måneder før ansøgningen nyhedsskadelig offentliggørelse af oplysninger om den opfindelse, der ligger til grund for en patentansøgning, kan der ifølge denne bestemmelse bortses herfra, når dette er en følge af "et åbenbart misbrug i forhold til ansøgeren eller nogen, fra hvem hans ret hidrører". Det pågældende misbrug kan f.eks. udspringe af et tjeneste- eller samarbejdsforhold, herunder ved brud på en hemmeligholdelsesaftale.

- HLL

I visse tilfælde understøtter lovgivningen en parts ønske om at holde information hemmelig. Inden for halvlederindustrien er det således almindeligt at forlade sig på aftalt beskyttelse, se nærmere *Risberg* i 1990 Wisconsin L.R. 241, s. 269 ff. Ifølge HLL § 5, stk. 1, er der mulighed for at udskyde registreringen af en topografi indtil 2 år efter den dag, topografien første gang blev udnyttet erhvervsmæssigt. I dette tilfælde er hemmeligholdelse praktikabel, fordi den kun skal effektueres i et afgrænset tidsrum. Dernæst giver §§ 6, 8 og 9 i halvlederbekendtgørelsen ansøgeren mulighed for at forlange dele af en ansøgning herom hemmeligholdt.

10.5.b. Mfl. § 10

Ifølge mfl. § 10 må den, der er i tjeneste eller samarbejdsforhold til en virksomhed eller udfører et hverv for denne, ikke på utilbørlig måde skaffe sig eller forsøge at skaffe sig kendskab til eller rådighed over virksomhedens erhvervshemmeligheder. Er man kommet til kendskab om, eller har man fået rådighed over sådanne hemmeligheder på retmæssig måde, må man ikke ubeføjet viderebringe eller benytte dem.

Beskyttelsen indebærer, at den berettigede på grundlag af § 10 kan få *fogedforbud* nedlagt mod en brug af de pågældende hemmeligheder, som tredjemand måtte effektuere i konsekvens af, at de pågældende oplysninger er blevet kompromitteret i strid med aftalens klausuler. Overtrædelse af et fogedforbud er strafbar, jf. rpl. § 651, stk. 1. Det forbud, der følger af § 10, er tillige *strafsanktioneret* i en periode på 3 år efter tjenesteforholdets, samarbejdsforholdets eller hvervets ophør, jf. mfl. § 22, stk. 4, og bemærkningerne hertil straks ovenfor. Inden for denne periode straffes erhvervsdrivende, der har fået kendskab til eller rådighed over en erhvervshemmelighed i strid med de førnævnte bestemmelser, og som ubeføjet viderebringer eller benytter den. Det civilretlige forbud mod uberettiget brug af erhvervshemmeligheder vedvarer uden denne tidsbegrænsning.

Fordelen ved at gøre brug af en aftalt beskyttelse består i, at beskyttelsen opnås uden formalia, og at den – modsat f.eks. patentet – kan effektuere en total hemmeligholdelse. Til gengæld fører den ikke til nogen *ene*ret. For det første er den berettigede ikke sikret mod, at udenforstående helt uafhængigt finder frem til genstanden for den aftalte fortrolighed. For det andet – og væsentligere – vil en aftalt fortrolighed med de begrænsninger, der følger af markedsføringslovens regler, jf. straks nedenfor, kun binde aftalens parter.

Beskyttelsen af erhvervshemmeligheder beror primært på, hvad der må anses som fortroligt i medfør af det pågældende kontraktsforhold. I samme omfang, som kontraktsforholdet udpeger forskellige oplysninger som mere eller mindre offentligt tilgængelige (eller i øvrigt forudsætter en sådan tilgængelighed), vil det ofte også anse andre for at være fortrolige og dermed henhørende til opdrags- eller arbejdsgiverens interne sfære.

Denne begrænsning er væsentlig, da den gælder sideløbende med den rettighedsoverførelse, der i øvrigt kan finde sted i medfør af kontraktsforholdet. Dette kan få praktisk betydning i aftaleforhold, hvor en konsulent skal udvikle et program. Selv om

aftalen måtte føre til, at konsulenten har eneret til en given udnyttelse, er konsulenten ikke nødvendigvis berettiget til at benytte den viden, han har om det, på en måde, der vil være konkurrencemæssigt skadelig for kunden. Dette vil f.eks. være aktuelt i relation til viden om markedsmuligheder og kundekrav mv.

10.5.c. Praktiske anvendelsesformer

Aftalens funktion

Vejen til en beskyttelse efter reglerne om erhvervshemmeligheder går gennem en aftale, der præcist angiver, hvad der skal betragtes som hemmeligt, og under hvilke omstændigheder. For en nærmere gennemgang af disse problemer henvises til *ET* s. 397 ff., der sondrer mellem *forudgående* hemmeligholdelsesaftaler (som indgås forud for etableringen af et aftaleforhold og uden nødvendig sammenhæng med dettes faktiske etablering), *oprindelige* hemmeligholdelsesaftaler (som indgås samtidigt med aftaleforholdet, typisk som en klausul heri) og *efterfølgende* hemmeligholdelsesaftaler (der indgås under et aftaleforhold, f.eks. samtidig med at den pågældende hemmelighed åbenbares).

Aftaleindgåelsen

Navnlig i relation til de forudgående hemmeligholdelsesaftaler kan der opstå et problem i, at den part, der pålægges hemmeligholdelsespligten, ikke nødvendigvis ved, hvad han nu forpligter sig til: Det kan jo tænkes, at han i forvejen kender til den information, som modparten anser for hemmelig. Dette problem gør sig dog primært gældende i relation til information, der indeholder mere generelle anvisninger (f.eks. for et forretningskoncept eller et enkelt led i en større – men kendt – procedure). Løsningen på problemet kan *enten* ligge i, at aftalen herom indgås i flere tempi, således at parterne gradvis kan indkredse karakteren af den pågældende hemmelighed, for på den måde at minimere risikoen for uforudsete og for vidtgående pligter vedrørende information, der viser sig "fælles", *eller* ved brugen af troværdige tredjeparter, der på forhånd tager stilling til, om der består et sådant – ukendt – fællesskab.

- koncepter mv.

Viser en sådan indledende sondring, at der er grundlag for at indgå en aftale om hemmeligholdelse af de pågældende tekniske og forretningsmæssige koncepter mv., giver en hemmeligholdelsesaftale mulighed for dels at opnå en i princippet uendelig beskyttelse (idet beskyttelsen først tabes, når hemmeligheden ikke længere værnes effektivt), dels at opnå denne beskyttelse på et tidligt tidspunkt. Navnlig den sidste effekt kan have betydning på de tidligere stadier af et IT-produkt, der forventes undergivet en innovativ udviklingsproces. En sådan aftale bør nærmere præci-

sere undladelsespligten og de betingelser, der effektuerer dens ophør mv. (herunder i forbindelse med en eventuel efterfølgende patentprocedure).

- licensaftaler

Et andet praktisk område for hemmeligholdelsesaftalen er licensaftaler vedrørende programmel, der installeres hos udvalgte kunder (og ikke gennem eksemplarfremstillinger, der spredes i den almindelige handel). Ved at pålægge en licenstager en pligt til ikke at give andre parter oplysning om, hvorledes *grænsefladen* på det licenserede program fungerer, vil rettighedshaveren til det pågældende program kunne opnå en *de facto* beskyttelse af denne grænseflade, der går videre end han ville have kunnet opnå gennem ophavsretlige regler (der forudsætter originalitet mv.) eller gennem andre beskyttelsessystemer.

Gyldigheden af sådanne aftaler kan give anledning til tvivlsspørgsmål i relation til ophl. § 37, stk. 3, der gør brugerens ret til at udføre reverse engineering af edb-programmer præceptiv. Spørgsmålet er, om en aftale, der pålægger licenstageren at hemmeligholde programmet, dermed er i strid med brugerens ret i medfør af ophl. § 37, stk. 2, nr. 2, til at videregive oplysninger indhentet i forbindelse med brugen, til tredjemand. Spørgsmålet drøftes i afsnit 7.4.g.

- ansættelsesforhold

En hemmeligholdelsesforpligtelse kan også optræde implicit. Har man i aftale eller ansættelsesforhold etableret en varig tilknytning til en anden part, følger heraf visse forpligtelser til at optræde loyalt. Dette indebærer bl.a., at man ikke må røbe erhvervshemmeligheder mv. til tredjemand, end ikke efter retsforholdets afslutning. Oplysninger, der må anses almindeligt tilgængelige, kan derimod frit anvendes.

Supplerende litteratur

Retsstillingen i dansk ret om *patentering af edb-programmer* må i vidt omfang udledes på komparativt grundlag. Den grundigste fremstilling heraf er af ældre dato. Den findes hos *H. W. A. M. Hanneman*: The patentability of computer software – an international guide to the protection of computer-related inventions. Kluwer, 1985. Se også *Per Håkon Schmidt* (1989), der behandler patentspørgsmålene på s. 268 ff. USPTO, EPO og det japanske patentkontor har i ICC 1990.817 ff. offentliggjort en rapport om "Patentability of computer-related inventions", der sammenstiller de tre patentkontorers praksis. Fra den intense debat om patentsystemets betimelighed på området for softwareopfindelser henvises til *Steven W. Lundberg m.fl.*: Twelve myths about patent protection for software, 5 Computer Lawyer (May 1988), s. 9 ff. Se også *Robert J. Hart* i ICLA (August 1989), s. 7 ff. om EPO-praksis' forhold til engelsk patentret. På hjemmesiden <www.softwarepatenter.dk>, der

drives af IT-politisk forening, finder man dernæst en kvalificeret samling af tekniske, retspolitiske og patentretlige synspunkter i debatten for og imod patentering af edb-programmel.

Problemerne vedrørende *halvlederbeskyttelsen* er herhjemme behandlet af *Per Håkon Schmidt* i U1988B.405 og i disputatsen Teknologi og immaterialret (1989), s. 316 ff. og af *Peter Blume* i Retsbeskyttelse af edb (1989), s. 87 ff. Se ligeledes indlæggene i NIR 1989, s. 401-461 fra det 20. nordiske møde for industriel retsbeskyttelse (august 1989). Washington-konventionen om beskyttelse af integrerede kredse, der er optrykt i *Bryde Andersen* (1991), s. 158 ff., er bl.a. kommenteret af *Jon Bing*, sst. s. 63 ff.

Kapitel 11.
KENDETEGNSBESKYTTELSE MV.

11.1. Varemærkeret

11.1.a. Almindelige regler

Oversigt

Når produkter markedsføres på det almindelige marked, sker det almindeligvis under navne eller varemærker, der knytter forbrugernes associationer om produktet til den pågældende producent. Som hovedregel vil producenten kunne gøre rettigheder gældende over sådanne navne og forretningskendetegn efter parallelle regelsæt. Efter reglerne i *varemærkeloven* kan der opnås en særlig varemærkeret til "særlige kendetegn for varer og tjenesteydelser, som benyttes, eller agtes benyttet i en erhvervsvirksomhed", jf. vml. § 1. Herudover kan der opnås en vis kendetegnsbeskyttelse efter de særlige regler i *markedsføringsloven*, *lov om erhvervsdrivende virksomheder* (§ 6) og – efter omstændighederne – *navneloven*. Denne beskyttelse giver i almindelighed ikke anledning til særlige problemer på IT-området, hvorfor der i hovedsagen kan henvises til de almindelige fremstillinger, herunder navnlig *Koktvedgaard* (2005), kap. VI. I det følgende omtales derfor kun et par varemærkeretlige spørgsmål, der kan give grundlag for opmærksomhed på IT-området.

Ved rådets forordning nr. 40/94 af 20. december 1993 er der indført regler om EU-varemærker, se EFT 1994 L 11/1. Varemærket efter disse regler erhverves gennem registrering i et særligt europæisk Harmoniseringskontor, beliggende i Alicante, Spanien. Også for en nærmere behandling af disse regler henvises til de almindelige fremstillinger.

Krav til mærket

Ifølge vml. § 1 kan et varemærke bestå af alle arter tegn, der er egnet til at adskille en virksomheds varer eller tjenesteydelser fra andre virksomheder. Der gælder dernæst et krav om *særpræg*, jf. lovens § 3, stk. 3, og § 13, stk. 1. Man kan følgelig ikke registrere "computer" som varemærke for IT-udstyr. Ifølge loven er det dernæst en forudsætning, at varemærket kan gengives grafisk; men bestemmelsen antages ikke at være udtømmende. Foruden

lyde kan også hologrammer beskyttes efter reglerne om varemærker, jf. *Wallberg* i NIR 1997.191 f. om nyere administrativ praksis for lydmærker og *Henrik Villumsen*s kommentar i NIR 1998.709 f. Gennem denne beskyttelse kan en producent f.eks. opnå eneret for de signaler – f.eks. en fanfare – der afgives under opstarten af visse programmer, og som for andre, der "lytter med" (f.eks. i et fly), kan indebære en kommercielt vigtig cementering af produktets dominans på et marked.

- tal-kombinationer

Varemærkebeskyttelsen dækker ifølge vml. § 1 "særlige kendetegn for varer eller tjenesteydelser, som benyttes eller agtes benyttet i erhvervsvirksomhed". Alle arter af tegn kan principielt blive genstand for varemærket, jf. nærmere § 2. De tal-betegnelser, der tidligere anvendtes for visse processorer (f.eks. INTEL's "8088"- og "80386" serier), kan dog kun opnå beskyttelse, hvis der foreligger det fornødne særpræg mv., hvilket forekommer for visse særligt indarbejdede IT-produkter, se *Koktvedgaard* (2005), s. 355 f., *U 2003.1020 H* og om Patentdirektoratets praksis, *Wallberg* i NIR 1997.190 f.

- udstyr

Der kan også gives varemærkebeskyttelse for varens form, udstyr eller emballage, lovens § 2, stk. 1, nr. 4. I IT-sammenhæng kan dette begrunde en beskyttelse for animerede varemærker, f.eks. et flag, der blafrer i vinden, eller en figur, der bevæger sig. Derimod kan der ikke erhverves varemærket til en udformning af varen, som er nødvendig for at opnå et *teknisk resultat*.

Retserhvervelsen

Varemærketten opstår enten gennem *registrering*, jf. § 3, stk. 1, nr. 1, eller ved den blotte *ibrugtagning*, jf. § 3, stk. 1, nr. 2 og stk. 2. Beskyttelsen gælder i givet fald kun inden for den pågældende kategori af varer, afgrænset for de registrerede varemærkers vedkommende efter et antal vareklasser. Som udgangspunkt er retsvirkningerne af de to former for retserhvervelse identiske, men på en række punkter er der forskelle. Når en varemærket er opnået gennem ibrugtagning, hviler bevisbyrden for, at retten eksisterer, som udgangspunkt på rettighedshaveren. Denne skal dels bevise, *hvornår* mærket er taget i brug og *for hvilke* varer eller tjenester. Dertil kommer, at de særlige regler, der giver mærkeindehaveren mulighed for at beslaglægge varemærkeforfalskede varer i forbindelse med import forudsætter, at mærket er registreret, jf. herom senere.

Brugspligt

Omvendt indebærer en registrering, at mærkeindehaveren er undergivet en vis pligt til at benytte mærket. Har indehaveren af et registreret varemærke ikke gjort "reel brug" af mærket, eller af ligeartede mærker (jf. nærmere stk. 2) her i landet i en periode på 5 år fra registreringsprocedurens afslutning for de varer og tjene-

steydelser, som mærket er registreret for, kan registreringen ophæves efter reglerne i lovens § 28. Det samme gælder, hvis brugen har været ophørt uden afbrydelser i 5 år. Ophævelse af en registreret varemærkeret kan ske ved dom eller administrativt, jf. nærmere §§ 29-30.

Registrering

Registrering foretages enten i Patent- og Varemærkestyrelsen i overensstemmelse med reglerne i vml. kap. 2 og de bekendtgørelser, der er udstedt i medfør af lovens § 48, eller ved den europæiske varemærkemyndighed. Direktoratet fører et varemærkeregister, hvor registreringerne offentliggøres, jf. § 12, stk. 3. Registrering kan dog ikke ske, hvis mærket er identisk eller forvekslelig med et ældre varemærke og de varer og tjenesteydelser, for hvilke mærket søges registreret, er af samme art som de varer eller tjenesteydelser, for hvilke det ældre mærke er beskyttet, jf. § 15, stk. 1. Som grundlag for vurderingen af, hvilke "varer og tjenesteydelser", der danner rammen for en sådan identitet eller forvekslingsrisiko, er etableret et system af vare- og tjenesteydelsesklasser, jf. nærmere vml. § 17 og bilaget til bekendtgørelse nr. 787 af 9. september 2003, med senere ændringer om ansøgning og registrering af varemærker og fællesmærker.

Funktioner

Varemærkerettens betydning for den almindelige markedsføring er åbenbar. Sikkerheden for, at et givet mærke associeres til virksomhedens egne varer og tjenester, begrunder de kostbare investeringer i markedsføring af "mærkevarer". Varemærkeretten indebærer dog også yderligere fordele. At en varemærkeret bl.a. giver sin indehaver ret til at forbyde erhvervsmæssig brug af tegn, der er identiske med, eller som ligner, varemærket, indebærer, at varemærkeretten kan anvendes til at understøtte retshåndhævelsen af produkter, der er genstand for systematisk plagiering eller piratkopiering. Når standardprogrammel kopieres ulovligt, indebærer dette således også en kopiering af programmets navn og varemærke. Den organiserede piratkopiering vil derfor indebære en krænkelse af de forskellige navne- og varemærkeregler. Da den ophavsretlige krænkelse, der sker ved kopieringen af programvaren, dog repræsenterer det mest indgribende retsbrud, vil det almindeligvis være denne rettighedsform, rettighedshaveren vil forfølge stærkest. Men det forhold, at der *også* sker en varemærkekrænkelse, kan have betydning i henseende til regelsæt, der knytter særligt an til disse regler.

Et eksempel herpå er den fremgangsmåde, rettighedshaveren kan gøre brug af i medfør af forordning 3295/94, EFT 1994 L 341/8 om foranstaltninger med henblik på at forbyde overgang til fri omsætning mv. af varemærkeforfalskede og piratkopierede varer. Forordningen giver toldmyndighederne ret til at gribe umiddelbart ind

over for varer, der mistænkes for at være piratkopierede eller varemærkeforfalskninger, uden at skulle afvente udfaldet af en national retsafgørelse. Den rettighedshaver, der mener sig krænket, henvender sig til toldmyndighederne, og en sådan indgriben kan i givet fald betinges af, at den berettigede stiller sikkerhed.

11.1.b. Brug af varemærker i funktionsbeskrivelser

En varemærkeret afskærer ikke konkurrenter fra at benytte varemærket som betegnelse for en teknisk funktion, hvis dette blot sker i overensstemmelse med god markedsføringsskik, jf. nærmere vml. § 5, stk. 3, der stiller som betingelse herfor, at "dette er nødvendigt for at angive anvendelsen af en vare eller tjenesteydelse, navnlig som tilbehør eller reservedele". Sådanne angivelser kan f.eks. tænkes ved betegnelser af typen "Dette tekstbehandlingsprogram understøtter printere mærket X, Y og Z". Se til illustration *U 2003.1020 H*, der gav en kaffefilterproducent adgang til at benytte de talangivelser, der benyttedes af den markedsdominerende producent af *Melitta*-kafferfiltre, i forbindelse med sin markedsføring af konkurrerende kaffefiltre. Afgørelsen er begrundet med, at det må anses for almindeligt at angive størrelsen af kaffefiltre med tre cifre, hvorfor tallene ikke var så stærkt indarbejdede, at de havde det fornødne særpræg til at nyde beskyttelse som varemærke.

Er den pågældende angivelse komplementær til det produkt, hvortil varemærket hører, vil sådanne henvisninger i almindelighed ikke være i strid med markedsføringsretlige regler, jf. mfl. § 1 (god markedsføringsskik) og § 5 (anvendelse af andres forretningskendetegn). Ofte kan en sådan benyttelse ligefrem være til gavn for rettighedshaveren, der dermed opnår støtte til afsætningen af sit eget produkt. Branchen har da også indrettet sig på den slags angivelser, der må siges at være helt sædvanlige.

Kompatibilitetsangivelser

Mere tvivlsomt er det, om producenten af et produkt, der i kraft af kompatibilitet udfører *samme funktioner* som det varemærkebelagte – og typisk markedsdominerende – produkt, kan anvende dette produkts varemærke i sin markedsføring, jf. den førnævnte afgørelse. Konkurrenten kan selvsagt ikke gøre varemærket til sit, hvilket da sjældent heller vil være tilsigtet; men spørgsmålet er, om det er tilladt at beskrive selve funktionen ved brug af varemærket. I disse tilfælde foreligger der således en direkte konkurrence mellem mærkeindehaveren og den konkurrent, der ønsker at anvende mærket i sin markedsføring.

Svaret på dette spørgsmål må hentes i læren om retsstridig markedsfortrængning, jf. nærmere *Koktvedgaard*: Lærebog i konkurrenceret (2003), kapitel VIII. Dette indebærer en afvejning, der bl.a. tager højde for, hvordan et marked af denne karakter fungerer bedst. På markedet for standardiserede IT-systemer indgår hensynet til fri konkurrence, åbne standarder mv. med betydelig vægt – hensyn, som bl.a. EU-myndighederne med stor intensitet søger at sikre. Loyale angivelser af, at et produkt er kompatibelt med et andet, vil næppe indebære en varemærkekrænkelse.

Spørgsmålet vil formentlig falde anderledes ud i amerikansk ret, jf. *Intel Corporation v. Advanced Micro Devices, Inc.,* 12 CLR 121 (District Court, ND CA, 7.8.1990), der fortolkede 15 U.S.C. § 1125 (a) om forbud mod "false designations or origin or false descriptions" som et forbud mod at gøre brug af betegnelser som "100% Intel compatible", "strictly compatible" mv.

11.1.c. Varemærkekrænkelse via domænenavne

Talrige varemærker optræder tillige som domænenavne under nationale eller generiske domænebetegnelser. Denne grænseflade mellem varemærkeretten og læren om domænenavne giver anledning til særlige problemstillinger for varemærkeretten. Om de modsvarende grænsefladeproblemer for læren om domænenavne henvises til afsnit 11.5.

Erhvervsmæssig brug?

Et første spørgsmål knytter sig til, om et domænenavn indebærer *erhvervsmæssig brug* af et varemærke, der falder sammen med domænenavnet. Problemstillingen har to sider: Hvis en rent teknisk "ibrugtagning" indebærer erhvervsmæssig brug, betyder dette på den ene side, at indehaveren af domænenavnet *krænker* den eksisterende varemærkeret (forudsat lovens øvrige betingelser for at antage en sådan krænkelse er til stede), men på den anden side også, at den tekniske ibrugtagning i sig selv vil kunne etablere en varemærkeret (ved ibrugtagning), for så vidt den ikke krænker en eksisterende navne- eller varemærkeret.

Svaret på disse spørgsmål beror på, hvorledes domænet er taget i brug.

Kun DNS-service

Er der alene opsat en navneservice (DNS) for et domænenavn, der er identisk eller forvekslelig med en varemærkeret, men ikke etableret funktionsdygtige web- eller e-post-adresser, følger det af hidtidig retspraksis, at denne registrering ikke i sig selv indebærer en erhvervsmæssig ibrugtagning af varemærker eller forretningskendetegn. Se således dommen i *U 2001.697 Ø*, hvor både by- og landsret fandt, at registreringen ikke i sig selv ud-

gjorde en varemærkeanvendelse. Spørgsmålet er dog ikke utvivlsomt, og også i udenlandsk praksis giver det anledning til tvivl. Se f.eks. *Academy of Motion Picture Art & Services v. Network Solutions*, 989 F.Supp. 1276 (1997) til støtte for antagelsen ovenfor, men muligvis modsat *Panavision International v. Dennis Toeppen*, 945 F.Supp. 1296 (1996). Man kan med en vis styrke argumentere for, at der foreligger en indirekte brug af varemærket i kraft af den meddelelse, hvorved den godtroende Internetbruger får melding om, at domænet ikke eksisterer, når han f.eks. leder efter en hjemmeside under det pågældende domænenavn eller konsulterer den "*whois*"-tjeneste, der er opsat for det pågældende topdomæne. Alt andet lige kommunikerer dette svar (f.eks. om, at der ikke er opsat DNS-service for domænet) jo, at varemærkehaveren enten ikke har sørget for at sikre sine domænerettigheder, eller ikke har truffet de processkridt, der i givet fald måtte kræves hertil. For så vidt kan man konstatere, at den "ikke-brug", der er tale om, rent faktisk skader varemærkehaveren. For at kunne statuere en egentlig varemærkekrænkelse baseret på denne argumentation for den blotte tekniske ibrugtagning af et domæne, må det dog kræves, at der i praksis kun er én krænket part, hvilket indsnævrer feltet til de såkaldte Kodak-mærker, jf. vml. § 4, stk. 2, hvor beskyttelsen gælder i relation til flere forskellige vareklasser. Dækker domænet derimod flere forskellige gyldigt bestående varemærker inden for forskellige vareklasser, kan det ikke antages, at der i og med domæneregistreringen effektueres en total og global varemærkekrænkelse af alle disse navne og varemærker.

- domænet tilbydes varemærkehaver

Situationen er en anden, hvis domæneregistranten tilbyder varemærkehaveren at købe domæneregistreringen. Østre Landsrets førnævnte dom i *U 2001.697 Ø* lagde som nævnt til grund, at der ikke forelå varemærkekrænkelse, sålænge domænet ikke var udbudt til andre end varemærkehaveren. Betragtningen skulle altså være, at der i så fald ikke er tale om, at domænet benyttes "som kendetegn for varer og tjenesteydelser", jf. vml. § 1, idet, det der søges solgt, netop er det pågældende kendetegn, som modtageren i forvejen benytter.

Med *U 2004.1561 H* er der opnået en vis afklaring om spørgsmålet. Dommen antager, at en IT-virksomhed, der havde registreret domænenavnet "br.dk", og som fremsatte krav om betaling af 300.000 kr., da legetøjsvirksomheden "BR" anmodede om at få domænet overført til sig, hermed havde udvist en markedsadfærd i strid med god markedsføringsskik, jf. mfl. § 1. Det lagdes til grund, at domænenavnet var registreret med kendskab til lege-

tøjsforretningens indarbejdede forretningskendetegn (og i øvrigt kort tid efter, at registranten var blevet dømt til at afregistrere et andet domænenavn, der bar en anden kendt virksomheds navn). På denne baggrund fandtes det ubetænkeligt at lægge til grund, at registranten, der ikke selv havde brugt domænenavnet <br.dk>, havde registreret dette med det formål at sælge det til overpris til indehaveren af "BR"-varemærket. Dommen begrundes med, at registranten herved havde afskåret legetøjsvirksomheden fra at få sit forretningskendetegn registreret som domænenavn. Registranten blev derfor pålagt at overdrage domænenavnet vederlagsfrit til legetøjsvirksomheden.

Det ligger omvendt klart, at en passiv brug, hvor der alene etableres DNS-service for domænet, men ikke lægges information ind på serveren, heller ikke etablerer en varemærkeret. Denne antagelse har navnlig betydning for den form for domæneregistrering, hvorved attraktive generiske domæner *hamstres* med henblik på salg til højestbydende.

Aktiv brug

Bruges domænenavnet aktivt som varemærke for varer og tjenester, der udbydes via Internet, kan det som udgangspunkt sidestilles med anden brug af forretningskendetegn, se f.eks. *U 2001.432 SH*, hvor rekvisitus efter et fogedforbud fortsat anvendte det pågældende varemærke som e-mail-adresse og som søgeord hos en søgetjeneste. Retten statuerer, at (også) denne anvendelse udgjorde en erhvervsmæssig anvendelse af mærket, jf. vml. § 4.

Dette udgangspunkt er tidligt fastslået i dansk fogedretspraksis. Den første afgørelse foreligger med Gladsaxe Fogedrets kendelse af 25. februar 1997 (FS 16/97) vedrørende <jobdanmark.dk>. Denne afgørelse er siden fulgt op af flere andre utrykte byretsdomme, henholdsvis Københavns byrets kendelse af 22. januar 1998 om <118.dk> og Københavns fogedrets kendelse af 31. oktober 1997 om <yellowpage.dk>. De nævnte afgørelser er tilgængelige fra <www.ipb.dk> Se i øvrigt *Lone Prehn* i U2001B.52 ff. med omtale af utrykt dansk praksis.

<haven.dk>

Ifølge den foreliggende praksis fra Klagenævnet for Domænenavne har det krav om særpræg, der kræves for at opnå en varemærkeret, ikke nødvendigvis betydning, hvis retten til et domænenavn hævdes på grundlag af et anbringende støttet på mfl. §§ 1 og 5. I sagen om <haven.dk> (18.1.01) antog nævnet således, at udgiveren af magasinet "Haven" kunne forbyde et hertil svarende domænenavn. Det pågældende domænenavn var erhvervet af den indklagede registrant (mod en købesum på 10.000 kr.). Registranten ønskede at oprette en haveportal og tog i den forbindelse kontakt med magasinets udgiver (Det Danske Haveselskab) med

henblik på et samarbejde. I sin afgørelse lægger nævnet vægt på, at det pågældende domænenavn i sin tid var blevet registreret med videresalg for øje og herefter købt af den indklagede registrant, som måtte have været bekendt med haveselskabets anvendelse af det pågældende navn for sit magasin, og som tilmed i sin indledende forberedelse ønskede at inddrage haveselskabet i sine portal-planer. Afgørelsens resultat er altså ikke støttet på varemærkeretlige regler, men indebærer en konkret anvendelse af almindelige markedsføringsretlige grundsætninger. Der var således intet til hinder for, at registranten kunne have gennemført sine portal-planer ved at anvende et lignende – men ikke identisk – tilgængeligt domænenavn, som f.eks. "haver", "haveportalen", "have" el.lign.

I *U 2002.1056 SH* fandtes domænenavnet <bynet.dk> at have tilstrækkeligt særpræg for de varer og ydelser, for hvilket det var blevet registreret (rubrikannoncering, Internet-udbydervirksomhed, underholdning og nyhedsformidling), hvorved dets indehaver kunne forbyde anvendelsen af domænenavnet <bynet-slagelse.dk> samt at anvende elementet "bynet" som søgeord i metatags. Se i øvrigt *Kim Bruun Clausen* og *Tue Frandsen* i *Justitia*, nr. 1, oktober 2002, s. 56 ff. Nyere praksis fra Klagenævnet for Domænenavne efterlader en vis tvivl om, hvornår man anerkender en kendetegnsbeskyttelse for generiske betegnelser. Se herved den tvivlsomme afgørelse i <dagbladet.dk> (2.6.03), der nægtede den kendte sjællandske avis *Dagbladet* det tilsvarende domæne som en person havde registreret uden at angive nogen konkret brug, og i <restaurationen.dk> (9.1.03), der derimod med rette gav den førende københavnske gourmet-restaurant *Restaurationen* medhold i, at en privatperson, der havde registreret dette domæne med henblik på at etablere en portal for restaurationer, ikke kunne opretholde denne registrering, da betegnelsen "restaurationen" ikke var en naturlig betegnelse for en sådan portal. Se ligeledes afgørelserne om <bønnen.dk> og <kaffebønnen.dk> (24.6.04), der anerkendte et kafferisteris berettigede interesse i disse kendetegn.

Tredjeordens domæner

Bemærkningerne ovenfor tager sigte på det, der i teknisk terminologi betegnes som andenordens-domænenavne, eller second-level domains. En person eller virksomhed, der blot ønsker at kunne nås på nettet, vil ikke nødvendigvis have brug for sit eget domænenavn. Til de fleste formål kan det være fuldt tilstrækkeligt at optræde med et *tredjeordens* eller *fjerdeordens* domæne, f.eks. med e-postadressen navn@jur.ku.dk (hvor second

level domænet "ku" står for Københavns Universitet og "jur" for det juridiske fakultet).

Der gælder ikke andre betingelser for at registrere sådanne domæner end de almindelige kendetegnsregler, således som de former sig i samspil med den aftale, der kan være indgået med den part, der råder over domænet i niveauet over (og dennes eventuelle aftaleforhold med mærkeindehaveren). I det omfang der fra sådanne sub-domæner markedsføres varer og tjenesteydelser ved brug af kendte varemærker mv., beror det på almindelige regler, om en sådan domæneregistrering kan opretholdes. F.eks. må et stormagasin i almindelighed være berettiget til at anvende sub-domæner, der angiver varemærkerne for de varegrupper, der markedsføres.

11.1.d. Meta-tagging mv.

Et særligt varemærkeretligt problem opstår ved såkaldt meta-tagging af hjemmesider: En "tag" er en kode, der indsættes i et dokument, og som beskriver, hvordan hele eller dele af dokumentet skal formateres. Tagging anvendes bl.a. i forbindelse med opmarkering under HTML-standarden til at justere margener, anbringe grafik el.lign., men også til at indikere, hvilke dele af dokumentet der skal være søgebart fra søgerobotterne på Internet. Dermed kan indehaveren af en hjemmeside eksponere sig for søgerobotter, der dermed leder brugeren direkte hen til hjemmesiden og således understøtter et større marked for de varer og tjenesteydelser, som måtte blive markedsført fra hjemmesiden. Da denne identifikation foregår skjult for brugeren (og altså gemt bag brugergrænsefladen), benævnes den undertiden "meta-tagging". Allerede fordi man gennem meta-tagging på effektiv vis kan trække et efterspørgende marked hen til en hjemmeside, er der ingen tvivl om, at meta-tagging under anvendelse af et varemærke indebærer kommerciel brug af dette varemærke, jf. vml. § 4.

Melitta-sagen

Dette resultat er ligeledes antaget ved *U 1999.531 Ø* om *Melitta* kaffefiltre. En virksomhed, der fremstillede kaffefiltre, der konkurrerede med det kendte *Melitta*-mærke, fandtes afskåret fra at benytte nogle talbetegnelser, som *Melitta* fandtes at have erhvervet varemærket til. Derimod fandtes konkurrenten berettiget til på *ikke fremhævet* måde at angive, at hans kaffefiltre størrelsesmæssigt passede til Melittas produkter. I konsekvens af sin ret hertil fandtes konkurrenten ligeledes berettiget til at meddele disse oplysninger på sin hjemmeside, også selv om dette under

søgninger via Internet-robotter med "Melitta" som søgekriterier kunne lede forbrugere hen til konkurrentens hjemmeside. Derimod fandtes konkurrenten ikke berettiget til at foretage særlige foranstaltninger med henblik på at sikre, at søgerobotter ved opslag på "Melitta" henviste til konkurrentens hjemmeside eller øvrige reklamer på nettet. En aftale med udbyderen af en sådan søgerobot, hvorefter konkurrenten fik tildelt en prioriteret plads ved opslag, ville således være retsstridig.

Dommen er fulgt op med *U 2003.1020 H*, der ligeledes forbød den konkurrerende producent at anvende "Melitta" som søgeord på nettet, ligesom brugen af betegnelsen "Melitta type" fandtes retsstridig. Derimod fandtes de talangivelser, der henviser til de enkelte typer af kaffefiltre, ikke retsstridige. Se ligeledes *U 2002.1056 SH*, hvor indehaveren af varemærket "bynet" fik medhold i, at portalen <bynet-slagelse.dk> ikke kunne anvende metatags med "bynet". I denne sag var der således ikke tale om en "kompatibilitetsangivelse" el.lign. men om ren snyltning på det beskyttede mærke.

Keyword advertising

Muligheden for at opnå Internet-trafik ved brug af søgeord har i øvrigt givet grundlag for en særlig form for markedsføring, der tager sit udgangspunkt i den mulighed, der består for at købe sig en højt prioriteret plads i de søgemaskiner, der anvendes på nettet. Denne såkaldte *keyword advertising* (eller blot *keying*) er for tiden en af de hurtigst voksende former for markedsføring på nettet. De keywords, der typisk betales det højeste vederlag for, er de generiske, som der sjældent vil være immaterialretlige problemer med at benytte. Men jo mere man nærmer sig keywords, der dækker særlige kendetegnsrettigheder, kan der opstå vanskeligheder. I Danmark må disse spørgsmål håndteres efter samme regler som dem, der er anført oven for om *mega tagging*. Praksis i USA er under hastig udvikling, se herved *Erik M. Feig & J.T. Westermeier* i 20 CLAB 2 ff .(2005).

II.I.e. Rettighedssubjektet

Ansættelsesforhold

Spørgsmålet om, hvem der har retten til navne- og varemærkerettigheder, der er blevet til som led i et opdrag giver sjældent anledning til vanskeligheder. Der vil som regel være enighed om, at opdrags- eller arbejdsgiverens konkurrencemæssige interesse i at anvende et navn eller varemærke skal gå forud for andres interesse i at kunne få andel af mærket, og herunder af den goodwill, mærket repræsenterer. Varemærket "tilhører" i en vis forstand den organisation, hvis identitet det netop skal symbolisere, og

følger – hvis ikke der er grundlag for at antage andet – organisationen.

Samarbejdsophør

Retten til et varemærke kan derimod give anledning til problemer ved opløsning af virksomheder, der har været baseret på brugen af det pågældende varemærke eller domænenavn. Hvis ikke det er muligt at foretage en opsplitning af domænenavnet, således at det forsynes med et "efternavn" svarende til hvert af de opsplittede forretningsområder, må der gennemføres en rettighedsfordeling i overensstemmelse med almindelige skifteretlige og samejeretlige principper.

Formel registrering

Det forekommer imidlertid ofte, at en domæneregistrering ordnes således, at den medarbejder, der tilfældigvis har stået for de praktiske tiltag ved registreringen, også – fejlagtigt – kommer til at optræde som registrant for domænet. I sådanne tilfælde vil der sjældent være materiel uenighed om, hvem der har ret til domænet; men den formelle tilstedeværelse af en medarbejder – der måske nu befinder sig i et indædt modsætningsforhold til sin tidligere arbejdsgiver – kan give anledning til chikanerier, herunder uberettigede overførelser af domænet. I mange tilfælde kan sådanne forhold berigtiges administrativt af den pågældende registrator – for .dk-domænet DK Hostmaster A/S – men ved substantiel uenighed må den gældende konfliktløsningsprocedure tages i brug.

11.2. Andre forretningskendetegn

11.2.a. Markedsføringslovens § 5

Ifølge mfl. § 5 må erhvervsdrivende ikke benytte forretningskendetegn og lignende, der ikke tilkommer dem, eller benytte egne kendetegn på en måde, der er egnet til at fremkalde forveksling med andres. Bestemmelsen fungerer som et supplement til de øvrige kendetegnsregler i varemærkeloven, navneloven og i de selskabsretlige regler.

I *U 2001.697 Ø* fandtes en person, der havde registreret et registreret varemærke til ibrugtagning som domænenavn, men som ikke havde taget dette i erhvervsmæssig anvendelse, ikke at have handlet i strid med mfl. § 5 ved at tilbyde dette domænenavn til varemærkehaveren. Da den nævnte handling derimod fandtes retsstridig som omfattet af mfl. § 1, blev registranten pålagt en erstatningspligt for det herved påførte tab. Erstatningen opgjordes til kr. 50.000,-.

II.2.b. Personnavne

Navneloven

Ifølge § 27 i navneloven, lov nr. 524 af 24. juni 2005, kan den, der kan godtgøre, at en anden uberettiget benytter vedkommendes navn eller et navn, der har en sådan lighed hermed, at forveksling let kan ske, ved dom få den anden tilpligtet at ophøre med brugen af navnet. Lovens § 3, stk. 1, fastslår i den forbindelse, at efternavne, der her i landet bæres af 2.000 personer eller færre, er beskyttede og ikke kan tages af andre. Beskyttelsen gælder dog ikke navne, der er omfattet af en særlig liste, der årligt udstedes af ministeren for familie- og forbrugeranliggender, jf. § 2, stk. 1, 2. pkt. Dernæst er reglen ikke til hinder for, at et navn kan tages i medfør af lovens §§ 4, 5 eller 7-9. Loven, der træder i kraft den 1. april 2006, indebærer en betydelig liberalisering i forhold til personnavneloven af 1981. Den efterlader imidlertid fortsat en beskyttelse, især af de ikke særligt udbredte personnavne (efternavne). Denne beskyttelse har ligeledes betydning i de tilfælde, hvor et sådant navn registreres som domænenavn.

Klagenævnspraksis

I den hidtidige praksis fra Klagenævnet for Domænenavne har man ydet fuld beskyttelse til personers navneret. Beskyttelsen er bl.a. antaget i sagen om <reinhardt.dk> (23.1.04), hvor den indklagede registrant alene havde registreret et beskyttet navn med sigte på at kunne sælge e-post-tjenester til dets rette bærere, og i <skjold.dk> (31.1.05), hvor en person ved navn Skjold Nielsen måtte afgive domænet <skjold.dk> til en person med efternavnet Skjold. Nævnet har i den forbindelse beskyttet fornavne på lige fod med efternavne, jf. <conrad.dk> (24.9.04), hvor en person med fornavnet Conrad i kraft af *first filed*-synspunktet kunne beholde dette domæne i konkurrence med en person, der havde Conrad som efternavn. Ligeledes har nævnet beskyttet domæner, der angiver det fulde navn på offentlige personer, se f.eks. <sorenpind.dk> (7.11.03). Navnebeskyttelsen er ligeledes fastholdt i situationer, hvor oprettelsen af et domæne er sket for at genere den pågældende person, se f.eks. <henrik-knudsen.dk> (2.4.04). Et personnavn vil ligeledes kunne opretholdes mod et varemærke, hvis personnavnet er registreret forinden, se herved afgørelsen om <gangsta-maersk.dk> (29.8.03), hvor en person ved navn Thomas Mærsk fik medhold i, at dette domænenavn kunne opretholdes trods indsigelse fra Mærsk-gruppen. Er registreringen derimod sket med henblik på en loyal benyttelse, f.eks. til brug for en portalløsning, har nævnet anset den for berettiget. Se herved <thomsen.dk> (23.1.04) og <olsen.dk> (12.2.04).

Omvendt kan indehaveren af et personnavn heller ikke forhindre, at en virksomhed anvender en betegnelse, der er sammenfaldende med personnavnet, jf. hertil Klagenævnets afgørelse i sagen om <sams.dk> (11.11.00). Når et personnavn registreres til ibrugtagning som domænenavn, vil der kun foreligge navnekonflikt, hvis domænet er fuldstændig identisk med et eksisterende personnavn, der allerede er registreret. I denne henseende gælder det navneretlige udgangspunkt om, at der ikke er ækvivalensbeskyttelse fuldt ud.

Som rolle i spil

Visse softwareprodukter inden for underholdningsindustrien fungerer ved hjælp af menneskelige roller, der optræder med personnavne overfor brugeren. Dette forekommer f.eks. hyppigt i computerspil, der udfører holdsport (f.eks. fodbold), hvor brugeren kan sammensætte et hold ved at udvælge navngivne spillere fra virkelighedens verden. Salgsværdien af sådanne spil er selvsagt højere, hvis brugeren kan vælge kendte og feterede spillere. En sådan anvendelse af et personnavn forudsætter imidlertid den pågældendes godkendelse.

Kan en spil-producent ikke opnå det fornødne samtykke til brug af et personnavn (f.eks. en kendt og feteret fodboldspiller), er det formentlig retligt uproblematisk at anvende et navn, der *leder tanken hen på* den pågældende spiller, men som med en helt anden stavemåde klart distancerer sig herfra. Her gælder formentlig et vist krav om ækvivalens. "Laudrup" kan således ikke erstattes med "Lautrup", men måske nok med "Lanstrup". Afgørende for vurderingen må være, om brugeren med rette kan tro, at der er tale om en autoriseret brug af navnet. Sager af denne art må løses efter de regler om personlighedsbeskyttelse, der antages at tilkomme kendte personer. Om et sådant misbrug foreligger, beror på en helhedsbedømmelse, hvori – foruden karakteren af den "fejlagtige" stavemåde – bl.a. indgår brug af andre kendetegn for den pågældende person (f.eks. en påklædning eller ansigtstræk): Vælges en meget aparte stavemåde, kan man gå "tættere" på personen. Er der tale om stort set sammenfaldende navne, vil alene et rollesammenfald kunne indebære en krænkelse. Det vil selvsagt ikke være i strid med markedsretlige eller immaterialretlige regler at overlade brugeren en mulighed for selv at ændre spillernavne.

11.2.c. Andre navneangivelser

Offentlige myndigheder har ikke noget naturligt hjemsted i den almindelige varemærkeret, når de optræder i rollen som udøvere

af en offentligretlig kompetence. Når det gælder retten til sådanne myndighedsnavne suppleres den varemærkeretlige beskyttelse imidlertid af andre regelsæt, der alt efter omstændighederne kan afskære den risiko for snyltning og forveksling, der ellers varetages af varemærkereglerne. Således antages det generelt, at ikke-kommercielle personer og institutioner mv. kan påberåbe sig kendetegnsretlige grundsætninger, der i det store og hele bygger på den kommercielle kendetegnsret. Se hertil *Peter Blok* i U1995B.418 ff. i kommentaren til *U 1995.211 H* (Dansk Handicap Forbund).

Strfl. § 131

Ifølge strfl. § 131 straffes den, som offentlig eller i retsstridig hensigt udgiver sig for at have en offentlig myndighed eller offentlig bemyndigelse til en virksomhed. Bestemmelsen kan tænkes anvendt i relation til ibrugtagning af domænenavne, som må formodes at tilkomme offentlige myndigheder (f.eks. <justitsministeriet.dk>), hvis den pågældende brug indebærer risiko for, at en bruger anser registranten for identisk med den pågældende myndighed. Problemet er måske ikke så stort, hvis domænet alene viser hen til en web-server; men i det omfang det viser hen til en server til e-mails, kan der opstå risiko for, at mails tiltænkt politiet modtages af den person, der – tilfældigt – har ibrugtaget domænet. DIFO har derfor fulgt en praksis, hvorefter man på begæring af den pågældende myndighed selv redelegerer domæneregistreringer, der er sammenfaldende med den almindeligt anvendte betegnelse for offentlige myndigheder, til den pågældende myndighed. Denne praksis, der endnu ikke er anfægtet, er fulgt med hjemmel i DIFO-reglernes pkt. 2.4.c.

Bynavne mv.

En vanskelig navnekonflikt kan forekomme, hvis et domænenavn både dækker et varemærke og en stedbetegnelse, f.eks. en by. En anerkendelse af, at mærkeindehaveren i overensstemmelse med *first filed*-princippet opnår retten til domænet forud for bystyret vil samtidig indebære en antagelse af, at den *offentlige* interesse skal underordnes den erhvervsinteresse, der tilgodeses i varemærketretten. Rene tilfældigheder (måske iblandet en velkendt langsommelighed hos visse offentlige myndigheder) kan ligge bag det forhold, at varemærket registreres som domæne før bystyrets navn gør det. Men skadevirkningen for det offentlige vil efter omstændighederne kunne være betydelig.

Klagenævnet for Domænenavne har her fastholdt princippet om *first filed* fuldt ud, se hertil afsnit 11.5.c. Dette er sket i sagen om <brørup.dk> (9.5.05), hvor Brørup Kommune havde rejst krav mod en person med efternavnet Brørup om overdragelse af dette navn. Nævnet begrunder afgørelsen med, at hverken kom-

munens eller indklagedes ret til kommunenavnet indebærer nogen fortrinsret. Medvirkende til afgørelsen har nok været, at der var tale om et nyt domæne (fremkommet ved åbningen af navnerummet i 2002), og at kommunen ikke havde gjort sin særlige ret til dette gældende i den periode, hvor der var givet offentlige myndigheder en sådan adgang.

Spørgsmålet har dog givet anledning til forskellige afgørelser i udlandet. Fra Schweiz foreligger således to højesteretsdomme vedrørende bynavnene *Lucerne* og *Montana* som domænenavne. Den første dom antager, at bystyret Lucerne kunne hævde eneretsbeskyttelse til sine navne i overensstemmelse med art. 29 i den schweiziske civillovbog (der omhandler retsbeskyttelse af personnavne). Retten henviste til, at bynavnet Lucerne er over 700 år gammelt, og at sagsøgtes anvendelse af navnet i forbindelse med en hjemmeside om byen ikke kunne føre til nogen fravigelse af byens navnerettigheder. I den anden sag var konflikten opstået mellem en skole og bystyret i Montana. Retten fandt her, at Montana som geografisk betegnelse var mere velkendt end navnet på den pågældende skole, hvorfor man gav bystyret medhold.

11.3. Snyltning og efterligning

11.3.a. God markedsføringsskik

Problemstilling

De fleste veludviklede retssystemer forbyder konkurrencemæssig adfærd, der enten fratager markedsaktørerne incitamentet til at konkurrere, og/eller som tjener til at forvirre eller ligefrem skade forbrugere eller andre. I dansk ret findes regler herom i mfl. § 1, som fastslår, at der i erhvervsmæssig virksomhed ikke må foretages handlinger, der strider mod "god markedsføringsskik". Dette rummelige begreb antages at ramme vidt forskellige former for markedsadfærd. Som nærmere udviklet i *Koktvedgaard* (2003), s. 325 ff., opløses generalklausulen bl.a. i et almindeligt forbud mod markedsføring af produkter, der kan siges at snylte på en konkurrents tidligere indsats (s. 327), hvad enten denne har teknologisk-innovativ eller markedsføringsmæssig karakter.

Betydning

Beskyttelsen efter mfl. § 1 kan for det første have betydning for de dele af et IT-system, der ikke kan beskyttes af andre regler, f.eks. et programs brugergrænseflade, dvs. den struktur af valgmuligheder, der skal indlæres af brugeren, for at han kan få nytte af programmet, jf. nærmere hertil afsnit 7.3.c. Men den kan også tænkes at danne grundlag for vurderingen af, om en markedsmæssig adfærd, der f.eks. indebærer henvisninger til konkurre-

rende virksomheders informationsprodukter eller markedsføringsmateriale på nettet i kraft af hypertekst-links, er berettiget, jf. herom i afsnit 8.5.

Sanktioner

Overtrædelser af mfl. § 1 er ikke – som overtrædelser af varemærkeloven, ophavsretsloven eller patentloven – belagt med straf, men giver grundlag for nedlæggelse af forbud mod den pågældende handling. Overtrædelse af sådanne forbud kan herefter straffes, jf. mfl. § 22. Endvidere kan der gives erstatning for handlinger i strid med god markedsføringsskik.

11.3.b. God domænenavnsskik

IDL § 12, stk. 1

Med bestemmelsen i IDL § 12, stk. 1, er der skabt hjemmel i dansk ret til at skride ind overfor domæneregistreringer inden for lovens område (dvs. indtil videre for .dk-domænet), der strider mod god domænenavnsskik. Det følger af forarbejderne til loven, betænkning 1450/2004, s. 207 ff., at denne generalklausul ikke tilsigter nogen binding til de principper, der er udviklet i medfør af mfl. § 1. Bestemmelsen vil således også kunne regulere privatpersoners, offentlige myndigheders og institutioners forhold.

Hensynsafvejningen

I den praktiske anvendelse af § 12, stk. 1, vil man ofte støde på modstående hensyn, som må afbalanceres over for hinanden. Det antydes således i betænkningen a.st., s. 209 f., at man med hjemmel i generalklausulen kan foretage en afvejning, hvor indehaverens rent private interesse i at bibeholde et domæne, der fremstår som egnet til at tjene en offentlig interesse eller privat interesse, kan vige overfor hensyn, der tilgodeser denne offentlige interesse. En sådan afvejning kan navnlig foretages, hvis domænet er registreret uden samtidig at være taget i brug.

Den nye generalklausul må forventes først og fremmest at blive udfyldt gennem den praksis, der i de kommende år vil udvikle sig fra Klagenævnet for Domænenavne. Ligeledes må det antages, at DIFO (eller en anden kommende registrator) vil søge at præcisere generalklausulen gennem de vilkår, der kan fastsættes med gyldighed for de af loven omfattede domæner i medfør af § 11.

Hamstring

Generalklausulen om god domænenavnsskik udbygges i et stk. 2, der forbyder registranter at registrere og opretholde registreringer af internetdomænenavne alene med videresalg og udlejning for øje. Den bestemmelse, der hermed er indført, løser et problem, som nødvendigvis følger af en åben domæneordning: Enhver kan registrere et domæne, der ikke er registreret i forvejen. Er registreringen *generisk* (dvs. knytter den sig til et almin-

deligt ord mv., der ikke falder sammen med et varemærke eller forretningskendetegn mv.), vil den som regel blive fulgt op med en nyttig tjeneste, typisk en hjemmeside. Men ikke sjældent sker registreringen alene med det formål at sikre registranten en mulighed for at gøre en god handel, når en anden melder sig med et reelt ønske om at nyttiggøre domænet. Denne mulighed afskæres nu med § 12, stk. 2. For domæner, der var registreret ved lovens ikrafttræden finder bestemmelsen dog først anvendelse fra 1. juli 2010, jf. § 27, stk. 3. Ældre, hamstrede, domæner kan derfor kun opretholdes i denne 5-årsperiode.

I Tyskland er man gået skridtet videre og har antaget, at registrering af generiske domænenavne i sig selv kan indebære en urimelig konkurrenceposition, se sagen *Grafe & Partner v. Maia Steinert & Coll*, hvor retten i München fandt, at registreringen af <rechtsanwaelte.de>, der alene indeholdt en link til registrantens hjemmeside <www.graefe-partner.dk> indebar en urimelig konkurrenceudnyttelse. Sagen er afgjort den 16. november 2000, sagsnr. 7 0 5570/00, jf. omtalen i World E-Commerce & IP Report 05/01, s. 13 f.

Særregler

Såvel generalklausulen som hamstringsreglen kan uddybes gennem de forretningsbetingelser og vilkår, som administrator kan fastsætte i medfør af IDL § 11. Sådanne regler gælder også for ældre domæner, jf. IDL § 27, stk. 2. Det siges udtrykkeligt i IDL § 1, stk. 2, at sådanne vilkår mv. kan indeholde regler om brugspligt, anvendelse af internetdomænenavne og inddragelse. Med denne regelændring har lovgiveren taget et væsentligt skridt hen i retning mod at lade administrator varetage andet end rent tekniske funktioner for administrationen af domænenavne.

Retsstridighed

Generalklausulen kan formentlig også anvendes på registreringer, der er foretaget under en retsstridig procedure, hvis registranten i ond tro medvirkede heri. Dette kan efter omstændighederne være aktuelt i relation til registranter, der deltog i de retsstridige forhold, der fandt sted i januar 1997, hvor man forlod den kontrollerede godkendelsesprocedure og lod alle registrere .dk-domæner efter *first filed*-princippet. Ved denne lejlighed fik en række registratorer med tilknytning til den daværende ejerkreds omkring DK Hostmaster A/S adgang til forud for andre at registrere attraktive generiske domæner, hvoraf mange i dag er til salg til højestbydende. Det har ikke tidligere vist sig muligt ad retlig vej at redressere disse retsbrud, hvis karakter er blevet fastslået ved en advokatundersøgelse udført af DIFO i 2002.

11.4. Reglerne om Internet-domæner

11.4.a Problemstillingen

Karakteristik

Som nærmere forklaret i afsnit 3.3.c foregår adressering på Internet ved hjælp af IP-numre, der fungerer som en slags telefonnumre for hver computer, der er tilsluttet Internet. For at gøre det lettere for brugerne at knytte kontakt uden at skulle anvende disse IP-numre (f.eks. når man sender e-mails eller henter information fra en hjemmeside), anvender man domænenavne. Domænenavne er mnemotekniske hjælpemidler, der knytter associationer til indehaverens *navn*, *varemærke* eller til den *funktion*, en hjemmeside mv. understøtter. Ved hjælp af den domænenavnstjeneste (også kaldet DNS, Domain Name Service), der er knyttet til et domænenavn på *højere* niveau (f.eks. et *top level*-domæne som .dk), ledes brugeren hen til det IP-nummer, som i databasen for denne DNS-tjeneste har registreret dette domæne.

En sådan referencefunktion giver kun mening, hvis der hersker en fuld entydighed om disse domænenavne på hvert enkelt niveau. Derfor må et domænenavn kun forekomme én gang under den struktur, det optræder i. Dette er åbenbart på det øverste niveau i domænehierarkiet, f.eks. i relation til ccTLD *top level*-domæner (Country Code Top Level Domains). Men også på næste niveau, dvs. i relation til de såkaldte *second level* domænenavne, kan det enkelte domæne kun optræde én gang under samme *top level* domæne. Derimod er der intet til hinder for, at samme *second level*-domænenavn kan optræde under forskellige *top level*-domænenavne. *Second level*-domæner som "taxa", "hotel" og "sport" optræder således under de fleste *top level*-domæner. Ligeledes vil en virksomhed med et stærkt varemærke ofte søge at beskytte dette gennem domæneregistreringer i et stort antal *top level*-domæner.

Ret og politik

Den retlige regulering af Internet-domæner søger på forskellig vis at løse de konflikter, der opstår i forbindelse med denne tildeling. Reguleringen er dels global, for så vidt som den knytter sig til fordelingen af de enkelte *top level*-domæner, dels følger den af nationale regler af generel og undertiden også specifik karakter. De internationale aspekter af denne regulering vanskeliggøres af, at domænesystemet er opstået i privat regi, hvor det i og for sig har fungeret fint. Det – forståelige – ønske, der i dag næres af regeringer og politisk ansvarlige for at sikre stabilitet og sikkerhed i dette system gennem lovgivning og konventioner, brydes dermed af interessen i også at sikre, at de markedsmekanismer og

den selvregulering, der i vid udstrækning har vist sig succesfuld på området, bibeholdes.

Beskyttelses-interesser

Hermed er allerede givet en antydning af de beskyttelsesinteresser, der gør sig gældende på området og som behandles i dette afsnit og afsnit 11.5.

De mest iøjnefaldende er *konkurrenceretlige og immaterialretlige*. Det er let at se den konkurrencemæssige interesse, man kan have i at kunne benytte et domænenavn, der viser hen til et varemærke (f.eks. <amazon.com>) eller til en bestemt aktivitet (f.eks. <musik.dk>). I det omfang et domæne tages i brug på en måde, der åbenbart krænker en *varemærkeret*, er selve den retlige regulering uproblematisk, se hertil afsnit 11.1.c. Men ofte er den varemærkeretlige krænkelsesvurdering problematisk, fordi man under ét og samme domænesystem jo kan have flere hver for sig lige gyldige varemærkerettigheder (inden for de forskellige vareklasser). Hertil kommer, at talrige af de navnekonflikter, der gør sig gældende i relation til domænenavne, slet ikke drejer sig om varemærkerettigheder men om andre typer af kendetegn, f.eks. personnavne, navne på offentlige myndigheder, el.lign. Disse spørgsmål er allerede berørt i afsnit 11.2. og behandles yderligere i afsnit 11.5. Domænenavnets retlige karakteristik analyseres i dette afsnit under 11.4.b.

Et andet spørgsmål angår de beslutningsprocesser mv., der finder sted i *det internationale system*, og som udmønter sig i de regler, der gælder for *top level*-domænenavne, dvs. på øverste niveau. Dette særlige aspekt af international politik er afgørende for forståelsen af, hvordan reglerne fungerer herhjemme og i andre lande. Disse spørgsmål behandles i afsnit 11.4.c.

En tredje beskyttelsesinteresse angår hensynet til den registrant, der ved at registrere et domænenavn udøver sin frihed til at *disponere* (og herved etablere retlige og faktisk-tekniske positioner som grundlag for disse dispositioner) og *kommunikere* (herunder i forbindelse med de ytringer registranten måtte ønske at fremsætte i et domænenavn). For den, der gør aktivt brug af et domænenavn, f.eks. som led i en erhvervsvirksomhed, vil en beslutning om, at dette domænenavn nu slettes eller suspenderes, føles indgribende.

Domænetjenesten

Set i et globalt perspektiv kan der peges på to principielt forskellige måder, hvorpå arbejdet med et *top level*-domæne varetages.

Den ene model, som benyttes i .dk-domænet, indebærer, at den udpegede hostmaster udfører alt arbejde med de enkelte *second level*-domæner, dvs. såvel registrering, administration og

betaling. I konsekvens heraf oplever den enkelte registrant et retsforhold direkte til hostmaster-virksomheden, typisk i form af et *aftaleforhold*.

I andre *top level*-domæner (for eksempel det meget benyttede .com-domæne) er denne opgave delt, idet selve DNS-tjenesten drives af én virksomhed (i dette tilfælde Verisign Global Registry Services, Inc.), medens arbejdet med at indgå aftaler med registranter, at registrere, redelegere og ophæve domæner samt at opkræve betaling herfor, er henlagt til et antal virksomheder, som udfører denne funktion efter aftale med Verisign. Man taler da om *shared registry*. IDL § 9 giver mulighed for at etablere en sådan ordning, som set fra Internet-leverandørens side har den fordel, at udgiften til selve DNS-tjenesten kan holdes skjult i det samlede beløb, kunden betaler for sine Internet-tjenester. I den danske ordning er prisen for selve domænenavnet kendt (p.t. 50 kr. ekskl. moms pr. år). Til gengæld indebærer denne ordning den vanskelighed, at DK Hostmaster A/S må holde styr på hver enkelt registrant, idet der opkræves betaling hos denne for hvert enkelt domænenavn.

Også i andre henseender varierer reglerne om, hvordan internetdomænenavne erhverves og ibrugtages, efter det enkelte *top level*-domæne. Under nogle *top level*-domæner registreres domænenavnet efter en forudgående *materiel* prøvelse af, om anmelderen har ret til domænet. Denne praksis er, ikke mindst efter de seneste års kraftige stigning i efterspørgslen efter domænenavne, stadigt sjældnere forekommende. De fleste *top level*-domæner bygger på et almindeligt princip om "først i tid, bedst i ret" (*first filed, first served*), hvorefter selve registreringen af et domænenavn ingen sikkerhed rummer for, at registranten har ret til at benytte domænenavnet.

First filed, first served-systemer indebærer en uundgåelig risiko for, at nogen registrerer et domænenavn, som tilhører andre, eller som har en sådan generisk karakter, at almenheden normalt vil *forvente*, at der til domænenavnet hører en tjeneste, der i en eller anden skikkelse er tilgængelig for almenheden. Det er fast antaget i dansk domænepraksis, at man kan registrere generiske domæner. Se f.eks. afgørelserne om <smørrebrød.dk> (28.12.04), <økonom.dk> (10.3.05), <domæne.dk> (9.5.05) og <webmaster.dk> (9.5.05) fra Klagenævnet for Domænenavne. Muligheden for at registrere domænenavne, der på denne måde kan vise sig lukrative for andre end registranten, har ført til en praksis for såkaldt "cybersquatting", hvor domænet registreres uden noget oprigtigt ønske om at benytte det i overensstemmelse

med disse forventninger. En stor del af den regulering, der findes for forskellige *top level*-domæner, har til formål at løse de vanskeligheder, der følger af en sådan cybersquatting.

11.4.b. Retlig karakteristik

Domænenavnet har endnu ikke fundet sin endelige retlige status. Alligevel er det muligt i dag at skitsere nogle karakteristika, som placerer domænenavnet i forhold til andre kommunikationstekniske fænomener, som gennem tiderne har været håndteret af kendetegnsretten.

Varemærke-funktion

Som nævnt oven for i afsnit 11.1.c. kan et domænenavn indebære en krænkelse af en varemærkeret. I en sammenligning med noget tidligere kendt er det her nærliggende at betragte domænenavnet på samme måde som et *telefonnummer*, til hvilket der knytter sig en særlig goodwill. Tidligere praksis har således også antaget, at telefonnumre (f.eks. 3 x 34 for taxameter-baseret varetransport og 4 x 35 for hyrevogne) og telegramadresser kan rumme forretningskendetegn, som kan beskyttes som sådanne. Beskyttelsen dækker ikke alene mod identiske men tillige mod forvekslelige betegnelser.

Om telefonnumre, se således *U 1960.417 SH*, der fandt det uberettiget, at en budcentral anvendte telefonnummeret "Byen 7677" i konkurrence med en budcentral, hvis telefonnummer var "Byen 7676". Praksis vedrørende telegramadresser er mere righoldig, se således *U 1948.420 SH*, hvor telegramadressen "Dicotex" fandtes forvekslelig med, og dermed uberettiget overfor, telegramadressen "Dicolex". I *U 1975.131 H*, der kendte "City Bank A/S" uberettiget til at benytte sit navn i konflikt med den kendte U.S. baserede bank af samme navn, blev det tillige påbudt den danske bank at afmelde "citybankas" som telegramadresse. I *SHT 1942.85* fandtes varmemålerfirmaet Calorius tilsvarende at kunne forbyde en konkurrent at benytte telegramadressen "Calorisum".

Teknisk funktion

Isoleret set rummer registreringen af et domænenavn derimod alene en markering af, at *registranten* hos den pågældende hostmaster har meddelt, at et givet domæne tages i brug for en IP-adresse, og at en *hostmaster* har meddelt, at der intet formelt er til hinder herfor, og rent faktisk har indført dette i sin database. I teknisk forstand indebærer registreringen således blot en markering i en DNS-database om, at der til det nævnte domæne er oprettet – eller påtænkes oprettet – navneservice til et bestemt IP-nummer.

Det er vigtigt at slå fast, at registrering af et domænenavn ikke er ensbetydende med, at der opstår en varemærkeret el.lign. til

navnet. Ej heller indebærer domæneregistreringen i sig selv en immateriel ret *sui generis*, jf. tilsvarende den meget indsigtsfulde afgørelse fra en appelret i Virginia i sagen *Network Solutions, Inc. v. Umbro International, Inc.*, 529 S.E.2d 80 (Va, 21. april 2000). Afgørelsen karakteriserer – med rette – den ret, registranten har til sit domænenavn, som en rent obligatorisk rettighed, der udspringer af det kontraktsforhold, han har med registratorvirksomheden, jf. generelt hertil *John L. Hines* i I World E-Commerce & IP Report 9.3 ff. (June 2001). Et tilsvarende resultat er lagt til grund ved Sø- og Handelsrettens dom af 15. juni 2004 i sagen vedrørende domænenavnet <co.dk>.

Den økonomiske værdi, der kan tænkes at knytte sig til et domænenavn, må i givet fald være et produkt af den investering, registranten har gjort for at tage det i aktiv brug til andet end e-post eller anden snæver anvendelse. Vil man karakterisere resultatet af denne samlede investering i rettighedstermer, må det rette prædikat være *goodwill*. I overensstemmelse hermed fastslår DIFO-reglernes pkt. 4.1, at der ved inddragelse af et domænenavn i almenhedens interesse kan tilkendes en rimelig godtgørelse, som udredes af DIFO, hvis domænenavnet har været taget i aktiv anvendelse som led i registrantens almindelige virke.

Retskildespørgsmål

Som hermed antydet står man i det praktiske arbejde med domænerettens problemer over for forskelligartede hensyn og tilsvarende retskilder. Nogle hentes fra kendetegns- og konkurrenceretten, andre fra aftaleretten, og endnu andre fra særlovgivningen, herunder navnlig IDL (lov nr. 598 af 24. juni 2005 om Internet-domæner, der særligt tildeles Danmark).

Efter indførelsen af IDL er en række centrale retsspørgsmål lovreguleret. I mange henseender fungerer loven alene som en rammelov. Således fremgår det af § 2, at internetdomæner, der særligt tildeles Danmark, tilhører den danske stat. I konsekvens heraf fastslår § 3, stk. 1, at internetdomænet .dk skal forvaltes efter reglerne i denne lov. Ved lovens ikrafttræden den 1. juli 2005 indebærer dette, at Dansk Internet Forum (DIFO) administrerer internetdomænet .dk. Administrationen gælder frem til det tidspunkt, hvor der første gang er udpeget og etableret en administrator i overensstemmelse med lovens § 4, stk. 1, der giver VTU-ministeren hjemmel til at gennemføre et offentligt udbud over blandt andet .dk-domænet.

Foruden en national lovgivning som denne gælder reglerne for det enkelte *top level*-domæne. Da disse regler er meget forskellige, eftersom de udspringer af det enkelte lands kultur og politik, ville det føre for vidt at skulle redegøre nærmere for dem her. Derfor er redegørelsen i det følgende begrænset til reglerne for

.dk-domænet. Se for en oversigtsmæssig gennemgang af enkelte andre *top level*-domæner, *Christian Kragelund m.fl.* (2003), s. 42 ff. Enhver hostmaster for et *top level*-domæne optræder med en hjemmeside, hvorpå man kan læse de regler, der gælder for *top level*-domænet, se f.eks. <www.difo.dk>. En oversigt over disse hostmasters findes på <www.iana.org/cctld/cctld-whois.htm>. I afsnit 11.4.e. redegøres kort for de regler, der gælder for .dk-domænet.

11.4.c. Den internationale regulering

Som nærmere forklaret i afsnit 3.3.d. styres tildelingen af de internationale *top level*-domæner af *The Internet Corporation of Assigned Names and Numbers* (ICANN). ICANN udleder sin kompetence af et *Memorandum of Understanding*, som blev indgået den 25. november 1998 med *US Department of Commerce*. At det således er det amerikanske handelsministerium, der har videredelegeret det politiske arbejde med at koordinere tildelingen af domænenavne på øverste niveau, skyldes den faktiske omstændighed, at *US Department of Commerce* af historiske grunde, fysisk og faktisk, råder over den computer (rodserver), som holder styr på disse centrale domæner. ICANN

ICANN viderefører det arbejde, der tidligere blev udført på privat initiativ, oprindeligt af en privatperson (*Jon Postel*), der arbejdede ved *University of Southern California*. Det RFC-dokument, med titlen "Domain name system structure and delegation", som Postel forfattede i marts 1994, fastslår selv i dag – trods fremkomsten af en række senere politiske dokumenter og standarder mv. – en række grundlæggende principper, som frem til i dag ligger grund for, hvordan domænenavne delegeres.

Relationen mellem ICANN og US Department of Commerce er i øvrigt illustrerende for den blandingsregulering, som domæneområdet er genstand for. På den ene side ligger det klart, at det offentlige har en væsentlig interesse i at sikre, at tildelingen af domænenavne foregår efter gennemsigtige og forsvarlige kriterier, og at de tekniske systemer, der understøtter den løbende henvisningsfunktion, er stabile. På den anden side er der et grundlæggende ønske om at overlade en stor del af retsdannelsen til selvregulering ved aftaler mellem de berørte parter. Som nævnt i afsnit 5.2.a. er domæneområdet et eksempel på, hvorledes lovgiveren har bevæget sig fra ønsket om *selv*regulering til i stigende grad at gøre Internet-relaterede retsspørgsmål til genstand for almindelig *lov*regulering. En tilsvarende bevægelse ses i en række andre lande, og så sent som i juni 2005 har den amerikanske regering udsendt et sæt "U.S. Principles on Internet's Domain Name and Addressing System", der bl.a. bekræfter, at "go-

vernments have legitimate public policy and sovereignty concerns with respect to the management of their ccTLD", og at man er "committed to working with the international community to address these concerns" med ICANN som den drivende kraft. Dokumentet findes på <www.ntia.doc.dov/ntiahome/domainname/>.

Nye *top level*-domæner

Set udefra fremtræder den mest synlige del af ICANN's arbejde i og med beslutningerne om at åbne for nye *top level*-domæner. Sådanne beslutninger angår typisk nye gTLD'er. I øjeblikket er følgende *top level*-domæner akkrediteret af ICANN: .aero (afgrænset til visse medlemmer af det internationale luftfartssamarbejde og varetaget af *Societe Internationale de Telecommunications Aeronautiques SC*), .biz, (afgrænset til forretningsmæssige formål og varetaget af *NeuLevel*), det mest udbredte .com (der varetages af *Verisign Global Registry Services*), .coop (der er forbeholdt kooperative virksomheder og varetages af *Dot Cooperation LLC*), .info (der varetages af *Afilias Limited*), .museum (der er afgrænset til museer og hertil knyttede personer og varetaget af *the Museum Domain Management Association, MuseDoma*), .name (afgrænset til enkeltpersoner og varetaget af *Global Name Registry*), .net og .org (der begge varetages af *Verisign Global Registry Services*) samt .pro (der er begrænset til særligt godkendte professionsudøvere). Herudover har ICANN for tiden bl.a. godkendt oprettelsen af *top level*-domænerne .xxx, der er afgrænset til pornografiske tjenesteydelser, samt .eu, jf. omtalen herom straks nedenfor. De to sidstnævnte domæner er endnu ikke sat i drift. En opdateret liste over de virksomheder, der servicerer de eksisterende gTLD-*top level*-domæner findes på <http://www.icann.org/registrars/accredited-list.html>. De respektive domæner er hver underlagt deres regelsæt, og afhængigt af hvilken procedure, der således er indført som grundlag for denne registrering, kan der opstå forskellige typer af navnekonflikter.

Lokale registratorer

For hvert *top level*-domæne udpeger ICANN en national registratorvirksomhed som ansvarlig for tildelingen af *second level*-domænenavne under det pågældende *top level*-domæne, jf. angivelsen ovenfor. Den danske registratorvirksomhed er Dansk Internet Forum, der er en privat forening, stiftet af branche- og brugerorganisationer med tilknytning til den danske del af Internet. Stiftelsen skete i 1999 efter pres fra Forskningsministeriet, jf. nærmere redegørelsen i betænkning 1450/2004, s. 32 ff. Globalt set fungerer der ca. 160 nationale registratorer. De fleste af disse opererer på privatretligt grundlag og uden særligt retsgrundlag. Ifølge rfc 1591 skal de virksomheder, der virker som registratorer under de geografiske *top level*-domæner, være "trustees for the

delegated domain, and have a duty to serve the community", dvs. "both the nation, in the case of a country code, and the global Internet community" (pkt. 3.2). Se om RFC 1591 betænkning 1450/2004, s. 47 ff.

Et landespecifikt domæne ccTLD signalerer almindeligvis, men ikke nødvendigvis, en tilknytning til det land, der korresponderer med den pågældende landekode. Der findes en mangfoldighed af landeforkortelser i den ISO 3136-standard, der ligger til grund for de landekoder der optræder i det internationale domænenavnssystem. Mange af disse nationalitetsbetegnelser angår små ø-stater, hvis forkortelser de færreste vil knytte geografiske associationer til, men som til gengæld vil kunne rumme en nyttig markedsfunktion. For eksempel anvendes *top level*-domænet "tv" (for øgruppen Tuvalu) for en række medievirksomheder, ligesom forkortelsen "nu" (for det lille ø-rige Niue i Stillehavet med 1600 beboere) er populært for nordiske registranter, som for eksempel kan lade domænet indgå i en tjeneste, der rummer en bestillingsfunktion (for eksempel <www.taxa.nu>).

DK Hostmaster A/S

DIFO har delegeret det praktiske arbejde med .dk-domænet til det helejede datterselskab, DK Hostmaster A/S. Det er dette selskab, der står for den praktiske administration af ansøgninger om nye domænenavne. Arbejdet består bl.a. i at kontrollere, at det ansøgte domæne ikke allerede er i brug (entydighed) samt at indføre domænet i navneservicen (den globale tilgængelighed). DK Hostmaster A/S udfører sine funktioner på grundlag af en aftale med DIFO, der formelt står som den juridiske person, der har fået tildelegeret det praktiske og tekniske arbejde med at varetage .dk-domænet. Danmark har i øvrigt to yderligere ccTLD'er, nemlig .gl for Grønland (for hvilket TELE Greenland fungerer som registrator/hostmaster, se hertil <www.nic.gl>) og .fo for Færøerne (for hvilket den private virksomhed Uni2 er hostmaster, se herved <www.nic.fo>).

.EU-domænet

Ved Europa-Parlamentets og rådets forordning nr. 733/2002 af 22. april 2002 om implementering af *top level*-domænet .eu er der nu taget skridt til at etablere en såkaldt akkrediteret .eu registrator, som skal "forvalte top level-domænet .eu i almenhedens interesse og ud fra principper om kvalitet, effektivitet, pålidelighed og tilgængelighed" (forordningens art. 4, stk. 2, litra a). I det nye *top level*-domæne skal ethvert foretagende, der har sit vedtægtsmæssige hjemsted, sit hovedkontor eller sin hovedvirksomhed i Fællesskabet, enhver organisation hjemmehørende i Fællesskabet (dog med forbehold af national ret) eller enhver fysisk person med bopæl i Fællesskabet kunne registrere domænenavne i dette *top level*-domæne. Den akkrediterede registrator er givet udtrykkelig hjemmel til at opkræve omkostningsbaserede geby-

rer samt at implementere konfliktløsningsprocedurer i overensstemmelse med anbefalingerne fra WIPO (som bl.a. indebærer, at parterne ikke berøves adgang til domstolsprøvelse). I forordningens art. 5 opstilles visse generelle rammer for virket som EU-administrator. Kommissionen får her hjemmel til at udstede generelle retningslinier for implementering af .eu *top level*-domænet, og disse retningslinier skal bl.a. omfatte "forebyggelse af spekulation i og misbrug af registrering af domænenavne". Det præciseres i den forbindelse, at der ved åbning af navnerummet skal gives mulighed for trinsvis registrering, således at navne- og varemærkeindhavere samt offentlige myndigheder får passende midlertidige muligheder for at foretage navneregistrering. Se hertil art. 5, stk. 1.

11.4.d. Internetdomæneloven

IDL gælder for Internet-domæner, der særligt tildeles Danmark (dog ikke Færøerne og Grønland, jf. § 29). Hertil hører på nuværende tidspunkt .dk-domænet, men loven vil også omfatte de domæner, der tildeles Danmark i forbindelse med fremtidens systemer til Internet-telefoni (det såkaldte ENUM-nummersystem, se herved betænkning 1450/2004, s. 40). Reglerne gælder både for den domæneadministration, der er i funktion i dag, og for den, der vil blive sat i funktion efter gennemførelsen af den udbudsforretning, der skal gennemføres i medfør af lovens § 4. Loven bygger på nogle få og enkle principper, der i vid udstrækning er hentet fra den konsensus, der været fremherskende herhjemme omkring arbejdet i DIFO og DK Hostmaster A/S. Hertil føjer sig nogle relativt komplicerede regler (som ikke omtales i det følgende) om denne udbudsforretning. De overvejelser, der ligger til grund for loven, er udmøntet i betænkning 1450/2004 om administration af domænenavne i Danmark.

Styring og medindflydelse

Siden domænenavnssystemets fødsel i 1980'erne har det været et bærende princip, at den, der forestår DNS-tjenesten for et CCTLD, skal repræsentere det samfund (dvs. den kreds af brugere), der kan antages at have nytte af dette domæne. I medfør af lovens § 6, stk. 1, har dette ført til en regel om, at administrator skal have en bred repræsentation af deltagere fra det danske internetsamfund. I overensstemmelse med den praksis, man hidtil har fulgt ved udpegningen af DIFO's bestyrelse, skal denne brede repræsentation sikres fra tre grupper, nemlig de private brugere (i DIFO's repræsenteret ved blandt andet Dansk IT og Forbrugerrådet), de professionelle brugere (f.eks. Dansk Handel og Service)

og internetbranchen (der først og fremmest repræsenteres ved IT-brancheforeningen).

Det er et særpræget, men væsentligt, træk ved den danske lovregulering, at administrators virksomhed ikke må udøves med gevinst for øje. Dette princip, der er indeholdt i lovens § 6, stk. 3, andet punktum, følges op af en pligt for administrator til at sikre virkeliggørelsen af det første af lovens formål, jf. § 1, nr. 1, nemlig sikringen af en "dynamisk og kvalitetspræget udvikling i det danske internet-samfund ved at tilvejebringe tilgængelighed, gennemsigtighed, effektivitet og sikkerhed om internet-domæner, der særligt tildeles Danmark", jf. henvisningen i IDL § 6, stk. 4, nr. 1. I tilknytning til lovens forbud mod at administrator driver erhvervsmæssig virksomhed fremgår det af IDL § 6, stk. 4, nr. 2, at administrator skal udvise omkostningsbevidsthed i sine dispositioner.

Driftsmæssige forhold

Formålet om at sikre tilgængelighed, gennemsigtighed, effektivitet og sikkerhed, jf. § 1, nr. 1, er i loven opløst i flere delreguleringer, der dels stiller krav til administrators identitet og demokratiske mandat, dels foreskriver en række konkrete pligter for administrator.

Krav om økonomi mv.

Ifølge § 6, stk. 2, skal administrator råde over tilstrækkelige faglige og økonomiske ressourcer til at kunne varetage sin opgave. Samme bestemmelses stk. 3 forbyder administrator at udøve anden aktivitet end administration efter loven.

God domænenavnsskik

IDL § 12, stk. 1, fastslår at registranter ikke må registrere og anvende domænenavne i strid med "god domænenavnsskik". Baggrunden for denne regel er angivet i betænkning 1450/2004, s. 206 ff. Man har ønsket at overføre den praksis, der følger af generalklausulen i mfl. § 1 til Internet-domæneområdet, således at den f.eks. også omfatter privatpersoner og offentlige myndigheder. Se nærmere herom afsnit 11.3.b.

11.4.e. Reglerne for .dk-domænet

Som tidligere nævnt indeholder de regler for registrering, administration og konfliktløsning vedrørende domænenavne under top level-domænet .dk, som DIFO har fastsat, det primære retsgrundlag mellem registranten og registrator. Indtil gennemførelsen af IDL var det antaget ved Sø- og Handelsrettens dom af 15. juni 2004 (der p.t. er under anke til Højesteret), at reglerne havde karakter af et aftalegrundlag mellem registranten og registrator. I overensstemmelse hermed giver reglerne DK Hostmaster mulighed for ved pligtbrud at "ophæve" aftaleforholdet mv. De gæl-

dende regler om registrering af domænenavne under .dk-domænet er vedtaget af bestyrelsen i DIFO og revideres løbende, senest med virkning for 1. juli 2005.

Fremgangsmåden

Det er både enkelt og billigt at erhverve et domæmenavn under .dk-domænet. Registrering foretages af en registrator, der har indgået aftale med DK Hostmaster A/S. Registratoraftalen er – sammen med ansøgningsformularer – tilgængelig fra <www.dk-hostmaster.dk>. Allerede i efteråret 2000 besluttede DIFO at lade den tidligere registreringsafgift til DK Hostmaster bortfalde til gengæld for en årsafgift, der i dag udgør 50 kr. pr. domæne – et beløb, som DIFO i 2005 har varslet nedsættelse af inden årets udløb. Reglerne for DIFO lægger ingen begrænsninger i, hvilket retsforhold registrator skal have til registranterne i relation til betaling. Derimod pålægger registratoraftalen registrator visse forpligtelser i henseende til kundebehandlingen, jf. nærmere reglerne i pkt. 4. Ligeledes indeholder aftalens pkt. 7 et forbud mod *warehousing*, som nu også følger af IDL § 12, stk. 2.

Tekniske krav

Ifølge DIFO-reglernes pkt. 2.1 kan et domænenavn alene registreres til ibrugtagning, såfremt oplysningerne på anmeldelsen er korrekte, registranten har indestået for, at registrantens brug af domænenavnet ikke krænker en tredjeparts navne- eller varemærkerettigheder eller i øvrigt må formodes at stride mod dansk lovgivning, og at registranten har afgivet en række oplysninger om sin egen juridiske identitet. Dernæst er det en betingelse, at anmeldelse indgives via en godkendt registrator.

Teknisk prøvning

For at DK Hostmaster skal kunne håndhæve princippet om *first filed, first served*, registreres ved hjælp af et tracknummer den rækkefølge, hvori anmeldelserne ankommer til DK Hostmaster. Ved anmeldelsens modtagelse fremsender DK Hostmaster tracknummeret til registrator som kvittering for modtagelse af og bevis for rækkefølgenummer for anmeldelsen. Kan DK Hostmaster efter opslag i sin database konstatere, at det ansøgte domænenavn ikke er i brug, og at betingelserne for registrering i øvrigt er opfyldte, registreres domænenavnet som ibrugtaget af registranten.

Ophør af registreringen

I konsekvens af den kontraktstanke, der ligger til grund for registrering af domænenavne under .dk-domænet, ophører domæneregistreringen, hvis der foreligger tilfælde af væsentlig misligholdelse fra registrantens side. De nærmere regler herom er indeholdt i DIFO-reglernes pkt. 2.4.1, der angiver en lang række situationer, hvor en domæneregistrering kan bringes til ophør. Den mest almindelige årsag til, at domæneregistrering ophører under .dk-domænet er, at registranten undlader at betale skyldige

ydelser, jf. pkt. 2.4.1, litra a. Derudover angiver bestemmelsen en række tilfælde, hvor forhold af mere teknisk karakter giver grundlag for en ophævelse af aftaleforholdet.

Kvalificerede domæner

At en domæneregistrering bringes ud af funktion på grund af manglende betaling kan være dybt problematisk for en virksomhed, som er vitalt afhængig af sine web-tjenester. For at minimere den risiko, sådanne virksomheder kan have for, at der utilsigtet sker sletning af et domænenavn som følge af manglende betaling, er der i DIFO-reglernes pkt. 2.5.7 indført særlige regler om såkaldt "kvalificerede domænenavne". Reglerne indebærer, at en registrant efter særskilt anmodning herom kan indgå aftale om at få sit domænenavn kvalificeret med den virkning, at DK Hostmaster i aftalens løbetid påser, at de angivne adresseoplysninger registreres (og at ændringer kun kan ske efter skriftlig henvendelse til DK Hostmaster). Hvor ophævelse normalt sker efter en forudgående elektronisk påkravsmeddelelse, får registranten af et kvalificeret domænenavn meddelelse ved anbefalet brev til den noterede registrant eller fuldmægtig. Årsafgiften for opretholdelsen af et sådant kvalificeret domænenavn er pt. 40 kr. ekskl. moms.

Prøvelsesspørgsmål

Som tidligere nævnt foretager DK Hostmaster ingen materiel prøvelse af ansøgerens ret til at anvende det pågældende navn. Denne politik følger internationale tendenser på området og må i øvrigt ses i lyset af, at det alligevel ikke ville være praktisk muligt for DK Hostmaster at foretage nogen udtømmende navneundersøgelse. Ansvaret for, at et domænenavn er taget lovligt i brug mv., hviler på registranten og – i kraft af den indgåede registratoraftale – i nogen grad på registrator. Ønskes en domæneregistrering ændret, må man derfor enten gå rettens vej (ved søgsmål eller gennem nedlæggelse af fogedforbud) eller klage til Klagenævnet for Domænenavne, jf. afsnit 11.4.f.

Dette udgangspunkt er dog modificeres på enkelte punkter:

Offentlig myndighedsbeslutning

Ifølge pkt. 2.4.1, litra b, kan den administrerende direktør i DK Hostmaster i samråd med bestyrelsen ophæve aftaleforholdet med registranten ved at slette eller ændre registreringen af et domænenavn, hvis der foreligger en anmodning herom fra en i henhold til lovgivningen kompetent myndighed, og domænenavnet åbenbart bliver brugt eller anvendt aktivt i strid med dansk lovgivning. Bestemmelsen er sjældent anvendt, eftersom der sjældent findes hjemmel til, at myndighederne kan meddele sådanne pålæg.

Almenhedens interesse

En anden modifikation er DIFO-reglernes pkt. 4.1, der giver DIFO ret til at beslutte, at domænenavne, der allerede er registreret til ibrugtagning, skal inddrages, hvis der skønnes behov for at

anvende domænenavnet i almenhedens interesse. Har domænenavnet været taget i aktiv anvendelse som led i registrantens almindelige virke, kan der tilkendes indehaveren en rimelig godtgørelse, som udredes af DIFO. Til dato har DIFO alene truffet beslutning om inddragelse af ét domæne, nemlig <co.dk>. Denne beslutning er efterfølgende underkendt ved Sø- og Handelsrettens dom af 15. juni 2004.

Suspension

Af større praktisk interesse er reglernes pkt. 4.2.1, hvorefter den administrerende direktør for DK Hostmaster og bestyrelsesformanden for DIFO i enighed kan suspendere et domænenavn (dvs. udelade navneserverhenvisningen), hvis registrantens aktive anvendelse af domænenavnet åbenbart har til *hensigt* på ulovlig vis at skabe *forveksling* med en tredjeparts identitet, domænenavn, hjemmeside, varemærke eller øvrige forretningskendetegn. Det er dog en betingelse herfor, at forholdene taler for ikke at afvente en afgørelse fra Klagenævnet for Domænenavne, fra domstolene eller fra offentlige myndigheder. Når behandlingen af en sådan suspension påbegyndes, skal registranten informeres herom enten pr. e-mail eller pr. telefon. Registranten skal samtidigt opfordres til at eliminere forvekslingsrisikoen. Sker suspensionen, og dokumenterer registranten ikke senest 14 dage herefter, at forvekslingsrisikoen er elimineret, overgiver DK Hostmaster sagen til Klagenævnet for Domænenavne med henblik på afgørelse af, om suspensionen skal videreføres. Som nævnt er *grundbetingelsen* for disse regler, at der foreligger en forvekslingsrisiko, som må anses tilsigtet af registranten.

I tillæg hertil fastslår DIFO-reglernes pkt. 4.2.2, at DK Hostmaster kan suspendere og slette et domænenavn af *sikkerheds- og samfundsmæssige hensyn*, hvis domænenavnet aktivt anvendes i forbindelse med "åbenbart ulovlige handlinger eller undladelser", der ikke er omfattet af reglerne i pkt. 4.2.1. Suspension kan kun ske, hvis de nævnte hensyn taler herfor, og disse hensyn ligeledes taler for ikke lade suspension eller sletning afvente en afgørelse herom fra Klagenævnet for Domænenavne, fra domstolene eller fra offentlige myndigheder.

Sådanne beslutninger kan derimod ikke forelægges Klagenævnet for Domænenavne. Dette hænger sammen med, at beslutningerne ikke angår kendetegnsforhold men alene sikkerheds- og samfundshensyn. Den beslutning, direktøren for DK Hostmaster træffer sammen med sin bestyrelsesformand, skal derimod forelægges for DIFO's bestyrelse, som herefter træffer den endelige afgørelse.

Da reglerne herom først træder i kraft den 1. juli 2005 er der i skrivende stund (juni 2005) endnu intet erfaringsmateriale herom.

Tegnsæt

I sin oprindelige skikkelse var det internationale domænesystem primært beregnet på domæner bestående af bogstaver fra det engelske alfabet, dvs. det såkaldte latin 1-alfabet bestående af bogstaverne fra A til Z og/eller tallene fra 0-9, med mulighed for adskillelse med bindestreger og med et karakterantal fra 1 til og med 63. I 2002 åbnedes .dk-domænet for registrering af yderligere specialtegn, nemlig æ, ø, å, ä, ö, ü og é. Reglerne herom findes i afsnit 2.2.2 og indebærer, at der i en periode på 30 dage, efter at DK Hostmaster har truffet den endelige beslutning om at udvide tegnsættet, sker en sideordnet registrering af de ansøgninger, der indgives om et specifikt domæne. Lignende regler gælder, når navnerummet åbnes for nye domæner og i relation til den venteliste-ordning, der ifølge reglerne gælder for allerede eksisterende domæner, jf. DIFO-reglernes pkt. 2.6.

Er der efter udløbet af 30 dages perioden flere ansøgere til et domænenavn, iværksættes en procedure, hvorefter de sideordnede ansøgere hver skal deponere et beløb på kr. 4.000,00 ekskl. moms for at være med i opløbet. Dette beløb stiger herefter til at udgøre i alt kr. 12.000,00 ekskl. moms, og er der fortsat flere kolliderende ansøgere på dette tidspunkt, sker der lodtrækning. Taberne får derefter de deponerede beløb frigjort. En tilsvarende procedure er i øvrigt fastsat i regelsættets afsnit 2.2.1, som indfører en særlig fremgangsmåde, hvorefter man kan blive optaget på venteliste med henblik på at indtræde i et allerede registreret domænenavn, såfremt dette (f.eks. ved manglende betaling af årsafgift) skulle blive ledigt.

11.4.f. Konfliktløsning

Problemstillingen

Tvister vedrørende retten til at registrere eller ibrugtage et domænenavn, kan enten indbringes for domstolene eller for en klageinstans, der yder konfliktløsningstjenester for det pågældende *top level*-domæne. I Danmark vil retssager om domænenavne kunne anlægges ved de almindelige domstole eller (inden for hovedstadsområdet) ved Sø- og Handelsretten i København, jf. rpl. § 9, stk. 1, nr. 6, jf. mfl. § 14 og vml. § 37. I mange tilfælde er den tid og de sagsomkostninger, der medgår ved en sådan retsprøvelse, ude af proportion med den værdi, registranten har udfoldet ved at registrere domænet. Dette har ført til en retsstridig praksis, hvor registranter registrerer domæner, der er sammenfaldende med kendte varemærker, vel vidende, at rettighedshaverne typisk må afholde betydelige sagsomkostninger for at kunne retsforfølge

deres domænenavn – tilmed med risikoen for badwill til følge. I sådanne tilfælde vil den krænkede part ofte vælge at "forlige" sagen mod betaling af et beløb på måske 10.000 eller 20.000 kr. for at få registranten til at slippe domænet. At man har oprettet et Klagenævn for Domænenavne, der mod betaling af et beskedent gebyr (500 kr. i erhvervssager, 200 kr. i forbrugersager) behandler tvister om domænenavne under .dk-domænet, er bl.a. begrundet i ønsket om at sikre en billig og effektiv prøvelse af disse sager, så krænkede parter ikke tvinges til at indgå sådanne forlig.

.dk-domænet

For domæner under .dk-domænet fastslår IDL § 28, stk. 3, at det af DIFO udpegede klagenævn for domænenavne fungerer i perioden fra lovens ikrafttræden og til der første gang er nedsat et klagenævn for internetdomænenavne. Dermed har Klagenævnet for Domænenavne allerede fra lovens ikrafttræden opnået den kompetence, der fremgår af lovens § 13, stk. 1. De vanskelige afgrænsningsspørgsmål, der tidligere har været om klagenævnets kompetence, har derfor kun retshistorisk betydning, se hertil 1. udgave af denne bog, s. 508 ff. Fra klagenævnets hjemmeside, <www.domæneklager.dk>, kan man dels hente yderligere information om nævnets virke, dels finde hele nævnets praksis.

Det fremgår af IDL § 16, stk. 1, at klagenævnets afgørelser er bindende, for så vidt som de ikke kan indbringes for nogen administrativ myndighed. Klagenævnets afgørelse kan derimod indbringes for domstolene senest 8 uger efter, at afgørelsen er meddelt den pågældende, jf. § 16, stk. 2. Klagenævnet kan tillægge en indbringelse for domstolene opsættende virkning, jf. § 16, stk. 3.

UDRP

I regi af ICANN er gennemført en såkaldt Uniform Dispute Resolution Policy (UDRP), som muliggør en hurtig påkendelse af åbenlyse krænkelsessager under de generiske top level-domæner samt enkelte landedomæner (herunder det i Norden ofte benyttede .nu-domæne). En part, der ønsker tvister afgjort ved et af de mest almindelige gTLD'er, .com, .org og .net – har mulighed for at gå frem efter denne procedure. For at begære et domæne slettet efter disse regler skal tre betingelser være opfyldte. Domænenavnet skal for det første være identisk eller lig et varemærke, som tilhører en anden. For det andet må registranten ikke kunne påvise nogen legitim interesse i at benytte domænenavnet. Og for det tredje – og vigtigst – må registranten have været i "ond tro" (*bad faith*) i forbindelse med registreringen. Alle tre betingelser kan give anledning til betydelig retlig og faktisk tvivl. På grundlag af reglerne er der truffet tusindvis af afgørelser af de ekspertpaneler, der nedsættes i medfør af UDRP-reglerne. Se nærmere om UDRP-

proceduren *Knud Wallberg* i U 2001B.47 ff. og *Lars Stoltze*: Internet Ret (2001), s. 154 ff. med omtale af praksis.

For at komme misbrug af domæneregistrering til livs har USA indført en Anti-cybersquatting Consumer Protection Act (ACPA), pub.law 105-113. Loven afklarer en række af de afgrænsningsproblemer, der knytter sig til samspillet mellem domæneregistreringen og varemærkesystemet, og den indfører herudover nogle særlige regler for at komme de omgåelseshandlinger til livs, som nettet ellers er særdeles velegnet til at understøtte: Hvor en krænker kan forsøge at smyge en ubehagelig retsafgørelse af sig ved at overdrage det omtvistede domæne, giver loven hjemmel for, at der rejses sag vedrørende domænet som en tinglig ret – såkaldte in rem-sager.

11.5. Navnekonflikter om Internet-domæner

11.5.a. Almindelige bemærkninger

Karakteren af de navnekonflikter, der kan opstå mellem Internet-domæner, beror på, hvilket domæne der er tale om, og hvilket regelsæt, der finder anvendelse herfor. Først og fremmest for at dæmme op for den misbrugsrisiko, der er omtalt s. 532 f., har der udviklet sig systemer for konfliktløsning for de enkelte domæner. Derfor gælder der ikke nødvendigvis samme regler om *grundlaget* for den prøvelse, der sker ved sådanne regler. Et panel, der virker efter ICANN's førnævnte UDRP-regler, har således ikke samme muligheder for at inddrage et domænenavn som det af DIFO nedsatte Klagenævn for Domænenavne har. Ligeledes vil en afgørelse truffet af domstolene på grundlag af almindelige regler dermed anvende et andet regelsæt end det, der gælder for det enkelte *top level*-domæne.

Til disse vanskeligheder kommer det problem, der kan opstå, når et domæne i ét land benyttes med henblik på markedet i et andet. Illustrerende herfor er den dom, Hanseatisches Oberlandesgericht afsagde den 2. maj 2002 om domænenavnet <hotel-maritime.dk>. Domænet var registreret af et dansk hotel fra hvilket hotellet drev en hjemmeside, der reklamerede for sin hotelvirksomhed – "Hotel Maritime" i København. Hjemmesiden indeholdt bl.a. informationer på tysk. Hotellet blev indstævnet under en forbudssag i Tyskland af den tyske hotelvirksomhed MARITIM Hotelgesellschaft mbH, der var indehaver af EU-varemærket "MARITIM" for hotelvirksomhed, og under henvisning til, at det danske hotel med domænenavnet krænkede de tyske varemærkerettigheder, uanset det danske hotel alene tilbyder sine ydelser i Danmark. Heri fik man

ikke medhold. Hverken Landesgericht Hamburg eller Hanseatisches Oberlandesgericht fandt, at den krænkelse, der måtte være begået i Danmark, havde relevans i Tyskland, eftersom det danske hotels tjenesteydelser alene kunne leveres i Danmark, uanset benyttelsen bl.a. også skete på det tyske sprog. Afgørelsen herom ville formentlig falde ud på samme måde efter danske regler.

Efter de gældende regler for .dk-domænet kan Klagenævnet for Domænenavne træffe afgørelse om, hvorvidt en registrering "er sket i strid med gældende dansk ret og nærværende regelsæt", se reglernes pkt. 5.2. Denne afgrænsning af nævnets kompetence har fortsat gyldighed, jf. IDL § 14, stk. 1, der overlader det til administrator at udarbejde regler for nævnets virksomhed. Udgangspunktet er derfor, at en afgørelse fra klagenævnet har samme indhold som en dom afsagt af en dansk domstol. Dette udgangspunkt er fra DIFO's side søgt cementeret ved sammensætningen af nævnet, jf. tilsvarende IDL § 13, stk. 6, 2. pkt. Klagenævnets formand har således siden dets etablering været højesteretsdommer, og dets ene medlem været professor i immaterialret.

I hidtidig praksis fra Klagenævnet for Domænenavne og fra de almindelige domstole har man dels anvendt varemærkeretlige regler, dels reglerne i mfl. §§ 1 og 5. Helt i overensstemmelse med de intentioner, der blev lagt til grund ved dets nedsættelse, har nævnet udviklet en righoldig og kreativ, men afbalanceret, praksis, der bl.a. inddrager almene synspunkter. Efter vedtagelsen af IDL og den heri indeholdte generalklausul (§ 12, stk. 1) må det antages, at praksis ved såvel klagenævn som i domstolene vil udvikle sig yderligere. Den praksis, der findes frem til nu (juni 2005), må derfor læses med tilsvarende forbehold.

11.5.b. Rene kendetegnskrænkelser

Hovedparten af de afgørelser, der træffes af Klagenævnet for Domænenavne angår egentlige kendetegnskrænkelser, herunder navnlig varemærkekrænkelser, hvor der ikke er nogen reel tvivl om klagerens ret til, forud for indklagede, at benytte det pågældende kendetegn. Det ville føre for vidt at nævne hele denne praksis her. Blandt de tidlige afgørelser kan nævnes afgørelsen i <scandrums.dk> (9.10.00), <gloridan.dk> (11.11.00), <thybiler.dk> (18.01.01), <ican.dk> (2.4.01), <powerware.dk> (2.4.01), <sonofontaletid.dk> (22.5.01) og <pollefrasnave.dk> (16.10.01). Yderligere praksis er gengivet hos *Kragelund m.fl.* (2005), s. 90 ff. og hos *Stoltze* (2001), s. 97 ff.

Ækvivalensvurderingen

Praksis fra Klagenævnet for Domænenavne har navnlig kastet lys over de særlige problemer, der opstår, når domænenavne regi-

streres med tilnærmelsesvis lighed med eksisterende varemærker. Se til illustration heraf sagen om <teledenmark.dk> (9.1.03). I sådanne sager foretages en ækvivalensvurdering, der er velkendt i varemærketretten. Se fra den tidlige praksis sagen om <gate2net.dk> (22.5.01), der fandtes forvekslelig med det stærkt indarbejdede <get2net.dk>, idet nævnet fremhæver den meget betydelige lighed mellem disse to navne, såvel lydmæssigt som visuelt.

Forkortelser

Består et varemærke af forkortelser, eller af få bogstaver, opstår to hovedspørgsmål. Det første drejer sig om, hvorvidt varemærket har særpræg. Det andet om, hvorvidt det hertil hørende domæne overhovedet krænker et andet domæne, der tilfældigvis (men med de få bogstaver, ikke helt usandsynligt) krænker det eksisterende varemærke. I denne vurdering vil man ofte foretage en integreret afvejning, der henser til, om der foreligger et *reelt misbrug*. Varemærketretten suppleres her med mfl. § 5, der forbyder erhvervsdrivende at benytte forretningskendetegn og lignende, der ikke tilkommer dem, eller at benytte egne kendetegn på en måde, der er egnet til at fremkalde forveksling med andres. Da mfl. § 5 kun gælder i erhvervsvirksomhed kan bestemmelsen ikke bruges direkte overfor privatpersoner, foreninger og offentlige myndigheder. Med vedtagelsen af generalklausulen i IDL § 12, stk. 1, vil en helt tilsvarende praksis dog nu kunne udvikle sig også uden for markedsføringslovens område.

Som eksempel på det vigtige samspil mellem varemærketretten og markedsføringsretten i den retlige regulering af domænenavne kan nævnes dommen i *U 2004.1561 H*. Her havde moderselskabet til BR-Legetøj A/S nedlagt påstand om at få overdraget domænenavnet <br.dk>, der var registreret af en Internet-virksomhed. BR-Legetøj A/S havde tilbudt at købe domænenavnet for 15.000 kr., men da registranten forlangte 300.000 kr., anlagde man sag. Højesteret fastslog, at den oprindelige registrant havde registreret domænenavnet for at hindre BR-Legetøj A/S i at registrere dette domænenavn for derefter at sælge det. Dette fandtes at være i strid med mfl. § 1 om god markedsføringsskik. Registranten blev derfor dømt til at overføre domænenavnet til BR. Dermed undgik man at tage stilling til, om forholdet også indebar en varemærkekrænkelse.

Legitim brug?

I de sager om varemærkekrænkelser via domænenavne, der når frem til domstolene, vil registranten ofte gøre gældende, at han har en legitim interesse i at bruge domænenavnet. En sådan brug kan f.eks. udspringe af, at domænenavnet anvendes som led i en markedsaktivitet, som mærkeindehaveren ikke kan modsætte

sig. I en sådan vurdering vil man foretage en *interesseafvejning*, hvor værdien af varemærket afvejes overfor registrantens interesse i at kunne råde over domænet.

Et eksempel herpå er Sø- og Handelsrettens dom i *U 2000.2300 SH*. I denne sag var domænenavnet <rolex.dk> taget i brug af en privatperson, som brugte det til køb og salg af brugte Rolexure. Ved dommen fik Rolex medhold i, at brugen af det pågældende domænenavn var uberettiget, og at det ligeledes var uberettiget at anvende, registrere eller opretholde andre domænenavne med navnet "Rolex". Retten lægger til grund, at brugen af det pågældende domænenavn var udtryk for, at sagsøgte uden Rolex's samtykke erhvervsmæssigt havde gjort brug af Rolex-varemærket, og at denne brug var egnet til at skabe forestillinger om sagsøgtes relationer til Rolex's virksomhed.

Dommens præmisser er næppe til diskussion for så vidt angår det domænenavn, der var stridens årsag. Det har utvivlsomt spillet en rolle, at man havde at gøre med et meget stærkt indarbejdet og kvalitetspræget varemærke. I en sådan situation bør domstolene ikke lade sig overbevise af halvkvædede viser om, hvilke "ideelle" motiver en registrant hævder at have for at sætte sig på domæner for store og indarbejdede mærker, som registranten i øvrigt ingen forbindelse har til. Tvivlsomt er det derimod, om sagsøgte også var blevet dømt, hvis han havde taget domænenavnet "salgafbrugterolexure.dk" i brug, jf. tilsvarende *Henrik Villumsen* i NIR 2001.261 ff. Som domskonklusionen er affattet vil en sådan ibrugtagning nu være uberettiget, men Sø- og Handelsretten kunne næppe have afsagt dom om, at et sådant domænenavn var i strid med den berømte urfabrikants rettigheder.

Klagenævnet har ofte set stort på de fantasifulde forklaringer, der kan fremkomme fra indklagede registranter på, at et domænenavn er taget i brug trods sammenfald med et indarbejdet eller i øvrigt kostbart varemærke. I sagen <group4.dk> (11.11.00) tilbageviste man en forklaring om, at det pågældende domæne, der var registreret samme dag som et stort børsnoteret selskab valgte at skifte navn til *Group 4*, skulle "anvendes i forbindelse med igangværende projektarbejde – bestående af tværfagligt samarbejde mellem 4 personer", og i <mercedesbenz.dk> (22.5.01) blev et påstået ønske om at bruge dette varemærke til en portal, der linkede til enkelte Mercedes-leverandører tilsidesat. Se tilsvarende sagen om domænet <jensen2najt.dk> (2.4.01), der fandtes krænkende overfor en restaurationsvirksomhed, der havde samme (varemærkebeskyttede) navn. Restaurationsvirksomheden vandt, trods registrantens forklaring om at ville benytte

domænet som grundlag for et debatforum vedrørende et tv-show af samme navn.

Tilsvarende er sket i amerikansk retspraksis. Et eksempel herpå er dommen om <panavision.com>, som en privatperson havde registreret. Domænet blev brugt til en hjemmeside, der viste luftfotografier ("vision") af byen Pana, Illinois, se *Panavision International, L.P. v. Dennis Toeppen*, 945 F.Supp. 1296 (1996), omtalt hos *Heine m.fl.* (2002), s. 518. Denne anvendelse fandtes at udgøre en krænkelse af det stærkt indarbejdede Panavision-mærke. Retten fandt i øvrigt, at det forsøg, Toeppen havde gjort på at sælge domænenavnet til Panavision for et beløb på 13.000 $, i sig selv udgjorde en kommerciel virksomhed. Det fremgik af sagen, at Toeppen havde domæneregistreret mere end 100 velkendte varemærker – et moment, der også i klagenævns- og voldgiftspraksis tillægges betydning som indikation for "bad faith".

11.5.c. *First filed, first served*-princippet

Problemstillingen

I sager, hvor to varemærkeindehavere kan hævde ret til samme varemærke men inden for forskellige vareklasser, opstår en konflikt, der kan tænkes løst efter to forskellige principper. Den ene består i at afveje, hvilke af de to mærkeindehavere, der reelt har størst brug for domænenavnet, dvs. hvilket varemærke, der er mest værd. En sådan vurdering er vanskelig at foretage og hører bedre hjemme i en aftaleforhandling, hvor indehaveren af det stærke varemærke køber sig til det hertil hørende domæne. Den anden mulighed består i at anvende et enkelt princip om først til mølle, det såkaldte *first filed, first served*-princip.

I dansk domænenavnspraksis har man fra et tidligt tidspunkt gjort brug af det sidstnævnte princip. En af de første afgørelser, hvor dette skete, var i sagen om <sams.dk> (11.11.00), hvor en privatperson med efternavnet Sams måtte acceptere, at en virksomhed, der lod sig forkorte gennem disse fire bogstaver, benyttede en hertil svarende domæneregistrering. Princippet er ligeledes lagt til grund i sagen om <playmaker.dk> (26.3.00), hvor to erhvervsdrivende inden for hver deres varegruppe anvendte dette identiske varemærke som domænenavn. Se ligeledes <ecco.dk> (3.10.03). Der er således tale om et princip, der nyder almindelig anerkendelse i sager om navnekollission.

Udgangspunkt om *first filed, first served* gælder kun, hvor domænet er registreret under samme *top level*-domæne. Det giver ikke nogen mening at anvende et sådant princip i relation til forskellige domænesystemer, hvor det netop *er* muligt at have sideordnede domæner (f.eks. <taxa.dk> og <taxa.nu>). En nav-

nekonflikt mellem kendetegnsrettigheder, der er registreret i sådanne forskellige *top level*-domæner, må løses efter almindelige kendetegnsretlige regler, hvor spørgsmålet om, hvem der har taget kendetegnet i brug først, indgår i samspil med andre retlige overvejelser.

U 1998.1464 Ø

Dette illustreres ved dommen i *U 1998.1464 Ø*. I denne sag fandtes en advokat, der alene havde anvendt betegnelsen "Dan Law" i Advokatsamfundets fortegnelse, ikke at kunne modsætte sig domænenavnet <danlaw.com>. Resultatet et klart: Der var tale om en forholdsvis generisk betegnelse, som advokaten kun havde taget i brug her i landet. En sådan national anvendelse kunne ikke begrunde en global anvendelse som den, der almindeligvis understøttes ved en .com-registrering. Skulle man lade den enkeltstående, nationale, ibrugtagning af en i øvrigt forholdsvis generisk betegnelse begrunde en fortrinsstilling under .com-domænet, ville man udvirke retsvirkninger, der går langt videre end hjemlet ved den nationale varemærkeret. Havde den advokat, der anvendte "Dan Law" som sin betegnelse, omvendt været *først i tid* i henseende til den pågældende .com-registrering, ville dette have sikret ham den pågældende registrering.

U 2002.2303 V

Et andet eksempel på denne afvejning er dommen i *U 2002.2303 V*, der fandt brugen af domænenavnet <elsalg.dk> uberettiget i forbindelse med e-mail og web-funktioner. Sagen var rejst af El-Salg A/S, som er et indkøbsselskab inden for el-varebranchen. Selskabet blev i 1998 omdannet fra at være et interessentskab, og i forbindelse med aktieselskabsstiftelsen fik de installatører, der havde indgået i interessentskabet, tilbud om at tegne aktier i det nye selskab. Sagsøgte var et installationsfirma, som i forbindelse med omdannelsen i 1998 ikke havde ønsket at tegne aktier i El-Salg A/S, men som utvivlsomt havde kendskab til dette selskabs aktiviteter. El-Salg A/S havde registreret et antal varemærker, hvori ordet "elsalg" indgik. Derimod havde man ikke taget domænenavnet <elsalg.dk> i anvendelse. Det gjorde den pågældende installatør derimod i juni 1998. Landsretten fandt, at betegnelsen "el-salg" var indarbejdet i markedet for engros-handel med el-artikler, og at navnet var egnet til at adskille de pågældende el-installationsforretninger fra forretninger, der ikke var aktionærer i El-Salg A/S. Installatørens fortsatte brug af domænenavnet <elsalg.dk>, efter at forretningsforholdet med El-Salg A/S var ophørt, fandtes at indebære et uberettiget forsøg på at drage fordel af El-Salg A/S' markedsføring og goodwill og var følgelig i strid med mfl. §§ 1 og 5 samt vml. § 4, stk. 1, 2.

punktum. Installatøren blev derfor tilpligtet at anerkende, at domænenavnet <elsalg.dk> skulle annulleres.

Forventelige kendetegn

First filed-princippet kan virke urimeligt, hvis en registrant får held til at registrere et domæne med et kendetegn, der endnu ikke er taget i brug, f.eks. fordi registranten "gætter" hvilket navn eller kendetegn en rettighedshaver senere vil vælge. Den "heldige" registrant kommer da rettighedshaveren i forkøbet ved at registrere domænet, før det egentlig er besluttet og anmodning om registrering afsendt. I disse tilfælde er det som regel enkelt at skyde igennem de "forklaringer", registranten fremkommer med som forsvar for sin registrering. Er der tale om en rent spekulativ handling, må domænet vige for den part, der efterfølgende vælger en aktiv brug. Denne aktive ibrugtagning etablerer nemlig en varemærkeret, som domæneregistranten ikke tilsvarende etablerer med sin registrering af domænet.

11.5.d. Hadedomæner

Det forekommer, at utilfredse forbrugere registrerer domæner, hvori indgår navnet på en leverandør, en myndighed eller en offentlig person, man stiller sig kritisk overfor. Domænet registreres da med hadeobjektets navn i kombination med et nedsættende ord. I den retlige vurdering af sådanne domæner er det væsentligt at sondre mellem registreringen af selve domænet og af den kombination af domæneregistrering og brug, der finder sted, når domænet anvendes som grundlag for en "hadeside" med information vendt mod en navngiven person eller virksomhed.

Angår hadedomænet et varemærke, og anvendes domænet til erhvervsmæssige aktiviteter, vil mærkeindehaveren almindeligvis kunne gøre indsigelse mod det. Således blev domænerne <fuckseoghor.dk> og <fuckseoghoer.dk> ved klagenævnets afgørelser af 2.12.04 overført til ugebladet Se og Hør. Afgørelserne er begrundet med, at der udover et debatforum blev udbudt produkter påtrykt "Fuck Se og Hør" fra domænet.

Er domænet derimod alene registreret med det hadefulde navn, men uden at der er gjort aktivt brug heraf i forbindelse med en web-tjeneste mv., vil det i almindelighed være vanskeligt for den krænkede part at komme igennem med en påstand om nedlæggelse af domænet. Men som regel understøtter domænet en hadeside, hvorfra der udveksles synspunkter vendt mod hadeobjektet.

I praksis for Klagenævnet for Domænenavne har man anlagt et konkret skøn over grovheden af det udsagn, der indeholdes i

domænet. I sagen om <lorte-seat.dk> (24.3.03) fremhæves det på den ene side, at registranten kunne have opnået sit formål med hjemmesiden gennem et mindre kraftfuldt udtryk. Under hensyntagen til flere momenter, herunder at klageren ikke havde anlagt injuriesøgsmål mod registranten, blev registreringen opretholdt. Se ligeledes <balkan-lorterejser> (19.6.03), hvor klagen ligeledes blev afvist.

Det kan undertiden spille ind, hvorledes registranten har optrådt overfor hadeobjektet. Ved nævnets afgørelse om <star-tur.dk> (1.5.02) blev dette domæne anvendt som hadeside vendt mod rejsebureauet Star Tour A/S. Registranten havde imidlertid tilbudt Star Tour A/S at overdrage domænet til rejsebureauet mod betaling af 20.000 kr. til dækning af indklagedes påståede udgifter ved en utilfredsstillende charterrejse. Klagenævnet fandt, at domænenavnet krænkede klagerens kendetegnsrettigheder, uanset at registreringen var sket med henblik på at fremsætte kritik. Domænet blev derfor anset for at være taget i brug med urette og overført til klageren.

Se i øvrigt til problemstillingen *Kragelund m.fl.* (2003), s. 106 ff. I tvivlstilfælde er udgangspunktet, at der gælder ytringsfrihed – også i den kommercielle verden. Efter sådanne synspunkter har man også i amerikansk retspraksis accepteret registrering af protestdomæner trods den anvendelse af varemærket, der herved finder sted, se f.eks. *Bally Total Fitness Holding Corp. v. Faber*, 29 F.Supp. 2nd, 1161 (C.D. Cal. 1998). Udfaldet har været et andet i Frankrig, jf. sagen *Société Compagnie Gervais Danone v. Société Le Reseau Voltaire et al.*, der har fundet sin afgørelse ved en byretsdom fra Paris fra maj 2001. Dommen fandt domænet <jeboycottedanone.net> retsstridig overfor fødevarevirksomheden Danone.

II.5.e. Domæner i strid med offentlig orden mv.

I kraft af den kompetence, Klagenævnet for Domænenavne har til at tage stilling til, om et domæne er registreret i strid med gældende dansk ret, har nævnet fra tid til anden skullet tage stilling til, om selve domænet krænker offentlige regler. I visse tilfælde, f.eks. når personer eller symboler fra eller med relation til Kongehuset har været inde i billedet, har nævnet uden videre skredet ind over for registreringen, se hertil sagerne om <kronprinsfrederik.dk>, <prinsessemary.dk> og <prinshenrik.dk> m.fl. (28.5.04). Det samme gælder, hvis der i loven har været anført en eneret el.lign. til at benytte et domæne og registranten åbenbart ikke besidder denne ret, se hertil klagenævnets samlede afgørelse af 8.5.03 om et antal advokat-relaterede domæner <ad-

vokat.dk>, <advokaten.dk>, <advokater.dk> og <advokaterne.dk>. Ved afgørelserne fik Det Danske Advokatsamfund medhold i, at registreringen af disse domæner var i strid med den beskyttelse af advokattitlen, der fremgår af rpl. § 120, se nærmere hertil *Bryde Andersen:* Advokatretten (2005), s. 453 f. Sagen er indbragt for domstolene.

Uden for disse tilfælde har nævnet derimod udvist en forståelig tilbageholdenhed med at skride ind over for registreringer. Som eksempel herpå kan nævnes sagen om <psykolog.dk>, (28.5.04), hvor nævnet trods bestemmelsen i psykologlovens § 21, der reserverer betegnelsen "psykolog" for den, der har bestået en højere eksamen i psykologi, ikke ville overføre dette domæne til en cand.psych., der ikke havde godtgjort særlige kendetegnsrettigheder til dette domæne. Sagen havde muligvis fundet et andet udfald, hvis den havde været indbragt af Dansk Psykologforening eller en lignende part med en almen interesse i benyttelsen af denne titel.

Er domænet registreret for en offentlig myndighed vil der almindeligvis ske overførelse til myndigheden. Dette er bl.a. antaget i sagen om <koldingkommune.dk> (24.6.04) og <grevebibliotek.dk> (12.4.05). Afgørelse herom kan også træffes af DK Hostmaster A/S på grundlag af DIFO-reglernes pkt. 4.2.2., se herom s. 542 f. Det retlige grundlag for en sådan inddragelse kan søges i strfl. § 131, se herom afsnit 11.2.c. Se også *U 2004.2209 Ø*, der fandt betegnelsen "netvokat" forvekslelig med advokatbetegnelsen, hvorved vinkelskriverloven var tilsidesat, se om denne lovgivning Bryde Andersen: Advokatretten (2005), s. 456 ff.

11.5.f. Oops-domæner

Mærkeindehaveren kan have en interesse i at registrere domænenavne, der ligger tæt på det egentlige mærke (f.eks. <microsft.com>) for at dække sig ind mod brugerens fejlagtige indtastninger i Internet-browserens navigeringsfelt. Sådanne registreringer – undertiden kaldet "*oops*-domæner" – er retligt uproblematiske, så længe trykfejlen ikke indebærer en isoleret krænkelse af et andet gyldigt bestående mærke. Hvis man uden rådighed over det pågældende navn eller mærke foretager en sådan registrering, vil registreringen kunne rammes efter almindelige varemærkeretlige regler, alt efter graden af den lighed, der består mellem mærket og oops-domænet, og alt efter mærkets styrke. I nyere tid er sådanne domæner blevet anvendt til at installere *malware*-programmel (f.eks. til brug for såkaldt *phishing*). I sådanne

sager vil DK Hostmaster nu kunne gøre brug af suspensionsreglen i DIFO-reglernes pkt. 4.2.2. Forud for indførelsen af disse regler har Klagenævnet for Domænenavnet afsagt et stort antal kendelser, der uden videre har fjernet registreringen af disse domæner. I de pågældende klagesager har registranten, der har befundet sig uden for Danmark, ikke svaret.

Supplerende litteratur

Der findes en righoldig litteratur om problemstillingen vedrørende *Internet-domænenavne*, herhjemme såvel som i udlandet. Ved læsningen af denne litteratur skal man i særlig grad være opmærksom på de meget skiftende regler og politiske løsningsmodeller, der har været gældende gennem tiderne. Dette gælder også de følgende fremstillinger: *Knud Wallberg* i U1997B.23 ff. (baseret på dagældende regler) og samme i U2000B.131 ff., *Henrik Villumsen* i U1997B.188 ff. og U1997B.566 f., *Erika Heveus* i NIR 1997.197 og *Lone Prehn* i U2001B.52 ff. med omtale af utrykt dansk praksis. Se ligeledes *Heine m.fl.*: InternetJura, 2. udg. (2002), kapitel 7, *Kragelund m.fl.:* Domænenavne – en juridisk håndbog (2003) og *Lars Stolze:* Internet-ret (2001), kapitel 4. Forholdet mellem varemærkeretten og domæneretten i internationalt perspektiv er for nyligt gjort til genstand for en svensk doktorafhandling, se *Ulf Maunsbach*: Svensk domstols behörighet vid gränsöverskridande varumärketvister – särskilt om Internetrelaterede intrång (Lunds Universitet, 2005).

De danske regler om konfliktløsning under .dk-domænet er behandlet af *Kasper Heine & Jakob Hedebrink* i U2001B.55 ff. Reglerne for konfliktløsning under de internationale topdomæner er behandlet af *Knud Wallberg* i U2001B.47 ff.

De amerikanske initiativer vedrørende dereguleringen af de generiske topdomæner samt konfliktløsningsproblematikken har givet anledning til en omfattende litteratur, der bl.a. stiller spørgsmålstegn ved det politisk ønskelige og juridisk holdbare i den form for selvregulering, man har gennemført. Se hertil *Mark Weston* i 16 CLSR (2000), s. 223 ff. samt det omfattende, men veldokumenterede, debatindlæg af *A. Michael Froomkin* i 50 Duke Law Journal 17 ff. (2000).

Problematikken om Internet linking og robottering er – som nævnt – behandlet i min artikel i U 2000.311 ff. Udover henvisningerne heri henvises til *Karl Svanström* i NÅR 2000.143 ff.

Kapitel 12. EJENDOMSRETLIGE SPØRGSMÅL

12.1. Information som sikringsaktiv

12.1.a. Problemstillingen

Fordi information fremtræder anderledes end de materielle aktiver, som tingsrettens regler tager sigte på, er det ikke uproblematisk at gøre information, og herunder navnlig digital information, til genstand for ejendoms- og panteretlige overdragelser. Information "overdrages" ved at blive genskabt og kan følgelig ikke uden videre "tages tilbage" i forbindelse med en *tvangsfuldbyrdelse*, jf. i det hele redegørelsen i afsnit 2.2.b. Dertil kommer at de *immaterialretlige regler* afgrænser parternes råderet anderledes end den almindelige ejendomsret, der udgør baggrundsretten for den almindelige pantsætningsaftale.

Vender vi os til de to fremtrædende aspekter ved digital information – det *kommunikative* (informationen som immaterielt aktiv) og det *immaterialretlige* (information som genstand for ophavsret, patentret mv.) – har dansk ret ikke opbygget regler om, hvordan – endsige hvorvidt – der kan stiftes tinglige rettigheder over den slags værdier. Systematisk har der ikke været behov for sådanne særregler, eftersom ejendoms- og panterettens almindelige regler principielt omfatter alle typer af formuegoder. Derfor står den ejendoms- og panteretlige retsanvendelse overfor en række IT-retlige *beskrivelsesproblemer*.

Ved bedømmelsen af, om der kan stiftes rettigheder over et informationsbærende *medium*, må man i den forbindelse anlægge forskellige sondringer. For det første må mediets rent materielle aspekter udsondres fra de immaterielle: Det er åbenbart, at man ikke ved at gøre udlæg i en bog, opnår nogen særlig ret til at benytte informationsindholdet i den på en særlig måde (f.eks. i strid med strafferetlige regler) endsige adgang til at disponere over forfatterens ophavsret. Udlægget knytter sig til det fysiske, "atomerne". Problemerne gør sig således gældende i relation til de immaterielle aspekter af bogen, "bits". Her må der indlægges

en række klare sondringer mellem, hvilken type information mediet (bogen) repræsenterer.

Når det gælder selve *informationssiden*, må der for det første sondres mellem de immaterielle rettigheder, der knytter sig til den pågældende information. Ubeskyttet – "fri" – information vil som regel kun have formueværdi i kraft af foranstaltninger af faktisk karakter, f.eks. til sikring af hemmeligholdelse. Heroverfor står den information, der beskyttes immaterialretligt, hvor man – alt efter, hvilken immaterialretlig beskyttelse der er tale om – kan etablere pante- og ejendomsrettigheder mv. Når det gælder *mediesiden*, må der for det andet sondres mellem de forskellige grader af fasthed, der kan bestå mellem information og medium.

Ved siden af den immaterialretlige beskyttelse må enhver beslutning om at finansiere IT-relaterede aktiver tage højde for de offentligretlige begrænsninger, der kan bestå i råderetten over forskellige typer af aktiver. For at kunne fuldbyrde et pant i et kundekartotek, må man f.eks. tage reglerne om persondatabeskyttelse i betragtning, sml. herved afgørelsen i *RÅB 1991.117*, der nægtede et konkursbo ret til at videregive medlemskartoteket med henblik på, at et selskab, der skulle videreføre dets aktiviteter, kunne foretage markedsføring mod de tidligere kunder.

I det følgende gennemgås nogle af de særlige problemer, der opstår ved etablering af tinglige rettigheder over information i vekslende faktiske og retlige fremtrædelsesformer. Kapitlet gennemgår ikke de almindelige regler om finansiering og sikkerhedsstillelse. Om finansiering af materielle aktiver henvises til de almindelige fremstillinger, se navnlig *W. E. von Eyben*: Panterettigheder, 8. udg., ved Henning Skovgaard (1987) og *Carstensen og Rørdam*: Pant, 7. udg. (2002).

12.1.b. Hensynsafvejning

Når man giver sig i kast med dette ejendoms- og panteretlige beskrivelsesproblem, er det væsentligt at holde fast ved de grundprincipper, som ejendoms- og panteretten er bygget op omkring:

Ligelighed

Ligelighedsprincippet går ud på, at en skyldners almindelige kreditorer som udgangspunkt skal have lige ret til skyldnerens aktiver. Princippet gælder først og fremmest ved universalforfølgning (konkurs mv.). Enkeltkreditorer har alene fortrinsret i et aktiv, hvis denne ret er ledsaget af den formalitet, sikringsakten udgør. Det nærmere indhold af denne sikringsakt beror på aktivets beskaffenhed og sikkerhedsstillelsens formål. Generelt tjener sikringsakten til at skabe *publicitet* omkring særrettigheden

og/eller til at *kontrollere*, at debitor ikke disponerer over aktivet i strid med rettighedshaverens interesser.

Publicitet

Publicitetshensynet tilgodeses ved, at sikringsakten indbefatter en offentliggørelse, hvorved eksisterende eller potentielle kreditorer advares om den særstilling, der er etableret. Formen for offentliggørelsen beror på formuegodets karakter. For fast ejendom, løsøre og værdipapirer sker den gennem registrering efter reglerne i TL §§ 1 og 47 samt § 66 i værdipapirhandelsloven. Registreringen kan afholde andre fra at give kredit i tillid til værdien af det pågældende formuegode. Publicitetshensynet varetages ligeledes i selskabsretten: Det begrænsede ansvar for aktie- og anpartsselskaber modsvares af en pligt for disse selskaber til at offentliggøre regnskaber. Undertiden kan kravet om publicitet ikke opretholdes konsekvent. Ejendomsrettigheder til ting består som bekendt uden nogen form for registrering, uanset om tingen er i ejerens besiddelse eller ikke. I relation til leasing med rent finansielt sigte (sale and lease back mv.) kan dette føles som en skævhed.

Kontrol

I visse tilfælde kan man fravige publicitetshensynet. Det gælder i særdeleshed, når der er mulighed for at kontrollere aktivets skæbne. Sikkerhedsstillelse over simple fordringer sker f.eks. gennem særskilt underretning til debitor (gbl. § 31). For at håndhæve ejendomsforbehold i forbindelse med konsignation kræves visse faktiske tiltag (rådighedsberøvelse, kontrolforanstaltninger mv.).

Individualisering

Det ligger underforstået i både publicitets- og kontrolhensynet, at en særrettighed altid må angå et aktiv, der kan identificeres. Uden et sådant krav ville debitor kunne underskyde andre aktiver under sikkerhedsretten og dermed bryde principperne om prioritet og ligelighed. Uden for tilfælde af virksomhedspant kan pant ikke stiftes i tingsindbegreb eller i samlinger af ensartede eller til et fælles brug bestemte ting, der betegnes ved almindelige benævnelser, TL §§ 47 a og 47 b. I et system, der bygger på registrering, er det forholdsvis let at tilgodese dette hensyn. Registreringen kan ske mere eller mindre nuanceret, hvorved der kan etableres mere eller mindre begrænsede rettigheder. I sammenligning hermed er et system, der kræver rådighedsberøvelse, mere kompromisløst. Kravet om, at debitor ikke må råde over det pågældende aktiv, svækker den almindelige brugsmulighed.

12.1.c. Er ubeskyttet information et formuegode?

Uafhængigt medium

Vil man stifte tinglige rettigheder over ubeskyttet information *som sådan*, dvs. information, der ikke er genstand for nogen form for immateriel retsbeskyttelse, må dette først og fremmest forudsætte, at denne information kan karakteriseres som et formuegode. Som hovedregel bør der kun kunne stiftes rettigheder over aktiver, der siden hen kan sikre kreditor en økonomisk interesse, der kan realiseres under en senere *tvangsfuldbyrdelse*. Såfremt tvangsfuldbyrdelsen ikke gør det muligt at realisere denne værdi, f.eks. fordi værdien ikke meningsfuldt kan bortsælges under tvangsauktion, taler meget for at nægte retsstiftelse i aktivet.

Forankret information

Når det gælder information, der er således forankret i et fysisk medium, at en eventuel tvangsfuldbyrdelse kan rette sig imod dette medium, er det for de fleste praktiske formål muligt at etablere sådanne sikringsrettigheder gennem tiltag mod selve mediet (rådighedsberøvelse af en harddisk med henblik på håndpant mv.). Omvendt er det klart, at information, der flyder frit i form af tanker, strømninger, idéer mv., ikke kan undergives en særlig form for retsbeskyttelse ved blot at blive genstand for en panteret el.lign. For nærmere at kunne afgrænse de tilfælde, hvor sikringsrettigheder kan komme på tale, må man derfor se på, hvilken grad af samhørighed der består mellem information og medium, jf. nærmere gennemgangen i afsnit 2.2.b.

Som her anført er visse typer information uløseligt fæstnet til deres medier, såkaldt *integreret information*. Eksempler herpå er de brugsting, vi omgiver os med: For forbrugeren er det ikke hverken praktisk muligt eller fristende at kopiere en kaffekande med et flot design. Den anden gruppe er den såkaldt *mediekompatible information*, f.eks. digital information på en diskette, som kendetegnes ved sin evne til at springe fra medium til medium gennem kopieringshandlinger, der både er nødvendige (hvis man f.eks. vil benytte sig af et program) og fristende (når licensforholdene ikke tillader det). I en tredje gruppe finder vi den *fleksible information*, som evner at springe ubesværet fra den ene type medium til den anden, f.eks. en litterær idé, som udtrykkes i samtale, nedfældes på papir, distribueres via e-post eller filmatiseres.

12.1.d. Integreret information

Integreret information indgår i de fleste formueaktiver, der er genstand for pant og andre sikkerhedsrettigheder og volder af samme grund ikke særlige vanskeligheder. Det er således åbenbart, at "informationen" om, hvordan en bil ser ud (med andre

ord bilens design), ikke påvirker muligheden for at stifte pant i bilbogen over den. Kun hvis man søger at stifte sikkerhed i *retten* til dette design, bevæger vi os udenfor den klassiske pantsætningslære. I talrige tilfælde vil overdragelsen af et informationsbærende medium alene tage sigte på, at erhververen skal have *rådighed* over et materiale samt – naturnødvendigt – over den information, der er uløseligt knyttet hertil (den integrerede information). Her kan de almindelige ejendoms- og panteretlige regler anvendes uden modifikationer.

Hvor denne erkendelse kan være enkel at nå til i relation til almindelige forbrugsvarer, kan den give anledning til vanskeligheder i relation til særlige typer af aktiver. Hvis et konkursbo sætter en harddisk med kundekartoteket til salg, må det bringes på det rene, om der blot sælges et stykke avanceret finmekanik eller om aftalen angår retten til at bruge kundekartoteket.

En lignende sondring er lagt til grund af *Robin Thrap-Meyer* i Complex 4/89, s. 24 ff. At sondringen ikke er udtømmende, ses bl.a. af, at IT-systemets forskellige komponenter kan være genstand for forskellige typer af immaterialrettigheder, der kommer til udtryk på hver deres måde. Den samtidige tilstedeværelse af forskellige rettighedstyper fører undertiden til regelkonflikter, f.eks. når de immaterialretlige regler fører til indgreb i et materiale (ødelæggelse af plagiater mv.) eller til tiltag, der afficerer den ejendomsretlige råden (sml. nedenfor under 12.2.b. om dommen om forlagskontrakterne *U 1988.619 Ø*).

12.1.e. Mediekompatibel information

Faktisk sikring

Faktisk hemmeligholdelse – og dermed "sikring" – af mediekompatibel information kan efter omstændighederne effektueres gennem foranstaltninger mod det medium, hvorpå informationen er fæstnet. Dette kan f.eks. ske ved, at dokumenter (f.eks. formularer) skjules, eller ved at adgangen til data forhindres ad fysisk eller logisk vej, jf. i det hele kapitel 4 om IT-sikkerhed. Dermed kan den pågældende information blive genstand for en eksklusiv råden udøvet af den person, der har kontrol over den pågældende hemmeligholdelse. Ved at gøre brug af programspærreanordninger, der sikrer mod uautoriseret kopiering af en *master-diskette*, kan licensgiveren sikre sig imod, at der tages flere kopier end hjemlet ved aftalen. Sådanne kopibeskyttelsesmekanismer indebærer en form for fysisk forankring i det medium, der danner grundlag for overdragelsen af informationsproduktet (f.eks. en diskette eller CD-ROM).

Drop dead-funktion

Ved at indbygge en såkaldt *"drop-dead"*-anordning mister programmet sin funktionalitet, hvis ikke der med brugerens betaling er givet adgang til særlige kodeord el.lign., og rettighedshaveren kan sikre sig, at programmet ikke anvendes efter et tidspunkt, hvor betalingen skulle have været effektueret. Som det nærmere fremgår af afsnit 17.5.b. straffer ophl. § 78 den, der forsætligt eller groft uagtsomt omsætter eller i kommercielt øjemed besidder midler, hvis eneste formål er at lette ulovlig fjernelse eller omgåelse af tekniske indretninger, som måtte være anvendt til at beskytte et edb-program.

Se nærmere om disse tekniske muligheder, *Robin Thrap-Meyer* i Complex 4/89, s. 32 ff. og *Andersen & Græbe* (1990) om de mekanismer, der hyppigt anvendes af shareware-producenter for at tilskynde til brugerregistrering. Anvendelsen af *drop-dead* anordninger kan være problematisk. Har anordningen hjemmel i parternes aftale, er der selvsagt intet til hinder for at forlade sig på en sådan form for sikring af leverandøren. Det problematiske opstår, hvis et senere omsætningsled lider skade ved anordningen. Er brugeren ikke advaret herom, vil leverandøren formentlig ifalde erstatningsansvar for adækvate datatab efter almindelige regler om ansvar for farlige produkter. Før den moderne harddiskteknologi blev mange PC-programmer afviklet fra originaldisketten. Dengang var det almindeligt at knytte programmet til en unik egenskab ved disketten, f.eks. et fejl-formateret spor. Svagheden ved en sådan kopibeskyttelse ligger dels i muligheden for at genskabe mediet med den pågældende egenskab, dels i de praktiske ulemper, den pålægger brugeren.

Hardware-integration

En særligt effektiv måde til kopisikring består i at lade programmet udgøre en integreret del af hardware, f.eks. således at det indbygges i en ROM-kreds. Denne praksis anvendes i mange mindre PC-systemer (laptops mv.); men muligheden står selvsagt kun åben for leverandører, der både leverer hardware og software. Dernæst kan fremgangsmåden komme i konflikt med nationale eller EU-retlige konkurrenceregler. Endelig forudsætter metoden, at man ved, hvilke programmer brugeren efterspørger. I praksis er metoden derfor mest velegnet til basale programtyper som f.eks. styresystemer og visse utilities. Standardprogrammel i den lidt mere kostbare ende, som leverandørerne ikke påregner noget stort markedsvolumen for, vil ofte gøre brug af hardware-baseret kopisikring: Brugeren påmonterer en "nøgle" ("dongle") på en af computerens udvidelsesporte, og systemet kræver nu, at brugeren indtaster et kundenummer for at kunne aktivere programmet. Mange brugere vil finde denne løsning tung, bl.a. fordi den kan afskære anvendelsen af den pågældende port til andre funktioner.

Kildetekst

Ved overdragelse af standardprogrammel får kunden – uden hensyntagen til omfanget af de rettigheder, der ledsager programoverdragelsen – sjældent rådighed over programmets kildetekstversion. Leverandøren ved, at en én gang "mistet" kildetekst kan reproduceres og efterfølgende dukke op i vidt forskellige sammenhænge mv. Ved alene at overdrage objektkoden kan rettighedshaveren etablere en faktisk sikring mod uberettiget anvendelse af kildetekst. Dette skaber en sikkerhed over den information, som ligger i kildeteksten, der i praksis har samme værdi som en tinglig retsstiftelse

Se modsat *Nørager-Nielsen* i Beck & Bruun Nielsen (1987), s. 73 ff., der vil behandle den sikkerhedsret, der etableres over kildeteksten til et program, som håndpant i løsøre, omend det erkendes, at betingelsen om rådighedsberøvelse "kan forekomme kunstig", al den stund leverandøren fortsat er i besiddelse af et eksemplar heraf. Som anført ovenfor i teksten kan man alene opretholde en håndpanteret i information, hvis pantsætteren afskæres fra at gøre brug af den. Da programmers funktion beror på objektkoden, må det i givet fald være den, der skal rådighedsberøves – eventuelt ved at panthaveren får rådighed over et password el.lign., der eksklusivt kan aktivere programmet. En sådan rådighedsberøvelse vil svare til nøglepant. Se ligeledes *Hanne Bender & Susanne Karstoft*, U1991B.83 f.

Vanskeligheder

Svagheden ved sådanne tiltag består i, at hemmeligholdelsen som hovedregel kun består, så længe de faktiske tiltag opretholdes. Hvis den produktionsproces, der netop kan profitere af informationen, kun kan opretholdes ved, at informationen anvendes af en flerhed af personer (produktionsmedarbejdere, kunder, rådgivere etc.), kan det være forbundet med uoverstigeligt praktisk besvær at håndhæve en hemmeligholdelse. Vel kan hvert enkelt led bindes op på kontraktsforpligtelser, og vel dækkes misligholdelse af sådanne forpligtelser i et vist omfang af de konkurrenceretlige regler (mfl. §§ 1 og 10), men vandtætte systemer er sjældne på dette område. Den værdifulde og nyttige information synes at følge en naturlov, hvorefter den dupliceres og spredes som ringe i vandet i takt med, at der er behov for at bruge den.

Selv om information som sådan ikke dækkes af en immateriel retsposition, er der intet *principielt* til hinder for, at den anvendes som finansieringsgrundlag. Hvis blot man holder sig på afstand af det forbud mod pant i "tingsindbegreb", der følger af TL § 47a (som først og fremmest bæres af interessen i at undgå, at pantsætter underskyder andre aktiver under pantet end dem, han har signaleret overfor omverdenen gennem sikringsakten), hersker der som udgangspunkt fuld aftalefrihed også i panteretten. Kan den panthaver, der har underpant i et kundekartotek, f.eks. leve

med den risiko for forringelse af pantets værdi, der vil være forbundet med, at andre tilegner sig informationerne heri, vil pantet i selve kartoteket være gyldigt. Sådanne kartoteker indgår i øvrigt ofte som led i de virksomhedsoverdragelser, der effektueres ved konkursbehandling, se f.eks. *U 1980.693 ØLK* om et patientkartotek, og for norsk ret *Rt. 1992.1629*.

Hemmeligholdelse

Ønsker kreditor derimod at sikre sig muligheden for eksklusivt at kunne udnytte en sådan informationsmængde, ligger den eneste mulighed herfor i en effektiv hemmeligholdelse. Den sikkerhed, man herved opnår, svarer imidlertid ikke til den, man opnår gennem sikkerhedsstillelse i ting (pant, tilbagetagelse mv.). De vanskeligheder ved at skulle tvangsrealisere en værdi, der udelukkende skyldes en aftalehjemlet flerhed af handlinger, vil formentlig stille sig til hinder for anvendelsen af de almindelige sikkerhedsregler.

Praksis om goodwill

Tilsvarende betragtninger finder udtryk i retspraksis vedrørende pantsætning af goodwill i forretninger. Tidligere landsretspraksis har været forbeholden overfor etablering af særskilte rettigheder i immaterielt prægede aktiver. I *U 1980.693 ØLK* fandt Østre Landsret, at et telefonabonnement, der var installeret i en tandlægeklinik, var omfattet af skyldnerens formue og derfor henhørte under konkursmassen, se også *U 1950.587 Ø*. I ingen af sagerne fik fallenten derfor medhold i, at telefonen skulle udgå af virksomhedsoverdragelsen. Omvendt nægtede *U 1990.796 ØLK* pantsætning af goodwill i en forretning drevet fra et lejemål uden afståelsesret. Denne dom er med rette kritiseret, og efter Højesterets dom i *U 1993.392 HKK* er praksis ændret. Dommen, der stadfæster en dissens til den indankede dom fra Vestre Landsret, lægger til grund, at goodwill må anses for et frit omsætteligt formuegode, og at den omstændighed, at panthaveren ikke kan sætte den pågældende goodwill på tvangsauktion, ikke berøver den tinglige ret enhver betydning. Under henvisning til, at den pågældende goodwill må anses for tilstrækkeligt specificeret, tillades underpantsætningen. Denne linje er senest fulgt op ved *U 1993.782 V*, der antog, at der ved en aftale om pantsætning af goodwill i en tandlægevirksomhed drevet fra lejede lokaler var sket fornøden individualisering. I dommen i *U 1993.543 V* antog Vestre Landsret, at pant i goodwill også omfattede mønstre og modeller mv. Se om disse domme *Anders J. Andersen & Knud Wallberg* i J1993.275 ff. og *Werlauff* i J1993.308 ff. og J1994.26 ff.

Anvendelse af mediekompatibel information giver anledning til særlige vanskeligheder ved gennemførelse af *ejendomsforbehold* og lignende. Disse spørgsmål behandles i afsnit 20.2. om køb af information.

Virksomhedspant

Efter de regler om virksomhedspant mv., der er indsat i tinglysningsloven ved lov nr. 560 af 24. juni 2005, er det blevet muligt at etablere pant i immaterialrettigheder på en ny og – set fra et finansieringsmæssigt synspunkt – mere effektiv måde end tidligere. Ifølge reglerne i TL § 47c, stk. 3, nr. 7, kan et virksomhedspant blandt andet omfatte "goodwill, domænenavne og rettigheder i henhold til patentloven, varemærkeloven, designloven, brugsmodelloven, mønsterloven, ophavsretsloven og lov om beskyttelse af halvlederprodukters udformning (topografi)". I det pantebrev, som etablerer et sådant virksomhedspant, skal pantsætteren (gennem afkrydsning) markere, om han ønsker pant i disse aktiver, ligesom han kan reflektere en sådan panteaftale i relation til andre af de aktiver, der nævnes i § 47c, stk. 3 (for eksempel simple fordringer, råvarer, driftsinventar og driftsmateriel, drivmidler og besætninger mv.). Virksomheden kan ligeledes tinglyse et dokument, som går ud på, at aktiver af den nævnte karakter ikke kan underpantsættes, jf. TL § 43, stk. 2.

12.1.f. Fleksibel information

Problemerne ved at "finansiere" *fleksibel information* er iøjnefaldende, hvis man foretager det tankeeksperiment at skulle etablere sikkerhed i selve den rådgivning, debitor investerer i hos en professionel rådgiver. Det lader sig selvsagt ikke gøre at stifte tingli-ge rettigheder over advokatens råd om, hvorledes man gennem en nøje planlagt transaktion kan spare skat.

Man kan diskutere, om det således er en gyldighedsbetingelse eller blot en praktisk common sense betragtning om, at retten ikke bør befatte sig med meningsløsheder, der ligger bag denne betragtning, jf. *Hanne Bender*: Edb-rettigheder (1998), s. 281 ff.; men denne diskussion har næppe den store praktiske betydning. Er der praktisk mulighed for at gennemføre tvangsfuldbyrdelse i et dokument eller en anden bærer af en informationsmængde, der isoleret set er ubeskyttet, og består der almindelig markedsmæssig efterspørgsel efter et sådant aktiv, må såvel rettighedsstiftelse som tvangsfuldbyrdelse være mulig, medmindre dette måtte være afskåret efter særlige regler.

For at kunne stifte fuldstændige eller begrænsede rettigheder over fleksibel information (der principielt kan løsrives fra mediet), må der kunne etableres en situation, der gør det muligt at gennemføre en tvangsfuldbyrdelse mod denne information. Hvis virksomheden har udviklet et idékoncept, der er nedfældet på et A4-ark, kan man ikke uden videre sælge denne information på tvangsauktion: Hvis en potentiel køber skal forventes at give bud

ved tvangsauktionen, vil han ønske først at stifte bekendtskab med den, dvs. læse den pågældende A4-side. Men gør han det, kommer han dermed til at stifte bekendtskab med informationen. Dette problem kræver praktiske løsninger. En løsning kan være indgåelse af forudgående hemmeligholdelsesaftaler efter en procedure, der sikrer, at den hemmeligholdelsesforpligtede ikke forpligter sig til at hemmeligholde information, han allerede råder over, eller som er tilgængelig via offentlige medier, jf. *PA* s. 628 ff.

12.2. Immaterialrettigheder som sikringsobjekt

12.2.a. Problemstillingen

Udgangspunktet

Som udgangspunkt er der aftalefrihed på immaterialrettens område. Den, der har ophavsret til et værk eller patentret til en opfindelse, kan disponere frit over sin ret med de begrænsninger, der følger af retssystemets almindelige regler, herunder aftale- og konkurrencerettens. Underforstået heri ligger en tilsvarende ret til at stifte alle de begrænsede rettigheder over den immaterielle ret, som retssystemet hjemler. De modifikationer, der gælder fra dette udgangspunkt, følger af de enkelte immaterialretslove.

Immaterialretten er en del af formueretten. Ser man bort fra de særlige ideelle rettigheder, som ophl. § 3 giver hjemmel for, må man betragte de immaterialretlige regler som konkurrencebestemte økonomiske retspositioner. Som udgangspunkt gælder derfor den regel, at rettighedshaveren kan "overdrage" disse retspositioner ved at lade andre indtræde i de beføjelser, som det pågældende regelsæt hjemler. På tilsvarende vis kan rettighedshaveren også stifte begrænsede rettigheder over sin ret som f.eks. ejendomsforbehold, tilbageholdsret og pant. Se *Knoph*: Åndsretten (1936), s. 138, *Nørager-Nielsen* i Beck & Bruun Nielsen (1987), s. 75 og i det hele *Robin Thrap-Meyer* i Complex 4/89.

Modifikationer

Dette udgangspunkt må dog efter omstændighederne modificeres. For det første kan det følge af de regler, der gælder for den pågældende immaterielle retsposition, at en bestemt overdragelse ikke kan gennemføres, se f.eks. ophl. § 3, stk. 3, der begrænser mulighederne for at overdrage de personlige rettigheder generelt. Ligesom rettighedshaveren i sagens natur kun kan overdrage en rettighed i det omfang den består, kan han kun overdrage de

rettigheder, der efter reglerne om den pågældende eneret er overdragelige. Gælder der et overdragelsesforbud, udtømmer dette rettens værdi.

Regler af den sidstnævnte karakter er der ikke mange af. Selv for ophl. § 3, gælder det – modsætningsvis – at disse kan frafaldes, for så vidt der er tale om "en efter art og omfang afgrænset brug af værket". De begrænsninger, der kan følge af droit moral-reglen, er yderligere varetaget gennem ophl. § 29 og ved den særlige bestemmelse om udlægsfritagelse i rpl. § 515, stk. 1, se til illustration *U 1985.812 Ø*, der gav ret til udlæg i de af en billedhuggers skulpturer, der tidligere havde været udstillet.

Interessen samler sig om de begrænsninger i rettens omfang, der kommer til syne ved en overdragelse. Problemgennemgangen koncentrerer sig derfor om de regler, der fastslår omfanget af en rettighedsoverdragelse. Disse regler veksler, alt efter om der overdrages eksemplarer, fuldstændige rettighedsmængder eller licenser.

12.2.b. Retsbeskyttede eksemplarer

Når en immateriel rettighed materialiseres i et (ophavsretligt) eksemplar eller et (patentretligt) produkt, og når dette eksemplar eller produkt overdrages i den almindelige omsætning, indsnævres rettighedshaverens krav i overensstemmelse med de regler, der gælder om immaterialretlig konsumption, se herom ophl. § 19, PL § 3, stk. 3, nr. 2, og HLL § 6, stk. 2, nr. 1. Til grund for disse konsumptionsregler ligger den betragtning, at den rettighedshaver, der har lagt sit retsbeskyttede produkt ud i fri omsætning for at høste frugterne af et marked, også må affinde sig med markedets vilkår, herunder med den kendsgerning, at varer og ydelser skifter hænder. Hvor meget rettighedshaveren må tåle, beror på reglerne for den pågældende eneret. Ophl. § 19, stk. 3, undtager f.eks. udlån af eksemplarer af edb-programmer udgivet i maskinlæsbar form fra den ophavsretlige konsumption. Omvendt omfatter den patentretlige konsumption alle efterfølgende handlinger, herunder også udlån og udleje. Halvlederlovens konsumptionsregel gælder alene, for så vidt rettighedshaveren har bragt produktet i omsætning i et EU-land (regional konsumption).

I det omfang, ophavsretten til et eksemplar er konsumeret, kan erhververen frit disponere over det. I så henseende begrænses han nu kun af de almindelige ejendomsretlige regler samt af særlige regler, der kan være til hinder for salg af et teknologisk produkt (eksportkontrol mv.). Blandt de regler, der kan tænkes at afskære

overdragelsen af et teknologisk produkt, kan nævnes reglerne om beskyttelse af personoplysninger (LBP), der vil være til hinder for videregivelse af oplysninger, der udgør registre om enkeltpersoners rent private forhold mv.

Er der indtrådt konsumption, kan den, der har pant i et patenteret produkt eller en ophavsretligt beskyttet bog eller videokassette, søge sig fyldestgjort heri uden hensyntagen til den immaterielle ret, eftersom dennes virkninger jo ikke længere griber produktet. Det samme gælder for den, der har pant i det udgivne eksemplar af et edb-program, da undtagelsesbestemmelsen i ophl. § 19, stk. 3, alene gælder for udlån. Er retten derimod ikke konsumeret, vil eneretten som hovedregel slå igennem og hindre, at der sker tvangsfuldbyrdelse over eksemplaret.

Konkursproblemet – licensaftaler

Man kan diskutere, hvornår der indtræder konsumption i relation til overdragelser, der effektueres på grundlag af en licensaftale med en licenstager, der siden går konkurs uden at kunne betale licensafgift. Har den fallerede licenstager inden konkursen overdraget de eksemplarer, han har fremstillet i henhold til licensen, til tredjemand, og har licensgiver ikke taget en form for "kontantforbehold" i forbindelse med sin licens, der kan håndhæves i overensstemmelse med princippet i kbl. § 28, stk. 2 (f.eks. således, at videreoverdragelse af de pågældende eksemplarer kun kan ske, når der er betalt licensafgift; nærmere herom nedenfor), fører konsumptionsreglerne til, at licensgiver ikke kan gøre yderligere krav gældende. Er eksemplarerne vel frembragt, men henligger de fortsat i den fallerede licenstagers varetægt, vil der ikke være indtrådt konsumption. Dermed opstår spørgsmålet om, hvorvidt eneretten da er til hinder for en overdragelse.

U 1961.148 H

Spørgsmålet er ikke ukendt i panteretlig teori. Kreditor i den sag, der blev afgjort ved *U 1961.148 H* (Motorhussagen), havde for Sø- og Handelsretten gjort gældende, at den licensafgift, der var forfalden til betaling før konkursen, var et massekrav. Dette anbringende blev ikke gentaget for Højesteret, hvor hovedproblemet var, om indbygningen af de pågældende motorer i den færdige produktion bevirkede, at et ejendomsforbehold var mistet. Sø- og Handelsretten fandt, uproblematisk, at den licensafgift, der var forfalden til betaling ved konkursens indtræden, ikke udgjorde et massekrav, og at boets efterfølgende salg af de pågældende motorer ikke bevirkede, at et sådant krav opstod. Kreditor havde *ikke* gjort gældende, at selve salget (og ikke blot produktionen) udgjorde en rettighedsbelagt handling, ligesom sagens patentretlige aspekter ikke blev fremdraget.

U 1988.619 Ø

Denne sidstnævnte problemstilling kom imidlertid frem i *U 1988.619 Ø*. Under konkursbehandlingen af et forlag erklærede boets kurator, at boet ikke ville indtræde i de kontrakter, forlaget havde haft med en række forfattere. Kurator indtog det standpunkt, at boet med dette afkald besad et varelager (de allerede producerede bøger), som det kunne disponere over her som i ethvert andet konkursbo. Da der ikke forelå nogen tinglig retsbeskyttelse vedrørende de pågældende bøger, kunne rettighedshaverne ikke rejse massekrav i forbindelse med varelagerets bortsalg. Deres tilgodehavender måtte anmeldes som simple krav på lige fod med andre kreditorers tilgodehavender. Heroverfor gjorde forfatterne gældende, at forlagsretten til bøgerne måtte falde tilbage på forfatterne ved boets manglende indtræden i forlagskontrakterne. Forfatterne påberåbte sig ligeledes overdragelsesforbuddet i ophl. § 28, stk. 2, nu – omend i ændret skikkelse – § 56, stk. 2.

Landsretten gav boet medhold ud fra den betragtning, at rettighedshaverne kendte til muligheden for videresalg, men desuagtet ikke havde sikret deres ophavsretligt begrundede krav efter sædvanlige formueretlige regler. Derfor måtte hensynet til konkursligelighed vinde. I et obiter dictum bemærker retten, at dette resultat indebærer, at rettighedshaverne "vil være henvist til at anmelde deres eventuelle fordringer i konkursboet på lige fod med andre kreditorer, hvis krav knytter sig til produktionen af nævnte bøger".

Diskussion

Den ret for boet til at overdrage retsbeskyttede eksemplarer, som dommen statuerer, må i almindelighed respektere den licensaftale, fallenten har indgået med rettighedshaver. Havde fallenten forud for konkursen fremstillet flere eksemplarer end hjemlet ved aftalen, var konkursboet afskåret fra at disponere over disse eksemplarer. I relation til programlicenser, hvor eksemplarfremstillingen sker stort set omkostningsfrit, skaber dette en skævhed. Har fallenten inden konkursen foretaget den eksemplarfremstilling, der er hjemlet ved licensaftalen, kan det senere konkursbo realisere dette varelager og henvise rettighedshaveren til at anmelde sit krav som simpelt krav. Er dette ikke sket; men giver licensaftalen fortsat mulighed for at fremstille eksemplarer, kan boet ikke foretage denne eksemplarfremstilling uden at indtræde i licensaftalen og dermed afregne royalty i medfør af den som massekrav. Skævheden til trods er resultatet klart og velbegrundet. Se i øvrigt *Mogens Munch:* Konkursloven med kommentarer, 9. udg. ved Lars Lindencrone Petersen og Anders Ør-

gaard (2001), s. 296 og 368 f., og *Hartvig Jacobsen:* Forlagsretten (1951) s. 228 f.

U 1983.545 H

I *U 1983.545 H* var et pladeselskab gået konkurs. Selskabet havde haft en aftale med Nordisk Copyright Bureau (der giver komponisters og musikforlags rettigheder i licens til brug bl.a. ved pladeproduktion) om at benytte NCB's repertoire mod vederlag. Ifølge aftalen indtrådte vederlagspligten "i det øjeblik pladen forlader producentens lager eller lagre", idet afregning skulle ske efterfølgende. Efter konkursen opsagde NCB aftalen med pladeselskabet, idet NCB gjorde gældende, at konkursboet efter pladeselskabet dermed mistede retten til at overdrage producerede plader. Højesterets, meget kortfattede, præmisser henviser til, at retten til at producere og videregive var overdraget til fallenten. Retten til at producere plader i henhold til aftalen var ophørt før konkursen. Retten til videresalg angik kun de plader, der lovligt var produceret før konkursen.

Løsningsmodeller

Skal licensgiver sikre sig mod en sådan situation, må dette være ved at tilrettelægge aftalen således, at salg af eksemplarer kun kan finde sted mod licensgivers løbende, *individuelle tilladelse*. Ulempen heri ligger i det administrative besvær: Licensvederlaget skal betales, før varen kan sælges. Omvendt er dette besvær ikke større end det, man i andre lignende sammenhænge (f.eks. ved nøglepant og konsignation) pålægger en rettighedshaver. Skal man overkomme dette problem, må der fires på begreberne, f.eks. ved at indføre kontrolmekanismer svarende til dem, man vil stille til konsignataren som betingelse for at opretholde dennes ejendomsforbehold i konsignationsvarelageret, se hertil *ET* s. 441. En anden, mere fristende, løsning kunne være at knytte en slags ejendomsforbehold til de *enkelte eksemplarer*. Men også denne model volder problemer, eftersom licensgiver jo ingen ejendomsret har til eksemplarer, men kun en forbudsret, der afskærer en brug af det, der strider mod hans ret.

Disponerer boet i strid med immaterialretlige begrænsninger, udvirker dette et selvstændigt retsbrud, der kan redresseres mod boet som massekrav i medfør af lovgivningens almindelige regler. Ligesom det ansvar, der gælder for bestyrelsen i en erhvervsdrivende virksomhed (f.eks. et aktie- eller anpartsselskab), er dette ansvar baseret på en culparegel, der er tolerant overfor den risiko, der er forbundet med at træffe forretningsmæssige dispositioner.

12.2.c. Fuldstændige rettighedsoverdragelser

Overdragelse og pantsætning af immaterialrettigheder (f.eks. ophavsretten til en roman – i modsætning til forlagsretten til den, altså retten til at udgive forlagsmæssige publikationer) sker som udgangspunkt efter reglerne om overdragelse og pantsætning af løsøre. Begrebet løsøre er således det residualbegreb, der indbefatter de rettighedstyper, der ikke udtrykkeligt er gjort til genstand for særlige regelsystemer, således som det f.eks. gælder om fast ejendom. Med løsøreregelerne har man et velkendt regelsystem, som uden vanskelighed kan anvendes. Den eneste vanskelighed ligger i at afklare, hvilke særlige begrænsninger de immaterialretlige regler sætter.

Ophavsret

Selv om ophavsretsloven – sammenlignet med andre immaterialretslove – rummer et vist beskyttelsespræceptivt element, er der intet til hinder for, at en ophavsmand overdrager samtlige økonomiske rettigheder til et værk, hvis det ellers har solidt fundament i en klar vedtagelse, jf. ophl. § 53, stk. 3. Er der balance mellem ydelser, er der heller intet realt til hinder for en sådan disposition.

Derimod indeholder loven en række begrænsninger i den ret, erhververen herefter indtræder i i mangel af særlig aftale. Efter ophl. § 56, stk. 2, må erhververen af retten ikke overdrage retten videre uden samtykke, medmindre videreoverdragelsen er sædvanlig eller åbenbart forudsat. Har rettighedshaveren givet samtykke til pantsætning, må dette samtykke forstås som et stiltiende samtykke til, at ophavsretten også kan videreoverdrages i forbindelse med tvangsfuldbyrdelse. En sådan tvangsfuldbyrdelse er netop kreditors formål med at stifte en panteret. Ophl. § 56, stk. 2, giver ikke direkte hjemmel for at stifte underpant i en erhvervet ophavsret og dermed videreoverdragelse af denne i forbindelse med en realisering af pantet. Om en sådan ret består, må bero på aftalens karakter. Som i de almindelige overdragelsestilfælde er det den part, der gør en ret til videreoverdragelse gældende, der har bevisbyrden herfor. Overdrageren vedbliver i alle tilfælde at være ansvarlig for, at aftalen med ophavsmanden bliver opfyldt, jf. § 56, stk. 2, sidste pkt.

Kildetekst overdragelse

Overdrages samtlige rettigheder til et edb-program til eje, vil der være en formodning for, at overdrageren ligeledes afstår eksemplarer af kildetekst og objektkode, og at overdragerens brugsret til disse eksemplarer i alle tilfælde ophører. Det vil ligeledes følge af en sådan total overdragelse, at overdrageren herefter ikke skal have ret til at videreudvikle eller bearbejde programmet.

Tilsvarende foranstaltninger vil man ikke træffe i forbindelse med underpantsætning af samtlige rettigheder til et program, hvor rettighedshaveren tilmed typisk vil foretage bearbejdninger og fejlrettelser mv. som led i sin normale virksomhed. Derfor vil det pantsatte program (i.e. den version, det eksisterede i, da sikringsakten blev effektueret) ofte være en ældre version end det program, som pantsætter er i besiddelse af på det tidspunkt, hvor retten realiseres.

Bearbejdninger

Uden en særlig aftalehåndtering af dette spørgsmål vil en gennemtvingelse af panthaverens ophavsretlige beføjelser over det underpantsatte program give udlægshaveren eller tvangsauktionskøberen ret til at forbyde pantsætteren/rettighedshaveren (eller dennes successor) at råde over programmet ved at foretage bearbejdninger af de pantsatte dele af det, jf. ophl. § 4, stk. 1, 2. led. Omvendt vil pantsætteren, der måske allerede har forberedt markedet på den kvalitetsforbedring, som ligger i bearbejdningen, kunne udhule markedsværdien af det underpantsatte program, hvis han nægter at give bearbejdningen i licens. Konflikter af denne art må imidlertid løses inter partes, f.eks. således at panthaveren opnår en ret til at erhverve ophavsretten til fremtidige værker. Det er derimod tvivlsomt, om videreudviklinger af et program kan betragtes som en individuelt bestemt ydelse, som der efter almindelige ejendomsretlige grundsætninger stiftes ret over ved aftaletidspunktet. Som udgangspunkt må det formentlig antages, at kreditor skal stifte tinglyst underpant i disse bearbejdninger, efterhånden som de foreligger, evt. således at der løbende sker tinglysning af pant i bearbejdninger i takt med, at disse implementeres. Der findes således ingen ækvivalent til TL §§ 37 og 38, der løser problemet.

Patent

Ligesom en ophavsret kan et patent overføres helt eller delvis. PL § 43 fastslår, at en licenstager, der har fået ret til erhvervsmæssigt at udnytte opfindelsen, ikke kan overdrage denne ret til andre, medmindre andet måtte være aftalt. Bestemmelsen må ses i sammenhæng med, at en patentlicens ofte vil give licenstageren et indblik i patenthaverens erhvervshemmeligheder mv.

Halvleder-rettigheder

Hvis retten til en registreret topografi overgår til en anden, eller hvis nogen opnår licens, herunder tvangslicens, indføres dette efter anmodning og mod betaling af et gebyr i registeret over topografier, HLL § 8. Loven indeholder ingen regler, der forbyder videreoverdragelse af retten til topografier.

12.2.d. Licenstilfælde

Angår overdragelsen kun visse nærmere angivne retspositioner (f.eks. en ret til at benytte en opfindelse, der er afgrænset i tid og territorium), taler man om, at der er meddelt licens. En licens vil altid knytte sig til en bestemt eneretsposition; den, der uden licensen ville gøre det muligt at forbyde den beskyttede handling. I det følgende bortses fra de ophavsretlige licenser, der knytter sig til enkelte programeksemplarer, jf. herom ophl. § 36. Opmærksomheden samles om de mere begrænsede tilladelser, typisk til en nærmere defineret eksemplarfremstilling.

Ophavsret

Som allerede nævnt fastslår ophl. § 56, stk. 1, den hovedregel, at overdragelse af ophavsret ikke giver erhververen ret til at ændre værket, medmindre ændringen er sædvanlig eller åbenbart forudsat. Bestemmelsen lægger op til et skøn, som kan være vanskeligt at udøve. Meningen har ikke været at begrænse anvendelsen til tilfælde, hvor der består et særligt personligt forhold mellem rettighedshaver og licenstager, som f.eks. i mange forlagsaftaler om udgivelse af skønlitteratur. Men der må foretages en kvalificeret vurdering af, om licensgiveren har gode grunde til at modsætte sig en videreoverdragelse, hvad enten disse grunde har økonomisk eller ideel karakter. Er der f.eks. tale om en kildetekstlicens, der er meddelt en lokal distributør med henblik på tilpasning til sproglige og andre lokale forhold, må det være åbenbart, at licensen ikke kan videreoverdrages: Kildetekst er for det første information, som håndteres under en høj grad af fortrolighed. Dernæst kan det have betydning for licensgiverens renommé, at den, der udnytter en licens, lever op til visse kvalitative krav. Det forhold, at licensgiveren i kraft af hæftelsesreglen i ophl. § 56, stk. 2, 2. pkt., modtager sin royalty fra en senere licenstager, kan være en spinkel trøst, hvis produktet i mellemtiden er kompromitteret på markedet.

Rettighedsforbehold

Ganske som overdrageren af løsøre kan forbeholde sig ejendomsretten til det overdragne, indtil betaling er sket, kan overgang af en immateriel retsposition være betinget af et vederlag. I overensstemmelse med princippet i kbl. § 28, stk. 2, forudsætter gyldigheden af et sådant forbehold, at det er taget senest ved overgivelsen, og at det opfylder visse krav om klarhed mv. En licensgiver, der har tilladt licenstager at udnytte en immaterialret til frembringelse af et vist antal eksemplarer, der dækkes af den pågældende ret, kan derfor som udgangspunkt ikke under henvisning til manglende betaling mv. modsætte sig, at der disponeres over disse eksemplarer.

Særlige spørgsmål

Når erhververen – licenstageren – alene indtræder i en begrænset del af ophavsretten til et værk, vil der i almindelighed ikke være tvivl om, at overdrageren – licensgiver – fortsat har ret til at *ændre* i værket. Er licensen ikke-eksklusiv, kan han tillige give det i licens til andre.

Patentret

I relation til patentregistreringsproceduren vil en delvis patentoverførelse, herunder en licens, indebære, at både licenstager og licensgiver sammen figurerer som indehavere af det pågældende patent, se herved PL § 44 og betænkning NU 1963:6, s. 17. Indførelsen i patentregisteret er hverken nogen gyldighedsbetingelse eller sikringsakt, jf. nærmere nedenfor. For at undgå tvivl om, hvorvidt licenstager har ret til at videreføre patentet, jf. PL § 43, fastslår § 54 i patentansøgningsbekendtgørelsen (bekendtgørelse nr. 6 af 6. januar 2003), at der på begæring skal ske notering om, hvorvidt sådanne rettigheder består.

Halvlederrettigheder

HLL § 9 regulerer både den fuldstændige og den delvise overgang af rettighederne til en halvledertopografi. For så vidt angår den delvise rettighedsovergang (licens), bestemmer § 19 i halvlederbekendtgørelsen (bekendtgørelse nr. 482 af 10. juni 2003 angående ansøgninger om beskyttelse af halvlederprodukters udformning (topografi)), at det efter begæring kan noteres, om registreringshaveren har ret til at give yderligere licens. I modsætning til den tilsvarende regel i patentansøgningsbekendtgørelsens § 54, er formålet her at skabe klarhed om, hvorvidt overdragelsen er total. Erhververen af en halvlederret har som udgangspunkt ret til videreoverdragelse.

12.2.e. Underpant

Udgangspunktet

Indholdet af sikringsakten ved stiftelse af pant i immaterialrettigheder fremgår af reglerne om løsøre. Pantebreve, der giver underpant i løsøre, skal efter TL § 47, stk. 1, tinglyses for at få gyldighed mod aftaler, der i god tro indgås med pantets ejer, og mod retsforfølgning. Tinglysning af løsørepant sker i personbogen, der for hele landet føres ved retten i Århus.

Identifikation

Underpant i løsøre skal identificeres. Som før nævnt kan denne identifikation være vanskelig at foretage, når der er flere mulige værdi-aspekter af det pantsatte. Såvel ved formuleringen af denne centrale del af panteaftalen som ved fortolkningen heraf må der tages udgangspunkt i, hvilken retsstilling man ønsker, når pantet realiseres. Er der f.eks. stiftet pant i "det til virksomheden hørende IT-system mrk. XXX", er det åbenbart, at formålet hermed er at lade panthaveren eller dennes successor indtræde med

en brugers rettigheder. Pantsættes "de til programmet hørende ophavsrettigheder", vil dette indbefatte samtlige overdragelige rettigheder til et program, altså en helt ubestemt flerhed af retspositioner. En sådan panteaftale må – som en tilsvarende overdragelsesaftale – fortolkes forsigtigt, jf. princippet i ophl. § 53, stk. 3. Formålet vil almindeligvis være at give panthaveren ret til at oppebære de beløb, retten kaster af sig, når den gives i licens, eller når den tvangsrealiseres. Princippet i ophl. § 53, stk. 3, vil typisk føre til, at der overdrages et antal rettigheder, svarende til den værksudnyttelse, der gøres brug af i pantsætterens virksomhed på det tidspunkt, hvor pantet stiftes. Uden nærmere vedtagelse indtræder panthaveren dermed ikke i licensrettighederne fra ukendte udnyttelsesformer. Dertil kommer, at licensindtægterne for de udnyttelsesrettigheder, der allerede er effektueret inden overdragelsen, må fraregnes – ophavsretten vedrørende disse stykker af lagkagen er jo allerede solgt.

Bearbejdninger

Tinglysning af underpant i et værk har altid relation til værket i den form, det har, når sikringsakten finder sted. Hvis et program f.eks. er genstand for løbende ændring, opdatering eller vedligeholdelse, må sikringsakten som før nævnt iagttages i relation til hver enkelt ændring i værket. Omvendt vil pantsætteren (ophavsretshaveren) efter omstændighederne være afskåret fra selv at udnytte licensretten, ligesom han vil være afskåret fra at foretage yderligere licensoverdragelser uden panthaverens samtykke. Derfor må panthaveren løbende give tilladelse til hver enkelt yderligere licens, idet han samtidigt hermed foretager denunciation i den fordring på royalty mv., der herved opstår mod licenstageren.

Frugter

Er panteaftalen formuleret således, at den omfatter "samtlige de til programmet hørende ophavsrettigheder *samt disses kendte og fremtidige frugter og surrogater*", vil panteretten tillige indbefatte licensrettigheder. Der er således intet til hinder for at tinglyse pant i en rettighed, der også omfatter frugterne af denne rettighed, f.eks. licensindtægter. Se herved dommen i *U 1984.1009 VLK,* der anerkendte tinglysning i sin helhed af et løsøreejerpantebrev i et edb-system, der tillige gav pant i "indtægter af pantet herunder leje og forpagtningsafgift samt erstatningssummer". For så vidt angår de indtægter, der kendes ved panteaftalens indgåelse, f.eks. indtægter fra indgåede licensaftaler, får panteaftalen den virkning, at panthaveren tillige får *sikkerhed* i de hertil hørende fordringer trods forbuddet mod pant i fordringer, jf. TL § 47, stk. 4, jf. herom ovenfor. Som anført her er sikringsakten ved pantsætning af licensindtægter denunciation til de enkelte licens-

debitorer. Mere tvivlsomt kan det være, om "fremtidige surrogater", der ikke kendes, når pantet stiftes, skal behandles på samme måde. Som udgangspunkt må de regler, der gælder for kendte surrogater, finde anvendelse, jf. *Carstensen & Rørdam* (2002), s. 77 ff. Det forhold, at indtægten er uforudset, bør ikke modificere dette resultat.

Registrering?

For immaterialrettigheder, hvis gyldighed beror på en registrering (patenter, rettigheder til halvledertopografier og varemærker), har det været overvejet, om registreringen kan erstatte tinglysningen. For at vurdere om en sådan registreringsadgang kan opfylde en retlig funktion som sikringsakt, må man bl.a. skele til, om registreringsproceduren udelukkende er indrettet på at skulle kontrollere, om de materielle betingelser for rettens tilstedeværelse er opfyldt, eller om myndigheden også forudsættes at tage stilling til tingsretlige spørgsmål i forhold til tredjemand. Sker registreringen ved en rent rettighedsregistrerende myndighed, som f.eks. Patent- og Varemærkestyrelsen er det i relation til patenter, varemærker, designs mv., må det som udgangspunkt antages, at denne registrering ikke i sig selv afføder tredjemandsvirkninger af tingsretlig art.

Patenter

For *patentrettens* vedkommende er dette bl.a. fastslået i *U 1935.799 Ø*, der tillod tinglysning af et løsørepantebrev (skadesløsbrev) i rettighederne efter et dansk patent og en engelsk patentansøgning. Tinglysningsdommeren havde afvist at tinglyse pant i patentansøgningen under henvisning til, at rettighedshaveren kunne foranstalte notering i patentregisteret. I et obiter dictum bemærker landsretten skarpsindigt, at en sådan notering under alle omstændigheder kun ville kunne omfatte det danske patent. Retten støtter imidlertid resultatet på en almindelig regel, hvorefter anmeldelse til patentregisteret ikke kan erstatte den tinglysning, der kræves efter TL § 47.

Reglerne om pantsætning af patentrettigheder er ikke ens i de øvrige nordiske lande. På grundlag af SOU 1985:10: "Pantsättning av patent", har Sverige indført udtrykkelige regler herom indført i 12. kapitel af den svenske patentlov. Pant i patentet eller ansøgningen registreres her hos patentmyndigheden. Lignende regler har man overvejet ved indførelsen af den danske patentlov af 1967. Man veg dog tilbage af frygt for at skabe mere uklarhed end klarhed gennem en sådan løsning. For finsk ret, se *Ilkka Rahnasto* i NIR 1992.368 ff., der analyserer en finsk højesteretsdom fra 1988.

EF-patentforslaget

Den 1. august 2000 har EU-Kommissionen fremsat forslag til rådsforordning om EF-patenter (KOM(00) 412 endelig udg.), se nærmere herom *Koktvedgaard* (2005), s. 195. Det foreslåede EF-

patent tænkes at finde anvendelse på ethvert patent, der er meddelt af den europæiske patentmyndighed i medfør af den europæiske patentkonvention, se forslagets art. 1. I forslagets art. 16-18 er der givet regler om den tingsretlige retsstilling. Ifølge art. 16, stk. 1, kan et EF-patent uafhængigt af virksomheden pantsættes eller gøres til genstand for anden tinglig ret. En sådan pantsætning skal – hvis en af parterne anmoder herom – indføres i EF-patentregisteret, jf. forslagets art. 56, og offentliggørelse i EF-Patenttidende, jf. forslagets art. 57. Denne offentliggørelse kan tænkes at have retsvirkninger gennem national ret, men som bestemmelsen er formuleret fastslås ikke umiddelbare EU-retlige, tingsretlige retsvirkninger heraf. Om tvangsfuldbyrdelse fastslår forslagets art. 17, at EF-patentet kan gøres til genstand for tvangsfuldbyrdelse. Såfremt en af parterne anmoder herom skal også tvangsfuldbyrdelse indføres i patentregisteret. Ligeledes følger det af art. 18, at et EF-patent kan indgå i konkursbehandling el.lign.

EU-varemærker

På *EU-varemærkeområdet* følger det af art. 23, stk. 1, jf. artiklerne 17, 19 og 22, i varemærkeforordningen (nr. 40/94), se EFT 1994 L 11/1), at overdragelse, pantsætning mv. og licens vedrørende sådanne rettigheder først opnår retsvirkning overfor tredjemand, når de er indført i registret. Bestemmelsen fastslår også, at der ikke indtræder ekstinktion, hvis erhververen er i ond tro. Bestemmelsen finder dog ikke anvendelse, hvis EU-varemærkeretten erhverves ved overdragelse af en virksomhed som helhed, se art. 23, stk. 2. Indtil fælles regler for medlemsstaterne vedrørende konkursbehandling træder i kraft, gælder lovgivningen i behandlingslandet eller den lovgivning, der udpeges i henhold til de konventioner, der måtte finde anvendelse.

I amerikansk praksis, se *In re Peregrine Entertainment, Ltd.*, 116 Bankruptcy Reporter 194 (1990), har man ladet meddelelse om overdragelse af en ophavsrettighed til U.S. Copyright Office – til trods for den fakultative adgang hertil efter den amerikanske ophavsretslov – være en gyldighedsbetingelse for etablering af en panteret i en flerhed af nærmere angivne ophavsrettigheder. Den pågældende praksis er omdiskuteret, se herved *Thomas P. Storer* i 12 CLR 6 (1990), og har næppe afklaret den bestående tvivl om retsstillingen på området. Dens argument om det hensigtsmæssige i en central registrering af sådanne rettigheder er vel sympatisk, men dækker kun de "amerikanske" dele af rettighederne, sml. præmisserne til *U 1935.799 Ø*. En så grundlæggende ændring af retsstillingen som den, dommen statuerer, må ske gennem lovgivningen og i givet fald følges op af tjenlige procedureregler for den pågældende myndighed.

De nævnte synspunkter mod at lade registreringen være afgørende for pante- eller ejendomsretten til et patent, er de samme for så vidt angår andre registreringer, der har formel karakter, som f.eks. ved registrering af halvledertopografier.

Domænenavne

Som nævnt i afsnit 12.1.e kan en virksomhed vælge at give rettigheder til "goodwill, domænenavne og rettigheder i henhold til … varemærkeloven" i virksomhedspant, jf. TL § 47c, stk. 3, nr. 7. Hverken loven eller den bagvedliggende betænkning om virksomhedspant (betænkning nr. 1459/2005) tager stilling til spørgsmålet, se herved betænkningen s. 126 ff. Klart er det imidlertid, som også anført i betænkningen, at der i praksis tinglyses underpant i domænenavne ved personbogen i Århus efter reglerne om løsøre.

Med vedtagelsen af lov nr. 598 af 24. juni 2005 om internetdomæner, der særligt tildeles Danmark (IDL) kan der være grund til at genoverveje denne praksis. I den betænkning (nr. 1450/2004), der ligger til grund for loven, antages det, at retten til et domænenavn er en *brugsret*, som giver en teknisk adgang til at råde over den post i DK Hostmasters navneserver, der sikrer, at en internetbruger dirigeres hen til den ønskede server uden at angive dennes ip-nr., se nærmere hertil betænkningens s. 120 ff.

Set i dette lys er det nok mest korrekt at beskrive det aktiv, der pantsættes, når der pantsættes et domænenavn, som en *obligatorisk* rettighed, nemlig som den fordringsret, registranten har mod den registrator, der driver den pågældende hostmasterfunktion. Ført ud i sin yderste konsekvens vil denne betragtning indebære, at domænenavne skal pantsættes efter reglerne om simple fordringer (nemlig fordringen på registrator om, at denne udfører de nødvendige databasefunktioner). På grund af den tilsyneladende lighed, der består mellem domænenavne og registrerede navnerettigheder (for eksempel varemærker), er det imidlertid almindeligt antaget at anvende løsøreregleme, således som dette ligeledes er sket i tinglysningspraksis. De forslag, der tidligere har været fremsat om indførelse af en særlig lovgivning til sikring af panterettigheder i domænenavne mv. (se herved *Thomas Munk Rasmussen* i U 2003B.7 ff. med mit gensvar i U 2003B.187 f.), må efter indførelsen IDL anses for uaktuelle.

12.2.f. Håndpant

Som betingelse for at stifte håndpant i løsøre opstiller man almindeligvis et krav om, at skyldneren berøves rådigheden over det pantsatte. Denne sætning kan imidlertid ikke uden videre anven-

des ved pantsætning af IT-baseret information (programmel eller data), hvor en rådighedsindskrænkning kan tænkes at tage sigte på forskellige aspekter.

Selve rettigheden

Der er principielt intet til hinder for at give programrettigheder i håndpant, men konstruktionen er upraktisk. Kravet om rådighedsberøvelse vil afskære pantsætteren fra at gøre brug af ophavsretlige beføjelser som f.eks. eksemplarfremstilling i forbindelse med egen brug, videreudvikling og overdragelse mv. Panthaver måtte følgelig selv forestå disse – for pantets værdi essentielle – handlinger. Den typiske panthaver (f.eks. en bank) vil hverken have interesse eller kyndighed til at forestå dette arbejde. I praksis vil udgangspunktet derfor være underpant.

Eksemplarer

Det ligger på den anden side klart, at der ikke etableres nogen rådighedsberøvelse over IT-baseret information gennem faktiske tiltag rettet mod en kopi af en given informationsmængde. Panteretligt vil en rådighedsberøvelse af en programkopi kun dække mediet. Da digital information i praksis altid fremtræder som kopier, må håndpant i digital information følges op med rådighedsberøvelse, der retter sig imod ethvert medium, der materialiserer den pågældende information. Er denne information beregnet til at komme til almenhedens kundskab (f.eks. standardprogrammel, offentlige databaser el.lign.), vil det være umuligt at effektuere et krav om rådighedsberøvelse. Det samme gælder for den information, som pantsætter forudsættes at gøre brug af som led i sin virksomhed (f.eks. kildetekst til brug ved fejlrettelse og opdatering).

Licensindtægter

Derimod kan der etableres rådighedsberøvelse mod de indtægter, en rettighed kaster af sig, dvs. indtægten ved overdragelse af kopier. Er produktet givet i licens, vil der typisk bestå et gældsforhold til licenstageren, hvorefter denne skal erlægge en licensafgift beregnet efter eksemplarfremstilling eller brug. Denne fordring kan pantsættes efter reglerne om simple fordringer. Sikringsakten består her i denunciation jf. gbl. § 31, en foranstaltning som panthaveren i egen interesse må drage omsorg for. En effektueret pantsætning og efterfølgende denunciation betyder dog ikke, at panthaveren kan hæve licensindtægterne, hvis de kommer til udbetaling, før panteretten er aktualiseret. Uden modstående aftale har den, der har pant i et gældsbrev med løbende udbetaling, heller ikke en sådan ret, se *von Eyben* (1987), s. 100 og *Carstensen & Rørdam* (2002), s. 75 f.

12.3. Vindikation og ekstinktion

12.3.a. Problemstillingen

I det foregående er reglerne om sikringsakter behandlet i relation til kolliderende kreditorkrav. Et helt andet spørgsmål angår panthaverens eller erhververens sikring mod kolliderende krav fra andre aftaleerhververe (dobbeltdispositioner). Når sådanne spørgsmål rejses i relation til en immateriel retsposition, kan det være vanskeligt at få overblik over, om der overhovedet er tale om en dobbeltoverdragelse. I den almindelige ejendomsret kan dette typisk afgøres ud fra en faktisk konstatering af, hvor tingen befinder sig, henholdsvis hvem der ønsker den udleveret. I immaterialretten kan flere rettigheder over værket mv. principielt godt eksistere side om side. Man må derfor dels se på karakteren af den ret, som den originære retserhverver kunne gøre gældende, dels på de efterfølgende dispositioner over den.

En rettighedsoverdragelse kan være mere eller mindre eksklusiv. I en *ikke-eksklusiv* licens (som den, der sædvanligvis ledsager et programprodukt) er licensgiveren ikke afskåret fra at meddele tilsvarende licenser til andre. Her kan spørgsmålet om dobbeltoverdragelse derfor ikke opstå. Til forskel herfra udelukker den *eksklusive* licens andre end licenstageren fra at udføre de handlinger, der dækkes af licensen, ligesom licensgiveren i almindelighed er afskåret fra – eventuelt begrænset i tid eller territorium – at disponere til anden side. Det er her spørgsmålet om dobbeltoverdragelse opstår.

Reglerne om vindikation og ekstinktion af tinglige formuegoder finder ikke anvendelse på uberettiget råden over immaterialrettigheder. Det er almindeligt antaget, at immaterialrettigheder ikke ekstingveres, som ejendomsrettigheder over ting efter omstændighederne gør det, jf. herved *Blomqvist:* Overdragelse af ophavsrettigheder (1987), s. 76 f. med henvisninger.

12.3.b. Uhjemlede eksemplarer

Licenstilfælde

Hvis licenstageren bryder en aftale, der giver ham ret til at frembringe et antal beskyttede værker, og frembringer flere eksemplarer, end aftalen hjemler, kan rettighedshaveren gøre de almindelige retsmidler gældende mod de overskydende eksemplarer. Denne regel er dog lettere at konstatere end at håndtere. Af det samlede varelager vil nogle eksemplarer være hjemlede, andre ikke. Da alle eksemplarer i sammenhængen udgør en generisk

bestemt ydelse, kan man ikke udpege netop de eksemplarer, der er "uhjemlede". Den person, der mødes med et krav om inddragelse mv., jf. f.eks. ophl. § 84, stk. 3, og PL § 59, vil derfor i almindelighed kunne hævde, at netop hans eksemplar faldt indenfor den hjemlede ret til eksemplarfremstilling.

Problemets praktiske konsekvenser fortoner sig noget, når rettighedslovene – og herunder de netop citerede bestemmelser – netop undtager den godtroende erhvervelse af eksemplarer fra reglerne om inddragelse mv. Tilbage står da den ondtroende erhverver, der efter vore indarbejdede traditioner ikke bør ekstingvere rettigheder. Overfor denne støder det næppe an mod afgørende betænkeligheder at anvende de almindelige regler om inddragelse mv.

Konsumption

Ejendomsrettens almindelige regler anvendes uden videre ved uberettiget råden over immaterialretligt beskyttede eksemplarer, når der er indtrådt immaterialretlig konsumption, jf. herom afsnit 6.4.d.

12.3.c. Tyveri

Et særligt problem ligger i ophl. § 36, der indebærer, at den ret, ejeren af et programeksemplar har til at tage kopier af programmet, ophører, hvis eksemplaret spredes videre eller eksemplarejeren i øvrigt mister retten til at benytte programmet. Hvis et tyveri af programmet (dvs. programpakken), anses som en *spredning*, vil den bestjålne ejer miste retten til at gøre brug af de kopier, han har taget af det (f.eks. til harddisken). Det kan imidlertid diskuteres, om der foreligger "spredning" ved tyveri. De eksempler på spredning, der omtales i ophl. § 2, stk. 3, nr. 1, rummer alle en disposition fra rettighedshaverens side, hvilket der – uden for omgåelsestilfælde – jo ikke er tale om ved tyveri. Alligevel taler afgørende kontrolhensyn (ejerens manglende tilskyndelse til i modsat fald at passe på programpakken) for i denne sammenhæng også at lade det omfatte tyveri. Da der består en betydelig risiko for, at enten tyven, dennes hæler eller en godtroende erhverver effektuerer en brug af programmet – hvorved der i givet fald vil bestå flere samtidige brugssituationer – tilsiger kontrolhensynet, at den bestjålne betragter sine kopier af det bestjålne licenseksemplar som ugyldige, således at den bestjålne enten må generhverve en programlicens eller – i det omfang dette er muligt – gennemføre krav om vindikation. Tilsvarende må den person, der mødes med et vindikationskrav vedrø-

rende den stjålne programpakke, ophøre med sin brug, når vindikationen er gennemført.

Det må dog erkendes, at spørgsmålet er tvivlsomt. Der kan også argumenteres for, at tyvens eller hælerens brug af det stjålne eksemplar i alle tilfælde vil være ulovlig (uanset om der i relation til en efterfølgende, godtroende bruger, vil være tale om en form for ulovlig brug, der ikke vil kunne rammes med ophavsretlige sanktioner før det tidspunkt, hvor rettighedshaveren melder sig med sit krav), og at der derfor *ikke* vil åbnes mulighed for mere end én lovlig brugssituation, selv om man antager, at den bestjålne bibeholder sin ret til at anvende det pågældende program.

12.4. Tvangsfuldbyrdelse

12.4.a. Singulærforfølgning

Uanset pantsætningskonstruktionen realiseres pantet efter de almindelige regler, dvs. typisk ved tvangsauktion, se nærmere *von Eyben* (1987), s. 302 ff. og *Carstensen & Rørdam* (2002), s. 364. Den, der ved tvangsrealisation overtager retten i henhold til pantsætningsaftalen, indtræder i de immaterialretlige beføjelser, den hjemler, på ganske samme måde som ved en frivillig total rettighedsoverdragelse eller licens.

Tvangsmæssig realisation af ophavsrettigheder er underlagt flere begrænsninger. Ophavsmandens eneret til at beslutte, om værket skal udgives, jf. ophl. § 2, stk. 1, er uomgængelig og kan end ikke fraviges ved forudgående aftale, jf. *Blomqvist* (1987), s. 112, og *Nørager-Nielsen & Theilgaard*: Købeloven med kommentarer, 2. udg. (1993), s. 275.

Ophl. § 62

En anden vigtig begrænsning følger af ophl. § 62. Efter denne bestemmelse kan ophavsmandens ret til at råde over sit værk ikke gøres til genstand for kreditorforfølgning, hverken hos ham selv eller hos nogen, til hvem retten er overgået ifølge ægteskab eller arv. Bestemmelsen begrænser alene ophavsmandens ret til at "råde" (ophl. § 2) over et "værk", jf. ophl. § 1. Singulær- eller universalforfølgende kreditorer kan herefter ikke gøre udlæg i de rettigheder, der består til et edb-program, som ophavsmanden endnu ikke har rådet over. En aftale, der stifter pant i et værk, indebærer i sig selv en råden; pantsætteren afskæres altså ikke fra tvangsfuldbyrdelse af sit pant. En aftale, der etablerer pant over noget, der ikke har manifesteret sig som et "værk", men f.eks. blot fremtræder som et idégrundlag, kan derimod aldrig indebære

nogen råden over det færdige værk. Ophl. § 62 modificeres af, at forbuddet kun kan gøres gældende af ophavsmanden selv, hans ægtefælle eller arvinger. Den rettighedshaver, der i medfør af lønmodtagerreglen i § 59 eller ved anden overdragelse er indtrådt i ophavsmandens rettigheder, kan således aldrig gøre bestemmelsen gældende.

Heri ligger omvendt også, at ophl. § 62 ikke er til hinder for, at ophavsmanden disponerer gennem pantsætning. I konsekvens heraf kan ophavsmanden ikke påberåbe sig § 62 mod en udlægssøgende kreditor, der er aftalepanthaver (og dermed har indgået aftale med ophavsmanden). Den vigtigste virkning af ophl. § 62 består i, at ophavsmanden kan modsætte sig, at der sker tvangsmæssig spredning eller offentliggørelse af et værk, som ophavsmanden ellers havde besluttet sig til at holde for sig selv.

Fremtidige værker

En aftale, der forpligter ophavsmanden til at overdrage ophavsretten til fremtidige værker, vil som udgangspunkt kun etablere en obligatorisk forpligtelse, jf. *U 1919.638 H*. I konsekvens heraf kan der næppe heller ske tvangsfuldbyrdelse i retten til de fremtidige vederlag, der ville blive udbetalt ved en senere offentliggørelse af et værk. Kreditorforfølgning i kopier af programmer, som ophavsmanden *har rådet* over, kan derimod godt finde sted, sml. ophl. § 62, stk. 2, der kun opstiller et sådant forbud i relation til manuskripter, stokke, plader, forme mv. samt eksemplarer af kunstværker, som ikke er udstillet. Man kan diskutere, om ophavsmandens panteretlige dispositioner over endnu ikke frembragte værker kan forstås som en betinget rettighedsoverdragelse, hvor betingelsen først realiseres ved ophavsmandens beslutning om at råde over værket. Konstruktionen ville i så fald indebære, at tvangsfuldbyrdelse først kan ske, når ophavsmanden udløser betingelserne og "dermed råder" over værket, jf. i samme retning *Jørgen Blomqvist:* Overdragelse af ophavsrettigheder (1987) s. 109 ff. og dommen i *U 1971.703 Ø*.

Som foreslået af *Óli Meinertson Hansen* i Justitia 2000 nr. 2, s. 61 (11) må det nok antages, at rettighedshaveren kan udtage en *masterkopi* eller andet eksemplar af programmet, for på den måde at blive sat i samme situation som den forfatter, der kan beholde selve sit manuskript.

12.4.b. Universalforfølgning

Ved insolvent bobehandling må de grundsætninger, der er skitseret i det foregående, undertiden modificeres efter konkurslovens regler og principper.

Licenstagers konkurs

Ved licenstagers konkurs er det altovervejende udgangspunkt, at boet ikke vinder større ret, end fallenten havde. I det omfang, der består et forbud mod videreoverdragelse af licensen, jf. ophl. § 56, stk. 2, er konkursboet afskåret fra at overdrage en licensret. § 28, stk. 2, i den tidligere ophl. gav udtrykkeligt boet adgang til videreoverdragelse, hvis overdragelsen skete som led i en virksomhedsoverdragelse. Da meningen med § 56, stk. 2, ikke har været at begrænse den hidtil gældende adgang til videreoverdragelse af ophavsrettigheder, må det antages, at kurator som udgangspunkt er berettiget til at foranstalte videreoverdragelse af ophavsrettigheder, hvis dette sker som led i en sædvanlig transaktion. Derimod må det formentlig antages, at rettighedshavere, for hvem den nye licenstagers identitet åbenbart vil være problematisk (f.eks. af konkurrencemæssige grunde), ikke skal anerkende en sådan overdragelse. Muligheden for at videreoverdrage licenser og ophavsrettigheder er i øvrigt i praksis reduceret ved, at overdrageren – boet – i givet fald vil hæfte for vederlaget, jf. bestemmelsens sidste pkt. En overdragelse må derfor i givet fald suppleres med bank- eller forsikringsgarantier, sml. om muligheden for et sådant debitorskifte *U 1981.300 H* om den chikanøse panthaver.

Licensgivers konkurs

Heller ikke *licensgiverens* konkursbo får større ret, end fallenten havde i medfør af en licensaftale. Har licensgiveren påtaget sig at vedligeholde et licensgivet program i en længere årrække, hviler disse forpligtelser – omend som simple krav – på boet. Dette udgangspunkt modificeres dog ved reglerne om *konkursregulering* (KL § 61), der efter omstændighederne giver boet ret til at opsige indgåede aftaler med kortere varsel.

Kildetekst

Et ofte diskuteret spørgsmål angår boets ret til at disponere over den kildetekst, der beror i den fallerede virksomhed. Hvis kildeteksten stammer fra et program, der er udviklet i den fallerede virksomhed, og som virksomheden havde den fulde ret til, kan boet frit disponere over kildeteksten. Stammer kildeteksten fra et samarbejdsforhold, fallenten havde med rettighedshaveren, vil boet være underlagt samme pligter til at hemmeligholde erhvervshemmeligheder, som fallenten var underlagt. Ligeledes vil boet være omfattet af de begrænsninger i adgangen til at disponere over de ophavsretlige beføjelser, der følger af aftalen og af ophl. § 56, stk. 2. I praksis betyder dette, at boet ikke kan udlevere kildeteksten som led i sin realisation af boets aktiver, med mindre der er hjemmel hertil i den pågældende aftale eller rettighedshaverens samtykke indhentes efterfølgende.

Supplerende litteratur

En række af problemerne vedrørende sikkerhed i rettigheder knyttet til edb-programmel er behandlet hos *Hanne Bender*: Edb-rettigheder (1998) og hos *Óli Meinertson Hansen* i Justitia 2000 nr. 2, s. 49 ff. Problemerne om *sikkerhedsstillelse* i information og immaterialrettigheder er herhjemme hovedsagelig fremstillet i de almindelige immaterialretlige monografier, se nærmere litteraturoversigten efter kapitel 6. Flere afhandlinger i det øvrige Skandinavien har dog taget nogle af de IT-retlige dimensioner af problemet til behandling, se *Robin Thrap-Meyer*: Pantsettelse av datamaskinprogrammer og databaser, Complex 4/89 og *Richard Berling:* Kreditsäkerhet i information. IRI rapport 1987:4. Herudover har *Nørager-Nielsen* i sin artikel: Sikkerhedsordninger vedrørende kildeprogrammel, trykt i Beck & Bruun Nielsen (1987), s. 73 ff., en diskussion af nogle panteretlige aspekter af disse ordninger. Se ligeledes *Hanne Bender og Susanne Karstoft* i U1991B.81 ff. For amerikansk ret henvises til *Roy N. Freed*s kyndige – omend efter de nugældende amerikanske regler delvis forældede – analyse: Security interests in the computer age: practical advice for the secured user, trykt i 101 Banking Law Review 404 (1980) og til *Robert A. Feldman* i 4 The Computer Lawyer (May 1987), s. 13 ff. med praktiske konciperingsråd. I øvrigt kan henvises til den almindelige panteretlige litteratur, der dog ofte kun behandler begrænsede dele af problemstillingen. Hos *Lynge Andersen og Werlauff*: Kreditretten (2000), s. 331 ff. er feltet "ægte immaterialrettigheder" i modsætning til goodwill således afgrænset til patent-, mønster-, varemærke- og brugsmodelrettigheder, men f.eks. ikke ophavsrettigheder.

Kapitel 13. PERSONDATABESKYTTELSE

13.1. Problemstillingen

13.1.a. Baggrund

Retlig systematik

Reglerne om persondatabeskyttelse er i familie med flere andre regelsystemer til beskyttelse af privatlivets fred. Det nærmeste slægtskab finder man i straffelovens regler om beskyttelse af privatlivets fred. Strfl. § 264d straffer således den, der "uberettiget videregiver meddelelser ... vedrørende en anden persons private forhold ... der med rimelighed kan forlanges unddraget offentligheden". I nær forbindelse hermed finder man regler om tavshedspligt i den offentlige forvaltning (forvaltningslovens kapitel 8, strfl. §§ 152c – 152f) og i særlovgivningen. Som anført nedenfor kan andre af persondatalovgivningens regler anskues som udtryk for den personlighedsret, der ligeledes kommer til udtryk i de ophavsretlige regler, ligesom dele af den ophavsretlige regelstruktur genfindes.

Som retsområdet har udviklet sig, fremstår det som en omfattende og kompleks mængde af regler med ganske uklare strukturer og med en ikke ubetydelig indre inkonsistens. Persondatabeskyttelsen i dag omfatter andet og mere end den retlige beskyttelse mod *kompromittering* af såkaldt følsomme oplysninger. Lovgivningen sætter også grænser for, *hvordan* persondata behandles i forskellige henseender, og hvilken *indsigtsret* den berørte person har. I det omfang, databehandleren er en offentlig myndighed, får retsgrundlaget såvel berøring med forvaltningsrettens almindelige regler om *god forvaltningsskik* som med de særlige regler om parters og andres *aktindsigt*. Er databehandleren erhvervsdrivende, er den tilsvarende analogi reglerne om *god markedsføringsskik*.

Udspring

Selv om den lovgivning, der regulerer retsområdet, er ny, er selve retsområdet det ikke. Så tidligt som i 1890 fremlagde *Samuel D. Warren og Louis D. Brandis* i Harvard Law Review (s. 193-220) deres store afhandling "The right to privacy", der udnævnte to basale rettigheder for individet, nemlig dels "the right to be left alone", dels "the right to self-determination". Artiklen

findes på <www.louisville.edu/library/law/brandeis/privacy.html>. En bredere interesse for problemerne vedrørende persondatabeskyttelse opstod dog først i efterkrigsårene, hvor George Orwells roman "1984" bidrog til at levendegøre de problemer, som kunne være forbundet med en ukontrolleret anvendelse af de nye informationsteknologier.

Den danske lovgivningshistorie kan føres tilbage til 1970, hvor Justitsministeriet nedsatte et registerudvalg, hvis betænkninger (687/1973 om private registre og 767/1976 om offentlige myndigheders registre) dannede grundlag for registerlovene af 1978. Lovene gennemgik en gennemgribende revision i 1987. I 1994 fik vi en særlig lov om massemediers informationsdatabaser, nr. 430 af 1. juni. Loven, der fortsat er gældende (som ændret i 2000), har rod i betænkning 1233/1992.

LBP

Ved betænkning nr. 1345/1997 fremlagde Justitsministeriets Udvalg om Registerlovgivningen et forslag til en *lov om behandling af personoplysninger* mv. (i det følgende LBP), der senere er indført som lov nr. 429 af 31. maj 2000 om behandling af personoplysninger. Loven implementerer det EU-direktiv om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT 1995 L 281/31), som Parlamentet og Rådet vedtog den 24. oktober 1995 (95/46/EF), og som ifølge art. 32 skulle være implementeret i national lovgivning senest den 24. oktober 1998. Dette skete ikke. I mellemperioden mellem dette tidspunkt og den 1. juli 2000, hvor LBP trådte i kraft, var direktivet derfor umiddelbart gældende i dansk ret.

Retsområdet

Som allerede antydet har den retlige regulering af behandling af personoplysninger fået stadigt stigende betydning.

- persondatas rolle

For det første "behandles" der langt flere personoplysninger i dag end nogensinde før: Informationsteknologien anvendes overalt i samfundet, og en væsentlig del af de informationer, der behandles (f.eks. ved betjening af kunder, opbygning af databaser eller afvikling af forskellige driftsfunktioner), indebærer, at der registreres og behandles oplysninger om, hvad personer har foretaget sig i forskellige henseender. Denne samfundsmæssige udvikling er sket i takt med, at man i LBP har ladet det meget vide begreb "behandling" danne grundlaget for den retlige regulering af retten til at registrere, behandle, analysere, samkøre og videregive disse oplysninger.

- persondata som aktiv

For det andet knytter der sig i dag en langt større *værdi* til personoplysninger, end der gjorde tidligere. Forklaringen herpå er ligetil: I takt med automatiseringens indtog i såvel private som

offentlige organisationer er det nødvendigt, at systemerne "ved" noget om de personer, virksomhederne til syvende og sidst har at gøre med – internt såvel som eksternt. Når en kundeorienteret privat virksomhed værdiansættes, f.eks. med henblik på salg, er det ikke mindst værdien af dens kundedatabase, der værdiansættes. Når der tales om effektivisering i den offentlige forvaltning (f.eks. i form af kontrol med "sort arbejde" og dobbeltudbetalinger) opstår konstant skismaer mellem effektivitet og retssikkerhed for de kontrollerede.

- "personoplysning"

Dertil kommer for det tredje, som en konsekvens af den gældende lovgivning, at selve begrebet "personoplysninger" er blevet ganske vidtspændende, jf. nærmere afsnit 13.3.b. Ifølge LBP § 3, nr. 1, der bygger på direktivets art. 2, litra a, omfatter begrebet "enhver form for information om en identificeret eller identificerbar fysisk person". I direktivet er dette begreb yderligere forklaret således, at det omfatter både den person, der kan identificeres direkte (f.eks. ved navn) og indirekte (f.eks. igennem identifikationsnummer eller igennem ét eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet). Dermed omfatter begrebet ikke alene de *egentlige personoplysninger* (f.eks. en persons navn, adresse, stilling, bopæl, alder, karriereforløb og familieforhold), men også det, man kan kalde *uegentlige personoplysninger*, der f.eks. blot efterlades som "elektroniske spor", når man anvender et betalingskort eller besøger en hjemmeside, hvis blot det er muligt at føre disse oplysninger tilbage til personen på grundlag af yderligere information.

Se ligeledes *Peter Blume* i U 2002B.112 ff. der i en analyse af den retlige beskyttelse af bipersonen sætter fokus på de rettigheder, bipersonen har i medfør af LBP §§ 28-29, problemerne vedrørende ansattes e-post samt tv-overvågning. Det konkluderes, at persondatabeskyttelse af bipersoner er vanskelig at håndtere, og at man derfor kunne overveje, om beskyttelsesbehovet er tilstrækkeligt tungtvejende til at sikre denne beskyttelse. Samtidig argumenteres for en smidig anvendelse af lovens regler, indtil en ændring af det bagvedliggende direktiv er gennemført.

International udvikling

Persondatabeskyttelse er ikke længere et rent nationalt anliggende. Allerede da Danmark i 1998 overskred fristen for implementering af 1995-direktivet, blev emneområdet EU-retligt, idet en stor del af direktivets bestemmelser herefter som sagt blev umiddelbart anvendelige i dansk ret i mellemperioden mellem 24. oktober 1998 og 1. juli 2000. Det er dog værd at mærke sig, at den EU-retlige dimension ikke udtømmer retsområdets internationale aspekter. Som følge af de regler, 1995-direktivet indehol-

der om eksport af persondata til tredjelande (se herved direktivets art. 25 og bemærkningerne herom i afsnit 13.9.), vil danske virksomheder, der behandler personoplysninger, ofte skulle forholde sig til reglerne om persondatabeskyttelse i tredjelande. Dette kan navnlig tænkes, hvis virksomheden ønsker at eksportere data hertil.

Omvendt kan det europæiske regime have betydning for virksomheder i tredjelande. Dette kan f.eks. tænkes, hvis de pågældende virksomheder behandler oplysninger under benyttelse af hjælpemidler, der befinder sig i Danmark (medmindre hjælpemidlerne kun benyttes med henblik på forsendelse af oplysninger gennem Det Europæiske Fællesskabs område), eller hvis den udenlandske virksomhed indsamler oplysninger her med henblik på behandling i et tredjeland, jf. nærmere LBP § 4, stk. 3.

USA 1974

En af de første lovgivninger på persondataområdet foreligger med den Privacy Act, som USA indførte i 1974. Loven tager dog kun sigte på at beskytte personoplysninger behandlet ved visse offentlige myndigheder. En række af de principper, der fandt udtryk heri, blev vedtaget af OECD's råd den 23. september 1980 som "*Guidelines on the Protection on Privacy and Transborder Flows of Personal Data*". Disse Privacy Guidelines fastslår en række principper for, hvorledes personoplysninger bør beskyttes, der efterfølgende er videreført af Europarådet i konventionen af 28. januar 1981 om Beskyttelse af det Enkelte Menneske i forbindelse med Elektronisk Databehandling af Personoplysninger. Hovedprincipperne i denne konvention er lagt til grund i EU-direktivet.

OECD-retningsliniernes grundprincipper ligger fortsat til grund for moderne persondatalovgivning. De lyder som følger: *The Collection Limitation Principle* (There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject), the *Data Quality Principle* (Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date), *The Purpose Specification Principle* (The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose), *The Use Limitation Principle* (Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the purpose specification principle] except: with the consent of the data subject; or by the authority of law), *The Security Safeguards Principles* (Personal data should be protected by reasonable security safeguards

against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data), *The Openness Principle* (There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller) og *The Individual Participation Principle* (An individual should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; to have communicated to him, data relating to him within a reasonable time, at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; to be given reasons if a request is denied, and to be able to challenge such denial; and to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.)

1978-lovene

Frem til indførelsen af den nye lov om behandling af personoplysninger var hovedhjørnestenene i dansk lovgivning om persondatabeskyttelse de to love om private og offentlige myndigheders registre. Disse to love ophævedes i konsekvens af indførelsen af LBP. I dag er udgangspunktet, at der gælder fælles regler om behandling af personoplysninger hos såvel private virksomheder som i offentlige myndigheder. Ved siden af dette generelle system findes der et betydeligt antal særregler om personregistrering, jf. afsnit 13.1.c.

Retskilder

På grund af sit EU-retlige udspring, emneområdets bredde og retskildematerialets forholdsvis unge karakter, bør man i almindelighed være forsigtig med at udtale sig med bestemthed om gældende ret vedrørende behandling af personoplysninger. Der foreligger på nuværende tidspunkt endnu ingen afgørelser fra EF-domstolen om nogen af de centrale – og i mange henseender vage – grundbegreber, som direktivet bygger på. Ej heller når det gælder de dele af LBP, der repræsenterer rent national lovgivning, er der retspraksis at støtte sig til. I denne generelle præjudikatmangel, kommer praksis fra Datatilsynet til at spille en særlig rolle, ligesom tilsynets mere generelle udtalelser må tillægges betydelig vægt. En særlig rolle spiller her de vejledninger, tilsynet har udarbejdet (herunder om registreredes rettigheder, datasikkerhed og anmeldelsesordningen), og som er tilgængelige fra tilsynets hjemmeside, <www.datatilsynet.dk>. Navnlig kan fremhæves vejledning nr. 126 af 10. juli 2000 om registreredes rettigheder efter reglerne i LBP kapitel 8-10. LBP er kommenteret af *Peter Blume* i en særskilt kommentarudgave (2000) og af *Kristian Korfits Nielsen & Henrik Waaben* (2001).

13.1.b. Persondatabeskyttelse mellem jura og politik

På grund af sin berøring til de dele af tilværelsen, som de fleste har et meget personligt og privat forhold til, er lovgivningen om persondatabeskyttelse et af de områder af IT-retten, som har givet anledning til størst retspolitisk interesse. Interessen skyldes først og fremmest, at det risiko-billede, der kan opstå ved en udstrakt brug af informationsteknologi til registreringsformål, er forholdsvis letfatteligt (som klart udtrykt ved *George Orwell*s roman "1984"): Det er forholdsvis enkelt at rejse en politisk "sag" i Folketinget, der tager udgangspunkt i et begivenhedsforløb, hvorved enkeltpersoner er blevet registreret på uforudsete måder, som man kan føle krænkende. Dernæst har emneområdet betydning for os alle, fordi intet menneske i det moderne samfund kan undgå i et eller andet omfang at blive genstand for registrering af personoplysninger.

Beskrivelses-problemet

At lovgive på området har dog vist sig ret så kompliceret. Komplikationerne er selvsagt ikke blevet mindre, efter at teknologien har ændret sig fra sit oprindelige maskin-fikserede udgangspunkt til det netværksparadigme, der præger nutidens IT-anvendelse. Der er nemlig mangfoldige måder at beskrive det relevante retsfaktum på. Ved den lovgivning om private og offentlige myndigheders registre, der blev indført i 1978, tog man udgangspunkt i begrebet "register", der dengang viste hen til forholdsvis velkendte maskinelle funktioner. Betragtningen var, at en personoplysning som udgangspunkt befandt sig på et register i en lokaliserbar computer, hvorfra den i givet fald kunne flytte over i et register i en anden computer, evt. gennem såkaldt "samkøring". Denne betragtning er ikke længere dækkende, bl.a. fordi nutidens systemer i langt højere grad end før indebærer, at informationssystemerne opbygges og tilpasses med sigte på den enkelte bruger, og fordi databehandlingsopgaver (hvortil registrering og anden behandling af personoplysninger hører) ofte "deles" mellem flere computere. En oplysning, der ligger i et "register" (i informationsteknisk forstand), kan således ligge på forskellige computere. At oplysninger skal være til rådighed for et varierende antal brugere i varierende funktioner indebærer, at den enkelte bruger måske slet ikke ved, hvor de enkelte oplysninger ligger.

Beskyttelses-interessen

Der har været gjort forskellige forsøg på at måle almenhedens sympati eller afsky for personregistrering. I det betænkningsarbejde, der førte til 1978-lovgivningen om private og offentlige myndigheders registre, lagde man uden videre til grund, at den

stigende IT-anvendelse "... har skabt en frygt i befolkningen for registreringsaktiviteterne og for, at de indsamlede oplysninger udnyttes på en måde, der krænker den personlige fred og frihed" (betænkning 687/1973 s. 38). I forbindelse med udvalgsarbejdet om informationssamfundet år 2000 (se hertil rapporten Info-samfundet år 2000, 1994, s. 41) blev den på daværende tidspunkt 15 år gamle registerlovgivning udsat for et retspolitisk serviceeftersyn. Det blev bl.a. opstillet som et princip, at person- og databeskyttelse skulle "sikres gennem en tidssvarende lovgivning, som giver mulighed for registrering, samkøring og brug af data til alle lovlige forvaltningsmæssige formål uden bureaukratiske procedurer". Denne generelle anbefaling havde bl.a. rod i de forslag, en arbejdsgruppe under Finansministeriet havde stillet i rapporten "Effektiv edb i Staten" (1992), der bl.a. fremlagde en tanke om (s. 35 ff.), at det offentliges data skulle kunne udnyttes effektivt via "datafællesskaber på tværs af organisatoriske grænser – mellem offentlige myndigheder indbyrdes og i samspil med private interesser".

Der er forskellige opfattelser af det berettigede i en sådan adgang til genanvendelse af data, jf. *Blume:* Databeskyttelsesret (2000), s. 131 ff., der generelt nærer skepsis mod sådanne løsninger, som "svækker borgernes muligheder for at kontrollere, hvad oplysningerne benyttes til og hvor de befinder sig". Den anførte betænkelighed rammer dog ikke det substantielle i forslagene om at opbygge datafællesskaber, nemlig at høste rationaliseringsgevinster gennem datagenbrug. Det kan således forholdsvis enkelt sikres, retligt såvel som teknisk, at der er den kontrol med brugen af de pågældende data, som skønnes fornøden.

Undersøgelser

Det har dog ikke altid være klart, hvilke mere specifikke ønsker til en lovgivning om persondatabeskyttelse almenheden har. En rapport fra 1993, afgivet af en arbejdsgruppe om registerlovgivningen nedsat af det daværende Teknologinævn, lagde f.eks. op til en – i forhold til tidligere – mere liberal registerregulering, der skelner mellem tre typer af personoplysninger: De *almindelige* (såsom navn, adresse og telefonnummer mv.), de *fortrolige* (herunder oplysninger om skat, kontoudtog og offentlige tilskud) og de *rent private* oplysninger (herunder om helbred, politiske og religiøse forhold). Gruppen foreslog fri adgang til at registrere almindelige oplysninger, specialregulering vedrørende fortrolige oplysninger samt en restriktiv adgang til registrering af private oplysninger. Dens forslag blev dog aldrig ført videre, idet forhandlingerne omkring det senere 1995-direktiv på dette tidspunkt allerede havde baseret sig på andre udgangspunkter.

1996-undersøgelsen

I januar 1996 udsendte Institut for Fremtidsforskning en undersøgelse med titlen "Danskernes holdninger til informationsteknologi". Undersøgelsen, hvis hovedresultater er gengivet i bilagshæftet til betænkning 1345/1997, s. 161 ff., viser bl.a., at befolkningens skepsis overfor informationsteknologi i almindelighed og personregistrering i særdeleshed beror på, om de modsvarende fordele ved en sådan registrering lægges frem. 61% af de adspurgte svarer f.eks. nej til spørgsmålet om, hvorvidt det offentlige må få flere oplysninger (overfor 35%, der svarer ja), men 84% svarer ja til, at det offentlige må samkøre (dvs. kombinere oplysninger fra forskellige registre for at uddrage et nyt informationsindhold heraf) med henblik på afsløring af socialbedrageri (mod 14%, der svarer nej hertil).

Retlig karakter

Man kan diskutere, hvilken generel karakter reglerne om beskyttelse af personoplysninger har. Efter indførelsen af LBP er det gjort til et generelt – om end ikke ufravigeligt – krav, at den registrerede skal give sit udtrykkelige samtykke til behandling af personoplysninger, se herved LBP § 6, stk. 1, nr. 1. I det omfang dette samtykkekrav er gældende, er det nærliggende at drage paralleller mellem persondatabeskyttelseslovgivningen og ophavsretslovgivningen. Selv om udgangspunktet i disse to love er fundamentalt forskelligt, leder det gennemgående samtykkekrav til den fælles betragtning, at den, der kan give samtykke, for så vidt besidder råderetten ("ejendomsretten") til de pågældende oplysninger, jf. nærmere min afhandling i Festskrift til Mogens Koktvedgaard (2003), s. 5 ff..

Også andre betragtninger er fælles mellem de to lovsystemer: Som nævnt i afsnit 6.1.c. er den kontinentale ophavsret traditionelt baseret på en forestilling om, at rettighedshaveren besidder visse ideelle rettigheder, som netop har forbindelse med hensynet til rettighedshaverens personlighed. Ligeledes kan man i lovgivningen om persondatabeskyttelse finde undtagelser (begrundet i almenhedens interesse i at kunne genbruge information), som kan siges at have paralleller i de indskrænkninger i ophavsretten, der er omtalt i kap. 2 i ophavsretsloven. Også reglerne om privatkopiering/privat anvendelse af personoplysninger har lighedstræk. Når disse iagttagelser gøres, kan der dog være grund til at understrege, at de to lovsystemer i bund og grund tjener vidt forskellige hensyn, og at den retlige vurdering som følge heraf er struktureret grundlæggende forskelligt. Men iagttagelsen tjener til at illustrere, hvor vanskeligt det er at gennemføre lovgivninger om "ejerskab" til information, jf. herved mine bemærkninger i bilagshæftet til rapporten om Info-samfundet år 2000 (1994), s. 121 ff. En variant af denne tankegang er lagt frem af *Julius C. S. Pinckaers* i doktorafhandlingen "From Privacy towards a new Intellectual Property Right in Persona", Kluwer

(1996), se navnlig s. 423 ff. Se ligeledes *Volker Beuthien & Anton S. Schmölz*: Persönlichkeitsschutz durch Persönlichkeitsgüterrechte (München, 1999). Se tilsvarende *Blume*: Databeskyttelsesret (2000), s. 30.

13.1.c. Særregler

Netop fordi lovgivningen om persondatabeskyttelse har givet anledning til så righoldige retspolitiske drøftelser er der gennem tiderne skabt en række særregler, der i mange henseender etablerer deres eget regime for persondatabeskyttelse. LBP tager højde herfor ved generelt i § 74 at give hjemmel for, at brancheforeninger eller andre organer, som repræsenterer andre kategorier af private dataansvarlige, i samarbejde med Datatilsynet kan udarbejde "adfærdskodekser, der skal bidrage til en korrekt anvendelse af reglerne i denne lov". Bestemmelsen giver dog ikke hjemmel til at modificere eller fravige lovens almindelige regler.

Der foreligger endnu ingen danske adfærdskodekser af denne art. På europæisk plan har The European Federation of Direct Marketing i 2003 udsendt en adfærdskodeks for brug af personoplysninger i forbindelse med direkte markedsføring, se herved den såkaldte Artikel 29-Gruppes anerkendende udtalelse nr. 3/2003 af 13. juni 2003, tilgængelig fra <www.datatilsynet.dk>.

I den følgende gennemgang præsenteres de undtagelser, der følger af særlige lovregler, i tilknytning til hvert enkelt reguleringstema. En kort oversigt kan dog være nyttig på dette sted, ikke mindst fordi omfanget og karakteren af disse fravigelser må forventes at smitte af på fortolkningen af de materielle regler i LBP. I et vist omfang gælder her loven om de forbundne kar: Det giver ikke mening at fastholde fortolkningen af et strengt og altomfattende regime under det generelle regelsæt side om side med massive undtagelsesregler, hvis eneste rationale er, at der er tale om lovgivning med en anden (ofte tilfældig) politisk og ressortmæssig forhistorie.

Statstidende

Ifølge § 1 i lov nr. om 419 af 31. maj 2000 om elektronisk statstidende er det bestemt, at forskningsministeren skal føre en database med de meddelelser, der optages i Statstidende, jf. forslaget herom i betænkning 1328/1997. Som udgiver af denne database har forskningsministeren udpeget Statens Information, jf. § 1 i bekendtgørelse nr. 799 af 24. august 2000.

Som udgangspunkt offentliggøres samtlige oplysninger i denne database. For personoplysninger gælder dog den regel, at sådanne personoplysninger, der *i anden sammenhæng* må anses for *fortrolige*, efter et år fra offentliggørelsestidspunktet skal gøres

usøgbare, for så vidt der søges på navn eller anden personidentifikation, jf. nærmere § 5, stk. 2. Eksempler herpå kan være oplysninger meddelt i forbindelse med konkurs, tvangsauktion eller gældssanering. De pågældende oplysninger skal dog fortsat ligge i basen. Personoplysninger må dog kun offentliggøres ved proklamaer i dødsboer (altså når personen er død). Masseudtryk kan dog finde sted i det omfang dette følger af anden lovgivning, jf. § 6, stk. 3.

Massemedier

Lov nr. 430 af 1. juni 1994 om massemediers informationsdatabaser (LMI) indeholder en sektorvis regulering af den behandling af personoplysninger, der sker i pressen. Det EU-retlige grundlag for denne særregulering findes i direktivets art. 9, der giver medlemsstaterne ret til at gøre indskrænkninger fra de centrale kapitler I, IV og VI. I overensstemmelse hermed bestemmer LBP § 2, stk. 6, at loven ikke finder anvendelse på informationsdatabaser, der er omfattet af lov om massemediers informationsdatabaser. Da denne lov, jf. § 1, stk. 2, ikke gælder for informationsdatabaser, hvori der udelukkende er indlagt allerede offentliggjorte periodiske skrifter eller lyd- og billedprogrammer mv., fastslår LBP § 2, stk. 7, at det således udelukkede område (dog med forbehold for erstatnings- og sikkerhedsreglerne i §§ 41, 42 og 69) heller ikke reguleres af LBP.

- sondringer

LMI sondrer mellem *redaktionelle informationsdatabaser*, der indeholder data, som journalister og redaktionsmedarbejdere ved det pågældende medium (og kun de, jf. § 4, stk. 1) selv betjener (jf. nærmere LMI § 3) og de *offentligt tilgængelige informationsdatabaser*, som for at blive omfattet af loven skal være tilgængelige for enhver på almindelige forretningsvilkår, jf. LMI § 6, stk. 1. For at begge typer af informationsdatabaser kan blive omfattet af loven (og dermed ikke være omfattet af LBP) skal der foretages anmeldelse til Datatilsynet, jf. LMI § 3, stk. 1, og § 6, stk. 1.

- redaktionelle

I relation til de redaktionelle informationsdatabaser er lovens praktiske konsekvens, at journalisten ikke behøver at yde de retssikkerhedsgarantier overfor den registrerede (i form af f.eks. registerindsigt, samtykke til behandling og indsigelse mod behandling mv.), som følger af de almindelige regler i LBP. Selv om der utvivlsomt er et stort behov for at sikre den registreredes retssikkerhed imod netop pressen – som jo ofte vil kunne gøre ubodelig skade, når der trykkes "historier" om enkeltpersoner på et urigtigt grundlag – har man fra politisk hold følt, at denne pris måtte betales for at sikre pressens frie arbejdsvilkår.

- offentligt tilgængelige

I relation til de offentligt tilgængelige informationsdatabaser indeholder loven en regulering, der ligger tæt op af reglerne om

berigtigelse mv. i medieansvarsloven. Tankegangen er, at den offentligt tilgængelige informationsdatabase skal betragtes som et massemedium, som alle har adgang til, som udgiveren derfor også bærer et vist ansvar for, men som til gengæld også må berigtige de fejl, der måtte opstå i informationsstrømmen. Sammenhængen ses bl.a. i LMI § 8, der fastslår, at en offentligt tilgængelig informationsdatabase ikke må indeholde informationer, der ikke lovligt kan offentliggøres i et massemedie (stk. 1), eller hvis offentliggørelse ville være i strid med god presseskik (stk. 2). Hertil føjer sig en berigtigelsesregel i § 9, hvorefter den, informationerne angår, kan forlange sletning, rettelse eller ajourføring, når de informationer, der offentliggøres i en sådan base, viser sig urigtige eller vildledende, eller når en tidligere omtalt retsafgørelse eller administrativ afgørelse er blevet ændret, eller strafforfølgning er afsluttet ved frifindelse eller påtaleopgivelse. I forlængelse heraf giver § 10 ret til genmæle. Slægtskabet med den presseretlige regulering understøttes i øvrigt af de administrative regler i LMI kapitel 4, der bl.a. henlægger administrationen af loven til Pressenævnet.

Betalingsmidler

Ifølge § 13 i lov om visse betalingsmidler (LVB) finder LBP anvendelse på sådanne midler med visse modifikationer. Udstederen skal for det første sikre, at brugerens CPR-nummer ikke kan aflæses fysisk eller elektronisk af andre end udstederen. Dernæst fastslår reglen, at oplysninger om, hvor brugeren har anvendt betalingsmidlet, og hvad han har købt, i mangel af særlig hjemmel kun må behandles til visse driftsmæssige formål eller i retshåndhævelsesøjemed. Dog har udstederen også mulighed for at behandle oplysninger om, *hvor* brugeren har anvendt betalingsmidlet, i rådgivningsøjemed og med sigte på systemtilpasninger.

CPR-registeret

Ved lov om Det Centrale Personregister, jf. lovbekendtgørelse nr. 140 af 3. marts 2004, er der givet særlige regler om tildeling af personnumre (CPR-nummer) og folkeregistrering. Ifølge lovens § 3 skal "enhver" have tildelt et personnummer, hvis vedkommende på grund af fødsel eller tilflytning (jf. nærmere lovens kap. 5) folkeregistreres her i landet, inddrages under ATP eller undergives skattesagsbehandling. Personnummeret er altså hverken udtryk for, at den pågældende har dansk statsborgerskab eller for, at der er gennemført en særlig identitetskontrol med vedkommende. Men personnummeret fungerer som indgangsnøgle til de oplysninger, som det offentlige registrerer om den pågældende, ligesom det knytter denne til en bopælsadresse (forstået som det sted, hvor vedkommende regelmæssigt sover uden for tilfælde af ferie, forretningsrejse, sygdom mv., jf. § 6, stk. 1.) Loven inde-

holder i øvrigt regler for, hvorledes oplysninger fra CPR-registeret kan videregives.

Patienter

Ved reglerne i Sundhedsloven, nr. 546 af 24. juni 2005, er der bl.a. givet regler om en række af de retlige problemer, der kan opstå i forbindelse med patientbehandling. Ifølge lovens § 37 skal en patient, der fremsætter begæring herom, have meddelelse om, hvorvidt der behandles helbredsoplysninger om vedkommende indeholdt i patientjournaler mv. Behandles sådanne oplysninger, skal der på patientens begæring og på en let forståelig måde gives patienten meddelelse om, hvilke oplysninger der behandles, behandlingens formål, kategorierne af modtagere af oplysningerne og tilgængelig information om, hvorfra disse oplysninger stammer.

Lovens § 41, stk. 2, fastslår dernæst, at oplysninger om patientens helbredsforhold, øvrige rent private forhold og andre fortrolige oplysninger i forbindelse med behandling af patienten kan videregives uden samtykke fra patienten, når det er nødvendigt af hensyn til et aktuelt behandlingsforløb for patienten og videregivelsen sker under hensyntagen til patientens interesse og behov, når videregivelsen er nødvendig til berettiget varetagelse af en åbenbar almen interesse eller af væsentlige hensyn til patienten, sundhedspersonen eller andre eller når videregivelsen sker til patientens alment praktiserende læge fra en læge, der virker som stedfortræder for denne.

Helbredsoplysninger

Ved lov nr. 286 af 26. april 1996 om brug af helbredsoplysninger mv. på arbejdsmarkedet er der givet særlige regler om brug af helbredsoplysninger i ansættelsesretlige relationer. Loven har til formål at sikre, at sådanne helbredsoplysninger ikke uberettiget anvendes til at begrænse lønmodtageres muligheder for at opnå eller bevare ansættelse, jf. § 1, stk. 1. Dette gælder uanset om oplysningerne hidrører fra genetiske undersøgelser, almindelige undersøgelser eller andre kilder.

Hovedtemaet for lovens regulering er arbejdsgiverens adgang til at *indhente* oplysninger, jf. nærmere lovens kapitel II. Hovedreglen er her lovens § 2, stk. 1, der alene giver arbejdsgiver ret til at anmode den ansatte om helbredsoplysninger i forbindelse med ansættelse eller under ansættelse med det formål at få belyst, om lønmodtageren lider eller har lidt af en sygdom eller har eller har haft symptomer på en sygdom, når sygdommen vil have *væsentlig betydning* for lønmodtagerens arbejdsdygtighed ved det pågældende arbejde. Denne regel modificeres dog ved lovens §§ 3 – 6. Væsentlig er her lovens § 6, der pålægger lønmodtageren at meddele helbreds- eller symptomoplysninger af væsentlig betydning for det pågældende arbejde. Inden ansættelsen skal lønmod-

tageren meddele disse oplysninger af egen drift, og under ansættelsen udløses pligten af arbejdsgiverens spørgsmål.

DNA-profil-registerloven

Ved lov nr. 434 af 31. maj 2000, som ændret ved lov nr. 369 af 24 maj 2005, er der oprettet et centralt dna-profilregister, der tjener som internt arbejdsregister for politiet i forbindelse med identifikation af personer i forbindelse med efterforskning af straffesager. Registeret består af en *persondel*, der indeholder personidentificerede dna-profiler, og en *spordel*, der indeholder ikke-personidentificerede dna-profiler, jf. § 1, stk. 2. Loven giver nærmere oplysninger om, under hvilke omstændigheder disse oplysninger skal slettes. I lovens § 6 er indeholdt en særegen regel om egenaccess. Det fremgår heraf, at en registreret person ved personlig henvendelse til politiet kan få *mundtlig* underretning om de oplysninger, der er registreret om vedkommende selv.

- persondel

I registerets persondel optages dna-profiler af personer, som er eller har været sigtet for overtrædelse af en række grovere forbrydelser i straffeloven, jf. nærmere lovens § 2, stk. 2, nr. 1. Det kræves dog, at dna-analysen er udført i den pågældende sag efter retsplejelovens regler om legemsundersøgelser (kapitel 72). Oplysninger i registerets persondel skal straks slettes, når en sigtelse opgives som grundløs, når der er forløbet 10 år fra frifindelse mv., når den registrerede fylder 80 år, når oplysningerne hidrører fra et uhjemlet tvangsindgreb, eller når andre særlige grunde undtagelsesvis taler derfor, jf. nærmere lovens § 3.

- spordel

Registerets spordel indeholder ikke-personidentificerede dna-profiler af biologisk materiale, der er fundet på gerningssteder, eller på effekter, personer eller steder med tilknytning til en forbrydelse, jf. § 2, stk. 2, nr. 2. Oplysninger heri skal slettes, når sporfundet er personidentificeret, jf. § 4, nr. 1. Dette kan eventuelt ske i forbindelse med en overførelse til registerets persondel. Dette skyldes netop, at spordelen kun skal omfatte ikke-personidentificerbare dna-profiler. Ligeledes skal oplysninger udgå fra spordelen, når de ikke længere har politimæssig betydning, eller når andre særlige grunde undtagelsesvis taler derfor.

Andre regler

Den ovenfor givne oversigt over særlig lovgivning om persondatabeskyttelse er langt fra udtømmende. Navnlig findes der talrige særregler inden for det offentlige område, hvor man har lovgivet for at skabe hjemmel for en særlig databehandling. Et eksempel herpå er lov om Det Fælles Lønindeholdelsesregister, jf. lovbekendtgørelse nr. 430 af 6. juni 2005. Loven har til formål at koordinere den indeholdelse i løn mv., der finder sted på grundlag af de afgørelser om lønindeholdelse, som offentlige myndigheder træffer i forbindelse med restanceinddrivelse.

Teleområdet

På grundlag af reglerne i direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor, se EFT L201/37 af 31.7.2002, er der endelig givet hjemmel i loven om konkurrence- og forbrugerforhold på telemarkedet jf. lovbekendtgørelse nr. 679 af 23. juni 2004, til at give regler for udbydere af offentlige elektroniske kommunikationsnet eller -tjenester om minimumskrav til behandling af personoplysninger i forbindelse med telekommunikation. Reglerne findes i bekendtgørelse nr. 638 af 20. juni 2005.

Også i den klassiske "lawyers law" finder man undertiden bestemmelser af betydning for persondatabeskyttelsen.

Tinglysning

Et eksempel herpå er reglerne om terminaladgang i tinglysningslovens §§ 50c og 50d, som ændret ved lov nr. 216 af 22. april 2002. Ifølge § 50c, stk. 2, er oplysninger i tinglysningsvæsenets edb-registre tilgængelige for enhver ved personlig henvendelse til tinglysningskontoret. Oplysninger kan videregives via terminaler, der oplyses på tinglysningskontorerne eller andre steder efter justitsministerens bestemmelse. Personnumre må dog ikke videregives, jf. § 50c, stk. 1. Ligeledes kan oplysningerne efter ansøgning videregives til enhver ved terminaladgang i øvrigt (såkaldt ekstern terminaladgang), jf. § 50c, stk. 3. Ifølge bestemmelsens stk. 7 er der lagt begrænsninger i adgangen til at anvende de således videregivne oplysninger. Der er således sket en formålsafgrænsning omkring overdragelse, forsikring, retsforfølgning og retsforhold i øvrigt vedrørende den faste ejendom. Overdragelse til markedsføringsformål er udtrykkeligt gjort til et illegitimt formål, hvorimod oplysninger, der videregives til massemedier, kan anvendes i journalistisk øjemed. Se ligeledes bekendtgørelse nr. 860 af 28. september 2001 om adgangen til at modtage oplysninger fra bygnings- og boligregistret (BBR) samt oplysninger sammenstillet med flere ejendomsdataregistre mv. og digitale kort, som ændret ved bekendtgørelse nr. 911 af 8. september 2004.

Finansiel virksomhed

Et andet eksempel er lov om finansiel virksomhed, jf. lovbekendtgørelse nr. 613 af 21. juni 2005. Ifølge denne lovs § 118 kan sædvanlige oplysninger om kundeforhold videregives til brug for varetagelse af administrative opgaver (i hvilke tilfælde den efter loven fastsatte tavshedspligt gælder for modtageren). Begrebet "sædvanlige kundeoplysninger i finansielle virksomheder" er i øvrigt præciseret ved en bekendtgørelse fra Finanstilsynet, nr. 1075 af 17. december 2001. Oplysninger om rent private forhold kan dog ikke videregives uden kundens samtykke, medmindre

videregivelsen er berettiget på et særligt grundlag, jf. § 6. Videregivelse til en finansiel virksomheds modervirksomhed til brug for risikostyring mv., kan dog ske i medfør af § 7. Loven indeholder særlige regler om videregivelse af oplysninger om privatkunder til brug for markedsføring eller rådgivning, jf. lovens § 8. Sådan videregivelse kan ikke finde sted, medmindre kunden har givet samtykke hertil. Dog kan der ske videregivelse uden samtykke til koncernvirksomheder, der er undergivet tavshedspligt, hvis der er tale om "generelle kundeoplysninger, der danner grundlag for inddeling i kundekategorier, og hvis videregivelsen er nødvendig for, at den virksomhed, som oplysninger videregives til kan forfølge en berettiget interesse, og hensynet til kunden ikke overstiger denne interesse". Dernæst kan der ske videregivelse af "sædvanlige oplysninger om erhvervskundeforhold" til brug for markedsføringen til finansielle virksomheder, der er underlagt tavshedspligt.

Intet tyder på, at denne fremvækst af ny lovgivning er for nedadgående, og med LBP (se navnlig § 2, stk. 1, og § 6, stk. 1, nr. 3) er det da også forudsat, at der kan være et generelt behov for en sådan særlig lovgivning. Når man afklarer retsstillingen på et specifikt samfundsområde må man derfor altid sikre sig, om sådanne særlige regler er gældende.

Sådanne regler vil undertiden befinde sig på bekendtgørelsesniveau. Ved telestyrelsens bekendtgørelse om nummeroplysningsdatabaser, nr. 665 af 6. juli 2000, er der f.eks. givet regler om, hvilke oplysninger om abonnentnumre der kan sælges af en teleudbyder (i form af telefonbøger mv.). Bekendtgørelsen er udstedt i medfør af loven om konkurrence- og forbrugerforhold på telemarkedet.

13.2. Lovens afgrænsning

13.2.a. Udgangspunktet

Generel anvendelse

LBP har et meget bredt anvendelsesområde. Medmindre andet er bestemt gælder den for enhver behandling af personoplysninger inden for såvel privat erhvervsvirksomhed som i det offentlige. Ifølge lovens § 2 gælder der nogle særlige undtagelser fra anvendelsesområdet, jf. afsnit 13.2.b. Men er man uden for dem, gælder den for både private virksomheder, organisationer og offentlige myndigheder. Også den private borger må altså efterkomme lovens regler, medmindre der gælder en undtagelse herfor. En

sådan findes i § 2, stk. 3, der lader loven vige for behandlinger, som en fysisk person foretager med henblik på udøvelse af aktiviteter af rent privat karakter. Ligeledes er Folketinget og dets institutioner undtaget, jf. § 2, stk. 5.

Domstolene

Med LBP er domstolene (nu) omfattet af den registerretlige regulering. Lovens kapitel 8 (om oplysningspligt over for den registrerede), kapitel 9 (om den registreredes indsigtsret) og §§ 35-37 (ret til indsigelse og berigtigelse) og § 39 gælder dog ikke for behandlinger, ved domstolene inden for det strafferetlige område, jf. § 2, stk. 4, 1. pkt. En tilsvarende begrænsning af lovens anvendelse (dog ikke for så vidt angår indsigtsretten), er gjort for behandlinger, der foretages for politi og anklagemyndighed inden for det strafferetlige område, jf. § 2, stk. 4, 2. led.

Edb-behandlinger

Ifølge § 1 regulerer LBP en række former for "behandling" af "personoplysninger". Den praktisk vigtigste behandlingstype, der er omfattet af loven, er den, der helt eller delvis foretages *ved hjælp af elektronisk databehandling*. Det er i den forbindelse uden betydning, om IT-behandlingen sker med det udtrykkelige og specifikke formål at behandle personoplysninger, eller om en sådan behandling blot opnås som en slags "sidegevinst" i forbindelse med anden databehandling. Transmission af oplysninger via Internet (f.eks. på en chat-side) er omfattet af begrebet "behandling". Det samme gælder den forudgående håndtering af de pågældende oplysninger, såvel som den efterfølgende bearbejdning (læsning, lagring mv.).

Manuelle behandlinger

Herudover omfatter loven tillige ikke-elektroniske behandlinger af personoplysninger, "der er eller vil blive indeholdt i *et register*". Sådanne behandlinger betegnes almindeligvis som *manuelle*, og afgørende for lovens afgrænsning i denne henseende er her begrebet "register". Dette begreb er defineret i lovens § 3, nr. 3, som "enhver struktureret samling af personoplysninger, der er tilgængelige efter bestemte kriterier, hvad enten denne samling er placeret centralt, decentralt eller er fordelt på et funktionsbestemt geografisk grundlag". Hvis man indsamler oplysninger manuelt med henblik på at lægge dem i et papirbaseret kundekartotek, en kartotekskasse eller journalkortsystem, er man altså indenfor lovens behandlingsbegreb, selv om denne behandling ikke er baseret på IT. Til de fleste praktiske formål er det dog den IT-baserede behandling, der spiller en rolle.

Blume: Databeskyttelsesret (2000), s. 126, antager, at kun enkeltstående manuelt behandlede data falder uden for lovens registerbegreb. I lovforslagsbemærkningerne til lovens § 3, nr. 3, antages det – med tvivlsomt føje – at manuelle akter, som indgår i konkret sagsbehandling eller samlinger af sådanne mapper, ikke er omfat-

tet. Hvis sådanne oplysninger (f.eks. om partsnavne mv.) kan identificeres ved hjælp af det journalsystem, der anvendes, må det antages, at de indgår i et register. Før vedtagelsen af LBP udtalte det daværende Registertilsyn, at logning af medarbejderes Internet-anvendelse udgør et register, der var omfattet af lov om offentlige myndigheders registre, men at en sådan registrering ikke kunne anses for stridende mod loven i det omfang den har et sagligt formål. Se i øvrigt om arbejdspladsovervågning afsnit 14.1.d. og nedenfor s. 567 f.

"Den registrerede"

Registerbegrebet spiller kun en selvstændig rolle i LBP, for så vidt der er tale om sådanne manuelle behandlinger. At loven – talrige steder – taler om "den registrerede" indebærer altså ikke en afgrænsning til tilfælde, hvor en person er genstand for behandling i et register. Der er tale om et terminologisk levn fra tidligere lovgivning, og begrebet "den registrerede" kan således oversættes til "den, hvis oplysninger er genstand for behandling efter lovens regler". I den engelske udgave af direktivet tales om "*the data subject*".

Anden systematisk behandling

Ifølge § 1, stk. 2, gælder LBP tillige for anden *ikke-elektronisk* systematisk behandling i den private sektor, hvis denne omfatter oplysninger om personlige forhold, "som med rimelighed kan forlanges unddraget offentligheden", såsom oplysninger om personers private eller økonomiske forhold. Denne udvidelse af lovens område til visse behandlinger i privat regi vil bl.a. kunne omfatte manuelle databaser med oplysninger om enkeltpersoners politiske sindelag eller etniske herkomst. En del af disse behandlinger udgår dog af loven, jf. LBP § 2, stk. 3, hvis de har "rent privat karakter" (hvilket de næppe har, hvis behandlingen sker som led i politiske aktiviteter el.lign.). Ved sådanne systematiske behandlinger, der altså er omfattet af loven, har den registrerede dog ikke oplysnings- og indsigtsret efter de regler herom, der findes i LBP kapitel 8-9.

13.2.b. Undtagne behandlinger

Ifølge LBP §§ 1-2 finder loven ikke anvendelse på en række områder, der pga. deres særlige karakter undtages under ét.

- private behandlinger

I modsætning til 1978-loven om private registre gælder loven således ikke for behandlinger, som en fysisk person foretager med henblik på udøvelse af aktiviteter af rent privat karakter § 2, stk. 3. Som anført af *Lindberg & Westman* (1999), s. 115, må dette begreb tillægges et mere snævert indhold end begrebet "ikke-kommerciel virksomhed". Man kan således ikke påberåbe sig denne undtagelse som hjemmel for at udbyde en "ikke-kom-

merciel" Internet-hjemmeside, hvorfra man spreder personoplysninger til almenheden, som ellers ville være omfattet af lovens almindelige regler (herunder samtykkekravet).

- kunst og litteratur

I medfør af LBP § 2, stk. 10, gælder loven ikke for behandling af oplysninger, som i øvrigt udelukkende finder sted i journalistisk øjemed. For sådanne behandlinger gælder alene reglerne om § 41 (behandlingssikkerhed) og § 42 (anmeldelsespligt), ligesom erstatningsreglen i LBP § 69 kan gøres gældende af den registrerede. I relation til journalistisk virksomhed gælder herudover reglerne i loven om massemediers informationsdatabaser (LMI), jf. bemærkningerne herom afsnit 13.1.c.

Loven finder som nævnt ikke anvendelse på behandling af personoplysninger, der foretages fra Folketinget og institutioner med tilknytning hertil (f.eks. Folketingets Ombudsmand), jf. stk. 5. Dernæst afgrænser § 2, stk. 6-9, loven overfor de særlige regler om informationsdatabaser på medieområdet.

13.3. Grundlæggende begreber

13.3.a. "Behandling"

Som allerede nævnt er lovens centrale begreb "behandling". Dette begreb indgår i de almindelige regler i LBP. Ifølge lovens § 3, nr. 2, defineres behandling som "enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger [underforstået personoplysninger] gøres til genstand for". Definitionen svarer til direktivets art. 2, litra b, der som eksempler på sådanne behandlinger nævner "indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse ved transmission, formidling eller enhver form for overladelse, sammenstilling eller samkøring samt blokering, slettelse eller tilintetgørelse".

Sagt under ét omfatter behandlingsbegrebet altså stort set alt, hvad man ved hjælp af IT kan udsætte en personoplysning for. Det er uden betydning, hvor lang *tid*, behandlingen varer. I princippet vil en behandling af blot få sekunders varighed være omfattet af behandlingsbegrebet, og hvis der som led i en sådan behandling efterlades et spor, der kan tænkes medvirke til en anden behandling, vil det da også være realt velbegrundet at anse en sådan behandling for omfattet af loven. I almindelighed må det dog antages, at sporadiske og atypiske IT-baserede behandlin-

ger falder uden for lovens område, jf. *Nielsen & Waaben* (2001), s. 93.

Behandlingen af personoplysninger er omfattet af lovens begreb, uanset om den er resultatet af en bevidst beslutning om at registrere. Dette subjektive krav har derimod betydning for, hvem der i givet fald kan gøres ansvarlig for en behandling, jf. bemærkningerne neden for om lovens § 3, nr. 3 og 4, der sondrer mellem pligtsubjekterne "dataansvarlig" og "databehandler".

Som definitionen hermed er lagt fast, er selv enkeltstående operationer (f.eks. sletning af en oplysning) en "behandling", der som sådan falder indenfor lovens område. Som fremhævet i betænkning 1345/1997 s. 433 skal udtrykket dog i relation til flere af lovens bestemmelser – herunder anmeldelsesreglerne i lovens afsnit V – forstås således, at der sigtes til en række af behandlinger.

13.3.b. "Personoplysning"

Det andet centrale begreb i lovteksten er "personoplysning", jf. de indledende bemærkninger herom under afsnit 13.1.a. Som her anført indbefatter dette begreb enhver oplysning, uanset hvor fragmentarisk den er, der kan henføres til en enkeltperson, f.eks. en persons navn, fødselsdato og adresse samt oplysninger om, at personens fætter er præst i Sønderjylland, og at han foretrækker det ene burgermærke frem for det andet. Også fotos kan betragtes som personoplysninger, hvis det er muligt at identificere den fotograferede, jf. *RÅB* 1997.87. Det samme gælder optagelser med web-kamera, hvis optagelsen gør det muligt at identificere enkeltpersoner, jf. Datatilsynets afgørelser af 3. juni 2002 og 8. juli 2003, begge tilgængelige fra <www.datatilsynet.dk>. De problemer, der opstår i forbindelse med sådanne behandlinger, behandles for tiden i et udvalg nedsat af Justitsministeriet. Krypterede data anses også for personoplysninger i det omfang der er mulighed for at dekryptere disse oplysninger og dermed identificere de personer, dataene angår.

Det er uden betydning for afgrænsningen af begrebet "personoplysninger", om de pågældende oplysninger er almindeligt kendt, eller om de kan skaffes til veje ved at man så at sige holder øjne og ører åbne. Man må dog nok stille krav om, at det skal være praktisk muligt – uden opøvelse af ekstreme ressourcer – at kombinere de foreliggende data med den person, der står bag. Har en for værten ukendt restaurationsgæst "efterladt" den personoplysning, der består i et fingeraftryk på et glas, kan disse data ikke betragtes som personoplysninger. Det kan de derimod, hvis værten gemmer dataene sammen med oplysninger (f.eks. fra et

betalingskort) om, hvem gæsten er, jf. nærmere *Jan Grijpink* i 17 CLSR 3.154 ff. (2001).

Oplysninger om genstande mv.

Det kan ofte give anledning til tvivl, om en oplysning, der umiddelbart angår en genstand, indirekte rummer en personoplysning, fordi den rummer et åbenbart potentiale for at indgå i behandlingen af en personoplysning. En af de nye problemstillinger, som tegner sig i dette grænseområde, er brugen af RFID-tags (*R*adio *F*requency *I*dentification *D*evice). En RFID indeholder en induktionsspole og en lille kobberantenne, som kan afgive information om, hvorfra et tilknyttet produkt stammer, samt hvilke egenskaber det har. I kombination med andre teknologier kan man herigennem tegne et mønster, der kan være nyttigt, f.eks. fordi det giver information om produktets bruger eller om andre, der kommer i kontakt med produktet. RFID-teknologien har et stort potentiale for datalagring, fordi det er muligt at aflæse data uden at produktet er i fysisk kontakt med en skanner. Så længe den slags applikationer udelukkende retter sig mod den pågældende genstand mv., er man som udgangspunkt uden for det lovregulerede område. Men i det øjeblik der opstår mulighed for at sammenstykke oplysninger om en genstands fysiske placering mv. med personoplysninger, bevæger man sig inden for lovens område. Et eksempel herpå er de overvejelser, Den Europæiske Centralbank har gjort om at indbygge RFID-tags i euro-pengesedler, således at man kan følge den enkelte pengeseddel og modvirke hvidvaskning og falskmøntneri. Tilsvarende problemer kan opstå, hvis RFID-teknologi anvendes til at lokalisere bøger, der udlånes fra offentlige biblioteker, eller jetoner, der udbetales fra kasinoer. En grundig analyse af disse spørgsmål er i øvrigt indeholdt i den udtalelse, Artikel 29-Gruppen har afgivet den 19. januar 2005 (WP 105).

Modifikationer

Loven indeholder nogle væsentlige modifikationer i denne brede afgrænsning.

For det første følger det af § 2, stk. 7 – 8, at loven ikke finder anvendelse på informationsdatabaser, hvori der udelukkende er indlagt allerede offentliggjorte periodiske skrifter eller lyd- og billedprogrammer, der er omfattet af medieansvarslovens § 1, nr. 1 eller 2, henholdsvis § 1, nr. 3, eller dele heraf. Det er dog en betingelse, at der ikke er sket ændringer i sådanne basers indhold efter indlæggelsen. I sådanne tilfælde gælder fortsat reglerne i § 41 om behandlingssikkerhed og § 42 om anmeldelsespligt, ligesom erstatningsreglen i LBP § 69 kan gøres gældende af den registrerede.

For det andet følger det af lovens § 7, stk. 2, nr. 3, at det er tilladt at behandle oplysninger, som er blevet *offentliggjort* af den registrerede, selv om der er tale om ellers følsomme oplysninger, herunder om den registreredes racemæssige eller etniske baggrund, hans politiske og fagforeningsmæssige tilhørsforhold eller hans helbredsmæssige og seksuelle forhold.

Vurderinger

Ifølge forarbejderne til den gældende lov anses også oplysninger om, hvorledes andre *vurderer* den registrerede (f.eks. i forbindelse med en kreditvurdering) for at være personoplysninger. Efter en stringent betragtning må man dog sondre mellem vurderingen og dens grundlag. En sådan sondring kan vel være vanskelig at gennemføre i tilfælde, hvor præmis (faktum) og konklusion (bedømmelse) er tæt forbundne: En udtalelse om, at NN ikke er kreditværdig, fordi han har afgivet insolvenserklæring, indebærer en vurdering, der er en umiddelbar følge af personoplysningen. Men forholdet stiller sig anderledes, hvis den manglende kreditvurdering af en person, der driver virksomhed inden for en bestemt branche, skyldes en nøje analyse af, at der på sigt ikke længere vil være nogen fremdrift i denne branche. En sådan vurdering kan ikke i sig selv siges at være en personoplysning, udover den information, der ligger i, at NN driver virksomhed inden for denne branche.

Juridiske personer

Udenfor begrebet falder bl.a. oplysninger om juridiske personer, medmindre der er tale om oplysninger om de enkeltpersoner, der fungerer som tegningsberettiget eller befuldmægtiget for den juridiske person. Visse af lovens regler kan dog også påberåbes af juridiske personer, således kapitel 5 om videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige og kapitel 6 om kreditoplysningsbureauer.

At man har indført et så vidtspændende begreb skyldes dels omgåelsesbetragtninger (var det tilladt at foretage registrering af enkelte fragmenter af personoplysninger uanset lovens regler, ville der herved åbnes mulighed for vanskelige afgrænsninger, som kunne udnyttes til omgåelse), dels den praktiske betragtning, at man ved brug af informationsteknologi ofte kan sammenstykke hele mosaikbilleder af disse enkelte fragmenter af personoplysninger. Til illustration herom nævnes det eksempel, der benyttes i *PA* s. 627: En pater ankommer for sent til et selskab, hvor han over for de andre deltagere undskylder sig med, at han havde et langvarigt skriftemål fra en person, der tilstod et mord. Kort efter ankommer en anden deltager i selskabet, der beklager sin sene ankomst med, at han var i kirken for at skrifte.

Denne mosaik-sammenhæng illustreres ved *U 1999.560 H*, hvor Højesteret fandt, at et dagblad kun-

ne gøres ansvarlig for en injurierende omtale af en ikke navngiven direktør, om hvem det dog var oplyst, at han indtil midten af 1994 havde været ansat som underdirektør i en stor bank.

Som følge af denne brede begrebsanvendelse indebærer LBP, at selv harmløse oplysninger, der transmitteres pr. e-mail via Internet, i princippet er omfattet af lovreguleringen, jf. Justitsministeriets notat af 28. oktober 1997 om personoplysninger på Internettet, optrykt i bilagshæftet til betænkning 1345/1997 s. 209 ff. (s. 213) samt generelt *Lucas Bergkamp & Jan Dhont* i 7 The EDI Law Review (2000), s. 71 ff. I de fleste tilfælde volder sådanne former for transmission dog ingen retlige problemer i relation til loven, bl.a. fordi parter, der vælger at kommunikere med hinanden via e-post, hermed også må antages at have afgivet det fornødne samtykke til denne gensidige informationsudveksling.

Bipersoner

LBP omfatter også de såkaldte "*bipersoner*". Herved forstås oplysninger om personer, der alene optræder i den pågældende behandling på grund af den registreredes tilknytning til en anden person – "hovedpersonen". I Datatilsynets vejledning nr. 126 af 10. juli 2000 om registreredes rettigheder efter reglerne i LBP kapitel 8-10 (tilgængelig fra <www.datatilsynet.dk>) nævnes som eksempler herpå oplysninger om pårørende til den registrerede eller om vidner i en civil retssag, se pkt. 1.5. Som nævnt sammesteds vil oplysninger om en biperson ofte være registreret i tilknytning til oplysninger om en hovedperson. Dette indebærer, at der af tekniske grunde ofte kun kan fås oplysninger om bipersonen via hovedpersonens navn, adresse og lignende. Bipersoner har imidlertid som udgangspunkt samme rettigheder som andre registrerede personer, herunder i henseende til adgangen til at gøre indsigelse mod en databehandling. Se nærmere herom *Blume* i U 2002B.112 ff.

13.3.c. Pligtsubjektet

I konsekvens af de afgrænsningsvanskeligheder, den moderne informationsteknologi har skabt i henseende til afgrænsningen af begreberne "registre" og "behandling", er det nødvendigt at få præciseret, hvilke parter der er genstand for de forpligtelser, LBP pålægger ved behandlingen af personoplysninger. Lovens § 3, nr. 4 og 5, sondrer her mellem to pligtsubjekter: Den dataansvarlige og databehandleren.

- den dataansvarlige

Som *dataansvarlig* (engelsk: "controller") anses ifølge § 3, nr. 4, den, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af per-

sonoplysninger. Den dataansvarlige er den person eller virksomhed, der bestemmer, hvad der skal ske med personoplysningerne. En dataansvarlig kan altså enten være en fysisk eller juridisk person, herunder en offentlig myndighed. Afgørende er, at den pågældende træffer de grundlæggende, til dels strategiske, beslutninger om, hvilke data der skal behandles, hvorfor og hvordan. Da disse strategiske valg således ligger i hænderne på den dataansvarlige, er det også denne, som står i centrum for lovens materielle forpligtelser, ligesom den dataansvarlige er genstand for det særlige erstatningsansvar i LBP § 69.

- databehandler

Databehandleren er derimod den – fysiske eller juridiske – person, der behandler oplysninger på den dataansvarliges vegne. Databehandleren træder dermed først frem på scenen i situationer, hvor den dataansvarlige ikke selv forestår driftsafviklingen af de IT-systemer mv., som personoplysningerne behandles i. Dette kan f.eks. tænkes, hvis den organisation, der anvender de pågældende data, har *outsourcet* sin IT-drift til en ekstern leverandør. Den eksterne leverandør bliver dermed "databehandler".

Repræsentation

Den registrerede kan som udgangspunkt give en anden fuldmagt til at udøve den kompetence, der efter loven tilkommer ham selv. Dette udgangspunkt modificeres dog på i hvert fald to punkter. I relation til *afgivelsen* af den pågældende fuldmagt må der for det første stilles visse krav om klarhed til den viljeserklæring, der ligger til grund for denne fuldmagt. Det er her nærliggende at skele til de krav til samtykkets karakter, der stilles jf. LBP § 6, stk. 1, nr. 1, og § 3, nr. 8. I relation til den *medkontrahent*, som dispositionen gøres gældende overfor, må der dernæst stilles visse krav om sikkerheden for, at der foreligger en fuldmagt, jf. nærmere afsnit 13.4.d.

13.4. Hvilke oplysninger må behandles?

13.4.a. Samtykketilfælde

Problemet

LBP stiller forskelligartede betingelser for, at en personoplysning må behandles. I § 6 opstilles nogle almindelige betingelser, der er gældende for alle typer af personoplysninger. Disse betingelser suppleres med yderligere betingelser om de såkaldt følsomme oplysninger i § 7, og de næstfølgende bestemmelser (§§ 8-14) giver herudover særlige regler for visse typer af personoplysninger. Ved siden af disse oplysningsspecifikke regler foreskriver

LBP § 5, *hvordan* oplysningerne skal behandles, jf. herom afsnit 13.5.

Udgangspunktet

LBP opstiller som en almindelig betingelse, at behandling af personoplysninger, der resulterer i en registrering, kræver den registreredes udtrykkelige samtykke, se LBP § 6, stk. 1, nr. 1. Bestemmelsen forudsætter, at der er tale om en personoplysning. En oplysning, der ikke – eller ikke uden en helt ekstraordinær indsats – kan føres tilbage til den registrerede, kan således indsamles uden samtykke. F.eks. er det tilladt, at et supermarked på grundlag af kasseapparaterne registrerer oplysninger om, hvilke varegrupper der købes på hvilke tidspunkter. Men hvis disse oplysninger kombineres med oplysninger om den enkelte forbrugers identitet (f.eks. baseret på det anvendte kreditkort), skal der indhentes samtykke (hvis ikke behandlingen kan støttes på andre regler).

En sådan kombination kan tænkes, hvis de personoplysninger, supermarkedet behandler, gøres til genstand for såkaldt *data mining*.

Ifølge § 3, nr. 8, foreligger der et samtykke fra den registrerede ved enhver frivillig specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilliger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling. Se i øvrigt om problemet *Peter Blume* i U2000B.77 ff., der på det retspolitiske plan stiller forslag om yderligere kvalificerede krav for at anse et samtykke for gyldigt.

Udtrykkelighedskravet

Selv om bestemmelsen stiller krav om, at samtykket skal foreligge "udtrykkeligt", må det antages, at betingelserne er opfyldte, hvis de almindelige krav for at anse en viljestilkendegivelse for et "samtykke" er opfyldte, jf. herved definitionen i lovens § 3, nr. 8, se således betænkning 1345/1997 s. 215 og 445. Også visse former for "konkludent adfærd" er således omfattet af begrebet, jf. tilsvarende *Nielsen & Waaben* (2001), s. 113 f., hvorimod det er vanskeligere at statuere den fornødne "udtrykkelighed" i form af en forudsætning, der blot søges indlagt i en handlemåde. Som vejledning for bedømmelsen kan man skele til, om den pågældende viljeserklæring i et *forbrugerforhold* ville være tillagt aftalevirkninger, sml. i samme retning *Blume* Databeskyttelsesret (2000), s. 95. Småttrykte vilkår i omfattende aftaledokumenter vil således ikke nødvendigvis opfylde samtykkekravet – trods "udtrykkelighed" og skriftlighed – hvorimod stiltiende markeringer kan, hvis den pågældende behandling åbenbart sker i den registreredes interesse.

Standardklausuler

I praksis vil samtykkekravet nok hyppigst give anledning til tvivl i relation til fortrykte samtykke-klausuler, som den (senere)

registrerede anmodes om at underskrive i forbindelse med indgangen til et kundeforhold, eller når der indgås aftale via en hjemmeside. I overensstemmelse med de principper, der gælder om vedtagelse af standardvilkår, se hertil *GA* s. 363 ff., må det derfor antages, at kravene til samtykkets styrke beror på, hvilke retsvirkninger samtykket tilsigter at godkende. Jo mere de pågældende oplysninger nærmer sig de tilfælde (jf. nærmere nedenfor), hvor samtykke er ufornødent, desto lavere krav må man stille til dets udtrykkelighed. Gælder samtykket derimod en helt atypisk anvendelse (f.eks. en tilladelse til at anvende oplysningerne til at tegne en nærgående personlighedsprofil), vil det i almindelighed ikke være tilstrækkeligt at henvise til en blandt talrige klausuler i et sæt forretningsbetingelser.

LBP tager ikke stilling til betydningen af, at et samtykke meddeles mod betaling. Der er som udgangspunkt intet til hinder for, at den registrerede stiller krav om betaling (eller opnår særlige rabatydelser) som betingelse for at afgive sit samtykke, men sådanne betalingselementer gør ikke i sig selv samtykket mere eller mindre "udtrykkeligt".

Et meddelt samtykke kan kaldes tilbage, jf. LBP § 38. Tilbagekaldelsen har i så fald kun virkning for fremtiden, men hvis der – som det ofte er tilfældet – er tale om en behandling, der har resulteret i, at den registrerede står anført i en database el.lign., er den nok så centrale virkning heraf, at den registrerede herefter må udgå af basen. Som følge af denne bestemmelse antages det at være i strid med god markedsføringsskik, jf. mfl. § 1, at en erhvervsdrivende betinger en aftale af, at forbrugeren giver samtykke til videregivelse af oplysninger til anvendelse uden for virksomheden. Tilbagekaldelse

13.4.b. Aftaletilfælde

Ifølge LBP § 6, stk. 1, nr. 2, kan personoplysninger behandles, hvis behandlingen er nødvendig af hensyn til opfyldelsen af en aftale, som den registrerede er part i (eller med henblik på foranstaltninger truffet på den registreredes anmodning forud for aftaleindgåelsen). Bestemmelsen har stor praktisk betydning, fordi den legitimerer den anvendelse af personoplysninger, der sker i forbindelse med hovedparten af den kommercielle kommunikation med kunder og forretningsforbindelser mv. En virksomhed behøver altså ikke sikre sig sin kundes samtykke til, at der oprettes et kartotekskort på kunden i virksomhedens database.

Med kravet om, at en sådan behandling skal være "nødvendig", er det ikke tilsigtet at forbyde enhver form for behandling, som strengt taget godt kunne udføres på anden måde. Det er nærliggende at læse bestemmelsen således, at nødvendighedskravet sættes i relation til databehandlerens mulighed for at drive virksomheden på en måde, der er *sædvanlig* for virksomheder af den pågældende type. Det har således aldrig været intentionen med en lovgivning om persondatabeskyttelse, at virksomheder og myndigheder skulle være afskåret fra at høste de rationaliseringsgevinster, en sædvanlig registrering og behandling af personoplysninger åbner mulighed for.

13.4.c. Retlig forpligtelse

Selv om der hverken foreligger samtykke eller behandlingen understøtter et aftaleforhold, kan den være legitim som nødvendig "for at overholde en retlig forpligtelse, som påhviler den dataansvarlige", jf. § 6, nr. 3. Med "retlig forpligtelse" sigtes til sådanne forpligtelser, der følger af lovgivningen eller administrative forskrifter fastsat i medfør heraf, f.eks. en læges pligt til at notere navnene på de patienter, der udstedes recepter til. Forpligtelsen behøver dog ikke have hjemmel i en regel, der specifikt omtaler en sådan forpligtelse til at opbevare personoplysninger.

Bevisregler

Et praktisk vigtigt eksempel på en retlig forpligtelse er de bevisretlige regler. Interessen i at kunne føre bevis til godtgørelse af retskrav kan legitimere opbevaring af bilagsmateriale mv., der indeholder personoplysninger, hvis en sådan opbevaring er forudsætningen herfor. Et andet eksempel er pligten til at udlevere visse oplysninger til det offentlige i forbindelse med kriminel efterforskningsvirksomhed, se herved § 15 i lov om konkurrence- og forbrugerforhold på telemarkedet, jf. lovbekendtgørelse nr. 679 af 23. juni 2004. Bestemmelsen har nær forbindelse med § 6, stk. 1, nr. 6, der legitimerer behandlinger, der er nødvendige af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som den dataansvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt.

13.4.d. Andre tilfælde

Vitale interesser

Ifølge § 6, stk. 1, nr. 4, er der hjemmel til at behandle personoplysninger, når behandlingen er nødvendig for at beskytte den registreredes "vitale interesser". Hermed menes, jf. betænkning 1345/1997, s. 446, interesser, som er af fundamental betydning

for den registrerede. Da man i almindelighed må formode, at den registrerede selv vil være parat til at meddele samtykke til en sådan behandling – hvis han kunne – har bestemmelsen sit primære anvendelsesområde i tilfælde, hvor den registrerede pga. sygdom eller bortrejse er ude af stand til at meddele sit samtykke til en behandling.

Samfundets interesse

Behandling kan også ske uden samtykke, hvis den er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse, LBP § 6, stk. 1, nr. 5. Når området for denne bestemmelse afgrænses, må det holdes for øje, at store dele af den samfundsmæssige interessevaretagelse, der sker i den offentlige forvaltning, som følge af det forvaltningsretlige legalitetsprincip vil være omfattet af § 6, stk. 1, nr. 3, om behandlinger, der har udslag af en (offentlig-)retlig forpligtelse. Som eksempler på opgaver i samfundets interesse, der ikke har denne lovbundne karakter, omtaler betænkning 1345/1997, s. 446, behandling i statistisk, historisk eller videnskabeligt øjemed samt i forbindelse med retsinformationssystemer. Det forhold, at behandling sker i et kommercielt øjemed, udelukker ikke, at den anses for at varetage almene interesser, jf. smst. s. 446 f.

"Berettiget interesse"

LBP § 6, stk. 1, nr. 7, indeholder en bredt formuleret afslutningsbestemmelse, hvorefter behandling kan finde sted, hvis denne er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, "kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse". Efter sin formulering rummer denne bestemmelse flere af de forudgående bestemmelser (herunder nr. 3, 4, 5, og 6), og dens funktion er da også at modvirke modsætningsslutninger fra disse forudgående bestemmelser.

Følsomme oplysninger

De foregående regler gælder for enhver oplysning, der har karakter af "personoplysning", uanset om den er banal, om den angår "personlige forhold" (jf. § 1, stk. 2) eller om den er af mere følsom karakter. Når det gælder de såkaldt følsomme (eller sensitive) oplysninger om "racemæssige eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold", opstiller LBP § 7 en række mere restriktive betingelser for behandlingen.

Udgangspunktet er – som i øvrigt i loven – at en behandling af sådanne oplysninger ikke må finde sted; men spektret af undtagelser er mere begrænset end efter § 6. Vel kan den registrerede, jf. § 7, stk. 2, nr. 1, i alle tilfælde give sit udtrykkelige samtykke hertil; men hvis ikke der foreligger et sådant udtrykkeligt sam-

tykke, er kun nogle af undtagelsesbestemmelserne anvendelige. I det omfang de er, er anvendeligheden begrænset i forskellige henseender. Når det gælder den registreredes vitale interesser, stilles som et yderligere krav, jf. § 7, stk. 2, nr. 2, at den pågældende ikke fysisk eller juridisk er i stand til at give sit samtykke, og når det gælder efterkommelsen af retlige forpligtelser, skal behandlingen være nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares, § 7, stk. 2, nr. 4.

Foruden disse, almindelige regler, er det under forskellige omstændigheder tilladt at registrere bestemte typer af følsomme oplysninger, eksempelvis oplysninger, der allerede er offentliggjort af den registrerede (f.eks. en politikers markering af et standpunkt i den offentlige debat), jf. § 7, stk. 2, nr. 3. Dernæst bestemmer § 7, stk. 3, at oplysninger om fagforeningsmæssige tilhørsforhold kan behandles, hvis dette er nødvendigt for at opretholde den dataansvarliges arbejdsretlige forpligtelser eller specifikke rettigheder. Det erindres i den forbindelse, at behandling af almindelige oplysninger om medarbejderes forhold er lovlig efter reglerne i enten § 6, nr. 2 (aftaleopfyldelse) eller § 6, nr. 3 (retlig forpligtelse).

De førnævnte regler kan betragtes som "indgangsbilletten" til at kunne foretage behandlinger af personoplysninger indenfor det område, LBP dækker. Men når det gælder den herpå følgende behandling af disse oplysninger, indeholder loven et kompliceret regelsæt, der dels indeholder visse generelle principper for, hvorledes behandling kan ske (§ 5), dels opstiller specielle krav om anmeldelse (lovens afsnit V), godkendelse (§ 50) samt om sikkerhedskrav (afsnit IV).

13.5. Hvordan skal oplysningerne behandles?

13.5.a. Almene krav

God databehandlingsskik

LBP § 5 opstiller en række generelle principper for, hvorledes behandling kan ske. Bestemmelsen er opbygget på grundlag af en bred retsstandard, jf. § 5, stk. 1, hvorefter oplysninger skal behandles i overensstemmelse med "god databehandlingsskik". Med denne formulering har Udvalget om Registerlovgivningen oversat ordene "fairly and lawfully" i direktivets art. 6, stk. 1, litra a, med en vending, der harmonerer med andre god skik-regler i dansk lovgivning (herunder god markedsføringsskik, god

revisionsskik, god advokatskik, god værdipapirhandelsskik, god presseskik mv.).

Når begrebet "god databehandlingsskik" skal udfyldes, kan man formentlig drage en parallel til reglerne om den legale programlicens i ophl. § 36. Således må det antages, at den dataansvarlige har ret til at foretage løbende sikkerhedskopiering af persondata i overensstemmelse med god sikkerhedspraksis. De således udførte kopier skal dog efterleve de sikkerhedsmæssige krav, loven opstiller, jf. nærmere § 41 og nærmere herom nedenfor.

Ligesom det kendes fra regelstrukturen i mfl. § 1 opløser princippet om god databehandlingsskik sig i en række delprincipper, der udmøntes i de efterfølgende stykker af § 5. Disse delregler kan føres tilbage til OECD's førnævnte Data Protection Guidelines. Hertil hører det i § 5, stk. 2, nævnte "*finalité*"-princip, hvorefter indsamling og senere behandling af oplysninger skal ske til "udtrykkeligt angivne og saglige formål" samt det i stk. 3 nævnte *bestemthedsprincip*, hvorefter behandlede oplysninger skal være "relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves for opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles". Ligeledes indeholder stk. 4 et princip om *datakvalitet*, hvorefter der skal ske fornøden ajourføring samt kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger, samt sletning eller berigtigelse i fornødent omfang. Endelig indeholder stk. 5 en regel om, at oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i længere tidsrum end det, der er nødvendigt til de formål, hvortil oplysningerne behandles. Temaet er altså generelt det, at enhver behandling af personoplysninger skal være *sagligt velbegrundet* og må ikke gå videre, end dette saglige formål retfærdiggør.

Arbejdspladsovervågning

Reglerne illustreres ved Datatilsynets afgørelse af 19. september 2000 i en sag, hvor et forsikringsselskab ønskede at logge medarbejderes brug af IT-systemerne, herunder også Internetbrug. Således loggede man oplysninger om dato og klokkeslet for søgninger på Internet, IP-adresser, http-adresser samt fejlkoder. Formålet hermed var at finde årsager til fejl og driftsforstyrrelser eller manglende adgang til eksterne sites, ligesom loggen gav mulighed for at rekonstruere en eventuel hackers besøg. Kun ganske få medarbejdere med administratorrettigheder havde adgang til loggen, og disse havde strenge pålæg om ikke at følge loggen på fysiske arbejdsstationer. Det var således helt undtagelsesvis og kun efter forudgående advis, at loggen blev konsulteret.

Efter i sin udtalelse at have slået fast, at de nævnte oplysninger har karakter af personoplysninger (idet de kan føres tilbage til den enkelte bruger) fandt Datatilsynet, at den pågældende logning af oplysninger måtte anses for at være indsamlet til "udtrykkeligt angivne og saglige formål" i overensstemmelse med § 5, stk. 2, i lov om beskyttelse af personoplysninger. Det forhold, at virksomheden gennemgik loggen i tilfælde, hvor der var mistanke om brug af Internet i strid med interne regler, fandt tilsynet heller ikke uforeneligt med de formål, til hvilke oplysningerne var indsamlet. Datatilsynet udtalte dog, at det var en forudsætning, at medarbejderne på forhånd på en klar og utvetydig måde var blevet informeret om logningen samt den eventuelle gennemgang heraf, jf. reglerne om oplysningspligt i den førnævnte lovs §§ 28 og 29. For så vidt angår e-post fandt Datatilsynet, at virksomhedens sikkerhedskopiering mv. var nødvendig for, at den kunne følge berettigede interesser, nemlig hensynet til drift, sikkerhed, genetablering af dokumentation samt hensynet til kontrol og brug. Også i så henseende var det dog en forudsætning, at de berørte medarbejdere på forhånd klart og utvetydigt var blevet informeret herom. Afslutningsvis bemærkede Datatilsynet, at den trufne afgørelse ikke indebærer nogen ret for virksomheden til at læse medarbejderes private post.

I en afgørelse af 30. oktober 2001 har tilsynet tilsvarende fastslået, at god databehandlingsskik tilsiger, at ansatte på forhånd på en klar og utvetydig måde er informeret om, at kontrol kan finde sted, jf. herved også reglerne om oplysningspligt i lovens §§ 28-29. Afgørelsen fastslår dernæst, at oplysninger om, hvilke hjemmesider en person har besøgt på Internettet, må betragtes som almindelige ikke-følsomme oplysninger, hvis lovlighed skal vurderes efter reglerne i lovens § 6, stk. 1, nr. 1-7. I den foreliggende sag fandt tilsynet, at virksomhedens gennemgang af medarbejderens Internet-browser og e-mails var nødvendig for, at virksomheden kunne undersøge en mistanke om, at den ansatte havde gjort omfattende privat brug af sin Internet-adgang. Gennemgangen havde ligeledes været nødvendig for, at virksomheden kunne få adgang til de heri indeholdte arbejdsrelaterede informationer. Derfor havde virksomheden haft en berettiget interesse i at foretage denne gennemgang.

13.5.b. Anmeldelsespligt

Det andet regelsystem for behandling af personoplysninger følger af LBP, afsnit V, der indeholder regler om anmeldelse af be-

handlinger, der foretages henholdsvis for den offentlige forvaltning (kapitel 12), for en privat dataansvarlig (kapitel 13) og for domstolene (kapitel 14). Efter disse regler skal der inden igangsættelse af en behandling foretages anmeldelse til Datatilsynet (§ 43 og § 48) medmindre behandlingen falder inden for en af de undtagelser, der er omtalt henholdsvis i § 44 og § 49. Tilsvarende gælder om ændringer i de pågældende oplysninger, jf. § 46 og § 51. Anmeldelsespligten er præciseret ved Justitsministeriets bekendtgørelse nr. 529 af 15. juni 2000, der gør undtagelse for visse behandlinger, der foretages for den offentlige forvaltning.

Anmeldelsen skal angive navnet på den dataansvarlige, behandlingens betegnelse og formål, en generel beskrivelse af behandlingen og af de typer af oplysninger, der vedrører enkelte kategorier af registrerede, modtagere af oplysninger, påtænkt dataeksport til tredjelande, sikkerhedsforanstaltninger samt start og sluttidspunkt, jf. nærmere § 43, stk. 2, og henvisning hertil i § 48, stk. 2. Når det gælder private databehandlere, er en række oplysninger dog undtaget for anmeldelsespligten, jf. § 49, stk. 1. Dette gælder således visse, nødvendige, oplysninger om ansatte, kunder og leverandører samt behandlinger, der sker med henblik på udførelse af visse markedsundersøgelser. Ligeledes er behandlinger foretaget af foreninger (nr. 6), advokater (nr. 7) samt visse former for godkendt behandlingspersonale (nr. 8-9) undtaget.

Se generelt om anmeldelsespligten, Datatilsynets vejledning nr. 125 af 10. juli 2000.

13.5.c. Tilladelseskrav

Det tredje led i reguleringen af behandlingen findes i de særlige tilfælde, hvor en behandling forudsætter tilladelse fra Datatilsynet. Regler herom findes i § 50. Bestemmelsen knytter sig til anmeldelsespligten i LBP § 48 og gælder derfor kun så langt den rækker. Pligten gælder således kun for private dataansvarlige, men ikke i relation til behandlinger, der er undtaget fra anmeldelse i medfør af LBP § 49, jf. undtagelsesbekendtgørelsen hertil, nr. 534 af 15. juni 2000, som ændret ved bekendtgørelse nr. 202 af 22. marts 2001. Tilsynets tilladelse er således nødvendig, når behandlingen omfatter følsomme oplysninger (jf. henvisningen til § 7, stk. 1) og – for privatpersoners vedkommende – "strafbare forhold, væsentlige sociale problemer og andre rent private forhold" (jf. henvisningen til § 8, stk. 4). Dernæst gælder tilladelseskravet i relation til advarselsregistre (nr. 2), kreditoplysningsbureauer (nr. 3), headhunterfirmaer (nr. 4) samt retsinformationssy-

stemer (nr. 5). Ligeledes gælder det generelt, at eksport af persondata forudsætter Datatilsynets tilladelse, jf. § 50, stk. 2.

13.5.d. IT-sikkerhed

Det fjerde niveau af reguleringen er de regler om behandlingssikkerhed, der findes i LBP afsnit IV. § 41, stk. 3, opstiller her en generalklausul, hvorefter "den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven". Denne regel gælder ikke alene for den dataansvarlige, men også for medarbejdere og samarbejdspartnere, jf. §§ 41, stk. 1, og 42. Kravene hertil er præciseret i Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000, som ændret ved bekendtgørelse nr. 201 af 22. marts 2001, om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

Legitimationskrav

En naturlig følge af kravet om oprettelse af en passende behandlingssikkerhed er kravet om, at den registeransvarlige ikke lader personoplysninger tilgå parter, der ikke er berettigede til at modtage dem pga. manglende kontrol med, hvem modtageren er. Efter den almindelige sikkerhedsregel i § 41, stk. 3, skal databehandleren sikre sig, at den, der meddeles oplysninger til, er rette person, så oplysninger om den registrerede ikke kommer til uvedkommendes kendskab. Dette antages i tilsynets praksis at indebære, at der kun må udleveres oplysninger, når vedkommende har *legitimeret sig* behørigt, eller når der på anden måde er skabt sikkerhed for, at den, der f.eks. fremsætter en indsigtsbegæring, er identisk med den person, som oplysningerne vedrører.

I Datatilsynets vejledning nr. 126 af 10. juli 2000 om registreredes rettigheder efter reglerne i LBP kapitel 8-10, pkt. 1.3, siges det, at kravet om legitimation kan fraviges, når der på anden måde er skabt sikkerhed for, at den person, som f.eks. fremsætter en begæring om indsigt, er identisk med den person, oplysningerne vedrører. Herved tænkes navnlig på den situation, at den medarbejder hos den dataansvarlige, som modtager begæringen, i forvejen kender den person, der fremsætter begæringen. Når en henvendelse er fremsat skriftligt, og hvis navn og adresse i brevet er identisk med de oplysninger, som i forvejen fremgår af sagen, vil der i almindelighed ikke være grund til at foretage særlige undersøgelser, inden oplysningerne sendes til den registrerede på den angivne adresse. "Særligt gælder det, at der bør udvises forsigtighed med fremsendelse af fortrolige oplysninger til en c/o-adresse, som den registrerede ikke

selv har oplyst." En generelt dækkende vejledning om etablering af tekniske og organisatoriske sikkerhedsforanstaltninger findes i DS 484: Norm for edb-sikkerhed.

13.6. Særlige behandlinger

13.6.a. Almindelig karakteristik

Foruden disse almindelige regler om behandling af personoplysninger, indeholder LBP og dele af særlovgivningen et virvar af særregler, som ud fra forskellige – ikke altid lige konsekvente – principper søger at tilgodese de særlige beskyttelseshensyn, der gør sig gældende på forskellige områder.

13.6.b. Personnummer

Problemstillingen

Reglerne vedrørende registrering af personnumre (CPR-numre) har givet anledning til intens retspolitisk debat samt til en lovregulering, der frem til vedtagelsen af LBP indebar, at sådanne identifikationsoplysninger kun måtte registreres efter de, strenge, betingelser, der stilledes for registrering af følsomme oplysninger. At personnummeret har været betragtet som specielt sensitivt hænger sammen med, at det ofte håndteres som en slags indgangsnøgle til de oplysninger, der er registreret om enkeltpersoner i den offentlige forvaltnings registre. Mange forvaltningsmyndigheder, pengeinstitutter, forsikringsselskaber og andre institutioner, hvis datakvalitet baseres på personnummeret, følger den tvivlsomme og i almindelighed retsstridige praksis at udlevere følsomme personoplysninger over telefonen til en person, der angiver sig som den registrerede og giver oplysninger om "sit" CPR-nummer. En sådan praksis kan vel kritiseres af retlige grunde (eftersom resultatet er en uberettiget videregivelse af disse følsomme oplysninger), men at den undertiden følges, skyldes ikke mindst, at der i dag reelt ikke er andre alment udbredte identifikationsværktøjer til rådighed (f.eks. i form af digital signatur el.lign.).

LBP

Spørgsmålet gav ligeledes anledning til intens diskussion i Justitsministeriets Udvalg om Registerlovgivningen, se hertil betænkning 1345/1997, s. 259 ff., hvor et stort flertal gik ind for en liberalisering af de tidligere restriktive regler. Ifølge LBP § 11, stk. 1, har offentlige myndigheder nu generelt adgang til at an-

vende CPR-numre med henblik på entydig identifikation eller som journalnummer. For private gælder denne ret kun, når dette 1) følger i henhold til lov eller bestemmelser fastsat i henhold til lov, 2) når den registrerede har givet sit udtrykkelige samtykke hertil, eller 3) når behandlingen alene finder sted til videnskabelige eller statistiske formål.

I tilknytning til den sidstnævnte bestemmelse er herudover indsat en bestemmelse om *videregivelse* af oplysninger om personnummer, som efter sin placering alene finder anvendelse i det omfang, der i øvrigt er ret til at behandle de pågældende oplysninger. En sådan videregivelse kan enten ske i tilfælde, hvor den er et naturligt led i den normale drift af virksomheder mv. af den pågældende art, og videregivelsen er af afgørende betydning for at sikre en entydig identifikation af den registrerede, eller i tilfælde hvor videregivelsen kræves af en offentlig myndighed (uden at dette i øvrigt er hjemlet, sml. stk. 2, nr. 1). I de tilfælde, der er omfattet af § 11, stk. 2, nr. 3, må der ikke ske offentliggørelse af personnumre uden udtrykkeligt samtykke, jf. § 11, stk. 3.

13.6.c. Kundeoplysninger

Som nævnt ovenfor kan man diskutere, om individets "ret" til sine personoplysninger kan karakteriseres som en ejendomsret. Uanset hvordan man forholder sig til denne diskussion ligger det klart, at der i mange henseender knytter sig væsentlige økonomiske interesser til en personoplysning, hvad enten den er følsom eller ikke. Dette gælder navnlig for oplysninger om en aktuel eller potentiel kundekreds. To situationer træder her frem:

- virksomheds-overdragelser

I det omfang disse kunder er enkeltpersoner – og ikke andre erhvervsdrivende juridiske personer – er det centralt for køberen at kunne disponere over det foreliggende *kundekartotek* uden at komme i konflikt med LBP. Efter en formel betragtning ligger det fast, at en videregivelse af et kundekartotek må betragtes som en selvstændig behandling, der må opfylde de almindelige regler for at være lovlig. I overensstemmelse hermed antog Registertilsynet i *RÅB 1991.117* ff., at en overførelse af kundeoplysningerne i et konkursramt motionscenter med henblik på, at køberen af centret kunne markedsføre sig overfor de hidtidige kunder, måtte anses som en videregivelse i medfør af § 4b i den tidligere lov om private registre, se nu LBP § 6, stk. 2.

Man kan diskutere afgørelsens rimelighed: I de tilfælde – som det foreliggende – hvor kundens tilknytning til en virksomhed primært knytter sig til virksomhedens produkt, snarere end dens indehaver, forekommer det unødigt formelt at knytte afgrænsningen af begrebet "overdragelse" til den juridiske persons identitet, når der i øvrigt ikke forekommer omgåelsesforsøg el.lign. Forholdet ligner i så fald den situation, der vil foreligge, hvis virksomhedsoverdragelsen realiseres som en aktieoverdragelse, og altså uden nogen formel overdragelse af de pågældende data til en ny juridisk identitet.

Direct marketing

Et andet særligt problem opstår ved målrettet anvendelse af personoplysninger til brug for markedsføring i form af *direct mail*, dvs. henvendelser til grupper af forbrugere afgrænset efter kriterier, der formodes at korrespondere med særligt købelystne markedssegmenter for bestemte varer og tjenester. Jo mere specialiserede og nicheprægede produkter, en virksomhed afsætter, desto mere værdifuld er kendskabet til potentielle kunder, der i kraft af tidligere efterspørgsel efter lignende produkter har røbet interesse herfor. Men den salgsmæssige interesse i at opnå en så høj datakvalitet som muligt (i form af så præcis afgrænsning af markedssegmentet som muligt) kolliderer her med det ønske, mange mennesker har i ikke at blive genstand for sådanne "personprofiler" – f.eks. manifesteret i et særligt "personligt" tilbud om køb af en bogtitel, der umiddelbart har lighed med en tidligere købt bog.

- den almindelige regel

Ifølge LBP § 6, stk. 2, må en virksomhed ikke videregive oplysninger om en forbruger til en anden virksomhed til brug ved markedsføring eller anvende oplysningerne på vegne af en anden virksomhed i dette øjemed, medmindre forbrugeren har givet sit udtrykkelige *samtykke* hertil. Et sådant samtykke skal indhentes i overensstemmelse med mfl. § 6a, se nærmere herom i afsnit 15.3.a.

- direct mail-virksomheder

Ifølge LBP § 12 må *direct mail*-virksomheder, der ikke har indsamlet deres oplysninger med den registreredes udtrykkelige samtykke, kun *behandle* oplysninger om navn, adresse, stilling, erhverv, e-post-adresse, telefon og telefaxnummer samt sådanne oplysninger, der indgår i erhvervsregistre eller i øvrigt er beregnet til at informere offentligheden. Direct mail-virksomheder må dog under ingen omstændigheder behandle oplysninger om enkeltpersoners rent private forhold, strafbare forhold, eller følsomme oplysninger, jf. § 12, stk. 2.

13.6.d. Kreditoplysningsvirksomhed

Som før nævnt skal den, der ønsker at drive virksomhed som kreditoplysningsbureau (defineret som "behandling af oplysnin-

ger til bedømmelse af økonomisk soliditet og kreditværdighed med henblik på videregivelse") *indhente tilladelse* fra Datatilsynet, inden behandlingen påbegyndes, jf. § 50, stk. 1, nr. 3, og § 19. Kreditoplysningsbureauer må kun behandle oplysninger, som efter deres art er af betydning for bedømmelse af økonomisk soliditet og kreditværdighed, LBP § 20. Følsomme oplysninger samt oplysninger om strafbare forhold må ikke behandles, jf. § 20, stk. 2, og kreditoplysninger, som er mere end 5 år gamle, må ikke behandles, medmindre det i enkelte tilfælde er åbenbart, at forholdet er af afgørende betydning for kreditvurderingen, § 20, stk. 3. Oplysninger om økonomisk soliditet og kreditværdighed må kun meddeles skriftligt. Summariske oplysninger kan dog meddeles mundtligt (eller på lignende måde), såfremt spørgerens navn og adresse noteres og opbevares i mindst 6 måneder, jf. § 23, stk. 1.

13.6.e. Whois-oplysninger

En særlig problemstilling knytter sig til de oplysninger om registranternes navn, adresse og telefonnummer, som DIFO (eller en anden kommende udbyder af .dk-administrationen) skal indeholde i sin database, jf. IDL § 8, stk. 1. Ifølge IDL § 8, stk. 2, skal administrator sikre, at oplysninger i denne base om registranternes navne, adresser og telefonnumre er offentligt tilgængelige. Bestemmelsen, der svarer til forslaget til betænkning 1450/2004 (se herved redegørelse og diskussion s. 192 ff.), men som ikke var med i ministerens oprindelige lovforslag, indeholder et vigtigt grundlag for den retsforfølgning, der ofte er nødvendig på nettet: Uden viden om, hvem der gemmer sig bag en hjemmeside eller som står bag en afsendt telefax, kan det være umuligt at forfølge retskrænkelser (f.eks. injurier eller ophavsretlige krænkelser) eller at foretage anmeldelser om strafbare lovovertrædelser. Mange af disse overtrædelser angår en særlovgivning, som politi og anklagemyndighed af ressourcemæssige grunde er nødt til at prioritere lavt. For det praktiske arbejde kan det derfor være nødvendigt med privat retshåndhævelse (søgsmål, forbudssager etc.), hvilket i sagens natur forudsætter kendskab til modpartens identitet.

Bestemmelsen modificeres ved IDL § 8, stk. 3, der pålægger administrator efter anmodning fra en registrant at sikre, at den pågældendes navn, adresse og telefonnummer ikke gøres offentligt tilgængelig, jf. stk. 2, hvis disse oplysninger i henhold til anden lovgivning er undtaget fra offentlighed. Oplysningerne vil

dog kunne videregives til Klagenævnet for Domænenavne i forbindelse med behandling af konkrete sager og til andre, i det omfang dette er berettiget i medfør af anden lovgivning i øvrigt. I den forbindelse kan bl.a. loven om det centrale personregister have betydning, se herved reglerne i kapitel 7 om navne- og adressebeskyttelse.

Ved § 11 i lov nr. 1439 af 22. december 2004 om pligtaflevering af offentliggjort materiale er der pålagt DIFO (eller den, der i øvrigt administrerer internetdomæner og lign., der særligt er tildelt Danmark), pligt til efter påkrav at aflevere en kopi i elektronisk form af listen over disse domæner samt oplysninger om registranterne (den såkaldte *whois-database*) til pligtafleveringsinstitutionen. Ifølge lovens § 19, stk. 3, indgår også dette materiale i de modtagende institutioners samlinger, idet adgangen til det pligtafleverede materiale dog kan være begrænset i medfør af anden lovgivning. Det forventes at der på grundlag af en udtalelse fra Datatilsynet vil blive fastsat nærmere retningslinjer for adgangen til de pligtafleverede (og dermed også tidligere) versioner af denne database.

13.7. Den registreredes rettigheder

13.7.a. Oplysningspligt

LBP opstiller en række retskrav for den registrerede, der tilgodeser dennes interesse i at få indseende med, hvilke oplysninger der behandles om den pågældende, samt i et vist omfang adgang til at modsætte sig videre registrering.

Meddelelsespligt

Ifølge LBP § 28 skal den dataansvarlige eller dennes repræsentant give den registrerede meddelelse, når der indsamles oplysninger hos den registrerede. I denne meddelelse skal den dataansvarlige give oplysning om sin identitet, hvad der er formålet med den pågældende behandling samt alle yderligere oplysninger, der må anses for nødvendige for, at den registrerede kan varetage sine interesser (herunder f.eks. hvem der vil modtage oplysningerne, om der er konsekvenser af ikke at besvare anmodningen, og hvilke regler der gælder om indsigt og berigtigelse af registrerede oplysninger).

Efter sit pålydende fremstår denne oplysningsforpligtelse – der har rod i direktivets art. 10 – som ganske vidtgående, og reglen har da også givet anledning til betydelig retspolitisk debat, såvel i forbindelse med direktivforhandlingerne som under det

efterfølgende danske udvalgsarbejde. En væsentlig modifikation af oplysningsforpligtelsen af stor praktisk betydning er imidlertid reglen i § 28, stk. 2, hvorefter oplysningsforpligtelsen ikke gælder, hvis den registrerede allerede er bekendt med de nævnte oplysninger. I praksis indebærer denne bestemmelse, at der ikke skal gives meddelelse om sådanne behandlinger, der sker i medfør af § 6, nr. 1 (samtykketilfælde), nr. 2 (gennemførelse af en aftale, som den registrerede er part i) og – alt efter reglernes indhold – også nr. 3 (overholdelse af en retlig forpligtelse, som påhviler den dataansvarlige). Det skal ligeledes fremhæves, at § 28 ikke opstiller noget krav om, at meddelelsen skal gives skriftligt eller under anvendelse af andre særlige formkrav. Vel kan den dataansvarlige have en egen interesse i at anvende bestemte former (herunder navnlig for efterfølgende at kunne dokumentere, at oplysningsforpligtelsen er overholdt), men i praksis er der intet til hinder for, at meddelelsen gives gennem tidligere opslag i forretningslokaler eller ved iøjnefaldende angivelse på en hjemmeside eller lignende.

Situationen er selvsagt anderledes, hvis oplysninger ikke er indsamlet hos den registrerede. I disse tilfælde pålægger LBP § 29 den dataansvarlige – eller dennes repræsentant – at meddele de førnævnte oplysninger senest ved registreringen eller – hvor de indsamlede oplysninger er bestemt til videregivelse – senest ved videregivelsen. Også her fraviges meddelelsesforpligtelsen, hvis den registrerede allerede er bekendt med de nævnte oplysninger. Ligeledes gælder meddelelsesforpligtelsen ikke, hvis videregivelsen er udtrykkeligt fastsat ved lov eller underretning viser sig umulig eller uforholdsmæssigt vanskelig, jf. § 29, stk. 2-3.

Undtagelser

Ifølge LBP § 30 viger meddelelsesforpligtelsen i medfør af §§ 28-29 "hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv". Med denne bestemmelse, som supplerer de undtagelsesbestemmelser, der følger af § 28, stk. 2, § 29, stk. 2-3, skal der i givet fald foretages en nøje afvejning af de interesser og hensyn, der i det konkrete tilfælde kan tale for at gennemføre, henholdsvis undlade, meddelelsesforpligtelsen. De private interesser, som kan komme på tale, kan f.eks. være ønsket om at bevare erhvervshemmeligheder, efterforskningshensyn el.lign. Der er altså ikke med denne undtagelsesbestemmelse åbnet op for en bred fravigelse af meddelelsesforpligtelsen.

13.7.b. Indsigtsret

Udgangspunkt

Ifølge LBP § 31 skal den dataansvarlige, på begæring fra enhver, give meddelelse om, hvorvidt der behandles oplysninger om den pågældende. Der gælder for så vidt en almindelig behandlingsindsigt (tidligere: "registerindsigt"). Behandles der oplysninger om den registrerede, har denne ret til – på en let og forståelig måde – at få meddelelse om, hvilke oplysninger der behandles, behandlingens formål, hvem der kan modtage oplysningerne samt information om – hvis denne er tilgængelig – hvorfra oplysningerne stammer.

Tidsfrister

Begæringer af den nævnte art skal besvares inden 4 uger efter modtagelsen, jf. § 31, stk. 2. Har man modtaget meddelelse efter disse regler, har man ikke – medmindre der godtgøres en særlig interesse – krav på at få en ny meddelelse, før der er gået 6 måneder, jf. § 33.

Retten til behandlingsindsigt – eller "egenaccess" – korresponderer i den offentlige forvaltning med de regler om aktindsigt, der følger af offentlighedslovens regler. For at sikre den fornødne korrespondens mellem de to regelsystemer fastslår § 32, stk. 2, at de undtagelser fra reglerne om dokument-offentlighed, der findes i offentlighedslovens § 2 samt §§ 7-11 samt 14, tilsvarende finder anvendelse, når den registrerede fremsætter begæring om indsigt, jf. § 31. Meddelelsen skal på begæring gives skriftligt (medmindre hensynet til den registrerede taler for, at den kan gives mundtligt) og der kan – i overensstemmelse med reglerne herom fastsat af Justitsministeriet – kræves betaling herfor, jf. § 34.

Undtagelser

Også indsigtsretten er underlagt visse undtagelser, jf. § 32. Den gælder således ikke, hvis hensynet til den registrerede viger for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv, jf. § 32, stk. 1, jf. § 30, stk. 1. For så vidt angår domstolenes behandling gælder den dernæst kun, hvis oplysningerne indgår i en tekst, som "foreligger i endelig form" (f.eks. som dom, beslutning eller kendelse), medmindre der er tale om oplysninger videregivet til tredjemand, jf. § 32, stk. 3. Indsigtsretten gælder heller ikke, hvis oplysningerne udelukkende behandles i videnskabeligt øjemed, eller med henblik på udarbejdelse af statistikker (§ 32, stk. 4).

13.7.c. Indsigelsesret

Udgangspunktet

Ifølge LBP § 35 kan den registrerede til enhver tid over for den dataansvarlige gøre indsigelse mod, at oplysninger om vedkommende gøres til genstand for behandling. Bestemmelsen indfører en formel *klageadgang* og tager altså ikke stilling til, om den registrerede rent faktisk har ret til at modsætte sig den pågældende behandling. Den indebærer, at den dataansvarlige har en strafsanktioneret (jf. LBP § 70, stk. 1, nr. 1) pligt til at tage stilling til, om indsigelsen er berettiget og – hvis dette er tilfældet – at ændre behandlingen således, at denne ikke længere omfatter de pågældende oplysninger, jf. stk. 2. Dette kan f.eks. tænkes, hvis der er tale om urigtige eller vildledende oplysninger, jf. nærmere LBP § 37.

Samtykke-tilbagekaldelse

Derimod giver LBP § 38 den registrerede ret til at tilbagekalde det samtykke, som ellers legitimerer den pågældende behandling. Loven tager ikke stilling til, om adgangen hertil er præceptiv, eller om den registrerede kan på forhånd kan give afkald herpå. Dens kerneområde er de tilfælde, hvor samtykket meddeles uden nogen egentlig modydelse. I disse tilfælde må formodningen være for, at der hersker præceptivitet – hvis ikke, ville reguleringen nærmest savne sit formål. Indgår samtykket derimod i en aftaleregulering, hvor transaktionen er betinget af, at de pågældende oplysninger kan anvendes, vil der ikke være tale om et enkeltstående samtykke, men om en behandling, der er legitimeret efter kontraktsreglen i LBP § 6, stk. 1, nr. 2. Et sådant indirekte "samtykke" kan ikke uden videre kaldes tilbage. Grænsen mellem de enkeltstående samtykketilfælde og tilfælde, hvor samtykket indgår som en integreret bestanddel af en aftaleregulering, kan dog være flydende.

Der er tale om en ganske vigtig undtagelse, givet de talrige bestemmelser i LBP, der betinger lovligheden af en behandling af den registreredes samtykke. Sådanne regler findes i LBP § 6, stk. 1, nr. 1 (den almindelige regel) og stk. 2 (videregivelse af oplysninger til markedsføringsformål), § 7, stk. 2, nr. 1 (følsomme oplysninger), og stk. 4 (videregivelse af følsomme oplysninger fra foreninger mv.), § 8, stk. 2, nr. 1 (videregivelse af semi-følsomme oplysninger fra den offentlige forvaltning), og stk. 4 og stk. 5 (privates behandling og videregivelse af oplysninger om strafbare forhold), § 11, stk. 2, nr. 2 og 3 (behandling af personnumre), § 12, stk. 1, nr. 3 (salg af adresseoplysninger med henblik på markedsføring) og § 27, stk. 2 (dataeksport til tredjelande).

Markedsførings-formål

En mere vidtgående indsigelsesret har den registrerede derimod, for så vidt angår oplysninger med henblik på *markedsføring*, jf.

LBP § 36. Fremsætter en registreret person indsigelser herimod, må sådanne oplysninger ikke behandles, selv om de måtte være legitimeret på andet grundlag. Bestemmelsen er suppleret med en oplysningsforpligtelse, hvorefter den dataansvarlige "udtrykkeligt" skal give oplysninger om indsigelsesretten, *inden* der foretages markedsføring overfor den registrerede. Når det gælder oplysninger til brug for markedsføring, har den dataansvarlige i øvrigt pligt til at give forbrugere meddelelse, inden første videregivelse, jf. nærmere § 36, stk. 2. I meddelelsen skal der udtrykkeligt gives oplysning om retten til at gøre indsigelse.

Adressebeskyttelse

Ifølge CPR-lovens § 28 har enhver ret til at få navne- og adressebeskyttelse ved henvendelse til bopælskommunen. Denne beskyttelse indebærer, at vedkommendes navn og adresse i CPR-registeret som udgangspunkt ikke må videregives til private. Videregivelse kan dog ske, hvis der er særlig hjemmel dertil, eller hvis Indenrigsministeriet giver tilladelse, jf. CPR-lovens § 34. Ligeledes kan kreditoplysningbureauer, som er godkendt af Datatilsynet, få navn og adresse oplyst fra CPR, jf. CPR-lovens § 38, stk. 4. Endvidere kan visse institutter, der er undergivet den finansielle tilsynslovgivning, jf. CPR-lovens § 42, stk. 3-5, få oplysning om civilstand og slægtskabsforhold. Endelig kan der ske videregivelse af beskyttede navne og adresser til private, der har en retlig interesse heri, hvis den pågældende på forhånd kan identificere vedkommende. Generelt gælder det, at en persons navne- og adressebeskyttelse ikke kan opretholdes over for kreditorer, der agter at foretage skridt til opkrævning eller inddrivelse af en forfalden fordring, jf. CPR-lovens § 42, stk. 5.

13.7.d. Berigtigelse

LBP § 5, stk. 4, opstiller en almindelig regel om datakvalitet, hvorefter behandling af oplysninger skal tilrettelægges således, at der foretages fornøden ajourføring og med kontrol for, at der ikke behandles urigtige eller vildledende oplysninger. Denne bestemmelse pålægger også den dataansvarlige at slette eller berigtige oplysninger, der viser sig urigtige eller vildledende, snarest muligt. I tillæg til denne almindelige forpligtelse giver LBP § 37 enhver registreret person ret til at fremsætte anmodning om berigtigelse af sletning eller blokering af oplysninger, der viser sig urigtige eller vildledende eller på lignende måde retsstridige. Hvis de pågældende oplysninger forinden er videregivet i deres fejlagtige eller retsstridige form, skal den dataansvarlige under-

rette modtageren om, at de videregivne oplysninger er berigtiget eller slettet, jf. § 37.

13.8. Tilsyn og kontrol

Tilsynet med lovens overholdelse påhviler i medfør af LBP § 55 Datatilsynet (tidligere Registertilsynet), der består af et råd og et sekretariat. Dog fører Domstolsstyrelsen tilsyn med behandling og oplysninger, der foretages fra domstolene, jf. § 67. Datatilsynet er organisatorisk placeret som en styrelse under Justitsministeriet, men skal i medfør af § 56 udøve sine funktioner i fuld uafhængighed. Ifølge § 58 påser tilsynet af egen drift eller efter klage fra en registreret, at behandling finder sted i overensstemmelse med loven og regler udstedt i medfør af loven, og efter reglerne i § 59 kan tilsynet påbyde en privat dataansvarlig at ophøre med en behandling, der ikke må finde sted efter loven samt berigtige dette eller blokere bestemte oplysninger, som er omfattet af en sådan behandling.

Foruden disse almindelige regler har tilsynet dispensationskompetence i medfør af lovens § 7, stk. 7 (følsomme oplysninger), § 10, stk. 3 (videregivelse af oplysninger fra videnskabelige og statistiske undersøgelser), § 13, stk. 1 (registrering af telefonnumre), § 27, stk. 4 og § 58, stk 2 (dataeksport). Herudover er der tillagt Datatilsynet afgørelseskompetence i medfør af reglerne om retsinformationssystemer (§ 9, stk. 3) samt om den registreredes rettigheder, jf. reglerne herom i del III (§§ 28-31, 32, stk. 1, 2 og 4 samt §§ 33-39).

Straffesager om overtrædelse af LBP rejses forholdsvis sjældent. Et eksempel herpå foreligger med *U 2004.2204 Ø*, der straffede en lokalpolitiker for fra sin arbejdsplads i et ejendomsmæglerfirma, der havde adgang til RKI Kredit Information A/S, at indhente oplysning om A og derefter videregivet denne, udelukkende til brug for sit lokalpolitiske virke, hvori også A deltog. Landsretten fandt ikke, at indsamlingen af oplysningen var sket til et sagligt formål, eller at der med behandlingen heraf var forfulgt en berettiget interesse, og idømte lokalpolitikeren en bøde på 5.000 kr.

13.9. Dataeksport

13.9.a. Problemstillingen

Det er helt almindeligt i dag, at informationssystemer kobles sammen gennem nationale og internationale datanet. En sådan sammenkobling kan foregå *bilateralt*, f.eks. inden for en virksomhed eller koncern eller overfor virksomhedens samarbejdspartnere. Men den kan også forekomme i relation til en *ubestemt flerhed* af potentielle modtagere. Det er ganske få virksomheder – om overhovedet nogen – der kan eksistere i dag uden at behandle personoplysninger, således som dette begreb anvendes i direktivet. For visse brancher er en sådan dataeksport vitalt afgørende for virksomheden. Det gælder f.eks. inden for den finansielle sektor, i forsikringserhvervet og i relation til en række liberale erhverv. Men også for talrige andre virksomheder vil der ofte opstå behov for at kunne overføre personoplysninger på tværs af landegrænser.

Behovet for at foretage en sådan dataudveksling kolliderer imidlertid med ønsket om at sikre et højt beskyttelsesniveau og undgå, at personoplysninger gøres til genstand for en ukontrolleret behandling i jurisdiktioner, der ikke har samme beskyttelsesniveau som herhjemme. Man befinder sig her i et klassisk skisma mellem på den ene side hensynet til effektivitet (som taler for at tillade dataeksport af personoplysninger) og individhensynet. På tværs af disse hensyn træder handelspolitiske hensyn ind. Vidtgående regler om databeskyttelse vil således indebære en slags tekniske handelshindringer, som reelt kan forhindre virksomheder fra tredjelande i at gøre sig gældende i konkurrencen. Netop denne betragtning var i sin tid en af hovedbegrundelserne for, at man valgte at harmonisere lovgivningen om persondatabeskyttelse.

I LBP er dette spørgsmål – i overensstemmelse med reglerne i direktivets art. 25 – reguleret i kapitel 7. Kapitlet består kun af en enkelt bestemmelse, § 27, men den er til gengæld ikke så lidt kompliceret, og det er ikke helt forkert at sige, at reglerne om dataeksport til tredjelande udgør en indgribende overbygning til den almindelige persondataregulering af stor praktisk betydning.

Ved et "tredjeland" forstås ifølge § 3, nr. 9, en stat, som ikke enten er EU-medlem eller har gennemført aftaler, der er indgået med EU, og som indeholder regler svarende til direktivets. Indtil aftaler af denne art er indgået, er man nødt til at gå frem efter direktivets almindelige regler.

13.9.b. Udgangspunktet

Som reguleringen tegner sig, er udgangspunktet klart. Der må kun overføres personoplysninger til tredjelande, hvis det pågældende land sikrer et tilstrækkeligt beskyttelsesniveau, jf. § 27, stk. 1. Med denne retlige standard lægges der op til en afvejning, der involverer "samtlige de forhold, der har indflydelse på en overførsel, herunder navnlig oplysningernes art, behandlingens formål og varighed, oprindelseslandet og det endelige bestemmelsesland, samt de retsregler, regler for god forretningsskik og sikkerhedsforanstaltninger, som gælder i tredjelandet", jf. stk. 2.

Det siger sig selv, at den dataeksportør, der under trussel om straf (jf. LBP § 70, stk. 1, nr. 1) i første række er overladt dette valg, vil være tilbageholdende med at medvirke til en sådan dataeksport. Bestemmelser, der hjemler straf for adfærd, der i en efterfølgende vurdering må antages omfattet af en retlig standard, er ikke i god harmoni med dansk strafferetlig tradition og bør generelt undgås eller i det mindste suppleres med mekanismer, der kan bibringe en form for afklaring af det essentielle skønselement, der indgår i standarden.

13.9.c. Godkendelsesordninger

I direktivet er denne form for afklaring søgt gennemført ved den procedure, der er lagt fast i art. 25. Heri foreskrives dels et system, hvorefter lande, der ikke sikrer et tilstrækkeligt beskyttelsesniveau kan *blacklistes* (stk. 3 – 4), dels et system, hvorefter lande, der på forhånd kan siges at være på det krævede niveau, *godkendes* efter den procedure, der er foreskrevet i direktivets art. 31, stk. 2 (høring af det særlige regeringsudvalg, der er nedsat ifølge art. 31, stk. 1). Befinder et land sig på en sådan liste, kan dataeksportøren uden videre betragte landets beskyttelsesniveau for "tilstrækkeligt", jf. LBP § 27, stk. 1.

Kommissionen har bl.a. truffet sådanne beslutninger i relation til Schweiz, Ungarn, Canada og Argentina. Derudover har Kommissionen i juli 2000 truffet en særlig beslutning vedrørende USA. Herom i det følgende.

13.9.d. "Safe Harbor"

I modsætning til Schweiz og Ungarn har USA ikke nogen generel lovgivning om persondatabeskyttelse, og trods langvarige forhandlinger mellem Kommissionen og Det Amerikanske Han-

delsministerium har det ikke været muligt at formå de amerikanske beslutningstagere til at udvirke en sådan lovgivning. Derfor er det vanskeligt at karakterisere USA – som tredjeland betragtet – som værende på et sådant "tilstrækkeligt" beskyttelsesniveau, at det kan anses for legitimt – uden videre – at eksportere persondata dertil.

Det kompromis, der nødvendigvis måtte opnås i en sådan situation (som ellers ville have udløst en handelskrig af uoverskuelige dimensioner), indebar et særligt kunstgreb. EU Kommissionen og U.S. Department of Commerce har opstillet et sæt såkaldte "Safe Harbor Privacy Principles", jf. bilaget til kommissionsbeslutningen af 26. juli 2000 (EFT 2000 L 215/7) og generelt <www.export.gov/safeharbor>. Man er således enig om at anse disse regler for at sikre et tilstrækkeligt beskyttelsesniveau. Det retlige grundlag herfor ligger i LBP § 27, stk. 4, der hjemler en særlig form for tilladelse fra den relevante tilsynsmyndighed til, at der overføres oplysninger til tredjelande, som ikke opfylder de krav, der er indeholdt i § 27, stk. 1. Kravet hertil er, at den dataansvarlige yder "tilstrækkelige garantier" for beskyttelse af de registreredes rettigheder. Der kan fastsættes nærmere vilkår for overførslen.

Safe Harbor-modellen fungerer således, at en virksomhed, der på forhånd tilslutter sig disse principper (ved at tegne sig på en liste, der siden 1. november 2000 har været ført af Department of Commerce), anses for at have opfyldt direktivets regler. Den pligt, virksomheden herved påtager sig, kan tænkes ført ud i livet gennem særlige mærkningsordninger, hvorved udbyderen af en hjemmeside eller et andet informationssystem på forhånd markerer, hvilke procedurer for persondatabeskyttelse man efterlever. Nærmere om disse mærkningsordninger afsnit 15.5.

Se nærmere hertil generelt *Blume*: Personoplysningsloven (2000.107 ff.) og samme: Databeskyttelsesret (2000) s. 201 ff. Se tillige *Blume* i International Journal of Law and Information Technology, nr. 8, s. 65 ff. (2000) og *Lee A. Bygrave* i 16 CLSR 252 ff. (July-August 2000). Safe Harbor-løsningen har ikke været en succes. Til dato (juni 2001) har kun et begrænset antal virksomheder tegnet sig på listen (dog enkelte store, herunder Microsoft), muligvis fordi man føler, at man dermed påtager sig forpligtelser uden egentlig at få noget til gengæld. Indtil man kender indholdet af de kontrakter, der ventes udarbejdet med henblik på dataeksport, jf. straks nedenfor, vil der således være et vist incitament til at vælge en "wait and see"-attitude.

13.9.e. Kontrakter

I direktivets art. 26, stk. 2, siges det udtrykkeligt, at de garantier, der kræves for at kunne eksportere data til tredjelande, "især" kan fremgå af "passende kontraktsbestemmelser." Ifølge direktivets art. 26, stk. 4, kan sådanne vilkår godkendes af Kommissionen efter høring af det særlige udvalg om persondatabeskyttelse, der er nedsat i henhold til art. 31, stk. 1. Ifølge den nævnte bestemmelse indebærer godkendelsen, at de pågældende medlemsstater skal træffe "de foranstaltninger, der er nødvendige for at efterkomme Kommissionens afgørelse", dvs. undlade at omgøre den pågældende godkendelse.

Kommissionen har truffet to beslutninger i medfør af denne bestemmelse.

Den 15. juni 2001 (EFT 2001 L 181/19) har man vedtaget, at bestemmelserne i en til beslutningen bilagt standardkontrakt anses for at "frembyde de tilstrækkelige garantier for beskyttelse af privatlivets fred, personers grundlæggende rettigheder og frihedsrettigheder", jf. artikel 26, stk. 2, i persondatadirektivet (95/46/EF). Beslutningen finder anvendelse fra den 3. september 2001. Bilaget hertil angiver et sæt "Standardkontraktbestemmelser" (nummereret fra 1 til 10), der hver for sig indeholder henholdsvis definitioner, en specifikation vedrørende den af kontrakten omfattede overførelse, visse standardbestemmelsers virkning over for tredjeparter, dataeksportørens pligter, dataimportørens pligter, ansvar, mægling/værneting, samarbejde med tilsynsmyndigheder, ophør og lovvalg. De centrale bestemmelser 4-6 (om henholdsvis dataeksportørens og dataimportørens pligter samt om ansvar) korresponderer med grundbestemmelserne i 1995-direktivet. Standardkontraktbestemmelserne er omtalt af *Peter Blume* i U 2001B.375 ff.

Derudover har Kommissionen den 27. december 2004 (EUT 2004 L 385/74) godkendt et alternativt sæt standardvilkår (dvs. en ny standardkontrakt), der udarbejdet af en række organisationer inden for den internationale handel. Denne kontrakt rummer en højere grad af fleksibilitet end de først godkendte og forventes derfor bedre at kunne opfylde erhvervslivets praktiske behov. Kontrakten er omtalt af *Peter Blume* i U 2005B.145 ff.

13.9.f. Tilbagefaldsreguleringen

Finder ingen af de ovenfor anførte regler anvendelse, må dataeksportøren gå frem efter reglerne i LBP § 27, stk. 3, der i hovedsagen

inkorporerer de krav, der stilles til nye behandlinger: Specifikt samtykke (nr. 1), aftaleopfyldelse (nr. 2), tilfælde, hvor den registrerede selv har interesse i dataeksporten (nr. 3), samfundsmæssig nødvendighed (nr. 4) og vitale interesser (nr. 5). Hertil føjes en række særlige undtagelsestilfælde, der knytter an til offentligretlig, efterforskningsmæssig eller efterretningsmæssig opgavevaretagelse (nr. 6-8).

Supplerende litteratur

Efter gennemførelsen af den nye lov om persondatabeskyttelse er der fremkommet flere fremstillinger af dette nye regime, således *Kristian Korfits Nielsen & Henrik Waaben*: Lov om behandling af personoplysninger (2001) og *Peter Blumes* lovkommentar Personoplysningsloven (2000) og den mere retspolitisk orienterede Databeskyttelsesret (2000).

Et andet vigtigt fortolkningsbidrag foreligger med de vejledninger, der er udarbejdet af Datatilsynet og som er tilgængelige fra tilsynets hjemmeside, <www.datatilsynet.dk>, samt de udtalelser fra Artikel 29-Gruppen, der også er at finde her. Ligeledes indeholder årsberetningerne fra Datatilsynet (tidligere Registertilsynet) talrige fortolkningsbidrag samt løbende omtale af praksis fra denne centrale myndighed.

Foruden den omtale af *Safe Harbor*-reguleringen, der findes på <www.export.gov/safeharbor> henvises til det materiale, der er tilgængeligt fra Federal Trade Commissions hjemmeside <www.ftc.gov/privacy/safeharbor/shp.htm>. Se ligeledes *Gillian Bull* i 17 CLSR 239 ff. (July/August 2001).

Kapitel 14. ARBEJDSPLADSSPØRGSMÅL

14.1. Ansættelsesregulering

14.1.a. Ansættelsesgrundlaget

Funktionærloven

Der findes ikke nogen klart afgrænselig "IT-ansættelse". IT-medarbejdere, der er beskæftiget med administrativ IT-anvendelse, vil ofte være omfattet af funktionærloven (FUL). Afgørende for de retlige rammer er den pågældendes arbejdsfunktion. Iflg. § 1, stk. 1, litra a), omfatter FUL "Handels- og kontormedhjælpere, beskæftiget ved køb eller salg, ved kontorarbejde eller dermed ligestillet lagerekspedition" – funktioner, der som sagt stort set alle understøttes med IT. Lovens § 1, stk. 1, litra b), omfatter herudover "personer, hvis arbejde består i teknisk eller klinisk bistandsydelse af ikke-håndværks- eller -fabriksmæssig art, og andre medhjælpere, som udfører et arbejde, der kan sidestilles hermed". At *skrive programmer* vil som regel falde ind under FUL. Spørgsmålet har så vidt vides ikke været pådømt ved domstolene, men den almindelige antagelse er, at programmører er funktionærer. I *U 1976.802 SH* ansås en elektrotekniker – under egenartede omstændigheder – som funktionær.

Blandede forhold

Er ansættelsesforholdet blandet, således at den ansatte ikke udelukkende udfører det pågældende arbejde, beror det på FUL § 1, stk. 1, litra d), om der består et funktionærforhold. Efter denne bestemmelse er dette tilfældet, hvis den pågældendes arbejde "overvejende" er af den under a) og b) angivne art. Efter litra a) og b) er det afgørende for lovens anvendelse, om de pågældende personkategorier selv udfører det nævnte arbejde. For personer, "hvis arbejde udelukkende eller i det væsentligste består i på arbejdsgiverens vegne at lede eller føre tilsyn med udførelsen af andres arbejde", gælder arbejdsleder-reglen i lovens § 1, stk. 1, litra c). Reglen har dog næppe stor praktisk betydning på IT-området, da det arbejde, der udøves af den, der *planlægger* en IT-udvikling eller IT-drift, typisk vil være kontorarbejde i lovens terminologi.

Foruden de anførte materielle kriterier må visse formelle betingelser være opfyldte, for at en person omfattes af FUL, se

nærmere § 1, stk. 2. Funktionæren skal være beskæftiget mere end *8 timer* ugentlig hos arbejdgiveren og skal befinde sig i et *tjenesteforhold*, altså være underlagt en pligt til at efterkomme tjenestebefalinger. Det sidstnævnte krav er centralt her som andetsteds i ansættelsesretten. Arbejdsgiveren må være beføjet til at instruere den ansatte om, hvorledes hvervet skal udføres. Beror det på den ansatte selv eller på en eventuel tredjepart, om arbejdet skal udføres og hvordan dette i givet fald skal ske, er der ikke tale om et tjenesteforhold.

Dermed er funktionærens opdrag anderledes end f.eks. konsulentens. En ekstern konsulent er ikke funktionær, uanset om han i længere perioder virker og arbejder mere end 8 timer ugentlig i kundens virksomhed. Han er sin egen herre, og denne personlige uafhængighed er ligefrem en del af grundlaget for hans ydelse. Selv i det tilfælde, hvor kunden "køber" en medarbejder af en leverandør til at udføre et på forhånd fastlagt arbejde "hos" kunden (såkaldt "body-shopping"), eller hvis medarbejderen som led i en facility management-aftale er fast stationeret i opdragsgiverens virksomhed, vil den pågældende under alle omstændigheder skulle modtage sine instruktioner af sin umiddelbare arbejdsgiver.

At Højesteret i *U 2000.2226 H* fastslog, at en edb-konsulent i skattemæssig henseende skulle betragtes som ansat konsulent, hang bl.a. sammen med, at konsulenten havde været lønnet med A-skattetræk. Der forelå i øvrigt en kontrakt, hvorefter konsulenten var indplaceret i lønsystemet for den pågældende arbejdsgiver (en kommune). Se tilsvarende *U 2005.1376 V*, der antog, at en familieplejer, der ikke var undergivet instruktionsbeføjelse, ikke var omfattet af FUL.

Overenskomstforhold

Pga. vanskelighederne ved at afgrænse "IT-faget" findes der ingen standardaftaler for IT-ansættelser. Der tegner sig heller ikke noget enkelt dansk forbund, der over en bred kam organiserer "IT-lønmodtagere", og man kan i det hele taget diskutere, om der eksisterer noget "IT-fag" ved siden af de fag, der i øvrigt præges af edb-teknologien (f.eks. kontorfaget, forskellige ingeniørfag etc.).

- PROSA

PROSA er den faglige organisation, der klarest og mest eksklusivt har orienteret sig mod *IT-ansættelser*, nærmere bestemt mod ansættelsen som programmør, operatør eller lignende ansættelser, uanset uddannelsesmæssig baggrund. PROSA betegner sig som "Forbundet af IT-ansatte" og har i denne egenskab indgået forskellige overenskomster for edb-medarbejdere i statens tjeneste.

På *kontorområdet* har HK (Handels- og Kontorfunktionærernes forbund) etableret den tværgående landsforening Sam-Data. Sam-Data organiserer programmører, operatører, dataloger mv. Medlemskab af Sam-Data forudsætter medlemskab af HK. Der foreligger bl.a. en række aftaler med HK for edb-medarbejdere i statens tjeneste, se f.eks. cirkulære af 12. marts 1998 om organisationsaftale for edb-medarbejdere (HK) i statens tjeneste. - Sam-Data

14.1.b. Distancearbejde

Den stigende anvendelse af telekommunikation har skabt nye muligheder for, at IT-medarbejdere – være sig ansatte eller selvstændige – udelukkende eller for en væsentlig del af sin tid udfører arbejde på et sted, der ikke har karakter af en traditionel arbejdsplads for sin arbejdsgiver eller klient. Når brugen af telekommunikation og avanceret IT indgår som en væsentlig del af arbejdets udførelse, taler man om *distancearbejde* eller *telearbejde*. Brugen af sådanne arbejdspladser giver anledning til en række praktiske problemer, hvoraf nogle giver anledning til retlige problemer.

Det er ikke nødvendigvis uproblematisk at indføre distancearbejde i en virksomhed. For arbejdsgiveren indebærer distancearbejdet en risiko for at miste *kontrollen* med den enkelte medarbejder: Det er vanskeligt at konstatere, om der rent faktisk arbejdes, når medarbejderen ikke befinder sig inden for virksomhedens fire vægge. Hvem dette er "værst for" beror på, om der på det pågældende fagområde er tradition for at arbejde i overkanten eller i underkanten af det pligtmæssige. Derfor kan man argumentere for, at sådanne ordninger primært egner sig for arbejde, der har præg af resultatforpligtelser snarere end arbejde, der betragtes som indsatsforpligtelser. Et andet problem er de praktiske vanskeligheder ved at foretage personaleudskiftninger mv., f.eks. under længerevarende sygdom mv.: Har en medarbejder som led i en permanent indrettet hjemmearbejdsplads fået en del af virksomhedens dokumentation flyttet hjem til sig (f.eks. et bogholderi), må dette materiale dels flyttes tilbage, dels må der være et kontor klar til den vikar, der skal træde ind i stedet. Fordele og ulemper

Arbejdsgiverens fordele ved distancearbejde ligger omvendt i muligheden for at få mere tilfredse medarbejdere, der foruden sparet transport f.eks. kan kombinere et intensivt arbejdsliv med familielivet. Hertil kommer en række afledte fordele, f.eks. mindre behov for kontorareal, mindre tidkrævende "hyggesnak" på arbejdspladsen mv. For arbejdstageren består fordelen – foruden

de førnævnte – i muligheden for større frihed i tilrettelæggelsen af arbejdet, færre forstyrrelser, mulighed for at fordybe sig i særlige opgaver samt muligheden for at tilbringe et mere sammenhængende liv i en vekselvirkning mellem arbejde og frihed. Hidtil har arbejdstagerorganisationerne dog vist modvilje mod distancearbejde. Udover de specifikke problemer, distancearbejdet rejser i relation til f.eks. regler om arbejdsmiljø, frygter man, at det vil nedbryde den faglige solidaritet mv.

Grundlæggende for de former for distancearbejde, der almindeligvis diskuteres, er anvendelsen af informationsteknologi samt den heraf følgende nedbrydning af dimensionerne tid og sted (medarbejderne kan udføre deres arbejde ved at koble deres pc-udstyr op til arbejdspladsens system, hvor som helst og på et hvilket som helst tidspunkt). Den heraf følgende fleksibilitet indebærer ligeledes en udvidelse af det relevante arbejdsmarked. Herudover sker der en række interne ændringer i de organisationer, der gør brug af distancearbejde: Der er en tendens til opbygning af mindre enheder, fladere hierarkiske strukturer samt en højere grad af delegation og horisontal kommunikation, og i konsekvens heraf nedbrydes tidligere organisatoriske grænsedragninger. Ledelsens fokus flyttes til i højere grad at orientere sig efter strategiske spørgsmål, og den gennemførte delegation indebærer, at arbejdet i højere grad beror på tillid end på kontrol. Se hertil Kommissionens Status Report on European Tele Work fra henholdsvis august 1998 og august 1999.

Retlige problemer

På enkelte arbejdspladser – offentlige såvel som private – findes der forsøgsvise aftaler om "hjemmearbejde", som man anvender til at indsamle erfaringsgrundlag for, hvorledes denne arbejdsform skal udfolde sig. For en medarbejder, der i forvejen er ansat i henhold til funktionærlovens regler, vil hjemmearbejdsformen ikke gøre nogen forandringer heri. Derimod er der uenighed mellem arbejdsmarkedets parter om anvendelsen af andre af ansættelsesforholdets regler i relation til hjemmearbejdet, herunder netop arbejdsmiljøreglerne. Særlige regler herom er nu fastsat i bekendtgørelse nr. 247 af 2. april 2003 om begrænsninger i anvendelsen af lov om arbejdsmiljø på arbejde, som udføres fra den ansattes hjem.

"Distancearbejdere", der arbejder for flere arbejdsgivere, hver med et timetal på under funktionærlovens mindstegrænse på 8 timer ugentlig, vil ikke være omfattet af funktionærloven, jf. lovens § 1, stk. 2. Hvis ikke anden aftale eller forudsætning foreligger, kan sådanne medarbejdere ikke gøre krav på beskyttelse efter lovens regler.

Forsikring

Hjemmearbejdspladser bør i almindelighed forsikres efter samme principper som de, der gælder for erhvervsmæssige ar-

bejdspladser. Om disse forsikringsmæssige problemer, se Arbejdsskadestyrelsens notat af 3. september 1996, optrykt i rapporten "En arbejdsplads i Danmark" (juni 1997), bilagshæftet s. 31 ff., bilag A1.

Sikkerhed

Er en arbejdsplads underlagt offentligretligt baserede sikkerhedsforsikringer, vil disse regler som udgangspunkt også gælde for de hjemmearbejdspladser, der etableres i tilknytning til hjemmearbejdspladsen, se hertil § 7, stk. 2, i bekendtgørelse nr. 528 af 15. juni 2000 som ændret ved bekendtgørelse nr. 201 af 22. marts 2001. I den forbindelse bør der træffes afgørelse om en række sikkerhedsmæssige forhold, herunder om der skal kunne ske lokal lagring og udskrivning af oplysninger på hjemmearbejdspladsen, om denne skal kunne anvendes til andre formål end de rent driftsmæssige, og om hjemmet skal underkastes samme form for fysisk sikkerhed som hovedarbejdspladsen.

Den aftaleretlige regulering af ansættelsesaftaler, der indebærer distancearbejde, er behandlet af *Nicolai Dragsted* i Aggergren m.fl. (2000), s. 104 ff. *Finanssektorens Arbejdsgiverforening* har i 1996 udsendt en pjece med titlen "Distancearbejde – en mulighed for den finansielle sektor". Emnet er genstand for temanummeret af tidsskriftet LOKE, nr. 1, 1. januar 1997. Finansministeriet har i 1998 udsendt en vejledning om distancearbejde i staten. Vejledningen, der er udarbejdet i samarbejde med Centralorganisationernes Fælles Udvalg (CFU), baserer sig på den rammeaftale om distancearbejde, som disse to parter har indgået i forbindelse med aftale- og overenskomstforhandlingerne i 1997 (gældende for tjenestemænd og tjenestemandslignende ansatte, dog ikke undervisere). Dens første del indeholder en egentlig vejledning om distancearbejde (hvilke opgaver der med fordel løses via distancearbejde, hvorledes bevares den sociale og faglige kontakt, og hvilke løn- og ansættelsesvilkår bør være gældende). Anden del gennemgår en række lovgivningsområder, der har betydning for distancearbejde (herunder skatteregler, forsikrings- og erstatningsregler, arbejdsmiljøregler, kontrolregler og registerregler). Det påpeges, at en række regler ikke tager højde for de særlige problemstillinger, som distancearbejde giver anledning til, og parterne i de lokalaftaler, der skal danne grundlag for distancearbejds-løsninger, opfordres derfor til at afklare disse spørgsmål i lokalaftalerne.

14.1.c. Særlige misligholdelsesspørgsmål

Fordi IT-anvendelse rummer andre farer og risici end maskiner og tekniske anlæg mv., kan det komme på tale at knytte sanktioner til handlinger, som kan forekomme harmløse.

Diskretionspligt

Dette gælder for det første medarbejderens omgang med erhvervshemmeligheder. Som anden information "stjæles" en er-

hvervshemmelighed ved, at den – i kommunikationsteoriens terminologi – genskabes. Hvor den bestjålne næsten altid vil opdage tyveri af ting, ved den forurettede ikke nødvendigvis, at han har "mistet" data, da de jo fortsat befinder sig i hans system. Retsbruddet kan derfor effektueres uden at blive opdaget og både før og efter samarbejdsforholdets ophør. Mfl. § 10 forbyder industrispionage og brud på erhvervshemmeligheder. Vil arbejdsgiveren sikre sig yderligere, kan han præcisere dette forbud ved aftale, jf. nærmere *ET* s. 397 ff.

Konkurrenceklausuler mv.

Arbejdsgiveren kan pålægge den ansatte en konkurrenceklausul, dvs. en aftale, der pålægger den ansatte ikke at tage ansættelse hos potentielt konkurrencetruende arbejdsgivere. For personer i funktionærforhold er muligheden for at påtage sig konkurrencebegrænsende aftaler begrænset af FUL § 18 (om konkurrenceklausuler) og § 18a (om kundeklausuler). Herudover kan konkurrencebegrænsende aftaler efter omstændighederne anfægtes efter aftl. § 36 (generalklausulen) og § 38c. Sidstnævnte bestemmelse fastslår, at en vedtagelse, hvorefter nogen forpligter sig til af konkurrencehensyn ikke at drive forretning eller anden virksomhed af en vis art eller til ikke at tage ansættelse i en sådan virksomhed, ikke er bindende, "for så vidt forpligtelsen med hensyn til tid, sted, eller andre forhold går videre end påkrævet for at værne imod konkurrence eller på urimelig måde indskrænker den forpligtedes adgang til erhverv". I sidstnævnte henseende skal der efter bestemmelsen også tages hensyn til den interesse, den berettigede har i, at vedtagelsen efterkommes. Se om problemstillingen *Mogens Munch* i U1981B.45 ff.

Medvirken til retsbrud

Et særligt problem – som ofte er rejst af de organisationer, der organiserer IT-medarbejdere – er, om en IT-ansat har pligt til at gøre noget, der efter hans egen vurdering indebærer et retsbrud. Fordi mange IT-handlinger er "usynlige" eller i hvert fald lette at skjule, vil det ofte være vanskeligt at kontrollere retsbrud. Denne følelse af, at retsbruddet ikke bliver opdaget, kan erfaringsmæssigt fjerne en del af den tilskyndelse, de fleste har til at overholde loven, specielt hvis loven forekommer ubegrundet, formel eller ligefrem urimelig. Det er f.eks. næppe urealistisk at tro, at lovgivningen om persondatabeskyttelse hyppigt overtrædes i såvel offentligt som privat regi, og at immaterielle rettigheder lige så hyppigt krænkes i form af uautoriseret programkopiering mv. af personer, som ellers ikke vil føle sig som retsbrydere.

Dette forhold får en særlig ansættelsesretlig dimension, hvis arbejdsgiveren direkte eller indirekte kræver af den ansatte, at han medvirker til retsbrud. I det psykologiske spil vil den ansattes

nægtelse ofte – med rette eller urette – blive opfattet som en besværlig obstruktion baseret på regelformalisme. Hvis retsbruddet i den pågældende organisation betragtes som en bagatel, vil den ansatte komme under pres mellem de ansættelsesretlige pligter på den ene side og på den anden side den almindelige eller specielle strafferet.

Problemet må som udgangspunkt løses på grundlag af strafferettens medvirkenslære i kombination med den almindelige kontraktsgrundsætning, hvorefter man ikke har pligt til at opfylde aftaler på en måde, der strider imod lov og ærbarhed, sml. herved DL 5-1-1.

For personer i offentlig tjeneste eller hverv straffer strfl. § 156 den, der nægter eller undlader at opfylde pligt, som tjenesten eller hvervet medfører, eller nægter "at efterkomme *lovlig* tjenstlig befaling". Heraf følger modsætningsvis, at den tjenestemand, der modtager en klart ulovlig instruktion (ordre) af sin overordnede, ikke har pligt til at efterleve denne. Der er ingen nyere trykt retspraksis om denne bestemmelse, hvis princip ligeledes finder anvendelse på afgrænsningen af ledelsesretten i private ansættelsesforhold. I den ansættelsesretlige teori antages det, at der tilkommer arbejdsgiveren et "fortolkningsfortrin" ved afgørelsen af, om en tjenestebefaling er ulovlig og dermed ikke egnet til at pålægge medarbejderen pligter. Dette fortrin må formentlig forstås således, at medarbejderen kun kan gøre en indsigelse om ulovlighed gældende, hvis det er *åbenbart*, at tjenestebefalingen er retsstridig i forhold til medarbejderen, og at denne kan risikere et selvstændigt erstatnings- eller strafansvar for medvirken ved at udføre handlingen. Se hertil *Lars Svenning Andersen:* Funktionærret, 3. udg. (2004), s. 212 og *Hasselbalch*: Ansættelsesretten, 2. udg. (1997), s. 662 f.

Det krav om "klarhed", der opstilles i strfl. § 156, genfindes ikke i ansættelsesretten, hvor kriteriet vil være, om den ansattes vægring mod arbejdsgiverens pålæg implicerer en "væsentlig" misligholdelse, sml. FUL § 4. Er det tvivlsomt, om pålægget er ulovligt, må den ansatte tage en standpunktsrisiko. Den endelige afgørelse af misligholdelsesspørgsmålet vil bero på dommen i den efterfølgende sag.

Pålæg om at udføre arbejde, der efter den ansattes personlige vurdering har *uetisk* karakter, kan som udgangspunkt ikke af denne grund danne grundlag for vægring. Udgangspunktet er her, at medarbejderen har pligt til at også at efterkomme tjenestebefalinger, han måtte anse for uetiske, hvis blot han ikke hermed kommer til at medvirke til et strafbart forhold. Efter omstændig-

hederne kan dette udgangspunkt modificeres, hvis det ligger klart for arbejdsgiveren, at medarbejderen (f.eks. pga. sin kendte religiøse overbevisning) må formodes at have anfægtelser ved at skulle udføre et bestemt arbejde. Som regel vil sådanne forhold dog blive klarlagt allerede ved indgåelsen af ansættelsesaftalen. Undlader medarbejderen her at rejse spørgsmålet, kan han ikke senere gøre sine etiske betænkeligheder gældende i form af arbejdsvægring. Problemet kan f.eks. tænkes at opstå ved ansættelse i virksomheder, der leverer IT-komponenter til brug i krigsmateriel, jf. lov nr. 400 af 13. juni 1990 om krigsmateriel mv. med senere ændringer.

Et helt andet spørgsmål er det, om den ansatte, der kontraktsmæssigt vælger at fratræde sin stilling som følge af modvilje mod den slags produktion, i konsekvens heraf mister retten til arbejdsløshedsunderstøttelse eller sociale ydelser. Samtidig med vedtagelsen af 1990-loven om krigsmateriel mv. er loven om arbejdsformidling og arbejdsløshedsforsikring mv. ændret således, at den slags vægring anses for fyldestgørende grund til at undlade at overtage arbejde eller ophøre med arbejde, se nærmere § 20 i bekendtgørelse nr. 514 af 17. juni 2003 om selvforskyldt ledighed.

Sikkerhedsregler

Frygten for angreb af programvirus og erkendelsen af, at risikoen for sådanne angreb stiger markant ved anvendelse af ikke-autoriseret programmel, har ført mange edb-følsomme virksomheder til at indskærpe, at anvendelse af programmel, der ikke er autoriseret af virksomheden (f.eks. medarbejderens egne, lovligt indkøbte programmer, eller programfiler mv. hentet fra Internet-sites), vil implicere en væsentlig misligholdelse, der kvalificerer som bortvisningsgrund.

Foreligger en sådan indskærpelse – der har saglige grunde – vil overtrædelse af forbuddet indebære en væsentlig misligholdelse. Forbuddet kan enten betragtes som en betoning af de særlige forudsætninger, der må varetages i den pågældende virksomhed, eller som en konsekvens af arbejdsgiverens ret til at lede og fordele arbejdet. Sådanne forskrifter vil typisk være lige så saglige som forskrifter på kemiske virksomheder om omgangen med eksplosivt materiale. Således antog *U 2003.1609 V*, at en systemadministrator, der havde udleveret sit kodeord og indkodet dette i sin hustrus pc, med rette var bortvist. Arbejdsgiveren havde forbudt medarbejderne at lade computeren "huske kodeordet", og der var ikke adgang til at benytte Internet til privat brug. Det blev lagt til grund, at disse bestemmelser var af væsentlig sikkerhedsmæssig betydning for virksomheden, og at medarbejderen i kraft af sin stilling som sikkerhedsadministrator var bekendt med, at den nævnte indtastning af kodeordet gav hustruen adgang til at

opnå internet-forbindelse via virksomhedens systemer. Bortvisningen fandtes derfor berettiget.

Resultatet blev et andet ved dommen i *U 2003.1430 Ø*. I denne sag havde en regnskabsassistent i sin arbejdstid ført en omfattende privat e-mail-korrespondance med bl.a. sex-relateret indhold. Som begrundelse for sin frifindelse af regnskabsassistenten fremhæver landsretten, at virksomheden ikke havde formuleret en politik vedrørende de ansattes brug af virksomhedens Internet-forbindelse. Landsretten lægger til grund, at regnskabsassistentens kommunikation på en række sex-relaterede chatsider ikke eksponerede virksomhedens domæne (og dermed dens identitet). En korrespondance med to personer fandtes sket under forhold, hvor medarbejderen havde grund til at forvente, at der ikke ville ske videresendelse. Selv om det måtte lægges til grund, at 50-70% af de e-mails, medarbejderen havde sendt via sin e-mail-adresse i virksomheden, var private, fandt landsretten ikke, at dette udgjorde grundlag for bortvisning, idet medarbejderens indsats i øvrigt ikke havde givet anledning til kritik. Se også den norske højesteretsdom i *Rt. 2001.1589*, hvor det fandtes bevist, at en medarbejder havde downloadet et stort antal musikfiler fra nettet, hvilket havde ført til driftsvanskeligheder for arbejdsgiveren. Medarbejderen var derfor ikke opsagt usagligt. Senest kan henvises til den norske højesteretsdom i *Rt. 2005.___* (22.4.05), der ikke ville godkende en opsigelse af to medarbejdere på en olieboreplatform for uberettiget download af pornografisk materiale. Medarbejderne havde vel udført et langvarigt og systematisk misbrug, men arbejdsgiveren havde ikke fulgt op på sagen, da misbruget var blevet opdaget.

14.1.d. Arbejdspladsovervågning

Et særligt spørgsmål i forbindelse med arbejdsgiverens sikkerhedsforanstaltninger angår muligheden for at *overvåge* den ansattes aktiviteter. Inden for andre dele af arbejdsmarkedet er arbejdsgiverens muligheder for at iværksætte kontrol eller overvågning begrænset. I skærende kontrast hertil står den mulighed, de fleste IT-systemer rummer for at registrere, hvornår og hvor længe den ansatte er koblet op på systemet. På de lidt større installationer vil den systemansvarlige medarbejder – som ofte er placeret tæt på management – almindeligvis kunne se, hvilke indtastninger medarbejderen foretager. Herudover kan det være et led i visse *sikkerhedsforanstaltninger*, at den enkelte medarbejders brug af en terminal "logges", dvs. registreres med henblik på, at hans færden senere kan rekonstrueres. Der opstår her en modsætning mellem på den ene side hensynet til medarbejderens interesser og på den anden side de kontrol- eller sikkerhedsmæssige hensyn, der ligger til grund for sådanne krav.

Spørgsmålet om ansattes ret til at modsætte sig sådanne former for overvågning er ikke reguleret i lovgivningen og vistnok heller ikke i nogen overenskomster. Derimod findes der en sporadisk regulering af enkelte former for ansættelsesovervågning rundt omkring i lovgivningen.

Telefonregistrering

Ifølge LBP § 13 må offentlige myndigheder og private virksomheder ikke foretage automatisk registrering af, hvilke telefonnumre der er foretaget opkald til fra deres telefoner. Registrering må dog ske efter forudgående tilladelse fra tilsynsmyndigheden (Datatilsynet eller Domstolsstyrelsen) i tilfælde, hvor afgørende hensyn til private eller offentlige interesser taler herfor. Der kan i den forbindelse fastsættes nærmere vilkår for registrering. Der er derimod ikke forbud mod at foretage registrering af de opkald, der tilgår en myndighed eller virksomhed (registrering, der i dag er mulig gennem såkaldt A-nummer-visning). Ej heller er der forbud mod at registrere medarbejderes brug af andre kommunikationsværktøjer, f.eks. til elektronisk post eller web-browsing. Forbuddet mod registrering af telefonnumre gælder kun telefonnummeret som sådant. Ifølge hidtidig praksis fra Registertilsynet (som må formodes videreført af Datatilsynet efter vedtagelsen af LBP) anses et opkaldsnummer, i hvilket der er sket udblænding af de sidste 2 cifre i et 8-cifret nummer, således ikke for at være et "telefonnummer", jf. betænkning 1345/1997, s. 102. Det er heller ikke forbudt at stille krav om manuel registrering af telefonopkald.

Ifølge LBP § 13, stk. 2, gælder forbuddet mod registrering af telefonnumre ikke, for så vidt andet følger af lov, eller for så vidt angår udbydere af telenet og teletjenesters registrering af, til hvilket telefonnummer der er foretaget opkald, hvad enten denne registrering sker til selskabernes eget brug eller til brug ved teknisk kontrol.

Om en registrering – og behandling – af medarbejderens anvendelse af centrale edb-systemer (f.eks. i form af logning af oplysninger om, hvilke e-mailadresser og hjemmesider der er kommunikeret med) er lovlig i medfør af LBP, beror herefter på, om de almindelige krav i denne lov er opfyldte. I det omfang registreringen har til formål at understøtte virksomhedens forpligtelse til f.eks. at kunne dokumentere retskrav mv., vil der være hjemmel hertil i LBP § 6, stk. 1, nr. 3. Hvorvidt videregående overvågningstiltag indebærer en sådan krænkelse af medarbejderens ære og værdighed, at der foreligger en misligholdelse, vil bero på en konkret vurdering.

Specifikke regler af dette indhold findes i visse fremmede retssystemers ansættelsesretlige lovgivning. Den norske arbejdsmiljølovs § 12, nr. 3, pålægger f.eks. arbejdsgiveren at holde medarbejdere orienteret om "styrings- og planleggingssystemer", hvilket sædvanligvis forstås som alle tekniske systemer, som kan udnyttes til at styre og kontrollere medarbejderne, jf. *Anne Kirsti Brække*: Fjernovervåking og informasjonstjenester i telenettet (Complex 8/91, s. 161). Lignende regler følger af de samarbejds- og teknologiaftaler, der indgås på det danske arbejdsmarked. Se i øvrigt om spørgsmålet, *Peter Blume* i U1999B.194 ff. og i J2001.144 ff. (med generelle retspolitiske synspunkter om tv-overvågning) og *Peter Blume & Jens Kristiansen*: Databeskyttelse på arbejdsmarkedet (2002).

Terminalovervågning

En egentlig lovregulering af spørgsmålet i dansk ret findes i bekendtgørelse om arbejdet ved skærmterminaler (nr. 1108 af 15. december 1992), der er udstedt i medfør af arbejdsmiljøloven til opfyldelse af det såkaldte skærmdirektiv (direktiv 1990/270). Bekendtgørelsens § 5 fastslår en pligt til at indrette skærmarbejdspladser i overensstemmelse med bilaget til bekendtgørelsen, og i dettes pkt. 3, litra b), findes et forbud mod at anvende kvantitativ eller kvalitativ kontrol uden de ansattes vidende. Bestemmelsen hviler dermed på samme *subjektive vurderingsprincip* som det, der er bærende for forståelsen af strfl. § 263 om uberettiget overvågning mv., jf. i det hele afsnit 17.4.

Begrebet "grafisk skærm" i direktivets art. 2, litra a), jf. tilsvarende bekendtgørelsens § 1, stk. 2, nr. 1), skal ikke forstås som begrænset til IT-arbejdspladser. Også et klippebord beregnet til redigering af film falder inden for begrebet, jf. EF-domstolens præjudicielle udtalelse af 6. juli 2000 i sagen C-11/99.

De strafferetlige spørgsmål om arbejdsgiverens ret til at overvåge medarbejderes Internet-kommunikation behandles i afsnit 17.4.b., hvortil i det hele henvises. Men arbejdsgiverens frihed hertil, der må antages at være afgrænset på samme måde strafferetligt og ansættelsesretligt, kan undertiden få ansættelsesretlige konsekvenser. Et eksempel herpå er dommen i *U 2005.1639 V*. Her fandtes en medarbejders e-mail, hvori virksomhedens økonomichef blev omtalt som "noget af en sæk", at være sendt som led i en privat korrespondance (selv om det var kendt at alle kunne læse hinandens e-mails), som medarbejderen ikke kunne regne med ville blive læst af andre. Derfor og på grund af den trods alt mindre grove karakter af udtalelsen gav udtalelsen ikke grundlag for en opsigelse.

Se ligeledes den illustrative og dramatiske byretsdom af 30. april 1992 fra *Asker og Bærum herredsret*. Edb-chefen i en virksomhed følte sig overvåget af virksomhedens direktør. For at konstatere,

om hans mistanke var korrekt, udarbejdede han en post-meddelelse til virksomhedens moderselskab, som var stærkt kritisk overfor direktøren. Han placerede nu denne meddelelse på sin computer, så det så ud som om den var sendt. Mistanken om direktørens aflytning viste sig berettiget, og direktøren blamerede sig nu overfor moderselskabet ved straks at tage kontakt til dette for at dementere oplysningerne i den elektroniske meddelelse. Da sagens rette sammenhæng gik op for direktøren, blev medarbejderen bortvist, og den efterfølgende sag drejede sig nu om, hvorvidt denne bortvisning var berettiget. I sin afgørelse herom udtaler retten bl.a., at "... det å gå inn på ansattes private fil på dataanlegget, uten at den ansatte på forhånd blir gjort oppmerksom på det i form av instruks, ved alminnelig kjent praksis eller ved innhenting av samtykke, må regnes som en krenkelse av de krav på beskyttelse av privat informasjon som arbeidstaker må ha overfor arbeidsgiver." Dommen er trykt i tidsskriftet Lov&Data, nr. 32, oktober 1992. At arbejdsgiveren går videre end berettiget i sin overvågning af medarbejdere berettiger normalt ikke til tortgodtgørelse, jf. *U 2005.1131 Ø*.

Forskrifter mv.

Navnlig på grund af de forskelligheder, der gør sig gældende i forskellige arbejdsforhold, kan der herske stor uklarhed om, hvilken overvågning en arbejdsgiver har ret til at foretage over medarbejderes arbejdspladser. For at afklare denne usikkerhed er det blevet stadigt mere almindeligt, at der på arbejdspladsen findes en forskrift, som angiver den privatlivsbeskyttelse, medarbejderne kan påregne. Spørgsmålet behandles i IT-sikkerhedsrådets "inspirationspapir" fra 2003 om Brug af e-post og Internet på arbejdspladsen, tilgængelig fra <www.rfits.dk>.

Videoovervågning

Til retsstillingen vedrørende overvågning af arbejdspladser hører også lov om forbud mod privat tv-overvågning mv., jf. lovbekendtgørelse nr. 76 af 1. februar 2000. Ifølge denne lovs § 1 må private ikke foretage tv-overvågning af gade, vej, plads eller lignende område, som benyttes til almindelig færdsel. Videoovervågning, der ikke er forbundet med optagelse, må dog ske i forbindelse med overvågning af egne indgange, facader, indhegning eller lignende. Private, der foretager tv-overvågning af steder og lokaler, hvortil der er almindelig adgang, eller af arbejdspladser, skal ved skiltning eller på anden tydelig måde give oplysning herom, jf. § 3, stk. 1. Det samme gælder offentlige myndigheder, der foretager tv-overvågning af steder og lokaler, hvortil der er almindelig adgang, *eller af arbejdspladser*, jf. § 3a.

14.2. IT-indførelse

Problemet

En succesfuld implementering af IT forudsætter nøje koordinering mellem system og brugerkreds. Om IT-indførelse viser sig

effektiv, beror i høj grad på den accept, hvormed den nye teknologi bliver modtaget af brugerne. Systemerne vil i visse tilfælde overflødiggøre eksisterende jobs og dermed skabe ængstelse hos truede personalegrupper. Dernæst kan IT-indførelse rejse behov for omskoling eller efteruddannelse, hvilket igen kan føre til nye professioner og heraf følgende nye behov for personalemæssige omstruktureringer. For at undgå, at en modstand på disse forskellige planer af organisationen bliver til en bremseklods for implementeringen, er det nødvendigt at tage højde for sociale og arbejdsretlige faktorer.

Som samlebegreb for disse organisatorisk-tekniske teoridannelser omhandler læren om IT-indførelse samspillet mellem de menneskelige og maskinelle ressourcer i en organisation, der anvender eller skal anvende IT. IT-indførelse afspejler sig i talrige juridiske aspekter. Gennem teknologi- og samarbejdsaftaler søger man på enkelte overenskomstområder at koordinere medarbejdernes ønsker til ny teknologi med virksomhedens behov. Sanktionering af sikkerhedskrav mv. giver anledning til en række ansættelsesretlige spørgsmål (væsentlig misligholdelse mv.), og kontroltiltag kan komme i konflikt med kollektive overenskomstforhold (regler om ære og velfærd) samt regler om persondatabeskyttelse.

Inden for forskellige lovområder er der pålagt arbejdsgiveren pligt til at inddrage medarbejderne i forhold, der kan få væsentlig indflydelse på arbejdssituationen, herunder i henseende til brugen af virksomhedens teknologiske systemer:

Almindelig informationspligt

Ved lov nr. 303 af 2. maj 2005 om information og høring af lønmodtagere er der givet regler om arbejdsgiverens pligt til at give lønmodtagerrepræsentanter oplysninger om "forhold af væsentlig betydning for de ansatte på virksomheden", jf. nærmere § 4. Informationspligten omfatter bl.a. "virksomhedens beslutninger, som kan medføre betydelige ændringer i arbejdets tilrettelæggelse og ansættelsesforholdene", jf. § 4, stk. 1, nr. 3. Dette gælder dog ikke i tilfælde, hvor en oplysningspligt alvorligt vil kunne skade eller påvirke virksomhedens drift, jf. § 5. Lignende regler findes i lov nr. 391 af 22. maj 1996 om europæiske samarbejdsudvalg med virkning for "fællesskabsvirksomheder og fællesskabskoncerner", jf. denne lovs §§ 4 og 5.

Arbejdsmiljøloven

Arbejdsmiljølovens §§ 7 og 9 foreskriver, at virksomhedens sikkerhedsorganisation skal inddrages i planlægningen af forhold, der har betydning for arbejdsmiljøet. Arbejdsgiveren skal sørge for, at sikkerhedsorganisationen får den nødvendige information og tid til at medvirke i planlægningen. I mindre virksom-

heder, hvor der ikke er en sikkerhedsorganisation, skal ledelsen og de ansatte samarbejde om ændringer i arbejdsmiljøet.

Teknologiaftaler

I visse tilfælde vil der i et kollektivt overenskomstforhold – enten på lokalt eller centralt plan – være indgået aftaler, der normerer dette aspekt. Aftalerne angår som regel indførelse af enhver form for teknologi – altså ikke blot IT – og betegnes derfor som *teknologiaftaler*. Aftaler, der særligt tager sigte på IT-indførelse, benævnes undertiden "dataaftaler".

Samarbejdsaftaler

I det statslige system er disse forhold en del af det almindelige samarbejdssystem, se herved cirkulære nr. 9609 af 29. maj 2002 om aftale om samarbejde og samarbejdsudvalg i statens virksomheder og institutioner, hvis pkt. 5 bl.a. giver samarbejdsudvalget kompetence til at drøfte konsekvenserne af større rationaliserings- og omstillingsprojekter samt projekter vedrørende bl.a. ny og ændret teknologi. I denne drøftelse skal bl.a. indgå forhold vedrørende teknik, økonomi, arbejdets tilrettelæggelse, personalebehov, uddannelse og arbejdsmiljø. Ligeledes skal samarbejdsudvalget drøfte projekter, der indebærer udbud og udlicitering ("outsourcing") af opgaver, samt nedsættelse af projektgrupper i forbindelse hermed. I nødvendigt omfang skal samarbejdsudvalget aftale retningslinjer for medarbejderrepræsentanters deltagelse i projektgrupper mv., der nedsættes i forbindelse med konkrete teknologiprojekter og projekter, som indebærer udbud og udlicitering af opgaver, samt retningslinjer for medarbejdernes adgang til foreliggende dokumentation vedrørende disse projekter.

Europæiske samarbejdsudvalg

Ved lov nr. 371 af 22. maj 1996 er der givet regler om europæiske samarbejdsudvalg. Lovens formål er at forbedre lønmodtagernes muligheder for information og høring om spørgsmål, der berører virksomheder i flere lande, ved oprettelse af samarbejdsudvalg eller indførelse af en informations- eller høringsprocedure. Loven har rod i direktiv 94/45, og den gælder ikke i det omfang der ved kollektiv overenskomst eller aftale er skabt minimumsrettigheder og -pligter svarende til direktivets regler. Ifølge lovens § 23 har det europæiske samarbejdsudvalg krav på at mødes med den centrale ledelse en gang om året for derigennem at få information om udviklingen i virksomheden eller dens aktiviteter, herunder "indførelse af nye arbejdsmetoder eller produktionsprocesser."

14.3. Arbejdsmiljøregulering

14.3.a. Retsgrundlaget

Problemet

IT og arbejdsmiljø har allerede givet anledning til en del debat (stråling fra edb-skærme, ozon-udskillelse fra laser-printere, ergonomiske gener, utilsigtet varmeafgivelse etc.). Problemet får stigende betydning med det større antal IT-arbejdspladser. Der må derfor ventes en blivende politisk bevågenhed på området. Kun få medarbejdere på nutidens kontorer optræder ikke på et eller andet tidspunkt af deres arbejdsdag som IT-brugere.

Arbejdsmiljøloven

Hovedgrundlaget for lovreguleringen er efter dansk ret den almindelige arbejdsmiljølov, jf. lovbekendtgørelse nr. 268 af 18. marts 2005. Loven suppleres med en række cirkulærer og bekendtgørelser, der i mere eller mindre generelle formuleringer sætter rammer for "hvilke krav der skal være opfyldt, for at arbejdet kan anses for fuldt forsvarligt planlagt, tilrettelagt og udført".

Arbejdets udførelse

§ 7 i bekendtgørelsen om "arbejdets udførelse" (nr. 559 af 17. juni 2004) fastslår bl.a., at arbejdet "i alle led" skal udføres "sikkerheds- og sundhedsmæssigt fuldt forsvarligt ud fra både en enkeltvis og samlet vurdering af de forhold i arbejdsmiljøet, som på kort eller lang sigt kan have indvirkning på den fysiske eller psykiske sundhed".

Skærmarbejdspladser

Særlige regler om IT-arbejdsmiljøområdet findes nu i bekendtgørelse nr. 1108 af 15. december 1992 om arbejde ved skærmterminaler. Bekendtgørelsen implementerer Rådets direktiv af 29. maj 1990 om minimumsforskrifter for sikkerhed og sundhed i forbindelse med arbejde ved skærmterminaler (90/270/EØF), EFT 1990 L 156/14 og er ligesom direktivet opbygget med et tilhørende bilag, hvori detailreglerne findes. Bekendtgørelsen trådte i kraft den 1. januar 1993, idet arbejdspladser taget i brug inden dette tidspunkt skal opfylde dens krav senest 1. januar 1997. En særlig bekendtgørelse om arbejde ved skærmterminaler på havanlæg foreligger som nr. 58 af 9. februar 1993.

Skærmdirektivet er et særdirektiv, der som sådant supplerer et overordnet, generelt EF-direktiv om "iværksættelse af foranstaltninger til forbedring af arbejdstagernes sikkerhed og sundhed på arbejdspladsen" (89/391/EØF af 12. juni 1989). Tilsvarende indeholder 1992-bekendtgørelsen supplerende detailregler i forhold til bekendtgørelsen om arbejdets udførelse. Direktivet er blevet fortolket i EF-domstolens dom (præjudiciel sag) af 12. december 1996 under

de forenede sager C-74/95 og C-129/95, der bl.a. fastslog, at medlemsstaterne råder over et vidt skøn i henseende til fastlæggelsen af, hvad der skal forstås ved anvendelse af en skærmterminal "regelmæssigt og i en ikke ubetydelig del af den normale arbejdstid".

Bekendtgørelsen regulerer ansattes arbejde ved en "skærmterminal", hvilket § 1, stk. 2 forstår som en "alfanumerisk eller grafisk skærm, uanset hvilken displayteknologi der benyttes". Ifølge § 2 er hovedreglen den, at skærmterminalarbejdspladser skal indrettes og forsynes med inventar, så arbejdet kan udføres sikkerheds- og sundhedsmæssigt fuldt forsvarligt, jf. reglerne om faste arbejdssteders indretning i bekendtgørelse nr. 96 af 13. februar 2001. Nærmere regler herom er fastsat i bilaget til bekendtgørelsen, jf. dennes § 5. Dog gælder bekendtgørelsen ikke for skærmterminaler, der almindeligvis ikke binder medarbejderen så stærkt til sig, jf. nærmere opregningen i § 3, stk. 2, samt for bærbare computere, som ikke fast bruges på en arbejdsplads.

I bilaget til bekendtgørelsen, der er opbygget i nøje overensstemmelse med bilaget til direktivet – omend med en række sproglige præciseringer – er der givet regler om henholdsvis udstyr (skærm, indlæsnings- og styringsudstyr, arbejdsbord eller -flade), arbejdsplads (pladskrav, belysning, reflekser og blænding, varme, stråling og luftfugtighed) og om samspillet mellem datamat og menneske. Bilaget forudsættes revideret i takt med den teknologiske udvikling. Med sin nuværende formulering er det bygget op om relativt upræcise standarder.

Bekendtgørelsen rummer en række regler af proceduremæssig karakter samt straffebestemmelser, se nærmere §§ 6 – 8. Ifølge § 6 har den ansatte ret til en passende undersøgelse af øjne og syn inden arbejdet påbegyndes, med jævne mellemrum herefter samt når der opstår synsproblemer, der kan skyldes arbejdet ved skærmterminalen.

14.3.b. Arbejdstilsynets vejledning

Arbejdstilsynet har udsendt en vejledning om arbejde ved skærmterminaler (nr. 4.0.1.1.). Vejledningen, der udkom i marts 1994, føjer sig nu til den vejledning fra Branchesikkerhedsråd 6, som omtales nedenfor. Ligesom branchesikkerhedsrådets vejledning, bygger Arbejdstilsynets på bekendtgørelsen om arbejde ved skærmterminaler, nr. 1108 af 15. december 1992.

Vejledningen indledes med en kort oversigt over indholdet af de gældende regler (ikke blot skærmarbejdsbekendtgørelsen, men også andre bekendtgørelser) på området. Dernæst følger en

række forslag til, hvordan disse bestemmelser kan (men ikke nødvendigvis skal) opfyldes. Det er op til den enkelte bruger-organisation at lægge sin egen politik inden for rammerne af de gældende bekendtgørelser.

Det hedder bl.a., at fastlåst eller bundet skærmarbejde bør afbrydes af perioder med arbejde med et andet belastningsmønster. Stiller skærmarbejdet kun få krav til viden og kunnen, bør det tilstræbes, at de opgaver, der veksles over til, stiller bredere og mere udfordrende krav. Som eksempler på sådan alternativ beskæftigelse nævnes planlægning, samarbejde og kvalitetskontrol.

Ifølge bekendtgørelse om arbejde ved skærmterminaler gælder disse regler, når en medarbejder "regelmæssigt og i en ikke ubetydelig del af sin normale arbejdstid" anvender en skærmterminal. Ved afgørelsen af, om dette er tilfældet, foreslår vejledningen, at man som udgangspunkt lægger til grund, om den ansatte så godt som dagligt anvender en skærmterminal, og om skærmen da anvendes mere end ca. 2 timer dagligt. For at sikre hensigtsmæssige arbejdsstillinger og arbejdsbevægelser bør tastaturet være så fladt som muligt. I 3. tasterække bør det ikke være højere end 3 cm. Den samlede højde af bordplade og tastatur bør ikke overstige 5 cm. Ved valg af mus bør der tages hensyn til udformning og betjeningsfunktion, så der opnås en neutral stilling for hånd og arm.

Vejledningen giver endvidere detaljerede regler om kravene til brugergrænseflader, herunder dens forslag til principperne for brugerens dialog med systemet. Således foreslås det, at samme kommandostruktur og -opbygning fastholdes gennem hele dialogen, og at programmellet indeholder kontekstsensitiv hjælp. Herudover foreslår vejledningen, at brugergrænsefladen tilpasses til arbejdsopgaven, bl.a. således, at brugeren har mulighed for at gemme en sammenhængende række af handlinger/-kommandoer og at genbruge denne sekvens ved hjælp af en simpel reference (f.eks. en bestemt tast eller ikon). Ligeledes bør det ifølge vejledningen sikres, at sammenhængende data eller ofte anvendte data kan samles på samme skærmbillede.

Vejledningen slutter med en række "software-ergonomiske" principper for bruger-dialogen: Den skal være velegnet til opgaven, selvforklarende, kontrollerbar for den ansatte, i overensstemmelse med den ansattes forventninger, fejltolerant, velegnet for individuel tilpasning og let at lære.

Branchesikkerhedsrådet for Kontor og Administration har udsendt en Branchevejledning med titlen Arbejde ved skærme (1. udg., 1996). Herudover har Det grafiske Branchesikkerhedsråd udsendt en branchevejledning med titlen Skærmarbejdspladser (3. reviderede udg., 1996). Sidstnævnte giver bl.a. konkrete anvisninger på, hvorledes skærmbilleder bør opbygges. Det hedder bl.a., at punktskrift må være på minimum 7 x 9 punkter, at teksten

ikke må være ulden i skærmens yderkanter eller blive uskarp, når kontrasten eller lysstyrken reguleres, og at linjeafstanden skal være så stor, at linjerne ikke flyder sammen ved længere tids betragtning.

14.3.c. Skærmstråling

Når man taler om skærmstråling, må der sondres mellem henholdsvis ioniserende stråling (dvs. røntgenstråler), det elektrostatiske felt, der dannes på skærmen (der fremkalder statisk elektricitet), og den elektromagnetiske stråling (dvs. radiobølger). Ved siden af disse tre hovedgrupper taler man undertiden også om den optiske stråling. dvs. skærmens lysafgivelse. Denne stråling betragtes dog ikke med nogen større alvor. Ifølge HK's pjece om arbejde ved skærmterminaler (oktober 1989) er den maksimale lysintensitet, der har kunnet konstateres, på ca. 1 % af de grænseværdier, enkelte lande har fastsat. I øvrigt vil brugeren typisk selv kunne indstille lysafgivelsen.

Ioniserende stråling

Den *ioniserende stråling* opstår, når elektronstrålen fra katodestrålerøret rammer indersiden af skærmen. Her bremses den, og der opstår da en såkaldt bremsestråling. En sådan stråling har kun en begrænset energimængde i sig og absorberes næsten fuldstændigt af billedrørets tykke glas. Den del, der slipper ud af billedrøret, er lille sammenlignet med den naturligt forekommende baggrundsstråling. Den kan normalt slet ikke måles.

Elektrostatiske felt

De problemer, der har at gøre med det elektrostatiske felt, har strengt taget intet med stråling at gøre. Omkring skærme med katodestrålerør opbygges der et højspændingsfelt på indersiden af skærmen, der danner statisk elektricitet på dens yderside. Dette sker særligt i tør luft, hvor støvpartiklerne ikke bindes i fugten. Den støv, skærmen tiltrækker, kan give kløen og svien i øjnene. Som anden statisk elektricitet kan dette problem dog afbødes relativt enkelt; f.eks. gennem påvirkning af luftfugtigheden eller ved opsætning af særlige filtre foran skærmen.

Elektromagnetisk stråling

De største strålingsproblemer – og de, der har givet anledning til den mest intense og følelsesladede debat – knytter sig til den elektromagnetisme, der afgives fra dataskærmens afbøjningsspoler. Disse stråler opstår uafhængigt af, hvor meget eller lidt skærmen lyser. Når man har koncentreret sig om disse, skyldes det bl.a., at de i større mængder kan mistænkes for at fremkalde celleforandringer og dermed øge risiko for, at der f.eks. opstår kræft eller (hos gravide kvinder) fosterskader.

Den hidtil største undersøgelse om skærmstråling er udført på initiativ af HK i samarbejde med Socialmedicinsk Institut ved Århus Universitet i 1989. Undersøgelsen konkluderer, at der ingen sammenhæng findes mellem negativt graviditetsudfald og skærmarbejde under ét, og at der heller ingen dosis-respons findes, dvs. at mange timer med skærmarbejde ikke giver større risiko end få timer med skærmarbejde. Ligeledes findes der ikke holdepunkt for, at stillesiddende skærmterminalarbejde udgør nogen overrisiko. Derimod er der en tendens til, at meget stressbelastet skærmterminalarbejde udgør en risiko for negativt graviditetsudfald.

Der findes ingen regler i dansk ret om stråling fra edb-skærme. Derimod indeholder arbejdsmiljølovens § 39, stk. 1, nr. 1, en regel, der bl.a. giver arbejdsministeren hjemmel til at fastsætte regler for at undgå bl.a. stråling. I § 7 i bekendtgørelsen om faste arbejdssteders indretning (nr. 96 af 13. februar 2001), hedder det bl.a., at nyindretning og ombygning af arbejdssteder skal ske således, at eventuelle farer og gener fra bl.a. stråling begrænses mest muligt. En tilsvarende hensigtserklæring findes i bilaget til bekendtgørelse nr. 1108 af 15. december 1992 om arbejde ved skærmterminaler, pkt. 2, litra f). Det hedder her, at stråling, der ikke stammer fra den synlige del af det elektromagnetiske spektrum, skal reduceres mest muligt af hensyn til beskyttelsen af arbejdstagerens sikkerhed og sundhed. Bestemmelsen svarer stort set til § 15 i bekendtgørelsen om arbejdets udførelse, ifølge hvilken det ved arbejdets udførelse skal sikres, at unødig påvirkning fra stråling undgås: "Påvirkningen fra stråling under arbejdet skal derfor holdes så lavt, som det er rimeligt under hensyntagen til den tekniske udvikling, og fastsatte strålingsnormer skal overholdes." Arbejdstilsynet har endnu ikke bragt denne bestemmelse i anvendelse, og de almindelige normer om ioniserende stråling har ingen betydning på IT-området. Der er heller ikke i øvrigt nogen lovgivning, der sætter grænseværdier for stråling fra edb-skærme mv. Den førnævnte vejledning fra Det grafiske Branchesikkerhedsråd begrænser sig til at anbefale, at man ved nyanskaffelser principielt bør vælge skærme med lav stråling (s. 12).

Standarder

I Sverige har Statens Strålskydds Institut (SSI) fastsat grænseværdier, hvorefter strålingen forudsættes at være 25 millitesla/sekund målt i en afstand af 30 cm fra skærmen etc. Der er ingen grund til at regne med, at vi får tilsvarende regler. De fleste af de skærme, der er produceret indenfor de sidste par år, ligger allerede under dette niveau. Den svenske centralorganisation for tjenestemænd (TCO) har udviklet en række standarder for miljøvenligheden af forskellige IT-produkter, se hertil <http://www.tco.se>.

Standarden til TCO/95 indbefatter f.eks. krav til PC'ers elektriske og elektromagnetiske udstråling, energi-effektivitet, stærkstrømssikkerhed, skærmfunktioner og ergonomiske kvaliteter. Disse standarder anvendes af mange leverandører som grundlag for markedsføring af udstyr.

Indkøbsregler

Heller ikke gennem statens indkøbspolitik er der afstukket klare retningslinjer for, hvilken stråling der anses for tilladelig. Den praksis, det offentlige følger, smitter som bekendt umærkeligt af på markedsstandarden. APD har udsendt en vejledning til de statslige arbejdspladser, hvor det fastslås, at stråling er uønsket, og at den skal ned på det lavest mulige niveau. Nogen grænseværdi for dette niveau er dog ikke defineret.

Stråling fra mobiltelefoner

Den tiltagende brug af mobiltelefoner har givet anledning til tvivl om, hvorvidt den elektromagnetiske stråling, der udgår herfra, skulle have skadevoldende virkninger. Da sådanne skadelige virkninger ikke hidtil har kunnet godtgøres, har der ikke været grundlag for lovregulering herom.

Spørgsmål har været rejst i EU-sammenhæng af flere medlemslande, herunder Danmark. Kommissionen har den 11. juni 1998 udsendt et forslag til rådshenstilling om begrænsning af befolkningens eksponering for elektromagnetiske felter (0 Hz-300 GHz), (KOM(98) 268 endelig udg.). Forslaget er ikke begrænset til IT-området, men tager udgangspunkt i det generelle problem, at befolkningen i stigende omfang udsættes for forskellige typer af elektromagnetisme, f.eks. fra elektriske apparater, jernbaner, radiosendere og mobiltelefoner, radarsystemer mv. Selv om der indtil videre kun er begrænset dokumentation for den helbredsskadelige virkning af visse af den slags felter, anser Kommissionen problemet for generelt at være egnet til regulering. Efter en gennemgang af de retsforskrifter, der allerede har reguleret enkelte aspekter af dette problem (f.eks. indenfor arbejdsmiljøområdet, produktsikkerhedsområdet og miljøområdet), foreslår Kommissionen, at der gennem henstilling fremsættes et sæt anbefalinger om, hvilke grænseværdier medlemsstaterne skal acceptere i de forskellige henseender. Anbefalingerne findes i et sæt tekniske bilagsdokumenter til henstillingen, som henstillingen foreslår, at medlemsstaterne gennemfører. Samtidig foreslås det, at medlemsstaterne øger kendskabet til elektromagnetiske felters helbredsvirkninger, bl.a. ved at fremme forskningen indenfor dette område.

For at give markedet mulighed for at forholde sig til disse risici har en række større mobiltelefonproducenter (Nokia, Ericsson og Motorola) fornylig taget initiativ til at udarbejde en global standard for måling af Specific Absorption Rates (SAR), dvs. hvorledes strålinger optages af menneskeligt væv. I USA har Cellular Telecommunications Industry Association allerede stillet krav om, at nyt udstyr markedsføres med oplysning om, hvorledes de

befinder sig i forhold til den SAR-standard, US Federal Communications Commission har udsendt. Der er dog – fortsat – ingen sikre beviser for, om stråling fra mobiltelefoner har sundhedsskadelige virkninger.

14.3.d. Andre skadetyper

Syns- og høreskader

Et af de problemer, der giver anledning til akutte gener navnlig ved anvendelsen af PC'er og printere, er støjen fra alt dette udstyr. Navnlig den blivende ventilatorstøj kan være et stort irritationsmoment. EF's skærmdirektiv pålægger arbejdsgiveren, at der i forbindelse med indretning af arbejdspladsen bl.a. skal tages hensyn til, at støj fra udstyr (printer, disketteenhed, apparaternes ventilatorer osv.) navnlig ikke må virke forstyrrende eller samtalehæmmende, se pkt. 2, litra d), i bilaget. I skønnet over de nærmere krav hertil må det tages i betragtning, at IT-systemer som regel er mindre støjende end f.eks. skrivemaskiner, ventilationsanlæg og telefoner.

Andre skader

Arbejdet ved skærmterminaler kan give anledning til gener som irriterede og røde øjne, synsforstyrrelser (uskarpt syn og "flimren"), hovedpine og træthed samt smerter i ryg, skuldre, nakke og håndled. I denne kategori er der navnlig fokus på de såkaldte "museskader", som kan opstå ved intensiv betjening af tastatur og mus. Der har igennem nogle år været usikkerhed om arbejdsgiverens erstatningsansvar for sådanne skader. Tvivlen har bl.a. knyttet sig til beviset for, at "musesyndromet" var kausalt forvoldt ved arbejdet med musen. Men efter at Retslægerådet har antaget en sådan sammenhæng, er retspraksis nu i bevægelse.

I *U 2005.1363 V* fik en teknisk assistent tilkendt erstatning for varigt men og erhvervsevnetab samt godtgørelse for svie og smerte for en påstået museskade, som Arbejdsskadestyrelsen havde afvist at anerkende som erhvervssygdom. Den tekniske assistent var beskæftiget med CAD-systemer hos Lego. Efter en IT-opgradering i 1997 krævede dette en intensiveret brug af musen uden mulighed for brug af genvejstaster. Retten fandt (under dissens), at Lego siden midten af 1990'erne var bevidst om, at arbejde med computermus kunne give gener i bevægelsesapparatet, og at det nye system ville indebære en større belastning. Ved ikke at tage initiativ til at ændre assistentens arbejdsfunktioner, sådan at antallet af timer med ensidigt computerarbejde blev nedsat til ca. 4 om dagen (som anbefalet af Bedriftssundhedstjenestens repræsentant) havde Lego tilsidesat sin forpligtelse til at sikre sikkerhedsmæssigt forsvarligt arbejde.

Brugervenlighed

I bilaget til bekendtgørelsen om arbejde ved skærmterminaler, pkt. 3, litra b), findes en regel om, at programmellet på skærmarbejdspladsen skal være "let at anvende og om nødvendigt kunne tilpasses brugerens kundskabs- og erfaringsniveau".

Supplerende litteratur

IT-ansættelsen har ikke været genstand for særlig opmærksomhed i dansk retslitteratur. De registerretlige aspekter af denne problemstilling er behandlet af *Peter Blume & Jens Kristiansen*: Databeskyttelse på arbejdsmarkedet (2002). På norsk findes en redegørelse for nogle af de arbejdsretlige problemer, som opstår ved indførelse af ny teknologi, i *Mette Borchgrevink*: Ny teknologi i arbeidslivet – rettslige aspekter (1985). En populær gennemgang af den kommunale sektors teknologiaftaler er udsendt af Landsorganisationen i Danmark (LO) i 1984 under titlen "Teknologiaftaler mv. i den kommunale sektor, Københavns og Frederiksberg kommuner". Se i øvrigt om samarbejdsaftaler *Ole Hasselbalch*: Kollektivarbejdsretten, 2. udg. (1999), s. 11 ff.

Problemerne om *edb og arbejdsmiljø* er behandlet i talrige pjecer fra Arbejdsmiljøfondet, se f.eks. "Svangerskab og skærmarbejde" og "Skærmarbejde – arbejdsmiljø, planlægning og indretning". Arbejdsmiljøfondet har i 1989 udgivet en Rapport fra en konference om arbejdsmiljø – barnløshed og fosterskader og i 1988 en rapport af *Jørgen Skotte* med titlen "Lavfrekvente felter ved dataskærme". Ligeledes har Branchesikkerhedsråd 6 udgivet pjecen: "Arbejde ved skærmterminaler". En rapport skrevet af *Jørgen Bach Andersen*: "Lavfrekvente elektromagnetiske felter – et miljøproblem?" er udgivet af Teknologinævnet som rapport no. 3, (1988). Også de faglige organisationer har behandlet problemerne ved skærmarbejde. Se f.eks. *HK*: "Skærmterminaler – en HK-håndbog om arbejde ved skærmterminaler". Oktober 1989. En praktisk vejledning foreligger med *Georg Strøm*: PC og arbejdsskader (1996).

Om de praktiske problemer ved indførelse af *distancearbejde* henvises til Arbejdsskadestyrelsens rapport: "En arbejdsplads i Danmark" (1998) samt til den case-studie, Dansk Teknologisk Institut udsendte i juni 1998 om et forsøg med distancearbejde gennemført ved Transportrådet. Problemstillingen er præsenteret af *Ruth Nielsen* i *Blume m.fl.:* IT-retlige emner (1998), s. 355 ff.

Kapitel 15.
MARKEDS- OG PRODUKTREGULERING

15.1. Problemstillingen

15.1.a. Internet som markedsføringsmiddel

I takt med sin udbredelse har Internet vist sig at have enestående egenskaber som medium for kommerciel markedsføring. Udover at understøtte og effektivisere de procedurer, der har at gøre med betaling, informationssøgning og underholdning, muliggør nettet en række nye typer af markedsføringshandlinger, der kan give anledning til retlige problemer.

For det første kan det tænkes, at den pågældende markedsføringshandling efter sin fremtrædelse strider mod markedsføringsretlige regler, f.eks. fordi den indeholder misvisende oplysninger eller er påtrængende *i sin form*. Dernæst kan det tænkes, at markedsføringshandlingen indebærer *risici* for forbrugeren, som lovgivningen ikke tillader. I den forbindelse kan det tænkes, at den brug af *personoplysninger*, der finder sted i forbindelse med markedsføringen, er i strid med reglerne om behandling af personoplysninger.

I dette kapitel omtales en del af de mangeartede problemer, der opstår ved markedsføring af varer og tjenester via nye elektroniske medier. Når det gælder den *tekniske* afgrænsning ligger fokus på Internet-tjenesterne World Wide Web og elektronisk post, men også andre nye medier, herunder SMS, berøres. Når det gælder den *retlige* afgrænsning samler opmærksomheden sig om de almindelige regler i markedsføringsloven (mfl.), idet tilgrænsende regler i særlovgivningen også berøres.

15.1.b. Retsgrundlaget

Retsgrundlaget for hovedparten af de retlige problemer, der opstår ved markedsføring på nettet, findes i *markedsføringsloven*, der senest er bekendtgjort ved lovbekendtgørelse nr. 699 af 17. juli 2000 med senere ændringer. Af betydning er ligeledes *telebe-*

kendtgørelsen (bekendtgørelse nr. 638 af 20. juni 2005 om udbud af elektroniske kommunikationsnet og -tjenester) samt *prismærkningsloven* (lov nr. 209 af 28. marts 2000 om mærkning og skiltning med pris). Hertil kommer betydningen af e-handelsdirektivet (2000/31/EF), som skal være implementeret senest den 17. januar 2002. Direktivets regler omtales i det følgende i relation til de markedsføringsspørgsmål, der berøres.

Mfl. § 1 forbyder handlinger, som strider mod "god markedsføringsskik". Bestemmelsen, der er udmøntet i en række specielle markedsføringsforbud, se lovens §§ 2-9, tager ikke hensyn til, hvilket *medium* den erhvervsdrivende anvender som grundlag for sin markedsføring. Forbrugerombudsmanden har derfor – inden for de territoriale grænser, loven sætter – mulighed for at ramme overtrædelser af reglerne om god markedsføringsskik, der begås under anvendelse af digitale netforbindelser, på ganske samme måde, som hvis disse markedsføringshandlinger var udført på traditionel vis (annoncering, direct marketing etc.).

For en jurist spiller det selvsagt først og fremmest en rolle, hvad der står i loven og følger af retspraksis mv. Men på markedsføringsområdet finder man en betydelig grad af selvregulering. Udover den selvregulering, der generelt finder sted i regi af Forbrugerombudsmanden (som led i dennes forhandlingskompetence, jf. mfl. § 16) kan hertil føjes de særlige mærkningsordninger, som i disse år er under udvikling. Disse regler omtales i afsnit 15.4

Adgangen til markedet

Den markedsadfærd, der udfoldes via Internet, er som udgangspunkt ikke underlagt retlige begrænsninger. Hvor et andet og i visse henseender lignende medium som tv- og radiospredning forudsætter forudgående godkendelse efter loven om radio- og fjernsynsvirksomhed, er der som udgangspunkt ingen særlige retlige barrierer i adgangen til at markedsføre sine varer og tjenester via nettet. Dette princip er nu knæsat i e-handelsdirektivets art. 4, stk. 1, hvorefter udbydere af informationstjenester ikke må mødes med noget krav om forudgående godkendelse eller lignende som betingelse for at udøve aktivitet som leverandør af informationssamfundstjenester. Bestemmelsen indebærer i praksis, at tjenester, der i forvejen lovligt kan udbydes, ikke må belægges med særlige begrænsninger, alene fordi de udbydes som informationstjenester.

E-handelsloven

Reglerne i e-handelsdirektivet er indført i dansk ret ved lov nr. 227 af 22. april 2002 om tjenester i informationssamfundet, herunder visse aspekter af elektronisk handel (i daglig tale e-handelsloven). Ligesom direktivet omfatter loven principielt kun of-

fentligretlige regler og altså ikke privatretlige, jf. hertil de kritiske bemærkninger hos *Ruth Nielsen* i Juridisk Instituts Julebog 2002, s. 225 ff. Foruden et væsentligt princip om hjemlandskontrol i lovens § 3 (se hertil bemærkningerne i afsnit 23.1.c.) pålægger loven leverandører af "informationssamfundstjenester" (jf. definitionen i § 2, nr. 1) en række oplysningsforpligtelser, der har væsentlig betydning for markedsføringen. Herudover indeholder loven en række ansvarsregler, der omtales nærmere i afsnit 17.1.e. Loven er kommenteret af *Jacob Plesner Mathiasen* m.fl. (2004).

Konkurrencebegrænsninger

Konkurrenceloven, jf. lovbekendtgørelse nr. 539 af 28. juni 2002, giver konkurrencemyndighederne en række beføjelser til at gribe ind overfor foranstaltninger, der hindrer en effektiv samfundsmæssig ressourceanvendelse gennem virksom konkurrence. Sådanne foranstaltninger kan enten tænkes at forekomme i relation til sådanne virksomheder, der udbyder Internet-adgang som deres ydelse (Internet-leverandører og leverandører af hertil hørende ydelser), som i relation til virksomheder, der anvender Internet til at kontakte deres kunder (f.eks. markedsføringskanal for levering af fysiske varer, ofte kaldet "indirekte elektronisk handel") eller som kanal til afsætning af deres varer i digital form (f.eks. leverandører af digital information, såkaldt "direkte elektronisk handel").

De danske konkurrencemyndigheder har endnu ikke truffet afgørelse i sager, hvor Internet på en af disse måder har været årsag til en konkurrencebegrænsende foranstaltning. Og det må da også antages, at der på nuværende tidspunkt udfolder sig en ganske effektiv konkurrence på nettet, hvor enhver virksomhed med et minimum af omkostninger er i stand til at placere sig på markedet og dermed – potentielt – nå alle nettets brugere.

Konkurrencestyrelsen gennemførte i 1997 et internt analysearbejde, der skulle vurdere styrelsens stilling i relation til Internet-konkurrence, men udredningen førte ikke til indgreb eller andre særlige initiativer. De konkurrenceretlige problemer, der gør sig gældende på markedet for standardprogrammel, behandles af *Dan Eklöf* i NIR 1999.157 ff. og af *Magdalena Jerner* i NIR 1999.189 (med særlig fokus på programlicenser) og i Konkurrencestyrelsens Konkurrenceredegørelse 2000, kapitel 5, s. 133 ff.

15.2. Reklamen

15.2.a. Push or pull?

I en vurdering af en markedsføringshandlings skadelighed og lovlighed spiller det bl.a. ind, hvem der har taget skridt til den. Er forbrugeren selv "ude og spørge", har den erhvervsdrivende videre frihedsgrader i form og virkemidler, end når reklamen rammer forbrugeren uopfordret, f.eks. gennem tv eller ved fremsendelse af uopfordrede henvendelser.

Pull

Denne forskel i den retlige bedømmelse, gør det hensigtsmæssigt at anlægge en sondring mellem to principielt forskellige teknikker til Internet-markedsføring. Efter det ene princip henter den enkelte Internet-bruger selv sin information hos den erhvervsdrivende. Denne fremgangsmåde betegnes ofte som *pull-teknologi*. Som udgangspunkt rummer den sjældent store faremomenter, fordi brugeren som nævnt selv har herredømmet. Særlige problemer kan dog opstå, når den information, der hentes, har et andet indhold end tilsigtet eller er urimelig mangelfuld. Disse spørgsmål behandles senere i dette afsnit.

Det klassiske eksempel på en pull-teknologi er kommerciel markedsføring fra hjemmesider på the World Wide Web (www). Den information, forbrugeren modtager herfra, vil altid fremkomme i direkte eller indirekte konsekvens af, at han har afgivet en *http*-request mod en hjemmeside, jf. nærmere herom i afsnit 3.3.e. Som led i finansieringen af populære sites vil indehaveren ofte sælge reklameplads til (andre) erhvervsdrivende ved at lade disse angive annoncer eller anden markedsføringsinformation på siden, jf. herom i afsnit 15.2.b.

Push

Er der derimod tale om, at nettet anvendes på samme måde som tv og radio til at støde information frem mod forbrugeren, såkaldt *push-teknologi*, er beskyttelsesbehovet større. Dette gælder uanset om en sådan informationsstrøm er udvalgt ud fra bestemte profiler af den enkelte bruger, eller blot sendes kritikløst ud (fordi de variable omkostninger herved er forsvindende). Den beskyttelsesinteresse, der her er på banen, udspringer i bund og grund af overvejelser om privatlivets fred, der – som nævnt i afsnit 13.1.a – bl.a. indeholder en "*right to be left alone*". Denne interesse er særligt beskyttelsesværdig, hvis de informationer, der modtages, er *overrumplende* eller på anden måde belastende for modtageren; men også uden for disse tilfælde er der et alment beskyttelsesbehov, f.eks. fordi selve modtagelsen af den kom-

mercielle information er forbundet med omkostninger til transmissionstid mv.

E-mail-markedsføring

Den hyppigste form for push-teknologi foreligger, når varer og tjenester markedsføres ved hjælp af *e-mails* til enkelte brugere. Dette kan enten ske på grundlag af en forudgående anmodning fra brugeren (i så fald typisk ved at denne tilmelder sig en liste, hvorfra der herefter modtages såvel annoncemateriale som nyhedsstof) eller helt uanmodet. Nærmere herom i afsnit 15.3.a. Det kan dog også forekomme, at den markedsførende virksomhed tager kontrollen over brugerens browser og lader denne åbne nye sites uden brugerens medvirken: Når brugeren forsøger at lukke et vindue, åbner systemet herefter et nyt, og processen hermed bringes først til ophør, når browserprogrammet afsluttes. Sådanne markedsføringshandlinger må almindeligvis betegnes som overrumplende og kan som sådanne almindeligvis forbydes efter mfl. § 1, hvis ikke efter nogle af de særlige markedsføringsforbud, der er omtalt i det følgende.

15.2.b. Bannerannoncering mv.

En hjemmeside kan – som bekendt – anvendes som ordinær "plakatsøjle" for annoncer for varer og tjenesteydelser. En sådan anvendelse er som udgangspunkt retligt uproblematisk. Udgangspunktet må være, at den, der henter information fra en hjemmeside, selv har truffet beslutning om at nå den, og at han derfor også – inden for lovens rammer – må tage hjemmesiden som den er. At bannerannoncering undertiden kan gøre det mere kostbart for brugeren at anvende hjemmesiden, er uden betydning for lovligheden af en sådan annoncering. Der er for det første tale om markedsføringshandlinger, der er helt sædvanlige. For det andet har brugeren mulighed for at fravælge de mest kostbare grafiske og animerede annoncer i sin egen browser, hvorved den rekvirerede information modtages i ren, tekstuel form.

Konvergens?

Markedsføring via hjemmesider er som udgangspunkt omfattet af de regler, der gælder for trykte medier. Selv om hjemmesiden indebærer faciliteter til visning af levende billeder eller i øvrigt er animeret, kan man ikke overføre de regler, der gælder for radio- og tv-spredning. Hvor der ikke gælder særlige regler på området (hvilket f.eks. er tilfældet i relation til markedsføring af lægemidler, se hertil lægemiddellovens §§ 26-31), falder man derfor tilbage på den almindelige regulering, herunder først og fremmest i mfl. § 1, der suppleres med de særlige markedsføringsregler i §§ 2-9.

Af de nordiske forbrugerombudsmænds Standpunkt til handel og markedsføring på internettet (oktober 2002) fremgår bl.a., at al markedsføring skal udformes og præsenteres på en sådan måde, at den tydeligt fremstår som markedsføring. Dette indebærer bl.a., at man ikke må benytte forvirrende dialogbokse i markedsføringen som kun har til formål at henlede opmærksomheden på en markedsføringsforanstaltning. Som eksempler kan nævnes et *pop-up vindue* der fremstår som en fejlmeddelelse, som forbrugeren må føle sig nødsaget til at klikke "ok" på, og et *lydsignal* svarende til det, der ellers varsler indkommende e-mail. Markedsføring, som ikke er en integreret del af en Internet-side, skal kunne fjernes enkelt, f.eks. ved "luk". Dominerende annoncer, f.eks. helsidesannoncer, skal forsvinde af sig selv efter en kort periode, og der bør sættes en grænse for antallet af eksponeringer af reklamebudskaber. Det hedder ligeledes, at markedsføring ikke bør afbryde redaktionelt stof eller andet indhold af informativ eller vejledende art på hjemmesiden. Retningslinierne har været mødt med generel skepsis fra en i forvejen trængt Internet-branche, som i de seneste års hårde tider ser muligheden for at generere et provenu gennem annoncemidler. Der foreligger endnu ingen tilfælde, hvor et påbud mv. fra den danske Forbrugerombudsmand under henvisning til disse retningslinier, har været prøvet ved domstolene.

Medvirkens-spørgsmål

Modsat dagblads- og tv-annoncer vil web-annoncer typisk dække over en link til en hjemmeside, hvor der findes mere information om den pågældende ydelse. Den, der udbyder en hjemmeside, står derfor på en anden måde end dagbladsudgiveren mv. bag den annonce, der udbydes. Hvis linken viser direkte hen til en hjemmeside, der indeholder information, der er retsstridig efter markedsføringsretlige eller andre regler, må han kunne gøres umiddelbart medvirkensansvarlig herfor, hvis det fornødne forsæt er tilstede. Dette er således antaget i *U 2001.1572 V*, hvor to unge mennesker bl.a. blev dømt medvirkensansvarlige for gennem links til ulovlige MP3-filer fra en hjemmeside at have "forøget mulighederne for, at de personer, der ønskede at kopiere musik, kunne finde musikken og foretage kopieringen på en nem og hurtig måde". I sådanne tilfælde kan de særlige regler om ansvarsudelukkelse i e-handelslovens §§ 14-16, ikke anvendes. Dette gælder uanset, om der er tale om et egentligt annoncemateriale (med særskilt tekst og billede) eller om bannerannoncer, der kun viser et logo eller varemærke, som dækker over en link til annoncørens hjemmeside.

Se tilsvarende pkt. 9 i de nordiske brugerombudsmænds standpunkt til handel og markedsføring på internettet (oktober 2002). Det fremgår heraf, at den erhvervsdrivende som regel også er ansvarlig for indholdet af det materiale (f.eks. producenters produktbeskrivelser), der fremgår af andre hjemmesider, som den erhvervsdrivende linker til. Endvidere fremgår det, at erhvervsdrivende ikke bør linke til hjemmesider eller materiale, der ved et umiddelbart gennemsyn ikke lever op til principperne i dette standpunkt. Bliver en erhvervsdrivende (gjort) opmærksom på, at en hjemmeside, som han linker til, rummer retsstridigt materiale, bør han fjerne det pågældende link – et resultat, der korresponderer med de regler om medvirkensansvar for "oplagring", der følger af e-handelslovens § 16, stk. 1, nr. 2, se hertil afsnit 17.1.e. Det hedder endelig, at det bør stå klart for forbrugeren, hvornår den aktuelle hjemmeside forlades i forbindelse med, at der linkes til andre hjemmesider.

Misvisende ikoner

Visse web-annoncer er indrettet i en grafisk form, der svarer til de dialogbokse, der indgår i kendte styresystemer – f.eks. med et "ok"-ikon i midten. Meningen hermed synes at være, at brugeren foranlediges til at klikke på "ok"-ikonet for – som det almindeligvis er tilfældet – at gøre systemet operationsdygtigt. I stedet aktiveres en link til udbyderens egen hjemmeside med reklamemateriale. Sådanne web-annoncer må som udgangspunkt anses for retsstridige efter bestemmelsen i mfl. § 2 om vildledning.

15.2.c. Oplysningsforpligtelser

Identitet

Markedsføring via Internet giver anledning til særegne forvekslingsproblemer, som der er en retlig interesse i at beskytte forbrugeren imod. Selv om der *principielt* er gode muligheder for at undgå utilsigtet forveksling, fordi web-adresser nødvendigvis må afgives med fuldstændig præcision, betyder nettets globalisering, at forbrugeren ofte ikke ved, hvor den forretningsdrivende befinder sig, endsige hvad det er for en type virksomhed, forbrugeren har foran sig. Ganske vist er det praksis, at alle registranter af domænenavne tilbyder en "whois" service, der giver oplysning om, hvilken identitet der står bag en domæneregistrering. For domæner, der er omfattet af IDL, er en sådan offentliggørelse ligefrem påbudt, se herved lovens § 8, stk. 2-3. Men denne service indebærer ingen sikkerhed for, hvem det rent faktisk er, der driver virksomhed fra den pågældende site. Hertil kommer, at de oplysninger, der er afgivet til en whois-service, ofte ikke kontrolleres af det pågældende domænes hostmaster.

E-handelsloven

Med § 7 i e-handelsloven er det pålagt en tjenesteyder (dvs. enhver fysisk eller juridisk person, som leverer en informationssamfundstjeneste) at give oplysning om (1) tjenesteyderens navn,

(2) den fysiske adresse, hvor tjenesteyderen er etableret, (3) e-post-adresse og eventuelt postadresse og andre oplysninger om tjenesteyderen, som gør det muligt at kontakte og kommunikere med tjenesteyderen, (4) CVR-nummeret, hvis tjenesteyderen er registreret i Det Centrale Virksomhedsregister, samt (5) tjenesteyderens tilhørsforhold til eventuelle godkendelsesordninger, herunder den relevante tilsynsmyndighed. En tjenesteyder, der udøver et "lovreguleret erhverv" i den EU-retlige betydning, der er angivet i lovens § 2, nr. 7, skal desuden give oplysning om (1) enhver brancheorganisation eller lignende, hvor tjenesteyderen er registreret, og om (2) erhvervsbetegnelsen og den medlemsstat, hvor den er givet, samt (3) en henvisning til de faglige regler, der gælder for det lovregulerede erhverv, og hvorledes der kan opnås adgang til disse, jf. stk. 2. Både tjenestemodtageren og myndighederne skal have let tilgængelig og vedvarende adgang til de i stk. 1 og 2 nævnte oplysninger, jf. stk. 3.

Teletjenester

Ifølge reglerne i *telebekendtgørelsen* (bekendtgørelse nr. 638 af 20. juni 2005 om udbud af elektroniske kommunikationsnet og tjenester) er der pålagt udbydere af sådanne tjenester en række oplysningspligter over for slutbrugere. Ifølge § 5 skal udbyderen sikre, at der foreligger en kontrakt som grundlag for ethvert kundeforhold med en slutbruger. Kontrakten skal indeholde de detaljerede oplysninger, der fremgår af stk. 2-3. Herudover pålægger bekendtgørelsen teleudbyderen en række oplysningspligter i løbet af kundeforholdet, f.eks. om løbende bevægelser i saldo mv.

Tilbuds-oplysninger

Der er både en almindelig konkurrenceretlig og en speciel forbrugerretlig interesse i, at forbrugerens dispositioner træffes på et så godt grundlag som muligt. Ifølge mfl. § 3 skal der ved tilbuds afgivelse, ved indgåelse af aftale eller efter omstændighederne på leveringstidspunktet gives en efter formuegodets eller ydelsens art forsvarlig vejledning, når denne er af betydning for bedømmelsen af godets eller ydelsens karakter eller egenskaber, herunder især brugsegenskaber, holdbarhed, farlighed og vedligeholdelsesmulighed. Efter praksis indebærer denne bestemmelse bl.a., at der skal gives en dansk brugsanvisning ved salg af varer og tjenester til danske forbrugere. Dette krav vil sjældent være opfyldt, når en udenlandsk erhvervsdrivende markedsfører sig globalt via Internet og dermed også når danske forbrugere.

Anden oplysningspligt

E-handelslovens § 9 indeholder dernæst en række krav til det markedsføringsmateriale, som indgår i en informationssamfundstjeneste: Al kommerciel kommunikation, der er en del af eller udgør en sådan tjeneste, skal udformes og præsenteres, så det tydeligt fremgår, at der er tale om kommerciel kommunika-

tion, dvs. om reklame. Det skal i den forbindelse tydeligt fremgå, på hvis *vegne* den kommercielle kommunikation udsendes, jf. stk. 1. Når reklametilbud som for eksempel *rabatter, tilgift og gaver* er tilladt (se herved reglerne i mfl. §§ 6, 8 og 9) skal betingelserne for deltagelse i disse foranstaltninger være let tilgængelige og fremlægges klart og tydeligt. Tilsvarende gælder for salgsfremmende *konkurrencer og spil*, der er tilladt. Disse regler gælder, uanset om den pågældende reklame mv. udføres over for forbrugere eller mellem erhvervsdrivende.

Betalingstjenester

En særlig oplysningsforpligtelse følger af § 7 i betalingsmiddelloven (LVB). Efter denne bestemmelse skal udstederen af et betalingsmiddel (altså den, som brugeren indgår aftale med om anvendelsen af dette, jf. § 3, stk. 2) stille informationsmateriale til rådighed for brugeren. Materiale skal i et let og forståeligt sprog sætte brugeren i stand til at anvende betalingsmidlet på en sikker og hensigtsmæssig måde. Det skal dernæst give oplysning om typiske omkostninger ved anvendelse af betalingsmidlet. Endelig skal der gives særskilt oplysning om de sikkerhedsmæssige krav, brugeren skal efterleve, samt det ansvar, han kan udsætte sig for ved tredjemands misbrug. Efter hver transaktion har brugeren dernæst krav på en kvittering, jf. LVB § 8.

Selvregulering

Som omtalt i afsnit 5.2.c. har erhvervsorganisationer både nationalt og internationalt på forskellig vis søgt at præcisere de krav, der bør opfyldes ved markedsføring af elektroniske tjenester på nettet. Indholdet af sådanne regler vil ofte få betydning, når generelle regler, f.eks. generalklausulen i mfl. § 1, skal udfyldes.

15.2.d. Prismærkning

Ifølge § 1 i prismærkningsloven, jf. lovbekendtgørelse nr. 209 af 28. marts 2000, som ændret ved lov nr. 1383 af 21. december 2004, skal den, "der erhvervsmæssigt udbyder varer i detailsalg" ved mærkning, skiltning eller på anden måde tydeligt give oplysninger om pris iberegnet moms og andre afgifter. Loven sondrer mellem den skiltning mv., der sker i selve forretningslokalet og den, der sker ved annoncering i forbindelse med fjernsalg. Ved fjernsalg gælder lovens almindelige regler i §§ 1-2, kun, når der ved annoncering gives oplysning om prisen for varer eller ydelser, jf. § 5, stk. 2. Der gælder altså ingen almindelig pligt til at give disse oplysninger ved fjernsalg. Om fjernsalg bestemmer lovens § 5, stk. 2, at der i forbindelse med meddelelse af prisop-

lysninger skal gives tydelig oplysning om rabat eller anden særlig fordel som nævnt i lovens § 1, stk. 2, 1. pkt.

Det må antages, at prismærkningslovens regler om annoncering også omfatter annoncering via en hjemmeside. Derimod kan man næppe sidestille den erhvervsdrivendes hjemmesider med hans forretningslokaler i henseende til den almindelige prismærkningspligt.

I Erhvervsministeriets rapport om Forbrugerens retsbeskyttelse i grænseoverskridende digitale net (juni 1997) anbefales prismærkningsloven ændret således, at virksomheder skal oplyse om priser mv., når de giver mulighed ved fjernsalg via Internet, og at virksomheder, der har en hjemmeside, skal give de samme prisoplysninger mv., som de skal ved opslag i forretningsstedet.

15.3. Enkelte markedsføringshandlinger

15.3.a. Uopfordret markedsføring

Problemstillingen

En hyppigt forekommende markedsføringsmetode i den elektroniske handel består i uopfordret forsendelse af reklamemateriale ved brug af elektronisk post og (undertiden) telefax til enkelte og identificerbare adressater. I Internet-slang betegnes sådanne markedsføringshandlinger som *spamming*. Den retlige regulering af dette fænomen er kommet til gradvis og med rod i forskellige EU-direktiver, og i dag tegner der sig en regulering af dette forhold, der er ikke så lidt kompleks. Reguleringen beror således på, hvem den pågældende information fremsendes til og under hvilke tekniske og retlige omstændigheder, og om modtageren har givet samtykke, henholdsvis efterfølgende har modsat sig at modtage en sådan information.

De nævnte direktiver er direktivet om behandling af personoplysninger (95/46/EF), fjernsalgsdirektivet (97/7/EF) og direktivet om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (2002/58/EF).

LBP

I det omfang en sådan markedsføring rammer *enkeltpersoner*, kan forholdet generelt rammes af LBP. Reguleringen indtræder i så fald på flere niveauer. For det første må henvendelsen ses som en "behandling" (eller en del af en sådan) af personoplysninger, der kun kan finde sted, hvis der er hjemmel hertil i de almindelige regler. Er der ikke udtrykkelig lovhjemmel hertil i loven, må man falde tilbage på LBP § 6, stk. 1, nr. 1, der indebærer, at markeds-

føringshandlingen alene kan ske over for enkeltpersoner, hvis de pågældende har givet deres udtrykkelige samtykke hertil. For det andet forbyder LBP § 6, stk. 2, virksomheden at videregive oplysninger om en forbruger til en anden virksomhed til brug ved markedsføring, medmindre forbrugeren har givet sit udtrykkelige samtykke hertil. Virksomheden må heller ikke anvende sådanne oplysninger på vegne af en anden virksomhed i dette øjemed uden samtykke. Et samtykke skal indhentes i overensstemmelse med reglerne i mfl. § 6 a.

Mfl. § 6a

Reglerne i mfl. § 6a indeholder et særdeles kompliceret sæt af regler. Reglerne blev i deres oprindelige skikkelse indsat i loven i 2000 med henblik på gennemførelse af persondatadirektivet (95/46), fjernsalgsdirektivet (97/7) og direktiverne om privatlivsbeskyttelse i forbindelse med telekommunikation (oprindelig 97/66, senere 2002/58). Reglerne gav anledning til en del kritik, se f.eks. *Blume* i U 2001B.99 ff., bl.a. om deres forenelighed med EU-retten. Siden er reglerne blevet ændret flere gange, senest ved lov nr. 450 af 10. juni 2003, ligesom de har givet anledning til en del retspraksis. Bestemmelserne er behandlet af *Peter Blume & Mette Reissmann*: Beskyttelse af forbrugeroplysninger (2003). Forbrugerombudsmanden har den 27. januar 2005 udarbejdet en vejledning om reglerne. Vejledningen, der præsenterer sig som en "generel forhåndsbesked", er tilgængelig fra <www.fs.dk>.

Udgangspunktet

Ifølge mfl. § 6a, stk. 1, må en erhvervsdrivende ikke rette henvendelse til nogen ved brug af elektronisk post, automatiske opkaldssystemer eller telefax med henblik på afsætning af varer, fast ejendom og andre formuegoder samt arbejds- og tjenesteydelser, medmindre den pågældende forudgående har anmodet herom. Med denne bestemmelse indføres en såkaldt "*opt in*"-model i relation til de nævnte tre kommunikationsformer. Bestemmelsen gælder, hvad enten modtageren er privat eller erhvervsdrivende, jf. ordet "nogen". Markedsføring ved hjælp af adresseløse forsendelser (hvor der ikke er nogen identificerbar adressat) er dog ikke omfattet, idet en sådan markedsføring ikke indebærer, at "nogen" står som adressat. Til gengæld er reguleringen begrænset til de tre nævnte teknologier: Elektronisk post (e-mail), telefax og automatiske opkaldssystemer. SMS-teknologi er ikke direkte omfattet, men vil i praksis være det, da det næppe er praktisk muligt for den erhvervsdrivende at fremsende direkte SMS-beskeder i markedsføringsøjemed uden brug af et automatisk opkaldssystem.

Bestemmelsen giver anledning til afgrænsningsproblemer i relation til løbende kundeforhold, hvor grænsen mellem "markedsføring" og "rådgivning" kan være flydende. Er det f.eks. "markedsføring" at meddele en forsikringskunde, at han kan opnå en præmiereduktion ved at slå tre særskilt tegnede forsikringsprodukter sammen til et? Ud fra én betragtning, ja: Tilbuddet ville næppe blive fremsat, hvis ikke det også indebar fordele for selskabet. Men ud fra en anden, nej: Kunden har selv en interesse i at få oplysning om, hvordan han kan tilrettelægge sine aftaleforhold på den optimale måde. Der må formentlig gives de erhvervsdrivende, der befinder sig i et sådant kundeforhold til modtageren, ret vide rammer til at orientere om kundeforholdet og om mulighederne for at ændre indgåede aftaler, uden at dette skal betegnes som "markedsføring". Grænsen må antages at gå, hvor der tilbydes varer og tjenester af en helt anden beskaffenhed end den oprindeligt leverede.

Tidligere kontakt

Det strikse udgangspunkt i § 6a, stk. 1, modificeres dog noget ved bestemmelsens stk. 2 (indsat ved den seneste lovændring), der gælder for den situation, hvor en erhvervsdrivende fra en kunde har modtaget dennes elektroniske adresse i forbindelse med salg af en vare eller en tjenesteydelse. Den erhvervsdrivende må da markedsføre sine egne tilsvarende produkter eller tjenesteydelser til kunden ved *elektronisk post*. Herved forstås såvel e-post i klassisk forstand (transmitteret via Internet) som elektroniske meddelelser, der formidles via mobiltelefoni, f.eks. SMS og MMS. Denne adgang forudsætter dog, at kunden har mulighed for let og gebyrfrit at frabede sig dette både i forbindelse med afgivelsen af adressen til den erhvervsdrivende og ved efterfølgende henvendelser. I forbindelse med købet skal der gives kunden meddelelse om, at der fremover vil blive sendt reklamer – og i givet fald af hvilken art (e-mail, SMS mv.). Lovændringen indebærer således, at der ikke længere kræves et positivt samtykke fra forbrugeren til markedsføring via elektronisk post.

Frabedelser

Mfl. § 6a, stk. 3, indfører en regel, der gør det muligt for "en bestemt fysisk person" at modsætte sig uanmodede henvendelser ved brug af andre midler til fjernkommunikation med henblik på afsætning som nævnt i stk. 1. En sådan frabedelse kan gennemføres på to måder. *Enten* kan den pågældende rette henvendelse til den erhvervsdrivende. *Eller* også kan han tilmelde sig en fortegnelse, som udarbejdes af Det Centrale Personregister (CPR) hvert kvartal. På denne såkaldte *Robinson-liste* (et øgenavn, som reflekterer den opfattelse, at personer, der ikke ønsker reklamer, befinder sig på en øde ø!) kan personen frabede sig henvendelser,

der sker i markedsføringsøjemed. Den erhvervsdrivende, der ved undersøgelse i denne liste er blevet bekendt med, at modtageren har frabedt sig sådanne henvendelser, må herefter undlade en sådan markedsføring. Ved telefonisk henvendelse til forbrugere gælder endvidere reglerne om uanmodet henvendelse i lov om visse forbrugeraftaler, nr. 451 af 9. juni 2004, se dennes §§ 6-8. Disse regler gælder dog ikke, hvis den pågældende person forudgående har anmodet om henvendelsen fra den erhvervsdrivende, jf. stk. 4. Tilsvarende regler gælder ved videregivelse af markedsføringsoplysninger, jf. LBP § 36, stk. 2.

Ved dommen i *U 2002.1282 SH* om Interessebank Danmark er det antaget, at undtagelsesbestemmelsen i mfl. § 6a, stk. 4 (dengang stk. 3) ikke alene fandt anvendelse på anmodninger over for den pågældende erhvervsdrivende, men også på anmodninger fremsat af forbrugere over for Interessebank Danmark, der – med henblik på salg af adresser til erhvervsdrivende – modtog tilmeldinger fra forbrugere med samtykke til markedsføring over for dem inden for bestemte interesseområder. Se ligeledes *U 2002.2277 SH*, hvor en samtykkeerklæring, som fremgik af et ikke særligt fremhævet afsnit i en abonnementsaftale vedrørende mobiltelefoni, ikke opfyldte klarheds- og fremhævelseskravene i bestemmelsen. Bestemmelsen gik ud på, at abonnenten gav "Tilladelse til, at Telia kan analysere hvordan jeg anvender min mobiltelefon, så jeg kan modtage målrettet information og markedsføring om teleservice fra Telia". Teleaftalen var indgået via en sportsklub, som havde uddelt tilmeldingsblanketter til sine medlemmer, hvoraf den pågældende bestemmelse fremgik.

Oplysningspligt

Robinson-systemet understøttes ved § 6a, stk. 5, der pålægger en erhvervsdrivende første gang han retter henvendelse som nævnt i stk. 3 til en fysisk person, der ikke er anført i Robinsonlisten, tydeligt og på en forståelig måde at oplyse om retten til at frabede sig henvendelser som nævnt i stk. 3. Den pågældende skal samtidig gives adgang til på en nem måde at frabede sig sådanne henvendelser.

Sanktioner

Domstolene har slået hårdt ned på overtrædelser af forbuddet i § 6a. Ved dommen i *U 2003.1855 SH* blev et aktieselskab pålagt en bøde på 15.000 kr. for at have udsendt ikke under 150 telefaxer og e-mails, hovedsagelig til erhvervsdrivende, uden at modtagerne forudgående havde anmodet derom. Ved strafudmålingen blev det lagt til grund, at hovedparten af modtagerne var erhvervsdrivende, der havde måttet spilde tid og arbejdskraft på at læse og behandle de pågældende henvendelser og skaffe sig af med dem. I *U 2004.1141 SH* blev bøden udmålt til 400.000 kr.

Den tiltalte virksomhed havde i perioden fra den 18. november 2002 til den 20. marts 2003 udsendt mellem 7.650 og 15.300 telefaxreklamer til modtagere, der ikke havde anmodet om disse forsendelser. Den hidtil største bøde er udmålt til 2 mio. kr. og idømt ved Sø- og Handelsrettens dom af 14. marts 2005 (tilgængelig fra <www.shret.dk>. Et teleselskab havde her udsendt ca. 40.000 uanmodede meddelelser i form af e-mails og SMS.

15.3.b. Betalingssystemer

Ifølge LVB § 4, stk. 2, skal et betalingssystem indrettes og virke således, at der sikres brugerne gennemsigtighed, frivillighed, beskyttelse mod misbrug samt fortrolighed om brugerens anvendelse af betalingsmidlet. Der skal løbende træffes de juridiske, organisatoriske, driftsmæssige, tekniske og sikkerhedsmæssige foranstaltninger, som er nødvendige for, at der er tale om et sikkert og velfungerende betalingssystem. Forbrugerombudsmanden skal ved forhandling søge forholdene ændret, hvis betalingssystemet ikke lever op til disse krav. Kontrollen indebærer bl.a. indseende med, at forretningsbetingelser eller praksis overfor brugeren eller en anden part ikke "ensidigt tilgodeser egne interesser eller i øvrigt er urimelige", jf. loven stk. 3, nr. 2.

FO's retningslinjer

Forbrugerombudsmanden har i 1996 udsendt et sæt retningslinjer om brug af betalingskort i forbindelse med Internet-handel, se hertil <www.fs.dk>. Det fremgår heraf, at en Internet-butik ikke må igangsætte en betalingstransaktion uden kundens udtrykkelige accept. Gør kunden gældende, at det enten ikke er kunden selv, der har foretaget eller givet tilladelse til betalingstransaktionen, at de bestilte varer ikke er blevet leveret, eller at kunden ønsker at udnytte en lovbestemt eller aftalt fortrydelsesret, har pengeinstituttet pligt til at stille betalingen i bero, og allerede debiterede beløb skal da tilbageføres.

15.3.c. Spil, væddemål og indsamlinger

En række spilleformer, som navnlig praktiseres fra Internet-sites uden for Danmark, er underkastet en national lovregulering, som afskærer en tilsvarende markedsføring af disse spil herhjemme.

Bortlodning

Ifølge § 2 i lotteriloven af 1869 med senere ændringer er al foranstaltning af lottospil her i riget, ligesom besørgelsen af dermed stående forretninger, forbudt under bødestraf. Forbuddet rammer spil, hvis udfald beror på tilfældet. Tipning mv. er ikke omfattet, da udfaldet af de kampe, der tippes om, må antages at

bero på den medvirkendes indsigt i spillet. Bestemmelsens stk. 2 giver dog hjemmel til at dispensere fra dette forbud. Reglerne herom er fastsat i Justitsministeriets bortlodningscirkulære, nr. 147 af 1. august 1994. Reglerne heri gælder uden videre også for Internet-baserede spil mv.

Spil og væddemål mv.

Ifølge lov om visse spil, lotterier og væddemål, jf. lovbekendtgørelse nr. 1077 af 11. december 2003, kan skatteministeren meddele bevilling til foranstaltning af spil, lotterier og væddemål mod betaling af en afgift til staten på 16% af indskudssummen. Foranstaltning her i landet af væddemål, der ikke har hjemmel i en sådan autorisation, samt formidling af deltagelse i udenlandske væddemål, straffes efter lovens § 10 med bøde eller fængsel indtil 6 måneder. Dette forbud rammer tipning og bookmakerspil, men ikke væddemål i forbindelse med heste- og hundeløb.

Indsamlinger

Ifølge § 2 i lov om offentlige indsamlinger, jf. lovbekendtgørelse nr. 623 af 15. september 1986, må offentlig gade- og husindsamling ved personlig eller telefonisk henvendelse ikke finde sted. Det samme gælder indsamling ved kædebreve. I domspraksis er denne bestemmelse fundet tilsvarende anvendelig for kædesystemer, baseret på disketter, jf. *U 1996.356 Ø*. En tilsvarende regulering gælder formentlig også, hvis der foretages indsamlinger ved hjælp af kædebreve distribueret via e-mail. En sådan indsamling skulle i givet fald understøttes af en elektronisk betalingsordning. Der har vistnok endnu ikke været eksempler herpå, men dette kan meget vel ændre sig, når der – i en næppe fjern fremtid – indføres almindelige systemer til såkaldte "mikro-betalinger" på nettet.

15.3.d. Indholdskontrol

Det retspolitiske behov for at beskytte forbrugere og andre præsumptivt svage kommunikationsparter (f.eks. børn) mod visse tilfælde af påtrængende markedsføring m.v., diskuteres i disse år i forskellige internationale fora, bl.a. i EU og OECD. Drøftelserne har nær sammenhæng med drøftelserne om mulighederne for at kontrollere spredning af strafbare informationer (børnepornografi m.v.) samt ophavsretlige krænkelser. Der er et stort behov for, at disse forskelligartede reguleringsinitiativer koordineres bedst muligt, så man undgår forskellige løsningsmetoder på basalt set ensartede problemstillinger.

CDA-sagen

De problemer, der er forbundet med at gennemføre indholdskontrol på Internet, belyses ved den sag, der fandt sin afgørelse ved en dom afsagt af USA's Supreme Court den 26. juni 1997 i

sagen *Reno v. American Civil Liberties Union* (200 U.S. 321). Ved dommen erklærede Supreme Court to bestemmelser fra the Communications Decency Act of 1996 (CDA) for ugyldige som stridende mod den amerikanske forfatning. Den ene bestemmelse – Title 47 U.S.C.A §243 (a)(1)(B)(ii) – kriminaliserede den bevidste spredning af meddelelser, der kan karakteriseres som "obscene or indecent" til modtagere under 18 år. Samme lovs sec. 223 (d) forbød den bevidste videresendelse af enhver meddelelse til personer under 18 år, som "in the context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." Sagen var rejst mod den amerikanske regering af en række borgerrettighedsorganisationer, som gjorde gældende, at de citerede bestemmelser ikke alene var vage og upræcise, men også umulige at håndhæve, og at de derfor ville være ensbetydende med, at ytringsfriheden på Internet ville blive stærkt begrænset.

Dommen indeholder en interessant analyse af Internet som kommunikationsmedium sammenlignet med radio og tv, og selvom Internet ikke på nuværende tidspunkt har samme udbredelse i befolkningen som disse medier, lægges det til grund, at en begrænsning af kommunikationsstrømmen på Internet vil få betydning for den almindelige udveksling af information i samfundet. På denne baggrund fandt retten ikke, at en så upræcis begrænsning i adgangen til informationsspredning som den, der er gennemført ved CDA, var forfatningsmæssig, og med en slet skjult kritik af det lovgivningsmæssige forarbejde, der ligger i CDA, fastslog retten, at der heller ingen fortilfælde er i USA for en så indgående begrænsning i ytringsfriheden. Tværtimod ville en sådan begrænsning afskrække borgerne fra brug af dette middel af frygt for ubevidst at forvolde overtrædelser af denne lov (der i parentes bemærket gav hjemmel for frihedsstraf op til to år). Dommen er omtalt af *Mette Lundberg & Birgitte Maare* i Justitia nr. 4, august 1997, s. 23 ff.

15.4. Certificering

15.4.a. Begrebsafgrænsning

Et certifikat er en erklæring om et produkts faktiske beskaffenhed, der er udstedt af en uafhængig person eller myndighed, og som tilsigter at skabe tillid til bestemte aspekter af det pågældende produkt. Som begrebet hermed er afgrænset, er der mange typer af erklæringer, der falder inden for, uanset hvilken terminologi der anvendes.

Indenfor visse brancher betegner *verifikation* det samme som certificering. *Validering* sigter typisk til en skønsmæssig vurdering af, om et produkt er fuldstændigt og konsistent. En tredje betegnelse, der navnlig anvendes i relation til de markedsføringsretlige regler, er *mærke*, se herved generelt Mærkningsudvalgets redegørelse af juli 1999, der kan findes på Forbrugerstyrelsens hjemmeside, <www.fs.dk>. Om disse og andre sondringer henvises til *Andrew Bradley* i Bernard de Neumann (ed.): Software certification (1989), s. 121. Ved skibsbyggeri kategoriseres forskellige skibstyper i klasser. Den erklæring, hvorved et skib konstateres at falde inden for én klasse betegnes ofte med termen *klassifikation* anvendt i samme betydning. Se herom *Per Brunsvig*: Konstruksjonsansvar ved bygging af skip (Oslo, 1973), s. 48 ff. I EF-sammenhæng benyttes *overensstemmelsesvurdering* som samlebegreb for såvel den private certificering som den offentligretlige kontrol f.eks. i form af de syn og attestationer, der foretages efter reglerne i færdsels- og bygningslovgivningen.

Grundlag

Udstedelse af et certifikat, certificering, sker altid på et grundlag, der er bestemt på forhånd. Certificeringen har netop til formål at godtgøre en overensstemmelse med en objektivt målelig norm for kvalitet eller sikkerhed. Certifikatet er bevismidlet for, at det pågældende produkt lever op til denne norm. Certificeringsgrundlaget tilvejebringes typisk – men ikke altid – af en anden instans end den certificerende. F.eks. fungerer Dansk Standard både som udsteder af standarder og som certificerende organ. Med rådets førnævnte henstilling af 7. april 1995 om ensartede kriterier for vurdering af informationsteknologisk sikkerhed (95/144/EF), EFT 1995 L 93/27, anbefales det medlemsstaterne at anvende the Information Technology Security Evaluation Criteria (ITSEC) som grundlag for certificeringsordninger. ITSEC foreligger som et særskilt dokument, der kan rekvireres hos Kommissionen (DG XIII/B.6 INFOSEC).

Certificering er et omdiskuteret emne. For mindre aktører i en branche, der ikke har råd til at etablere det apparat, der er nødvendigt for at opnå en certificering, vil krav om certificering indebære en teknisk handelshindring, der holder nogen ude fra det gode selskab. Ikke desto mindre blæser der kraftige vinde til fordel for de generelle certificeringsordninger. Dette industripolitiske styringsinstrument anvendes først og fremmest i EF-samarbejdet. Ved sin resolution af 7. maj 1985 om en ny metode i forbindelse med teknisk harmonisering og standarder (EFT 1985 C 136/1) påpegede Rådet, at EF's politik om at lade produktegenskaber og -kvaliteter definere ved hjælp af standarder måtte følges op af en politik for vurdering af overensstemmelsen. Dette er senere sket med Rådets afgørelse af 13. december 1990 (EFT 1990 L 380/13)

om modulerne for de forskellige faser i procedurerne for overensstemmelsesvurdering med henblik på anvendelse i direktiverne om teknisk harmonisering. Nævnes kan også Rådets resolution af 21. december 1989 (EFT 1990 C 10/1), der opfordrer til detaljerede initiativer med henblik på at tilvejebringe en global metode for overensstemmelsesvurdering.

15.4.b. Forholdet mellem certifikatudsteder og -modtager

Privatpersoner har som hovedregel ingen pligt til at indgå aftale med andre. Tværtimod kan man som hovedregel selv vælge, hvem aftalen skal indgås med, og hvad den skal gå ud på.

Denne hovedregel begrænses af de konkurrenceretlige regler, der undertiden pålægger aftaleparter, der besidder et monopol, en egentlig kontraheringspligt. I overensstemmelse hermed pålægger § 17 i bekendtgørelse nr. 1136 af 15. december 2003 om akkreditering af virksomheder til certificering af personer, produkter og systemer mv., akkrediterede virksomheder (certificeringsorganer) en pligt til efter anmodning at foretage certificering henholdsvis inspektion inden for akkrediteringsområdet.

Om der er pligt til at udstede certifikat, beror på den indgåede aftale og på certificeringsgrundlaget. Formodningen må være for, at certifikatudstederen har eksklusiv kompetence til at udføre et sagligt skøn, for så vidt der er grundlag for at fortolke certificeringsgrundlaget. Derimod vil organet være afskåret fra at lægge usaglige kriterier til grund ved afgørelsen af, om der skal gives certifikat. Klienten vil almindeligvis have en retlig interesse i at kunne få disse spørgsmål påkendt i et anerkendelsessøgsmål. De erstatningsretlige spørgsmål vedrørende certificering omtales i afsnit 18.2.c.

15.4.c. Den retlige ramme for certificeringen

Da et certifikat isoleret set er en ytring og dermed underlagt almindelige grundsætninger om ytringsfrihed mv., er der som udgangspunkt ingen retlige restriktioner i muligheden for at etablere et certificeringssystem. Derimod kan der være restriktioner i adgangen til at anvende et certifikat. Mfl. § 2, stk. 1, og § 3, afstikker f.eks. rammerne for, hvilke angivelser der må ledsage varer og tjenesteydelser. Der må ikke anvendes urigtige, vildledende eller urimeligt mangelfulde angivelser, som er egnet til at påvirke efterspørgsel eller udbud. Ved tilbuds afgivelse skal der

gives en efter ydelsens art forsvarlig vejledning, når denne er af betydning for bedømmelsen af ydelsens karakter, egenskaber mv. Bestemmelserne har været brugt i en sag om salg af pantebreve mod "pantebrevscertifikat", se *JÅF 1989.29*, der kritiserer disse certifikater for ikke at være tilstrækkeligt fyldestgørende.

§ 14 i lov nr. 602 af 24. juni 2005 om erhvervsfremme giver hjemmel til at regulere certificeringssystemer. Bestemmelsen giver erhvervsministeren hjemmel til at udstede regler om akkreditering (dvs. autorisering) af virksomheder, laboratorier og andre organisationer til teknisk prøvning, inspektion og certificering samt regler om inspektion og certificering af personer, produkter og systemer. Hjemlen dækker såvel Erhvervsministeriets egen ressort som andre områder (f.eks. ordninger til miljøstyring og miljørevision), idet regler uden for lovens område dog kun kan fastsættes efter aftale med vedkommende myndighed, § 10, stk. 3.

DANAK

Hjemmelen er udnyttet ved den førnævnte bekendtgørelse nr. 1136 af 15. decemer 2003. Bekendtgørelsen danner det formelle grundlag for den akkreditering, der udføres af DANAK ("Dansk Akkreditering") under Erhvervs- og Byggestyrelsen.

Bekendtgørelsen sondrer mellem certificering (dvs. konstatering og attestation) af henholdsvis personer, produkter og systemer. En *produktcertificering* udtaler sig om, hvorvidt et nærmere identificeret produkt, en service- eller tjenesteydelse er i overensstemmelse med en angiven standard eller anden specifikation; en *systemcertificering* udtaler sig om, hvorvidt en virksomheds kvalitetsstyringssystem er i overensstemmelse med angivne standarder eller andre specifikationer, og en *personcertificering* om, hvorvidt en persons kvalifikationer er i overensstemmelse med "angivne standarder eller andre specificerede krav".

Produkt-certifikater

Produktcertifikater kendes primært inden for hardware-området, hvor de indtil gennemførelsen af EU's certificeringspolitik har været varetaget mere eller mindre ukontrolleret af vidt forskelligartede private og halvoffentlige organer. Vanskelighederne ved at opstille kvalitative krav for edb-programmering har hidtil været til hinder for produktcertificering af software.

System-certifikater

Systemcertifikater vil typisk have grundlag i en kvalitetssikringsstandard. Et sæt toneangivende standarder for kvalitetsstyring ligger i ISO 9000-serien, der giver retningslinjer for, hvorledes en virksomhed kan udvikle et kvalitetsstyringssystem og gennemføre det i praksis. ISO 9000 standarden har tre undergrupper; ISO 9001, 9002 og 9003, hvoraf ISO 9001, der opstiller krav

ved udvikling/konstruktion, produktion, installation og service, har den største interesse for udviklingsvirksomheder.

15.4.d. Anvendelsen af certifikatet

Hovedbegrundelsen for at lade en virksomhed eller et produkt mv. certificere ligger i certificeringens værdi for markedsføringen. Derfor vil en certifikatmodtager almindeligvis ønske at lade certifikatet fremtræde overfor omverdenen. Markedsføringslovens regler om misvisende produktoplysninger mv. indeholder som allerede nævnt en vis regulering af produktangivelser mv. Andre – og mere væsentlige – regler følger af reglerne om garantimærker i fællesmærkeloven, lov nr. 342 af 6. juni 1991 om fællesmærker.

Garantimærke

Ifølge denne lovs § 1, stk. 1, er et fællesmærke enten et kollektivmærke eller et garantimærke. Sidstnævnte begreb defineres i samme bestemmelses stk. 3 som et særligt kendetegn, der tilhører en juridisk person, der fører kontrol med eller fastsætter normer for varer eller tjenesteydelser, og som benyttes eller agtes benyttet til de varer eller tjenesteydelser, der er genstand for kontrol, eller for hvilke normer er fastsat. Fællesmærker kan indehaves såvel af private organisationer mv. som af offentlige myndigheder. Varemærkelovens regler gælder for fællesmærker i det omfang, de efter deres beskaffenhed kan finde anvendelse, medmindre andet følger af fællesmærkeloven.

Anvendelsen af fællesmærker kan hæmme konkurrencen på en måde, der strider mod de konkurrenceretlige regler, jf. nærmere *von Eyben*: Monopoler og priser (1980), s. 49 f. Bl.a. for at modvirke sådanne effekter giver fællesmærkeloven hjemmel til at ophæve en fællesmærkeregistrering, hvis mærket strider mod almene samfundsinteresser, lovens § 8, nr. 2.

Ifølge § 25 i bekendtgørelse nr. 1136 af 15. december 2003 skal akkrediterede virksomheder anvende betegnelse og logo i overensstemmelse med bestemmelserne herfor. Nærmere regler om disse logoer er givet i bekendtgørelse nr. 9230 af 2. maj 2005 om DANAK's akkrediteringsmærke og henvisning til akkreditering.

15.5. Mærkningsordninger

15.5.a. Problemstillingen

I takt med det stigende behov for at regulere informationssamfundets retlige problemer gennem selvregulering er der opstået en række mærkningsordninger, som søger at løse forskellige typer af disse problemstillinger ad frivillighedens vej. Typisk søger disse ordninger at præcisere en retlig regulering gennem et regelsæt, som en brugerkreds præsenteres for i kraft af et ikon eller andet særligt kendemærke. I nogle af tilfældene udgør ikonet et *certifikat*, jf. om dette begreb og dets regulering, afsnit 15.4. I andre tilfælde tjener det blot som "pegepind" for det regelsæt, der tilsigtes lagt til grund for den pågældende relation. For nogle af ordningernes vedkommende er baggrunden herfor et *politisk* ønske om at regulere det pågældende problem. Andre er etableret på frivilligt *brancheinitiativ*, og ofte med udenlandsk forbillede.

Også genstanden for regulering kan variere. Nogle ordninger søger gennem inkorporering at gøre det muligt for parterne i et aftaleforhold på forhånd at vedtage nogle spilleregler for transaktionens gennemførelse, medens andre på forhånd fastslår, hvad den part, der henviser til regelsættet, agter at gøre i en eller flere henseender, f.eks. i relation til persondatabeskyttelse og sikkerhed. Et kendskab til reglerne vedrørende disse ordninger kan derfor kun opnås gennem studier af den enkelte ordning. I det følgende præsenteres nogle af de mere udbredte.

15.5.b. E-mærkningsordningen

Herhjemme har den såkaldte "e-kreds", der består af Dansk Dataforening, Dansk Handel & Service, Dansk Industri, Handelskammeret, Finansrådet, Forbrugerrådet, Foreningen for Dansk Internet Handel, HK, IT-brancheforeningen og ITEK, under medvirken af Erhvervs- og Forskningsministerierne udviklet en dansk mærkningsordning. Mærkningsordningen administreres af en særlig fond, e-handelsfonden, der ledes af et sekretariat (en "administrator") under E-kredsen.

Som nævnt i afsnit 5.2.c. er *e-mærket* skabt af en række organisationer, der repræsenterer brugere og leverandører i den danske e-handel. Baggrunden herfor har navnlig været ønsket om at reducere utrygheden vedrørende betaling og videregivelse af personlig information, som anses for at være en af de største barrierer for e-handelen. I princippet kan alle websites opnå retten til at

bruge e-mærket – blot de overholder de bestemmelser, der er fastsat af e-handelsfonden, og som knytter sig til forskellige led i en digital transaktion.

Hovedparten af disse regler gengiver gældende dansk ret, men enkelte går videre. Det gælder f.eks. forbuddet i pkt. D.6 mod at udsende nyhedsmateriale i chat-fora, og reglerne om elektronisk aftaleindgåelse i pkt. F. Andre af bestemmelserne præciserer lovgivningen. Se ligeledes pkt. D.6, der forbyder den erhvervsdrivende at integrere markedsføringsmateriale, der stammer fra tredjemand, i eget markedsføringsmateriale, eksempelvis ved brug af hyperlinks og/eller *frames*, hvis dette markedsføringsmateriale ikke lever op til retningslinierne.

15.5.c. WebTrust

WebTrust er en international mærkningsordning, der oprindeligt blev skabt i samarbejde mellem de amerikanske og canadiske foreninger af statsautoriserede revisorer (AICPA og CICA) i samarbejde med den private CA-virksomhed Verisign (Californien, USA). Herhjemme administreres ordningen af Foreningen af Statsautoriserede Revisorer (FSR). For at en virksomhed skal kunne opnå ret til at benytte WebTrust-logoet, skal den gennemgå en sikkerhedsundersøgelse hos en statsautoriseret revisor, der er særligt uddannet hertil (en såkaldt e-handelsrevisor), og som – hvis de fastlagte krav er opfyldt – afgiver en erklæring, der efter en 60 dages prøveperiode giver grundlag for udstedelsen af et certifikat. Denne erklæring skal herefter gøres tilgængelig fra virksomhedens hjemmeside. Recertificering skal ske senest hver 90. dag.

Nærmere oplysninger om WebTrust kan hentes fra	<www.aicpa.org> og <www.fsr.dk>.

15.5.d. TrustE

TrustE er en amerikansk baseret mærkningsorganisation, der hviler på et ideelt grundlag, og som har til formål at gennemføre certificering af hjemmesider med henblik på sikring af visse krav til persondatabeskyttelse. TrustE besluttede i november 1999 at placere sit europæiske hovedsæde i København i en særlig europæisk udgave, der tager højde for direktivet om persondatabeskyttelse. Dette er dog endnu ikke sket, og netop pga. direktivet om persondatabeskyttelse må det antages, at behovet for en sådan mærkningsordning er noget mindre presserende i EU end i USA.

Nærmere oplysninger om TrustE kan hentes på <www.truste.org>.

15.6. Produktsikkerhed

15.6.a. Produktsikkerhedsloven

På grundlag af et rådsdirektiv af 29. juni 1992 om produktsikkerhed i almindelighed (92/59/EØF), EFT L 228/24, er der i dansk ret indført en lov om produktsikkerhed, lov nr. 364 af 19. maj 1994 med senere ændringer. Loven, der kan ses som et offentligretligt modstykke til produktansvarsloven, indfører den almindelige regel, jf. § 8, at kun sikre *produkter* må bringes i omsætning, ligesom *tjenesteydelser* kun må udføres, hvis de er sikre. Et produkt er sikkert, jf. § 6, hvis det ikke indebærer sundheds- og sikkerhedsfare for personer eller ejendom, når det anvendes til det forudsatte formål eller på en måde, som det forventes at blive anvendt på.

Findes der ingen sundheds- eller sikkerhedskrav i lovgivningen, vurderes produktets eller tjenesteydelsens sikkerhed i forhold til følgende faktorer, jf. § 7, stk. 3:

1) en dansk standard, der er baseret på andre europæiske standarder end dem, der er omhandlet i stk. 2,
2) en dansk standard,
3) henstillinger fra Europa-Kommissionen, som fastlægger retningslinjer for vurdering af produktsikkerhed,
4) adfærdskodekser for produktsikkerhed inden for den pågældende sektor eller
5) andre relevante forhold, herunder den aktuelle viden og teknologi samt den sikkerhed, som brugerne med rette kan forvente.

Overtrædelse af pligten til kun at markedsføre sikre produkter er strafsanktioneret, jf. lovens § 27. Sikkerhedsstyrelsen, der ifølge lovens § 17, stk. 2, er udnævnt til residuel kontrolmyndighed efter loven (hvor særlig lovgivning ikke peger på anden myndighed), forestår kontrollen med produkters og tjenesteydelsers sikkerhed. Bl.a. kan styrelsen bestemme, at produkter mv. kun kan markedsføres med angivelse af nærmere oplysninger om sikkerhedsrisiko mv., ligesom den kan nedlægge påbud og forbud, og herunder stille krav til produkternes indhold, jf. nærmere §§ 11 – 13. Af særlig betydning er her den hjemmel, lovens § 12, stk. 1, giver kontrolmyndigheden til at pålægge en part, der har bragt et produkt i omsætning, der viser sig farligt, efterfølgende at give

oplysning om faren (og om hvordan denne kan forebygges), at afhjælpe forhold, som er årsag til faren, at trække produktet tilbage, og/eller at destruere produktet på forsvarlig måde. I tilfælde, hvor der nedlægges et påbud om tilbagekaldelse eller destruktion, suspenderes den frist for fremsættelse af køberetlige mangelsindsigelser, der følger af købelovens §§ 54 og 83, jf. produktsikkerhedslovens § 12, stk. 3.

Loven omfatter såvel produkter, der bringes i omsætning, som tjenesteydelser, der har tilknytning til et produkt, og uanset om der for produktet eller tjenesteydelsen betales vederlag. I bemærkningerne til forslagets § 1, stk. 1, hedder det, at tjenesteydelser ikke har noget præcist juridisk indhold i dansk ret, og at de er af meget forskellig karakter. Som eksempler på denne forskelligartethed nævnes håndværksydelser, transport, rådgivning, reparation og vedligeholdelse, leasing eller software-ydelser. Består den erhvervsdrivendes ydelse alene i en arbejdspræstation, som f.eks. rådgivning af andre i tilknytning til liberalt erhverv, falder den uden for lovforslagets område.

IT-produkter har endnu ikke givet anledning til sikkerhedsmæssige problemer, der har fremkaldt særskilte initiativer efter produktsikkerhedsloven. De produktområder, hvor sådanne indsatser kan tænkes, er henholdsvis mus, se herom afsnit 14.3.b, og udstrålingsrisici fra mobilt apparatur, herunder navnlig GSM-telefoner. Men som her anført er der endnu for usikre oplysninger om de skadelige virkninger af disse produkter.

15.6.b. Elektrisk materielkontrol

Lov nr. om elektriske stærkstrømsanlæg og elektrisk materiel, jf. lovbekendtgørelse nr. 990 af 8. december 2003, opstiller en række sikkerhedskrav for anlæg til produktion, transmission og distribution af elektricitet med så høj strømstyrke, at der kan opstå fare, samt alle tilsluttede elektriske installationer, brugsgenstande og lignende.

Loven er en rammelov, der i §§ 6-7 giver Økonomi- og erhvervsministeren hjemmel til bl.a. at fastsætte bestemmelser om tilsyn og kontrol med stærkstrømsanlæg og el-materiel samt prøvning og certificering af el-materiel. De for praktikeren relevante bestemmelser herom findes i stærkstrømsreglementet – et digert ringbindsværk, der efter særlig anordning er undtaget fra kravet om offentliggørelse i Lovtidende. Heri finder man bl.a. regler om sikkerheden ved elektrisk materiel, herunder PC-udstyr.

15.6.c. Elektromagnetiske forstyrrelser

En række elektriske produkter afgiver en elektromagnetisk stråling, der kan forstyrre andre elektriske produkters funktion (støj på TV- og radiomodtagere mv.) og ligefrem få utilsigtede konsekvenser for kommunikative processer i sådanne produkter (f.eks. at signalet fra en trådløs telefon får lågen i en vaskemaskine til at springe op, så kogende vand fosser ud). Da den slags signalforstyrrelser kun opstår, når der foreligger en (utilsigtet) kompatibilitetsgrænseflade, siges der at være tale om et udslag af elektromagnetisk kompatibilitet eller EMC (= Electromagnetic Compatibility).

Loven om radio- og teleterminaludstyr og elektromagnetiske forhold, jf. lovbekendtgørelse nr. 912 af 5. november 2002, regulerer denne risiko. Loven udspringer af et EU-direktiv, Rådets direktiv af 3. maj 1989 om indbyrdes tilnærmelse af medlemsstaternes lovgivning om elektromagnetisk kompatibilitet (89/336/EØF), se EFT 1989 L 139/19, det såkaldte EMC-direktiv. Den gælder, jf. § 2, for markedsføring, ibrugtagning og tilslutning af radioudstyr, teleterminaludstyr og andre elektriske og elektroniske apparater. Sådanne apparater skal være konstrueret på en sådan måde, at de ikke frembringer kraftigere elektromagnetiske forstyrrelser, end at radio- og telekommunikationsapparater samt andre apparater kan fungere i overensstemmelse med deres formål, jf. § 5, stk. 1, nr. 1. Dernæst skal de have tilstrækkelig indbygget immunitet over for elektromagnetiske forstyrrelser, så de kan fungere i overensstemmelse med deres formål, og herunder overholde nærmere fastsatte regler herom (beskyttelseskrav), jf. § 5, stk. 1, nr. 2. Lovens regler suppleres med bekendtgørelse nr. 132 af 4. marts 2003.

Efter lovens nærmere regler må apparater kun markedsføres, tages i brug eller anvendes, hvis de følger disse krav, og når overensstemmelsen hermed er angivet ved EF-overensstemmelsesmærket (CE). I overensstemmelse med den nye metode i forbindelse med teknisk harmonisering og standarder, der blev indført i 1985 (se EFT 1985 C 136/01), anses overensstemmelseskravet for at være opfyldt, hvis apparatet følger nationale standarder til gennemførelse af de harmoniserede EMC-standarder eller nationale standarder, hvis referencer er blevet offentliggjort i EFT, når sådanne EMC-standarder ikke findes. Dermed er den praktiske udfyldning af direktivet overladt til den vesteuropæiske standardiseringsorganisation for elektronik (CENELEC), jf. nærmere direktivets præambel.

Ifølge lovens § 17 fører IT- og Telestyrelsen kontrol med reglernes overholdelse. Styrelsen kan bl.a. meddele påbud om tilbagetrækning af apparater fra markedet, herunder påbud om annoncering heraf, og påbyde, at apparater ikke længere må tages i brug eller tilsluttes, eller nedlægge forbud herimod.

15.6.d. Miljøregulering

Ifølge § 9j i miljøbeskyttelsesloven skal producenter og importører for egen regning foranstalte tilbagetagning samt genanvendelse eller særlig håndtering af affald af elektrisk og elektronisk udstyr (som nærmere defineret i lovens § 9i), som er markedsført af producenten eller importøren efter den 31. december 2005, medmindre der er fastsat andre regler i medfør af lovens § 44 og § 45, stk. 2. Denne forpligtelse kan også opfyldes gennem tilbagetagning samt genanvendelse eller særlig håndtering af samme mængde af tilsvarende udstyr markedsført i Danmark af andre producenter eller importører. Bestemmelsens stk. 2 fastslår, at forpligtelsen efter stk. 1 kan opfyldes gennem deltagelse i en kollektiv ordning. En sådan ordning er gennemført under navnet "Elretur" af en til formålet stiftet organisation for de elektroniske producenter (EPA), der som sine medlemmer tæller de væsentligste brancheorganisationer, herunder Brancheorganisationen for Forbrugerelektronik (BFE), Foreningen af fabrikanter og importører af elektriske husholdningsapparater og Dansk Industri/ITEK.

Ordningen, der forventes at træde i kraft den 1. april 2006, indebærer i korthed, at alt elektrisk og elektronisk affald skal skrottes via en ordning, som producenterne eller importørerne af det pågældende udstyr er ansvarlige for. Forbrugerne vil ikke mærke nogen væsentlig forskel, idet affaldet fortsat skal afleveres på de kommunale affaldspladser, men virksomhederne skal fremover finansiere den videre bortskaffelse. Se nærmere på <www.elretur.dk>. Reglerne indfører reglerne i det såkaldte WEEE-direktiv (Europa-Parlamentets og Rådets direktiv 2002/96/EF om affald af elektrisk og elektronisk udstyr med senere ændringer, se EFT 2003 L 37/24).

Miljøbeskyttelseslovens § 9j, stk. 3, giver i øvrigt miljøministeren adgang til at fastsætte regler om en *tildelingsordning* for affald af elektrisk og elektronisk udstyr fra husholdninger omfattet af stk. 1 og § 9l, stk. 1, herunder om den geografiske fordeling mellem producenter og importører, tidsfrister for afhentning og

udveksling af beholdere i forbindelse med afhentningen af det tildelte affald mv.

Ifølge lovens § 9n kan miljøministeren fastsætte regler om oprettelse af et *producentregister* om producenters og importørers pligt til at tilmelde sig registeret og om deres pligt til at indgive oplysninger hertil. Ministeren kan i den forbindelse fastsætte regler om, at distributører og forhandlere ikke må aftage og forhandle udstyr fra producenter og importører, som har tilsidesat registreringspligten, jf. stk. 2. Endvidere kan ministeren fastsætte regler om producentregisterets bearbejdning og videregivelse af oplysninger, herunder om hvilke oplysninger producentregisteret skal give til ministeren eller en anden offentlig myndighed, samt om at oplysninger kun må videregives i bearbejdet form, stk. 3.

Supplerende litteratur

For en gennemgang af de generelle markedsretlige regler henvises til den almindelige lærebogslitteratur, herunder *Koktvedgaard*: Lærebog i konkurrenceret, 4. udg. (2003), navnlig kapitel 11 om markedsføringslovgivningen, samt *Palle Bo Madsen*: Markedsret, Del 2, 3. udg. (2003), kapitel 5. Se ligeledes kapitel 7 i Erhvervsministeriets redegørelse: Forbrugerens retsbeskyttelse i grænseoverskridende digitale net (juni 1997), *Lars Stoltze*: Internet Ret (2001), kap. 7 og *Peter Blume & Mette Reissmann:* Beskyttelse af forbrugeroplysninger (2003).På Forbrugerstyrelsens hjemmeside, <www.fs.dk>, findes en række vejledninger om anvendelsen af de almindelige forbrugerbeskyttelsesregler i relation til elektronisk handel. Derudover kan henvises til den af Forbrugerrådet og Foreningen for Dansk Internet Handel oprettede hjemmeside <www.forbrugersikkerhed.dk>.

Kapitel 16. ELEKTRONISK DOKUMENTHÅNDTERING

16.1. Problemstillingen

16.1.a. Papirdokumentet og det digitale medium

Mediets funktion

Hvor det kan være en enkel sag at konstatere, om et dokument er blevet forfalsket, kan en digital meddelelse – som nærmere udviklet i afsnit 4.2.a. – på et magnetisk medium forfalskes til perfektion. Det ene eksemplar af meddelelsen er fuldstændigt identisk med det andet. En bevisførelse om, hvornår meddelelsen blev afsendt og modtaget, kan som regel ikke foretages ud fra det anvendte medium (ofte vil der tilmed ikke være ét, men mange medier). Den vil ofte skulle basere sig på en række oplysninger fra det informationssystem, der er anvendt (i form af primære filer, logfiler mv.). Dermed får ikke alene bevisførelsen, men også dokumenthåndteringen en ganske anden karakter end i papirets verden: Fokus retter sig imod disse omkringliggende systemer og deres opbygning.

Lovgivning

Lovgivningen indeholder enkelte regler om disse forhold – regler, der inden for hver deres område gør det muligt at håndtere forpligtende meddelelser ved brug af digital teknologi. Uden for området af sådanne særregler har praksis udviklet sig inden for rammerne af de tidligere lovgivningssystemer, uden at særlige lovændringer har været nødvendige.

I dette kapitel præsenteres en række af de problemer, der opstår ved overgangen fra papir til papirløs håndtering af forpligtende meddelelser. Som det vil fremgå, berører denne problemkreds emneområder, der systematisk hører til andre kapitler af denne fremstilling. Fremstillingen må således læses med skelen til de tekniske problemer (kapitel 4), de databeskyttelsesretlige (kapitel 13) og de strafferetlige (kapitel 17). De problemer, der i øvrigt indgår i læren om digital dokumenthåndtering, berører såvel formueretlige (se herom afsnit 16.2), procesretlige (afsnit 16.3) som forvaltningsretlige (afsnit 16.4) regler. Særligt omtales

de nye regler om elektronisk signatur (afsnit 16.5) og om elektronisk bogføring (afsnit 16.6).

16.1.b. Sikkerhed og dokumenthåndtering

Som hermed antydet beror mange af de problemer, der opstår ved overgangen fra papirhåndtering til digital informationsteknologi, på hvor *sikkert* et digitalt informationssystem anses at være til den pågældende anvendelse. Som nærmere udviklet i afsnit 4.1.d. er der sjældent noget absolut udtryk for, hvilken løsning der er "sikker" til et bestemt formål. Der er tale om en afvejning, der må foretages på ledelsesplan ud fra en overvejelse af, hvad sikkerheden (*benefit*) koster (*cost*).

Tinglysningsvæsenet er et eksempel på et område, der gennem tiderne har stået overfor nye typer af medier og hvor man har skullet træffe den slags afvejning på grund af skiftende tiders formkrav i form af skriftlighed og dokumenttvang. Studerer man den retspraksis, der findes herom, samt de bagvedliggende hensyn, ses det klart, at domstolene snarere anser det for afgørende, om den nye teknologiske løsning, der er tale om at skulle tage til sig, har opnået en sådan *indarbejdelse*, at der i bredere kredse knytter sig lid til den, end om sagkyndige erklæringer kan føres frem til støtte for, at der er tale om "sikre" teknologiske løsninger.

"Varig skrift"?

Et illustrerende eksempel herpå foreligger med Højesterets kendelse i *U 1959.40 HKK*, der for første gang tillod brug af kuglepen som medium til at underskrive et privat pantebrev. Landsretten, der havde stadfæstet tinglysningsdommerens afvisning af et skadesløsbrev underskrevet med kuglepen, havde ved sin kendelse i *U 1958.443 ØLK* afvist at anerkende en kuglepen som medium for "tjenestlige udfærdigelser", og man havde en vis støtte herfor i Justitsministeriets cirkulære nr. 702 af 30. august 1948. I landsrettens begrundelse henvises til interessen i "at sikre bevisforholdene med hensyn til ægtheden af udstederens underskrift på et dokument, der ønskes tinglyst", hvilket førte til et krav om "at underskriften er skrevet med varig skrift". Efter de oplysninger, retten var i besiddelse af, nærede man tvivl om, hvorvidt skrift med kuglepen opfyldte dette krav. Disse bevisforhold forelå anderledes i Højesteret, der henviste til, at "kuglepenne i betydeligt omfang anvendes til skriftlige udfærdigelser, hvortil der tidligere benyttedes pen og blæk". Højesteret fandt herefter ikke, at der forelå betænkeligheder ved at anerkende underskrifter med kuglepen.

I lyset af den nuværende brug af kuglepenne kan det være fristende umiddelbart at anlægge en overbærende attitude til denne retsafgørelse. Imidlertid er det vigtigt at bemærke det grundlag, den er truffet på. Det førnævnte cirkulære af 30. august 1948 var således udstedt på grundlag af oplysninger hidrørende fra forsøg foretaget af Statsprøveanstalten med holdbarheden fra skriftprøver med kuglepenne. Disse forsøg viste, at denne skrift "selv efter kortere Tids Kvartsbelysning afbleges overordentligt stærkt". På grundlag af disse oplysninger havde Undervisningsministeriet den 15. januar 1948 udfærdiget en bekendtgørelse vedrørende autorisation af blæk mv. Tinglysningsdommeren og landsretten var dermed på linje med landsretspraksis. Allerede i *U 1928.340 VLK* var det slået fast, at tinglysningsdokumenter ikke kunne underskrives med blyant – en kendelse, der også er udtryk for gældende dansk ret i dag. Se nærmere om kendelsen min redegørelse i *Peter Garde m.fl.*: Mindeværdige retssager (2002), s. 93 ff. Se i øvrigt *U 2000.1869 VLK*, hvor et tilsvarende problem blev påkendt ved brug af IT-baserede tingbogsattester, og *U 2001.1980 HK*, der stadfæster Østre Landsrets afvisning i *U 2001.252 ØLK* af, at en begæring om tvangsopløsning af et andelsselskab kunne ske på grundlag af en maskinelt udskrevet anmodning, der ikke bar underskrift. Afgørelsen støttes på rpl. § 261, stk. 2, der stiller krav om, at et processkrift er underskrevet af en mødeberettiget partsrepræsentant. I SvJT 2005.273 ff. har *Per Fuhrberg* gennemgået de ideelle krav, der bør stilles til, at en myndighed (eller domstol) anerkender en "inkommande handling" i elektronisk form.

16.2. Formueretlige formkrav

16.2.a. Problemstillingen

Udgangspunktet

Som tidligere nævnt gælder det udgangspunkt i dansk ret, at aftaler er gyldige uanset deres form. At det er således, hænger sammen med flere forhold, der er fælles for de nordiske landes formueret: Aftaleretten er tæt forankret til viljesbetragtningen (forestillingen om, at en forpligtelse anerkendes som retligt gyldig, fordi den udspringer af en vilje til at være forpligtet), og efter den procesordning, der er gældende her, er der righoldige og fleksible muligheder for at dokumentere denne vilje. En underskrift på et stykke papir er én metode hertil, men langt fra den eneste.

Modifikationer

Dette historiske og retssystematiske udgangspunkt er dog i stigende grad blevet modificeret gennem talrige *lovkrav* om skriftlighed. I nyere tid er det primært beskyttelseshensynet (advarsels- og bevisfunktionen), der ligger bag sådanne krav. *For-*

brugerretten frembyder den mest righoldige samling af eksempler herpå, se f.eks. kreditaftaleloven § 8, forbrugeraftaleloven § 15, pakkerejseloven (§ 6) og lov om omsætning af fast ejendom (§ 10). Et andet væsentligt område er *lejeretten*. Ifølge lejelovens § 4 skal lejeaftalen udfærdiges skriftligt, såfremt en af parterne kræver det. Herudover indeholder lejeloven en række regler, der knytter formkrav til de forskellige påbud, der udveksles i en lejeaftale (f.eks. om opsigelser, lejeforhøjelser el.lign.). *Ansættelsesretten* er et tredje eksempel. Med loven om ansættelsesbeviser er der givet detaljerede regler for, hvilke vilkår i et ansættelsesforhold arbejdsgiveren har pligt til at give medarbejderen underretning om. Herudover finder man skriftlighedskrav i en række ansættelsesretlige love, se f.eks. funktionærlovens § 2, stk. 5, § 5, stk. 2, og § 18 og handelsagentlovens § 30.

Formål og funktion

Et krav om, at en privatretlig disposition, for at være gyldig, skal foreligge i en bestemt form, kan tjene vidt forskellige formål: Det kan sikre, at den forpligtede part er klar over konsekvenserne af sin forpligtelse og dermed lade den skriftlige manifestation fungere som et *advarselssignal*. Denne funktion understøttes f.eks. ved arvelovens regler om oprettelse af testamenter, hvor formkravet går ud på, at en tredjemand kontrollerer den disponerendes habilitet. Dernæst kan formkravet sikre *beviset* for, at en disposition havde et bestemt indhold, hvilket dels kan lette parternes efterfølgende sagsførelse, dels understøtte retspositioner overfor tredjemand. Der kan endelig være *administrative* grunde til kravet (f.eks. ønsket om at kunne håndtere en check eller veksel efter de særlige regler herom, at kunne tinglyse et dokument, der stifter rettigheder over fast ejendom, eller registrere en selskabsvedtægt), ligesom formkravet kan tjene *almene samfundshensyn* (som ved de konkurrenceretlige regler, der pålægger parter i visse konkurrencebegrænsende aftaler at anmelde disse). Ofte vil flere af disse hensyn, der generelt kan betegnes som *beskyttelseshensynet, bevishensynet, notoritetshensynet* og *publicitetshensynet*, spille sammen.

Herudover kan det være foreskrevet, at et skriftligt dokument skal præsteres under særlige former, f.eks. således at et dokument skal *vedkendes for en notar* og herefter udleveres. Den tyske forbundshøjesteret har således fastslået, at en garanti afgivet pr. telefax var ugyldig, se Zeitschrift für Wirtschaftsrecht 1993.424. Garanten havde vedkendt sig garantien for en notar, som havde videresendt den til beneficianten, der var bosat i Spanien, under den forudsætning, at det originale dokument ville blive eftersendt, hvilket ikke skete.

Virkning

I det omfang, der stilles formkrav, indebærer tilsidesættelse heraf i almindelighed *ikke ugyldighed*, se hertil *U 1970.298 H*, hvor parterne i et lejeforhold ikke som foreskrevet havde anvendt en statsautoriseret formular, jf. de førnævnte regler. Som nærmere udviklet nedenfor, vil det i almindelighed have formodningen imod sig, at en signatur skal foreligge ved egenhændig underskrift. Hvis blot en signaturform sikrer, at den forpligtede har villet tiltræde aftalen, må der være en formodning for, at forskelligartede signaturformer kan finde anvendelse.

Princippet om funktionel ækvivalens

Som hovedregel må det antages, at krav om, at der skal foreligge et "dokument", der fremtræder "skriftligt", almindeligvis også kan omfatte data lagret på digitale medier, f.eks. på disk, diskette eller på optiske medier (CD ROM mv.). Dette princip er i overensstemmelse med udgangspunktet i artikel 6 i UNCITRAL-modelloven om Electronic Commerce, der som tidligere nævnt kræver, at den digitale meddelelse, der ækvivalerer med et skriftlighedskrav, er "accessible so as to be usable for subsequent reference". Princippet er ligeledes lagt til grund i nyere lovgivning, men må formentlig gælde generelt, hvis ikke helt særlige forhold taler i modsat retning. Et eksempel på udtrykkelig lovhjemmel er pakkerejselovens § 6, der pålægger rejsearrangøren at give kunden visse angivne oplysninger "skriftligt eller på anden dertil egnet måde".

Se om dette krav betænkning 1240/1992 om pakkerejser, s. 142, med henvisning til den råds- og kommissionserklæring, der blev truffet i forbindelse med vedtagelsen af det bagvedliggende direktiv af 13. juni 1990 om pakkerejser mv. (90/314 EØF). Erklæringen, der er optrykt sst. s. 244, angiver, at kravet herom i direktivets artikel 4 kan opfyldes ved brug af digitale medier, forudsat at oplysningerne let kan forstås.

INCOTERMS

Det stigende ønske om at anvende digital teknologi til at understøtte aftalehåndteringen i kommercielle forhold førte allerede i 1990 til en ændring af de standard handels-klausuler (såkaldte INCOTERMS), der er udsendt af ICC til brug for den internationale handel, og som senest foreligger i en udgave fra 2000. Efter den således indførte nye formulering sidestilles fremskaffelse af skriftlige udfærdigelser som f.eks. en salgsfaktura mv. med "den tilsvarende elektroniske meddelelse". INCOTERMS suppleres på dette område af de regler, som Comité Maritime International (CMI) har vedtaget med titlen "Rules for the Electronic Transfer of Rights to Goods in Transit", der vil gøre det muligt at afskaffe det fysiske konnossement til fordel for EDI-løsninger.

16.2.b. Det digitale originaldokument

Det digitale medium kommer imidlertid til kort på formuerettens område, når lovgivningen knytter retsvirkning til selve *besiddelsen* af et dokument. I disse tilfælde knyttes retsvirkningerne til dokumentet – typisk fordi det tjener en *symbolfunktion*; den, der besidder dokumentet, besidder rettigheden.

Generelle principper

For at kunne anvende digital teknologi til dokumenthåndtering, hvor der gælder krav om ihændehavelse af originaldokumenter, kræves såvel tekniske som retlige redskaber. Det *tekniske* redskab vil være en troværdig tredjepart (f.eks. en værdipapircentral, et kontoførende pengeinstitut eller et tinglysningskontor), der alt efter øjemedet kontrollerer de dispositioner, der træffes vedrørende det pågældende aktiv. De *retlige* redskaber vil være indeholdt i de retsregler, der giver hjemmel til at erstatte tidligere krav om dokumentbesiddelse med meddelelsen til den troværdige tredjepart. Retlige systemer, der ikke forudsætter en sådan tredjeparts tilstedeværelse, vil ikke kunne håndtere krav om negotiabilitet.

Omsætningsgældsbreve

Dette problem gør sig gældende i relation til omsætningsgældsbreve, hvor kravet om dokumentindehavelse indebærer, at de let kopierbare digitale meddelelser – der i praksis aldrig eksisterer som "originaldokumenter" – må frakendes retlig gyldighed: At antage, at en skyldner gyldigt kunne udstede et omsætningsgældsbrev ved e-post, ville være ensbetydende med, at enhver indehaver af en kopi af denne e-mail ville være legitimeret til at oppebære fordringen, jf. gbl. § 19, og hævde ret til den i rettighedskonflikter, jf. gbl. § 14. Ligeledes savner det mening at forlange "udlevering" af gældsbrevet ved indfrielse, jf. gbl. § 21.

Transportdokumenter

Den manglende mulighed for at udstede digitale gældsbreve spiller ikke den store rolle for det praktiske forretningsliv. Uden for pantebrevenes verden (hvor der i praksis altid vil ske tinglysning) er det forholdsvis sjældent forekommende, at der indtræder kreditorskifte, og det er først og fremmest i disse situationer, at negotiabilitetsreglerne har praktisk betydning. Et større praktisk problem volder den manglende mulighed for at etablere "digital negotiabilitet" for transportdokumenter som f.eks. konnossementer. Da sådanne dokumenter ofte må transporteres fra sted til sted, er der navnlig i den internationale handel og transport et stort behov for at kunne erstatte dem med digital transmission.

En grundig, men nu tildels forældet, gennemgang af problemerne vedrørende digitale konnossementer, findes hos *Boris Kozolchyk*: Evolution and Present State of the Ocean Bill of Lading from a Ban-

king Law Perspective, 23 Journal of Maritime Law and Commerce (1992), s. 161-245. Et større projekt vedrørende digitale konnossementer, kaldet BOLERO, er i disse år under opbygning i regi af den internationale maritime organisation (CMI), jf. nærmere <www.boleroltd.com>. Om muligheden for at anvende papirløse billetter efter de skriftlighedsregler, der gælder for international luftbefordring af passagerer (jf. luftfartslovens § 92), se *Peter Lyck* i U1997B.559 ff.

VPHL

Ved lov om værdipapirhandel mv., jf. lovbekendtgørelse nr. 1269 af 19. december 2003 med senere ændringer, er der nu givet almindelig hjemmel til, at private pantebreve kan registreres i elektronisk form med bevarelse af de negotiabilitetsregler, der følger af gældsbrevsloven. Ifølge § 1, stk. 1, gælder loven for "værdipapirhandel", men § 2, stk. 1, nr. 11, lader også lovens bestemmelser om værdipapirer finde anvendelse på "omsættelige pantebreve med pant i fast ejendom eller løsøre". Når lovens § 59, stk. 1, derfor giver hjemmel for, at værdipapirer kan udstedes og overdrages i papirløs form (dematerialiseret) som fondsaktiver, der er registreret i en værdipapircentral (§ 59, stk. 2), betyder dette, at de centrale virkninger i lovens kapitel 22 om retsvirkninger af registrering mv. også gælder for disse omsættelige pantebreve. Denne adgang til at udstede pantebreve gennem en værdipapircentral benyttes dog – endnu? – ikke i praksis.

Simple fordringer

Simple fordringer behøver ikke at foreligge på skrift. Et telegram eller en telexmeddelelse anses almindeligvis at opfylde det krav om skriftlighed, der ligger til grund for gældsbrevsloven, se nærmere *Lynge Andersen m.fl.*: Gældsbrevsloven med kommentarer (1997), s. 31. Det er imidlertid værd at påpege, at reglerne om simple fordringer ved at lade skyldneren være centrum for denunciation mv. netop opererer med skyldneren som "troværdig tredjepart", om end med den modifikation at skyldneren som betaler af den pågældende fordring jo indtager en ganske central placering i transaktionen!

16.2.c. Underskriftskrav

Det hører til undtagelsen, at formueretlige lovregler stiller krav om, at et dokument er underskrevet, hvis ikke man befinder sig på et område, hvor der gælder lovregler, der knytter ihændehavervirkninger til dokumentet (jf. således checklovens § 1, nr. 6 og vekselloven § 1, nr. 8). En sådan hjemmel findes f.eks. i kreditaftalelovens § 36, stk. 1, nr. 1, hvorefter den ejendomskøbekontrakt, der giver adgang til tilbagetagelse af det solgte, skal være skriftlig og underskrevet og stiller krav om, at underskriveren får genpart heraf.

Andre underskriftsregler må derimod betragtes som rene ordensforskrifter. Et eksempel herpå er handelsagentlovens § 3, der giver de respektive parter i en aftale om handelsagentur ret til fra den anden part at få udleveret et underskrevet eksemplar af den indgåede aftale.

Man kan overveje, om krav herom skal indfortolkes i de almindelige skriftlighedskrav, der gælder på området. Som anført i *GA* s. 230 f., kan et sådant krav ikke opstilles. Kan det godtgøres på anden vis, at dokumentet er vedkendt, må skriftlighedskravet anses for opfyldt alene ved den skriftlige udfærdigelse. Derimod vil underskriften i almindelighed udgøre et ganske håndfast bevis for, at et dokument er tiltrådt, sml. *U 1990.485 VLK*. Omvendt er selve det forhold, at der befinder sig en underskrift på et dokument, ikke noget endegyldigt bevis for, at dokumentet er tiltrådt, sml. *U 1978.373 VLK*, hvor underskriften var placeret på en side, der ikke angav det omtvistede vilkår om ejendomsforbehold. Vilkåret fandtes følgelig ikke tiltrådt.

16.3. Domstolsprocessen

16.3.a. Formkrav

En række retsplejebestemmelser foreskriver eller forudsætter, at en processuel handling fuldbyrdes i dokumentform. Sådanne regler tjener forskellige typer af formål, hvoraf man navnlig kan fremhæve to. Det ene – *ordensmæssige* – spiller den største rolle: Det dokument, der modtages, skal kunne håndteres på en måde, så der ikke lægges urimelige administrative byrder på domstolsvæsenet og modparten. Dette taler i sig selv for en praksis, hvorefter dokumenter overføres på A4-papir. Det andet hensyn er *sikkerhedsmæssigt*: Der skal være klarhed om, hvorledes parterne har disponeret under processen, og – når der gælder tidsfrister herfor – ikke mindst *hvornår* dette er sket. Ellers risikerer man, at en part kan effektuere en proceshandling på en måde, som modparten ikke er i stand til at overskue, og under omstændigheder, hvor han måske tilmed kan fragå den pågældende disposition. Begge hensyn spiller en særlig rolle omkring tidsfrister, hvor det er vigtigt, at parternes dispositioner kan erkendes og tidsfæstes.

Telefax

Danske domstole har vist stor beredvillighed til at udvikle nye retsprincipper, når nye teknologiske medier har gjort deres indtog i retssystemer. Allerede ved dommen i *U 1907.530 LoST* antoges det, at en skyldner kunne indgive begæring om konkurs telegra-

fisk. I *U 1991.411 HKK* lagde Højesterets kæreudvalg til grund, at en ankefrist var overholdt, selv om ankestævningen alene var sendt pr. telefax til landsretten inden fristens udløb. Stævningen opfyldte de formelle krav, og originaleksemplaret af stævningen blev modtaget dagen efter ankefristens udløb. "I hvert fald under de således foreliggende omstændigheder" fandt Højesteret ikke tilstrækkeligt grundlag for at afvise anken. Retten bemærker, at den nævnte procedure er i overensstemmelse med en praksis, der efter det oplyste hidtil er fulgt af begge landsretter. Dommen i *U 1993.532 ØLK* antager, at ankestævning pr. telefax også kan afbryde eksekutionsfristen. I *2001.2398 VLK* kunne en kære indgivet ved telefonopringning til dommerkontoret ikke antages med den begrundelse, at kære alene kan ske ved indlevering af kæreskrift og ved, at kære fremsættes mundtligt til retsbogen.

- maskinen optaget

Efter praksis bærer afsenderen risikoen for, at den telefaxmaskine, hvortil en telefax-stævning agtes transmitteret, er optaget. Dette er således slået fast i *U 2000.2461 HK*, der antog, at en ankestævning modtaget pr. telefax på ankefristens sidste dag efter kontortids ophør ikke var rettidig, idet det måtte være den ankendes risiko, at telefax-maskinen havde været optaget allerede fra kl. ca. 15.30. Resultatet er velbegrundet: at tillade en fremsendelse efter tidspunktet for fristens ophør ville for det første være i direkte modstrid med fristbestemmelsernes ordlyd. For det andet støttes resultatet af almindelige risikobetragtninger: det forekommer i sagens natur, at telefax-apparater (ligesom telefoner mv.) er optaget. Jo tættere man nærmer sig tidspunktet for en frist, desto mere stiger risikoen for, at en optaget-situation bliver kritisk. Som den, der vælger tidspunktet for transmissionen, er afsenderen imidlertid nærmest til at bære denne risiko. I *U 2002.1383 ØLK* var kære iværksat ved telefaxskrivelse af 21. januar 2002 (fristens sidste dag), som imidlertid først blev efterfulgt af et originalt kæreskrift afsendt den 31. januar 2002. Landsretten fandt under de anførte omstændigheder, at kære var iværksat for sent, jf. rpl. § 394, stk. 2, jf. stk. 1. Se ligeledes *U 2003.58 H*, hvor en byretsdom var blevet anket ved telefaxankestævning af 2. november 2001 (en fredag). Da den originale ankestævning først blev modtaget i landsretten den 7. november 2001 – og dermed ikke var blevet ekspederet således, at den måtte forventes at være fremme første hverdag efter ankefristens udløb – fandtes anken at være for sent iværksat.

Se generelt om telefax-anker *Kim Trenskow* i Advokaten 2/1997, s. 30 ff., bl.a. med henvisning til utrykt praksis. Se ligeledes *Peter Seipel* i JT 1993-94, s. 374 ff. med omtale af *NJA 1993.308*, der afviser en telefax-anke.

- begrundelse

At netop telefax har vundet anerkendelse skyldes imidlertid dels, at der er tale om en teknologi, der baserer sig på velkendte og anerkendte *standarder*, dels at telefax-transmissionen resulterer i et papirdokument i et *format*, som uden videre kan danne grundlag for den videre papirhåndtering, sml. princippet i den førnævnte *U 1959.40 HKK*. Dermed har man i praksis kunnet indkapsle det kritiske spørgsmål til det principielle problem, om dokumenter, der er frembragt på denne måde, kan sidestilles med papirdokumenter.

Det er imidlertid væsentligt at fremhæve, at den førnævnte praksis om telefax-ankestævninger mv. alene tillader, at telefax-teknologien anerkendes som *fristafbrydende*. Praksis forudsætter, at en ankestævning efterfølgende fremsendes i underskreven form på papir. Det må formodes at være noget mere problematisk at skride til en mere fuldstændig elektronificering (via telefax) eller digitalisering af domstolenes dokumenthåndtering, således at processkrifter og bilag i det hele udveksles og behandles digitalt, f.eks. ved e-post. En sådan løsning vil kræve indgående overvejelser til sikring af, at alle berørte parter kan få det fornødne kendskab til dokumenternes indhold uden risiko for, at afgørende informationselementer er udeladt. Tilsvarende er tinglysningsvæsenets overgang til papirløs teknologi sket på grundlag af indgående forarbejder, der forholder sig til de tekniske, retlige og sikkerhedsmæssige problemer, der opstår i den forbindelse.

E-post?

Man kan derimod stille spørgsmålet, om en ankestævning tilsvarende også kan anses for fristafbrydende, når den modtages i form af en elektronisk post-meddelelse eller ved filoverførelse. Svaret herpå beror igen på, hvordan de pågældende systemer anvendes i praksis. Så længe der ingen sikker praksis findes om, hvilke formater der anvendes ved dokumentudveksling, vil der opstå risiko for efterfølgende tvivl om indholdet af det dokument, der overføres, sml. igen princippet i *U 1959.40 HKK*. I den udstrækning en sådan tvivl foreligger, vil der være risiko for, at det digitale dokument ikke repræsenterer en endelig og uigenkaldelig procesdisposition. Man må da afvise sådanne digitale dokumenter som fristafbrydende. Hvis – og når – der måtte dannes en almindelig praksis for, hvilke dokumentformater der kan udstedes digitalt mellem offentlige myndigheder, og hvilken sikring disse dokumenter skal forsynes med (f.eks. ved brug af en avan-

ceret elektronisk signatur baseret på et kvalificeret certifikat), vil denne risiko kunne reduceres, og en anerkendelse af sådanne digitale dokumenter som fristafbrydende må da være mulig.

I dette lys er det velbegrundet, at Østre Landsret i *U 2005.1413 ØLK* afviste en begæring om kære af en fogedkendelse, der var afgivet ved e-mail. I denne sag havde rekvisitus påkæret en arrestkendelse ved e-mail – et medium, som ikke opfylder retsplejelovens krav om skriftlighed og underskrift, jf. rpl. § 587, stk. 1, jf. § 393, stk. 3. Som begrundelse for afvisningen anfører landsretten, at e-mailskrivelsen "ikke [er] fulgt op med originalt kæreskrift", hvorfor kære ikke var iværksat inden kærefristens udløb. Det er nærliggende at læse denne bemærkning som en henvisning til den ovennævnte praksis om, at en anke iværksat ved telefax kan være fristafbrydende.

Et særligt teknologikontor i Domstolsstyrelsen tager sig af planlægningen af IT-initiativer ved domstolene; men tiltag af denne art er vanskelige at føre ud i livet, bl.a. fordi man vil kunne argumentere for, at en for stærk statslig styring af domstolene vil blive betragtet som stridende mod magtfordelingsprincippet i grundlovens § 3. I 1992 oprettedes Domstolenes Teknologiråd som et ledelsesforum bestående af repræsentanter for dommerne og Justitsministeriet og med den specifikke opgave at sikre det nødvendige grundlag for den overordnede planlægning af ledelsesbeslutninger vedrørende ny teknologi ved domstolene.

2004-reformen

Ved lov nr. 447 af 9. juni 2004 er retsplejeloven ændret på en række områder med det formål at understøtte brugen af digital teknologi i retsagsbehandlingen. Lovændringen er en opfølgning på regeringens handlingsplan fra 2002 om modernisering af formkrav i lovgivningen, og lovændringen indebærer, at formkrav om skriftlighed eller underskrift ikke længere kan være til hinder for, at meddelelser til retten kan sendes ved brug af digital kommunikation, f.eks. ved e-mail. En generel bestemmelse herom er indsat i rpl. § 148a, stk. 1. Det stilles dog som krav, at sådanne meddelelser er forsynet med en digital signatur. De nærmere regler herom fastsættes ved bekendtgørelse af domstolsstyrelsen, jf. stk. 2. I forbindelse med ændringen af retsplejeloven er der ligeledes sket ændringer af konkursloven (ved indsættelse af nyt kapitel 29a), i dødsboskifteloven (jf. det nye kapitel 31a) og i fællesboskifteloven (jf. §§ 92a-92b).

Meddelelser til retten

Lovreformen indeholder en række nye regler om meddelelser *til og fra retten*. Reglerne beskæftiger sig ikke med domstolenes adgang til at håndtere bilagsmateriale digitalt – et spørgsmål, der navnlig giver anledning til praktiske vanskeligheder i omfattende sager om økonomisk kriminalitet. Dette spørgsmål berøres i be-

tænkning 1454/2004 om Behandlingen af større sager om økonomisk kriminalitet mv., s. 92 ff., uden at der dog fremsættes forslag om en særlig lovgivning herom. Det antages vistnok generelt, at retten i kraft af sin almindelige procesledelse har adgang til at anordne digital dokumentbehandling i samråd med de procederende forsvarere og anklagere. For en nærmere drøftelse af de vanskeligheder, der er forbundet med en sådan procesform, henvises til *Lars Kjeldsens* indlæg i Lov & Ret, juli 2004, s. 14 ff. Ej heller fraviger lovreformen det almindelige krav om, at dokumenter i form af stævninger og bilag fremsendes i fysisk form. Det er alene "meddelelser", som nu opnår (en bestyrket) retsgyldighed.

Ifølge rpl. § 148a, stk. 3, anses en digital meddelelse for at være *kommet frem*, når den "kan gøres tilgængelig" for retten. Det afgørende er altså, at en medarbejder ved den pågældende ret har *mulighed* for at gøre sig bekendt med informationsindholdet i meddelelsen uden særlige anstrengelser. Fremkomsttidspunktet er altså ikke det tidspunkt, hvor medarbejderen ved retten rent *faktisk* har læst den pågældende e-mail mv. I stk. 4 er det dernæst bestemt, at en digital meddelelse, der ikke er forsynet med digital signatur eller er behæftet med andre fejl, der gør den uegnet til at indgå i rettens behandling af en sag, kan afvises af retten. Retten kan dog også beslutte at fastsætte en frist for afhjælpning af manglen. Beslutning herom kan efter begæring træffes ved kendelse.

Meddelelser fra retten

Lovændringen ændrer også reglerne om, hvorledes meddelelser fra retten skal gives til parterne. I tilknytning til den almindelige regel herom i rpl. § 154, stk. 1 (hvorefter det er rettens formand, der træffer beslutning herom, medmindre der gælder andre regler), kan der nu, jf. en ny stk. 2, anvendes digital kommunikation "hvis modtageren har samtykket i at modtage meddelelser på denne måde". Dette gælder dog ikke i de tilfælde, hvor der skal ske digital forkyndelse, jf. herom straks nedenfor.

Digital forkyndelse

Der er ligeledes indført regler om digital forkyndelse i § 155, hvis nye nr. 2 gør det muligt at anordne en sådan ved, at en meddelelse *gøres tilgængelig* ved digital kommunikation for den pågældende, der samtidig anmodes om at bekræfte forkyndelsen. Ordningen, der hjemlet i § 156a, minder om brevforkyndelse (se herom § 156): Forkyndelsen anses for sket, når den pågældende har bekræftet at have modtaget meddelelsen. Dette kan enten ske ved en meddelelse, der sendes digitalt (med anvendelse af digital signatur), eller ved at den pågældende sender en personligt underskrevet kopi af den forkyndte meddelelse. Forkyndelse anses

herefter for sket den dag, modtageren anfører at have modtaget meddelelsen. Er ingen modtagelsesdag anført, eller er den angivne modtagelsesdag senere end det tidspunkt, der er registreret som modtagelsesdato for den digitalt fremsendte bekræftelse, anses forkyndelsen for sket på den registrerede modtagelsesdag. Sendes kvitteringen pr. brev, anses poststemplets dato for afgørende.

16.3.b. Underskriftskrav

Procesdokumenter

En særlig problemstilling opstår i relation til den underskrift, der efter retsplejeloven kræves på et processkrift (stævning, ankestævning, svarskrift etc.). Det følger af rpl. § 261, stk. 2, at retten *ex officio* skal tilbagevise processkrifter, der er underskrevne af andre end parten og de i bestemmelsen nævnte mødeberettigede personer. Bestemmelsen er i *U 2001.1980 HK* fortolket således, at der skal foreligge en underskrift på et procesdokument, selv om dette udgår fra en myndighed, der ikke optræder ved advokat. I den pågældende sag havde Erhvervs- og Selskabsstyrelsen fremsendt en skifteretsbegæring om tvangsopløsning af et aktieselskab som en automatiseret maskinudskrift. Man kunne således ikke se, hvilken person der stod bag beslutningen (formentlig fordi denne var automatiseret). Afgørelsen kan dog næppe forstås således, at der i alle tilfælde skal foreligge en fysisk underskrift afgivet af en person. Havde Erhvervs- og Selskabsstyrelsen fremsendt den pågældende begæring med en facsimile-underskrift, burde den nok have været antaget, jf. den førnævnte praksis om inkassostævninger. Kravet kan muligvis udtrykkes således, at der skal foreligge en manifestation af en vedkendelseshandling fra dokumentudstederens (myndighedens) side, der på entydig vis kan føre dokumentet tilbage til en identificerbar person.

Når et dokument produceres pr. telefax, vil det kunne forekomme, at de første sider af dokumentet – uden underskriften – modtages før fristens udløb, medens det sidste – med underskriften – modtages efter.

I *U 1992.15 V* antog Vestre Landsret, at en anke ikke var iværksat rettidigt, da kun første side var modtaget inden ankefristens udløb, hvorimod siderne 2-4 kom efter. Denne praksis er dog fraveget ved *U 1995.767 V*, hvor anke ansås iværksat rettidigt, idet første side – bortset fra underskriften – indeholdt kravene til et kæreskrift. Den tidlige praksis var i overensstemmelse med praksis om underskrift ved ikke-mødeberettiget advokat: Advokatens underskrift følger almindeligvis på sidste side, hvor-

for man måtte nå til, at første side pr. definition ikke kunne opfylde de formelle krav. Senest har Højesteret i *U1997.358 H* fastslået, at en part, der efter iværksat telefax-anke undlader at fremsende en lovformelig *underskreven* stævning, bør have lejlighed til at afhjælpe denne mangel. Se også *U 1998.430 HK*, der i en situation, hvor landsretten ikke straks havde afvist en ankestævning med en underskriftsmangel, som straks var blevet afhjulpet, med rette fandtes at have admitteret anken.

En række amerikanske stater har indført lovgivning, der giver udtrykkelig hjemmel for at anvende fax som grundlag for processuelle erklæringer. Se herved *David A. Sokasits*: The long arm of the fax: service of process using fax machines. 16 Rutgers 531 (1990) og debatten i 53 Albany L.R. 143 ff. (rapport fra The commercial and federal litigation section of the New York State Bar Association) og 153 ff. Sverige synes ikke at anerkende telefax som medium for processuelle dokumenter, se NJA 1993.308 og *Seipels* kommentar hertil i 5 JT 374 (1993-94).

Inkasso

Domstolenes praksis med hensyn til anerkendelsen af alternative midler til *underskrift* har undertiden varieret fra retsområde til retsområde. Når det gælder underskrifter på stævninger – i hvert fald i inkasso-sager – anerkender man almindeligvis underskrift ved faksimile-stempel udvirket af det advokatkontor, der repræsenterer sagsøgeren. Denne velvillighed skal formentlig ses på baggrund af, at den part, der *anlægger* en sag, dermed ikke udsætter sig for andet retstab end de omkostninger, han i givet fald vil blive pålagt modparten – omkostninger, som advokatkontoret i givet fald indestår for, hvis faksimile-stemplet er anvendt med urette.

Tinglysning

Praksis går derimod i en anden retning på tinglysningsområdet. *U 1988.741 Ø* nægtede at lægge et faksimile-stempel til grund for en tinglysningsekspedition. Det kan herimod antages, at repræsentanter for visse virksomheder, der bærer personnavn, sædvanemæssigt signerer dokumenter hidrørende herfra ved med egen håndskrift at skrive dette navn (f.eks. "A.P. Møller" påført i hånden af en reder og medinteressent). Forskellen mellem disse tilfælde og faksimile-sagerne ligger i, at der her er tale om et personligt – og ikke automatiseret – navnetræk.

Se nærmere om praksis vedrørende faksimile-underskrifter, *Palle H. Dige* (1945), s. 85 ff. Se herved *Roger Henriksen* (1982), s. 39 f. Underskrifter, der påføres efter en sådan praksis, vil ligeledes kunne binde virksomheden. Se herved dommene i *U 1960.975 Ø*, hvor en egenartet underskriftspraksis ikke var registreret i handelsregisteret (tinglysning af pantebrevstransport nægtet), og *U 1961.662 Ø*, hvor registrering var sket (tinglysning gennemført). Som anført

s. 187 stiller tinglysningspraksis i visse henseende strengere krav til den underskrift, der afgives af et vitterlighedsvidne, end til udstederens egen underskrift.

Blankettvang

Derimod synes domstolene velvilligt indstillede overfor at skulle håndtere de krav om anvendelse af særlige blanketter mv., der følger af tinglysningsregulativerne, gennem brug af nye medier. Et eksempel herpå er kendelsen i *U 2000.1869 VLK*, der i en begæring om tvangsauktion anerkendte, at en tingbogsattest, der var trukket af den rekvirerende advokat via dennes IT-system, blev fremlagt. Landsretten fandt, i modsætning til fogedretten, at en sådan blanket måtte sidestilles med den i rpl. § 560, stk. 1, 2. pkt. omtalte tingbogsattest. I præmisserne, der i det hele henviser til den kærende advokats procedure, lægges det til grund, at de sikkerhedsmæssige betænkeligheder ved at anvende en sådan IT-baseret attest, dels er overskuelige (risikoen kan således udmåles til, at en panthaver ikke indkaldes lovformeligt, hvorved der i givet fald må berammes ny auktion), dels er lavere end ved anvendelse af en manuelt udfærdiget (fotokopieret) tingbogsattest.

16.4. Forvaltningsprocessen

16.4.a. Almindelige problemstillinger

Brugen af IT i den offentlige forvaltning rejser en række forvaltningsretlige spørgsmål, hvoraf hovedparten befinder sig indenfor læren om sagsbehandling. På det generelle plan kan der imidlertid være grund til at pege på, at det skisma, der almindeligvis præger forvaltningsretlig argumentation – nemlig modsætningen mellem effektivitet og retssikkerhed – ikke optræder i samme skikkelse, når problemet er, hvilke regler der bør regulere forvaltningens digitale dokumenthåndtering. Hensynene synes at gå hånd i hånd: På den ene side er der kolossale effektiviseringsgevinster at hente i systemer, der tillader borgerne "selvbetjening" via hjemmesider etableret i den offentlige forvaltning eller (som det har været foreslået) med den enkelte borger som centrum for en "personlig hjemmeside". Men hvis ellers de IT-sikkerhedsmæssige problemer kan løses, er der i tillæg hertil en betydelig retssikkerhedsmæssig gevinst at høste: Med moderne selvbetjeningssystemer kan borgeren få bedre *information* om de sager, han er involveret i, bedre *indblik* i, hvad det offentlige "ved" om ham, bedre *klagevejledning* og lettere vej til at effektuere forskellige *sagsbehandlingsskridt*, f.eks. ved klage mv.

Diskussionen om brugen af IT i den offentlige forvaltning har imidlertid kredset om andre temaer, hvoraf følgende tre fortjener særlig omtale.

Sikkerheds-spørgsmål

Det første tema drejer sig om de sikkerhedsmæssige krav, myndighederne skal opfylde: Hvem skal definere disse krav, og hvad skal kravene gå ud på? Denne problemstilling indebærer vanskelige grænsedragninger, fordi høj sikkerhed kan koste såvel besvær som penge. Problemerne herom behandles nærmere i kapitel 4.

Bestemmelsesret

Det andet spørgsmål drejer sig om, hvem der skal beslutte, hvilke administrative løsninger der skal gennemføres. Som udgangspunkt definerer den enkelte myndighed sin egen IT-strategi. Giver man imidlertid fri adgang til, at den enkelte myndighed opbygger sine særlige løsninger, risikerer man, dels at der opstår en række indbyrdes inkompatible løsninger, dels at der spildes dyre skattekroner, når hver enkelt myndighed skal "genopfinde hjulet". Vil man på samfundsmæssigt plan spare disse penge, må dette – direkte eller indirekte – ske på bekostning af den enkelte myndigheds selvbestemmelsesret.

Som anført i afsnit s. 245 frembyder en statslig central IT-styring vanskeligheder. De forsøg, der har været gjort på at samle denne styring i et centralt IT-ministerium, p.t. VTU-ministeriet, har kun kunnet fremvise beskedne resultater, se herved statusbilledet i mit indlæg i Kommunestyre i retlige rammer – en antologi i anledning af Kommunekredits 100 års jubilæum (1999) s. 94 ff. At der i de seneste par år for alvor er kommet fart i digitaliseringen af den offentlige forvaltning kan primært tilskrives en politisk vilje i Finansministeriet (nærmere bestemt den under ministeriet nedsatte Digitale Taskforce) til at sætte magt bag ønskerne om digitalisering, bl.a. gennem afholdelsen af de såkaldte "e-dage", se <www.e.gov.dk/edag>. Første "e-dag" var 1. september 2003, der blev sat som skæringsdato for offentlige forvaltningers overgang til digital kommunikation. "E-dag2" havde skæringsdato 1. februar 2005 og indebar krav om, at kommunikationen også kan sikres med henblik på følsomme og personlige oplysninger. Medvirkende til de seneste års mere effektive udvikling af den digitale infrastruktur er også, at projekter med digital forvaltning nu er forankret i de enkelte ressortministerier.

A og B-hold?

Et tredje, og i den politiske verden måske mest betydningsfulde, problem er bekymringen for, at man ved indførelse af digitale løsninger i den offentlige forvaltning, der tilgodeser nogle, men ikke andre, etablerer et skel mellem et *A-hold*, der i kraft af dets beherskelse af og adgang til IT har bedre muligheder for at "klare sig", og et *B-hold*, der ikke kan profitere af en sådan beherskelse og besiddelse. Hvilken valør dette hensyn har, beror i hovedsagen

på det klientel, der er tale om. Yngre, veluddannede personer vil sjældent nogen føle denne betænkelighed som særligt tungtvejende. Indvendingen kan være mere på sin plads overfor ældre persongrupper. Et krav om, at ansøgninger om folkepension blev afgivet digitalt og understøttet med en avanceret elektronisk signatur, ville uden tvivl medføre, at relativt mange af disse ansøgninger ikke blev indgivet med samme effektivitet som nu, hvor der anvendes papirbaserede ansøgningsblanketter.

Problemet med "A- og B-holdet" giver anledning til stor retspolitisk bevågenhed og har givet anledning til talrige politiske udredninger på højt plan. Fremtrædende eksempler herpå er Dybkjær/Christensen-rapporten om Info-samfundet år 2000 (1994), de herpå følgende årlige handlingsplaner og netværksredegørelser fra Forskningsministeriet samt senest rapporten om "Det digitale Danmark" (1999), jf. nærmere herom afsnit 5.1.c.

16.4.b. Formkrav til sagsbehandlingen

Pligt til at kommunikere digitalt?

I den offentlige ret skal der normalt være hjemmel til at stille skriftlighed som betingelse for at modtage og behandle en henvendelse. En sådan hjemmel bør følge af lov eller bekendtgørelse fastsat i medfør af lov. Sådanne hjemmelsbestemmelser er typisk givet af ordens- eller bevismæssige grunde. Det kan ikke antages, at myndigheden uden sådan hjemmel – som "anstaltsanordning" – kan stille formkrav, der håndhæves gennem fristregler. Netop hvis der er tale om at skulle anvende den slags sanktioner, må det kræves, at sådanne formkrav har udtrykkelig lovhjemmel. Se herved *FOB 2002.268*, hvor Ombudsmanden lagde til grund, at det kræver lovhjemmel at pålægge borgerne pligt til at benytte digital kommunikation ved henvendelse til offentlige myndigheder. Følgelig kunne et universitet ikke kræve eksamenstilmelding via Internet som en obligatorisk ordning.

Ret til at kommunikere digitalt?

Et andet spørgsmål er, om borgeren har *ret* til at fremsende en digital meddelelse til en myndighed i tilfælde, hvor brugen af det digitale medium ikke er udtrykkeligt foreskrevet i lovgivningen. Hvis ikke myndigheden er forberedt til at skulle håndtere digitale meddelelser, vil en almindelig pligt til at tage sådanne meddelelser under behandling på samme måde som skriftlige meddelelser kunne være forbundet med uforholdsmæssigt store omkostninger. Hertil kommer, at visse former for sagsbehandling kan håndteres langt enklere på papir (f.eks. på grundlag af ansøgningsskemaer, der fungerer som sagsomslag mv.) end digitale meddelelser – en risiko, der består så længe der ikke er gennemført veletablerede standarder i samfundslivet for digital kommunikation.

Endelig kan en almindelig adgang til at fremsende digitale meddelelser rumme risiko for, at myndigheden slet ikke kan erkende indholdet af det fremsendte.

Fortolkningen af formkrav

Der kan næppe opstilles klare regler om, hvorledes lovkrav om skriftlighed skal fortolkes i relation til digitale meddelelser, henholdsvis hvornår myndigheden kan dispensere fra dem. Da de fleste formregler er skrevet uden tanke på muligheden for at overføre meddelelser på andet end skrift, gælder der nok en formodning *mod*, at skriftlighedskrav skal fortolkes efter pålydende, hvis de hensyn, der ligger bag et krav om skriftlighed, kan varetages på anden vis, sml. praksis ovenfor om telefax-anke.

På visse retsområder ligger det dog klart, at indførelsen af et digital medium vil kræve tilbundsgående ændringer i retsgrundlaget, sml. herved overvejelserne i betænkningerne 1093/1987 og 1177/1989 (edb-tinglysning), 1394/2000 (papirløs tinglysning), 1190/1990 (om bilbogssystemet), 1001/1984 og 1144/1988 (databaser med retsinformation), 1400/2000 (formkrav og digital signatur), 1456/2004 (e-signaturs retsvirkninger) og 1461/2005 (varetagelsen af tinglysningsopgaven).

Henvendelser fra borgeren

Ifølge § 32a i forvaltningsloven kan vedkommende minister fastsætte regler om ret til at anvende digital kommunikation ved henvendelser fra borgeren til den offentlige forvaltning og om de nærmere vilkår herfor. Den pågældende bekendtgørelse kan herunder fravige formkrav i lovgivningen, der hindrer anvendelsen af digital kommunikation. Bestemmelsen giver imidlertid ikke i sig selv borgeren nogen ret til at anvende digital teknologi, lige så lidt som den pålægger borgeren nogen sådan *pligt*. Lovændringen er gennemført på grundlag af det forslag, der blev fremsat i betænkning 1400/2000, jf. bemærkningerne herom s. 720.

Henvendelser til borgeren

Loven indeholder ingen tilsvarende bestemmelse om myndighedens ret til at anvende digital kommunikation overfor borgeren. Spørgsmålet må finde sin løsning ud fra en vurdering af de interesser og hensyn, der spiller ind i forbindelse med den enkelte kommunikationshandling. I denne vurdering må navnlig bevismæssige hensyn og proportionalitetshensyn tillægges vægt. Jo mere indgribende en afgørelse er, desto større krav vil man stille til formalia. I *FOB 2001.290* kunne det under de foreliggende omstændigheder ikke kritiseres, at en ansøgning om uddannelsesorlov af en offentlig arbejdsgiver var besvaret med en e-mail; myndigheden burde dog enten have gemt en udskrift af sin e-mail eller gemt e-mailen i elektronisk form.

Autenticitet

I visse tilfælde knytter lovgivningen retsvirkninger til et autentisk dokument. Kopier af det kvalificerer altså ikke som selve

dokumentet. Dette gælder f.eks. for adkomst- eller bevisdokumenter (pas, kørekort), der kun forudsættes at eksistere i ét eksemplar, samt for dokumenter, der af ressourcemæssige eller andre grunde alene forudsættes at eksistere i et begrænset antal (pengesedler, rationeringsmærker). På disse områder kræver det som hovedregel særskilt hjemmel at fravige kravet om skriftlighed og autenticitet.

16.4.c. Underskriftskrav

Problemet

Talrige love og bekendtgørelser for den offentlige forvaltning foreskriver, at (skriftlige) henvendelser til forvaltningen skal være forsynet med underskrift. I papirets verden volder den slags formkrav sjældent vanskeligheder. Personer, der er fysisk ude af stand til at underskrive, vil som regel kunne gøre dette i kraft af en fuldmægtig eller værge. Og myndighederne vil ganske ofte vælge at anse dokumenter fremsendt pr. telefax for at omfatte disse krav.

Den digitale verden har ikke umiddelbart nogen ækvivalent til den håndskrevne signatur. Hvornår en regel om (papir)-underskrift skal erstattes med en elektronisk eller digital signatur beror derfor som udgangspunkt på fortolkningen af det underliggende regelgrundlag. I denne fortolkning spiller det navnlig en rolle, hvorledes den pågældende myndighed rent praktisk er i stand til at kunne verificere modtagne signaturer, altså om den har opbygget den fornødne public key infrastruktur (PKI).

LES § 13

Med LES § 13 er en begrænset del af denne usikkerhed søgt imødegået. Ifølge denne regel skal bestemmelser i lovgivningen, hvorefter *elektroniske* meddelelser skal være forsynet med signatur, anses for opfyldt, hvis meddelelsen er forsynet med en avanceret elektronisk signatur (jf. herom LES § 3, nr. 2), der er baseret på et kvalificeret certifikat (jf. herom LES § 4), og som er fremstillet ved brug af et sikkert signatur-genereringssystem (jf. herom §§ 14-15). Ved transmission af elektroniske meddelelser til og fra en offentlig myndighed gælder dette dog kun, såfremt andet ikke følger af lov eller bestemmelser fastsat i medfør af lov.

Det er vigtigt at understrege, at LES § 13 alene finder anvendelse inden for de tilfælde, hvor det ligger klart, at et underskriftskrav kan opfyldes ved brug af en elektronisk signatur. Bestemmelsen har således ikke betydning for spørgsmålet om, hvornår dette er tilfældet, jf. bemærkningerne ovenfor, ligesom den ej heller tager stilling til, om det relevante regelsæt implicerer andre formelle krav til den pågældende signatur. Derimod indebærer

bestemmelsen, at der ikke kan stilles strengere krav til elektroniske signaturer end de anførte. Dermed tilgodeses det harmoniseringshensyn, som ligger bag bestemmelsen, jf. den bagvedliggende artikel 5 i direktiv 1999/93/EF.

16.4.d. Journaliseringsregler

Der er endnu ikke dannet nogen fast praksis for, hvorledes elektronisk journalisering skal finde sted ved offentlige myndigheder. På grundlag af Ombudsmandens udtalelser om myndighedernes forpligtelser til at overholde "god forvaltningsskik" kan man udlede visse principper for denne adgang, se hertil Forskningsministeriets vejledning, Elektronisk Dokumenthåndtering og Forvaltningsregler (juni 1996), side 31 ff. og IT-sikkerhedsrådet: Digitale dokumenters bevisværdi, bilagshæftet, s. 129 ff. Den eneste begrænsning, offentlighedsreglerne sætter i adgangen til at digitalisere myndighedens dokumenter, ligger således i, at myndigheden må være i stand til at sikre de pågældende oplysninger og give adgang til dem ved brug af det relevante medium.

FOB 1997.198

Disse krav belyses i en udtalelse fra Folketingets Ombudsmand, som er gengivet i *FOB.1997.198*: En folkepensionist klagede til Ombudsmanden over kommunens brug af et forkert beregningsgrundlag for pensionen. Pensionisten havde i sin ansøgning om folkepension henvist til en allerede indgivet selvangivelse, som indeholdt de relevante oplysninger. Kommunen lagde imidlertid nogle automatisk overførte – og ukorrekte – oplysninger om den personlige indkomst til grund for beregningen, hvilket bevirkede, at pensionisten fik en mindre pension, end han var berettiget til. Kommunen og klageinstanserne erkendte fejlen. De afviste imidlertid at berigtige denne under henvisning til, at pensionisten havde udvist passivitet ved først at henvende sig til kommunen i foråret efter det pågældende pensionsår. Myndighederne fandt derfor, at pensionisten måtte bære risikoen for fejlen.

Den fejlagtige beregning (der i øvrigt var forholdsvis kompliceret i det pågældende tilfælde) fremgik af meddelelser, som pensionisten havde fået tilsendt i januar henholdsvis juli måned i pensionsåret. Under Ombudsmandens behandling af sagen viste det sig imidlertid, at kommunen var ude af stand til at fremlægge kopi af de omtalte pensionsmeddelelser. Meddelelserne var udskrevet fra et edb-register, og de oplysninger, som blev brugt til at danne meddelelser af denne type, blev slettet i registeret, når oplysninger vedrørende det følgende år var klar.

Ombudsmanden udtalte bl.a., at pensionistens henvisning til sin selvangivelse ikke fritog kommunen for at opfylde de almindelige forvaltningsretlige regler og retsgrundsætninger om sagsoplysningen (officialprincippet). Ombudsmanden mente endvidere, at det forhold, at pensionsmeddelelserne ikke kunne rekonstrueres, ville gøre det vanskeligt at afgøre, hvorvidt en hurtigere reaktion fra pensionisten kunne være krævet, og at risikoen for denne bevisusikkerhed måtte hvile på det offentlige. Ombudsmanden henstillede, at sagen blev genoptaget, hvilket skete, og fejlen blev berigtiget.

Sagen gav Ombudsmanden anledning til nogle generelle udtalelser om tilfælde, hvor myndigheden anvender digital dokumentbehandling. Med henvisning til en tidligere sag udtalte Ombudsmanden, at forvaltningsmyndigheder af hensyn til reglerne i forvaltningsloven og offentlighedsloven om aktindsigt og af hensyn til sikring af bevis bør sørge for, at der i myndighedens sager opbevares kopier af udgående post.

Efter Ombudsmandens opfattelse må det for at kunne overholde forvaltningsloven, offentlighedsloven og grundlæggende dokumentationskrav i forvaltningssager være et ubetinget krav, at en myndighed enten i sagen har en kopi af dokumenter, som myndigheden har udfærdiget, eller med sikkerhed med meget kort varsel fra et edb-anlæg vil kunne frembringe en fuldstændigt nøjagtig udskrift (svarende til en kopi) af dokumentet. Ombudsmanden udtalte endvidere, at en myndigheds valg af et elektronisk, i stedet for et papirbaseret, medium ikke berettiger en kassation af et dokument på et tidligere tidspunkt, end hvis det havde foreligget i papirform.

Om den konkrete sag bemærkede Ombudsmanden, at der for sager om folkepension er fastlagt en kassationsfrist på mindst 10 år, når det drejer sig om ikke afdøde personer.

16.4.e. Egenaccess og aktindsigt

Et vanskeligt afgrænsningsspørgsmål opstår i forbindelse med spørgsmål om aktindsigt i elektroniske dokumenter. Efter de nugældende regler beror dette spørgsmål på, om der foreligger et register eller en anden systematiseret fortegnelse, jf. offentlighedslovens § 5, stk. 2. Er dette tilfældet, gælder reglerne om egenaccess i LBP kapitel 9. Betragtes datasamlingen derimod som en elektronisk optegnelse mv., der ikke indgår i et "register", behandles den efter reglerne i offentlighedsloven, der ifølge § 5, stk. 1, nr. 2, også sikrer borgeren ret til aktindsigt i "indførelser i

journaler, registre og andre fortegnelser vedrørende den pågældende sags dokumenter". Se om afgrænsningen *Steen Rønsholdt*: Forvaltningsret – Retssikkerhed, proces, sagsbehandling (2001), s. 442 ff. og 470 ff. og *RÅB 1998.50*, hvor Registertilsynet udtalte, at adgangen til registerindsigt ikke omfatter oplysninger om logning af transaktioner, der er foretaget i et register.

De vidtgående svenske regler om aktindsigt ("tryckfrihet") har her ført til en anden praksis. Det er således antaget, at almenheden kan få adgang til *cookie-filer* genereret ved offentlige myndigheder ud fra den betragtning, at sådanne filer skal anses som "handlingar" (meddelelser), som er adresseret til den offentlige forvaltning, se herved Regeringsrättens dom 3148-1998 14. april 1998, der som begrundelse herfor henviste til, at cookie-filen ikke kan siges udelukkende at tjene en teknisk funktion, eftersom brugeren har mulighed for at slå denne facilitet fra. Problemet er omtalt i "E-post i förvaltningen – en rättslig översikt", Statskontoret 1999:3.

16.4.f. Fristregler

Problemer svarende til de, der har fundet deres afgørelse i praksis om telefax-ankestævninger, opstår i relation til hver af de talrige forskrifter, der fastslår frister for indgivelse af ansøgninger mv. Om sådanne frister kan opretholdes ved brug af elektronisk kommunikation – f.eks. i form af telefax eller elektronisk post – beror på en fortolkning af den enkelte forskrift. På det generelle plan er der næppe grundlag for at fremsætte andet og mere end en generel udtalelse om, at *almindelige* bevisretlige eller forvaltningsretlige regler i hvert fald ikke afskærer myndigheden fra at anerkende sådanne digitale henvendelser og – inden for samme rammer – at fastlægge en praksis for, *hvornår* sådanne dokumenter kan siges at være kommet frem.

Spørgsmålet er foreslået lovreguleret i Finland i november 1999, jf. i øvrigt om stillingen i finsk ret *Matti Niemivuo* i NAT 1999.93 f. med henvisning til den finske Högsta Domstolens dom af 9. juni 1997, der først anså en telefax-henvendelse for modtaget på det tidspunkt, hvor samtlige sider var modtaget, sml. for dansk ret *U 1992.495 V* om en frist for udøvelse af en forkøbsret.

I det omfang lovgivningen opstiller fristregler for modtagelse af skriftlige udfærdigelser, og sådanne udfærdigelser gyldigt kan indleveres ved brug af telefax, må man falde tilbage på de principper, der er udviklet ved domstolenes praksis for modtagelse af telefax. Et eksempel herpå er Fødevaredirektoratets afgørelse i *Tidsskrift for Landbrugsret 2000.138*, der antog, at en telefaxan-

søgning modtaget efter kontortids ophør på datoen for en frists udløb, var for sen.

Antages brug af e-post som fristafbrydende, må tidspunktet, hvor den pågældende e-post-meddelelse er *modtaget* af myndigheden, være afgørende. Se hertil *U 2001.25 99 Ø*, hvor en arbejdssøgendes afstempling med dagpengekort fandtes at være sket rettidigt, selv om der ikke var sket registrering i arbejdsformidlingens IT-system. Den pågældende arbejdsløshedskasse var følgelig berettiget til refusion af de udbetalte dagpenge. For en nærmere fastlæggelse af dette tidspunkt henvises til drøftelsen i afsnit 19.1.e om "fremkomst". Modtagelse af en e-post kan vanskeliggøres af uforudsete flaskehalsproblemer som følge af nettets overbelastning el.lign., og disse problemer vil ofte ikke være kendt af afsenderen. Derfor kan det – i relation til fristreglerne – være risikabelt at forlade sig på e-post-meddelelser som fristafbrydende. Risikoen for sådanne problemer påhviler afsenderen, jf. tilsvarende ovenfor om telefax-ankestævninger.

16.4.g. Arkivregler

Ifølge reglerne i arkivloven, lov nr. 1050 af 17. december 2002, skal myndighederne drage omsorg for varetagelse af arkivmæssige hensyn, herunder at arkivalier opbevares på betryggende måde. Omfattet af loven er offentlige arkivalier vedrørende al virksomhed, der udøves af den offentlige forvaltning og domstolene. Den omfattende arkiveringspligt begrundes først og fremmest med ønsket om at sikre landets historiske kilder for eftertiden. Loven kan dermed ses som en parallel til de regler om pligtaflevering, der er omtalt i afsnit 9.6.

Reglerne i arkivloven har i flere henseende IT-retlig interesse. For det første afføder de en række pligter for de offentlige myndigheder, der får virkning for, hvordan myndighederne indretter deres (elektroniske) arkiver. For det andet berører loven en række af de beskyttelseshensyn, der også varetages af loven om persondatabeskyttelse.

Arkivretten er imidlertid en så omfattende og kompliceret disciplin, at det ville føre for vidt her at behandle disse regler i enkeltheder. Til loven hører tre cirkulærer, alle af 8. marts 2002: Cirkulære nr. 25 om statslige myndigheders aflevering af elektroniske arkivsystemer til Statens Arkiver, cirkulære nr. 23 om anmeldelse af statslige myndigheders elektroniske registre (databaser) og cirkulære nr. 24 om anmeldelse og godkendelse af elektroniske journaler og elektroniske dokumenthåndteringssyste-

mer. En god indgang til retskildegrundlaget finder man på hjemmesiden for Statens Arkiver <www.sa.dk>.

I det følgende påpeges nogle enkelte dele af den retlige regulering.

Elektroniske arkiver

Arkivloven pålægger ikke myndighederne pligt til at anvende elektroniske arkiver. Det nærmeste man kommer en sådan pligt er bestemmelsen i lovens § 11, der giver kulturministeren hjemmel til – efter forhandling med VTU-ministeren – at fastsætte bestemmelser om, at "statslige myndigheder, der inden en nærmere fastsat dato ikke er overgået til elektronisk arkivering, skal betale for omkostningerne ved bevaring i Statens Arkiver af arkivalier, der efter den nævnte dato dannes på papir". Denne hjemmel er imidlertid endnu ikke udnyttet, og det er forudsat, at den først vil blive det efter en udredning, der iværksættes for at afklare, hvornår det vil være teknisk, økonomisk og organisatorisk forsvarligt at fastsætte en frist for overgang til elektronisk sagsbehandling og arkivering.

Lovens regulering af de elektroniske registre er herefter begrænset til § 8, stk. 2, hvorefter myndighederne skal drage omsorg for, at arkivalier, der er lagret på elektronisk medium, bevares således, at de kan afleveres til offentlige arkiver. De krav, der herved stilles, følger af de tre nævnte cirkulærer.

Ifølge cirkulære nr. 24 af 8. marts 2002 om anmeldelse og godkendelse af elektroniske journaler og elektroniske dokumenthåndteringssystemer må et elektronisk arkivsystem, som nærmere angivet i § 2, ikke tages i brug, før Statens Arkivers godkendelse foreligger, § 5, stk. 1. Cirkulæret gør det muligt for myndighederne at operere med systemer med elektronisk registrering af sager og dokumenter og arkivering af dokumenter *både* på papir *og* i elektronisk form, jf. § 2, nr. 2. For sådanne systemer fastslår cirkulærets § 6, stk. 2, at der skal være en klar organisatorisk eller emnemæssig afgrænsning af de områder, hvor der anvendes papirarkivering, og af de områder, hvor der anvendes elektronisk arkivering. Overgangen fra papirarkivering til elektronisk arkivering skal gælde *alle* dokumenter og sager indenfor det pågældende område og ske på samme dato.

Egenacces

Arkivlovens § 42 regulerer spørgsmålet om *egenacces*, dvs. personers ret til at få indblik i, hvilke oplysninger der fremgår om dem i arkiverne. Ifølge stk. 1 kan en person over for et offentligt arkiv fremsætte begæring om indsigt i oplysninger om den pågældende af den art, som er omfattet af LBP, og som er overført til opbevaring i det pågældende offentlige arkiv. Begæringen skal angive den myndighed, der oprindelig har behandlet de pågæl-

dende oplysninger. Angår den indsigt i private arkivalier, som er afleveret til et offentligt arkiv, og som er omfattet af LBP, træffer det pågældende arkiv afgørelse efter bestemmelserne i denne lov. Begæringen skal til dette brug angive den dataansvarlige, der oprindelig har behandlet de pågældende oplysninger. Ifølge lovens § 9 kan kulturministeren efter indhentet udtalelse fra Datatilsynet fastsætte nærmere regler om offentlige arkivers opbevaring af materiale af den art, der er omfattet af LBP.

16.5. Den elektroniske signatur

16.5.a. Problemstillingen

I afsnittene 4.2.d. – 4.2.f. præsenteredes den sikkerhedsløsning, der betegnes som digital signatur – en teknik, hvorefter digitale meddelelser forsynes med et digitalt "fingeraftryk", der forbinder dem med en part, der har vedkendt sig deres indhold. I omtalen af LES (afsnit 4.2.f.) var fokus lagt på den lovgivning, der på horisontalt plan (altså uanset hvilket formål signaturen understøtter) er gennemført herom.

I dette afsnit er fokus anderledes. Spørgsmålet er nu, hvilke retlige problemer der opstår for en organisation (det være sig privat virksomhed eller en offentlig myndighed), der ønsker at understøtte sin kommunikation overfor omverdenen med digital ("elektronisk") signatur.

16.5.b. Opbygningen af en PKI

Problemstillingen

Det nuværende tidspunkt af den teknologiske udvikling bærer præg af, at der ingen klar praksis er for, hvordan afsendere og modtagere af digitalt signerede meddelelser vælger at gå frem. Indtil sådanne typeforudsætninger danner sig – generelt eller inden for enkelte samfundssektorer – vil enhver beslutning herom uvilkårligt være et ledelsesanliggende. At ledelsen må tages på råd skyldes ikke alene de *økonomiske* konsekvenser, der kan være forbundet med utilsigtet afgivelse af sådanne meddelelser, men nok så meget de *organisatoriske* forandringer, denne teknologi nødvendigvis må medføre: I bund og grund er der tale om at erstatte et dybt indarbejdet medium (den mundtlige aftale, henholdsvis det skrevne ord) med en højteknologisk løsning, der kan forekomme usikker, og med en utvivlsom påvirkning af arbejdsprocesserne i virksomheden.

Udviklingsopgaven

Ofte vil ønsket om at etablere en sådan infrastruktur komme fra et led i organisationen, der har konstateret muligheden for herigennem at gennemføre besparelser eller effektivisering. Sideløbende med denne beslutning vil der allerede være taget stilling til, om den nødvendige infrastruktur vil skulle erhverves udefra, eller om den – helt eller delvis – skal baseres på egen udvikling.

Anskaffelsen

Kontraktsforhold om levering af en *public key infrastruktur* (PKI) kan tænkes varieret på mange måder. I nogle tilfælde vil leverandøren stille alle led i infrastrukturen til rådighed (softwareleverancer, tjenester til identitetskontrol, certifikat- og revokeringstjenester mv.); men ganske ofte vil brugeren se sin fordel ved at variere leverancerne, således at nogle ydelser erhverves fra én leverandør og andre fra en anden. Såvel ved indgåelsen af den slags aftaler som ved opbygningen af den nødvendige PKI vil der således ofte ske en rollefordeling, hvorved enkelte af disse funktioner fordeles mellem forskellige typer af virksomheder.

Som nævnt i afsnit 4.2.f. vil man ofte ønske at henlægge LRA-funktionen til en instans, der enten må formodes at have kendskab til nøgleindehaveren, eller som har særlige forudsætninger for at skaffe sig den fornødne sikkerhed for nøgleindehaverens identitet. For hver part, hvis rolle således udskilles, vil der være behov for et kontraktsforhold, der udtømmende fastslår de respektive parters roller, forpligtelser og ansvar overfor hinanden.

Signaturinstruks

Uanset hvilken fremgangsmåde der anvendes, vil disse strategiske beslutninger involvere en risikoafvejning, hvor sikkerhedshensynet afvejes overfor hensynet til at minimere udgifterne og besværet ved at gennemføre et højere sikkerhedsniveau. I IT-sikkerhedsrådets vejledning om praktisk brug af kryptering og digital signatur (2000), s. 27 ff., anbefales det, at ledelsen i den organisation, der står overfor beslutningen om at indføre digital signatur eller kryptering, gør disse spørgsmål til genstand for indgående overvejelser og nedfælder resultatet af disse overvejelser i en såkaldt *signaturinstruks*.

16.5.c. Hæftelsesspørgsmål

Et af de centrale spørgsmål i en signaturinstruks drejer sig om beslutningen om, hvem der skal kunne tegne organisationen digitalt. Selv om det er uklart, hvilken *hæftelse* en digital signatur påfører afgiveren, ligger vel så meget fast, at det som udgangspunkt er vanskeligere for afgiveren at fragå en meddelelse, der afgives utilsigtet med en digital signatur, end det er at fragå med-

delelser, der på anden vis utilsigtet eller retsstridigt afgives i den angivne persons navn.

Der er flere metoder, hvorpå disse hæftelsesforhold kan bringes til omverdenens kendskab.

Personlig signaturnøgle

Efter én metode kan den enkelte medarbejder underskrive meddelelsen med sin *personlige signaturnøgle*, f.eks. en signaturnøgle opnået i privat øjemed. Modtagerens sikkerhed for hæftelsesforholdene beror i så fald på andre forhold, f.eks. (verificerbare) oplysninger om, at den pågældende er ansat eller i øvrigt tilknyttet afgiveren på en måde, der giver beføjelse til at disponere som sket. Svagheden ved denne metode er, at modtageren af den signerede meddelelse i givet fald selv skal anstille de nødvendige undersøgelser, f.eks. ved opslag i offentlige registre. Omvendt må det siges, at denne svaghed også gør sig gældende i papirets verden, hvor der også består risici for kompetenceoverskridelser begået af den underskrivende person.

Attributcertifikat

En anden metode går ud på, at der udstedes særlige certifikater, kaldet *attributcertifikater*, hvis indhold netop går ud på at signalere overfor omverdenen, hvilken kompetence signaturindehaveren har. I regi af det Forum for Digital Signatur, der er etableret under Dansk Standard, er f.eks. defineret et såkaldt "medarbejder-certifikat", som angiver, hvorledes den enkelte medarbejder kan forpligte den organisation, hvortil han er tilknyttet. Fordelen ved denne løsning ligger i, at der skabes fuldstændig transparens overfor omverdenen om, hvorledes den enkelte signaturindehaver kan disponere. Ulempen er, at den øverste – eller i hvert fald tegningsberettigede – ledelse i den pågældende organisation skal "ulejliges" i forbindelse med udstedelse og fornyelse af de pågældende certifikater, der måske umiddelbart fremstår som en rent teknisk opgave.

Afdelingsnøgle

En tredje metode består i at etablere en *afdelingsnøgle* for den gren i den pågældende organisation, som signaturens afgiver er tilknyttet. Adgangen til at benytte denne nøgle styres da af systemer, der er indrettet til kun at give adgang til signering for de personer, der har den fornødne kompetence.

I IT-sikkerhedsrådets vejledning om praktisk brug af kryptering og digital signatur (2000), præsenteres disse forskellige muligheder s. 29 ff., idet det anbefales, at man ved digital signering af *meget kritiske* meddelelser generelt støtter sig på bilaterale aftaler mellem afgiver og modtager. I relation til helt *ukritiske* meddelelser vil der som regel ikke være noget behov for at anvende digital signatur.

Hæftelse ved uberettiget brug

Spørgsmålet om hvilken hæftelse, der påhviler indehaveren af et certifikat til elektronisk signatur, er behandlet i betænkning 1456/2005 om e-signaturs retsvirkninger, s. 104 ff. Udvalget finder, at almindelige formueretlige principper om falsk også finder anvendelse her og finder ikke grundlag for at forslå særlige regler for anvendelsen. Spørgsmålet er genstand for *Henrik Udsens* ph.d.-afhandling, Den Digitale Signatur – ansvarsspørgsmål (2002), kapitel 2-3.

16.5.d. Identitetskontrollen

Et af de vanskelige problemer ved modtagelse af en elektronisk signatur angår sikkerheden for, at signaturen virkelig hidrører fra den afgivne part. Når dette spørgsmål søges løst, må man afklare, hvilken form for *identitet* der er afgørende for det pågældende formål. Der findes ingen regler i dansk lovgivning, der ultimativt slår fast, hvorledes en persons identitet defineres, endsige fastslås. Ud fra en teoretisk betragtning må man slå fast, at begrebet identitet er *formelt* og *relativt*, for så vidt som det knytter sig til, og udspringer af, forskellige retlige sammenhænge og formål: I talrige offentligretlige sammenhænge er den identitet, der godtgøres gennem en skatteretlig eller socialretlig sagsbehandling – og som understøttes ved CPR-nummeret – afgørende. Inden for den enkelte virksomheds rammer er den identitet, der godtgøres i forbindelse med ansættelse og aflønning, afgørende. For et lægeligt behandlingsformål er de medicinske prøver, røntgenbilleder og optegnelser, der ligger til grund for behandlingen, afgørende.

At den disponerendes identitet er et formelt og relativt begreb får betydning i relation til den identitetskontrol, der skal gennemføres ved udstedelse af certifikater til kryptering og digital signatur. Problemet er størst ved udstedelse af signaturcertifikater. Ifølge § 6, stk. 1, i bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav til nøglecentre, er der indført særlige regler om identitetskontrol ved udstedelse af kvalificerede certifikater. Forud for udstedelsen af et sådant certifikat skal underskriveren over for nøglecentret fremvise relevant legitimation, der mindst omfatter navn, adresse, CPR-nummer (eller – hvis den pågældende ikke har et sådant – anden lignende dokumentation) samt dokumentation for andre forhold vedrørende underskriveren. Disse oplysninger skal fremgå af certifikatet. Bestemmelsens stk. 2 foreskriver ligeledes, at underskriveren som udgangspunkt skal være *fysisk til stede* i forbindelse med, at denne identitetskontrol foretages. Dette krav kan dog fraviges, hvis nøglecentret på for-

hånd har kendskab til underskriverens person (f.eks., hvis der er tale om en medarbejder).

Som forudsat ved denne bestemmelse er det nærliggende at anvende CPR-nummeret i forbindelse med denne identitetskontrol. Det må imidlertid fremhæves, at CPR-nummeret vel giver en vis *formel* sikkerhed svarende til de procedurer, der generelt anvendes overfor CPR-nummerets indehaver (herunder om vedkommendes adresse, sml. herved CPR-lovens kapitel 3 om kommunernes folkeregistrering). CPR-nummeret implicerer imidlertid ingen *materiel* sikkerhed for den pågældendes identitet. En usikkerhed i den sidstnævnte relation kan navnlig opstå i relation til personer, der flytter til landet, og som tildeles et personnummer i henhold til CPR-lovens § 16.

16.5.e. Modtagelse

Ved modtagelse af meddelelser, der er krypteret med modtagerens offentlige nøgle med henblik på at sikre, at modtageren – og kun denne – får kendskab til meddelelsen (gennem dekryptering under anvendelse af den hemmelige nøgle), må der lægges procedurer for, *hvilken hemmelig nøgle* der så skal anvendes. Anvender man her en "afdelingsnøgle" til dekryptering, ofres meddelelsens konfidentialitet på afdelingsplan. Men hvis kendskabet til meddelelsen i øvrigt deles af alle de medarbejdere, der har adgang til afdelingsnøglen, repræsenterer dette ikke noget problem. På denne baggrund anbefaler IT-sikkerhedsrådet i sin vejledning om praktisk brug af kryptering og digital signatur (2000), s. 32, at meddelelser til en organisation, der ønskes krypteret, krypteres på grundlag af en offentlig nøgle, der korresponderer med en hemmelig nøgle, der er fælles for samtlige medarbejdere i organisationen eller den pågældende afdeling.

Dette udgangspunkt kan dog fraviges, hvis der er tale om særligt kritiske meddelelser. I så fald bør krypteringsadgangen dog suppleres med en mulighed for ved såkaldt *key recovery* at skaffe sig adgang til de krypterede informationer uden brug af den forudsatte krypteringsnøgle.

16.6. Elektronisk bogføring

16.6.a. Problemstillingen

I dag foregår hovedparten af den bogføring, der finder sted i regnskabspligtige virksomheder og institutioner mv., ved brug af IT (ERP-systemer, regneark, bogholderisystemer etc.). Ligeledes forekommer det stadigt hyppigere, at bilagene vedrørende de transaktioner, der ligger til grund for denne bogføring, alene foreligger digitalt. Siden 1990 har denne praksis haft udtrykkelig hjemmel i bogføringslovgivningen. Dette er sket gennem en gradvis udvikling, hvorefter den regnskabspligtige i takt med digitaliseringen har underkastet sig en stadigt øget ekstern revisionskontrol, der sikrer korrektheden af den stedfundne bogføring.

I forhold til den tidligere bogføringslov af 1990 indeholder den nye lov nogle lempelser, der kan ses i sammenhæng med den øgede dokumentationsevne, de moderne bogføringssystemer tillader: Det er ikke længere et krav, at den bogføringspligtige fører et betalingsregnskab (kasserapport), og originale bilag, der mikrofilmes eller overføres til elektroniske medier, skal ikke længere opbevares i 1 år efter, at årsregnskabet er underskrevet. Derimod skal systembeskrivelser nu opbevares i 5 år (modsat tidligere 1 år), altså i overensstemmelse med, hvad der gælder for det øvrige regnskabsmateriale. En oversigt over de retlige problemer vedrørende papirløs dokumenthåndtering må derfor indbefatte en præsentation af disse regler. Reglerne findes i dag i bogføringsloven, nr. 1006 af 23. december 1998. Til loven hører en omfattende Bogføringsvejledning af juni 1999, der er tilgængelig fra Erhvervs- og Selskabsstyrelsens hjemmeside, <www.eogs.dk>.

16.6.b. Hovedprincipper

I bund og grund har bogføringsreglerne til formål at sikre, at de transaktioner, der foregår i en bogføringspligtig virksomhed, kan eftervises. Da dette først og fremmest er nødvendigt af hensyn til virksomhedens regnskabsaflæggelse overfor told- og skattemyndigheder, tilsynsførende myndigheder og selskabsregistre, har lovgivningen offentligretlig beskaffenhed.

Registreringskravet

Det operationelle grundkrav i bogføringslovgivningen er en regel om, at alle transaktioner skal *registreres* (§ 7, 1. pkt.) og at hver enkelt registrering skal kunne dokumenteres ved *bilag* (§ 8, 1. pkt.). Begrebet registrering anvendes i dag i stedet for det tidligere anvendte begreb "bogføring", som leder tanken hen på

ældre tiders teknologi (men som dog fortsat indgår i lovens betegnelse). Hvordan registreringen skal ske beror på virksomhedens art og omfang, jf. § 7. Der er andre krav til registrering af de bananer, frugthandleren sælger fra sin bod på torvet, end til den, der finder sted, når et skibsværft afleverer et nybyggeri. Generelt gælder det, at registreringen skal ske *snarest muligt* efter, at de begivenheder, der ligger til grund for den, har fundet sted.

Terminologi

Bogføringsloven anvender betegnelsen "spor" om de midler, hvormed man således kan eftervise den enkelte transaktion og dens registrering. Begrebsopbygningen beror på, om der tages udgangspunkt i den enkelte transaktion eller i det overordnede system, der behandler disse transaktioner.

En identisk terminologi anvendes i bekendtgørelsen om statens regnskabsvæsen, nr. 1486 af 13. december 2004, se dennes § 27. Opbevares regnskabsmaterialet på elektronisk medie, mikrofilm eller anden lignende måde, skal det uden bearbejdning, beregninger eller tilpasninger kunne udskrives i klarskrift, jf. bekendtgørelsens § 46, stk. 2. Udstedte eller modtagne elektroniske bilag til brug for regnskabsføringen skal opbevares i deres oprindelige form og format. Opbevaringen skal ske på en sådan måde, at kravene til ægthed og integritet overholdes og sådan, at data ikke mistes helt eller delvis som følge af fejl, nedbrud eller andre driftsforstyrrelser, uanset om data opbevares i den registrerede virksomhed eller hos en tredjepart, jf. stk. 3.

Transaktionsspor

"Transaktionssporet" er, jf. § 4, 1. pkt., information om den *sammenhæng*, der består mellem de enkelte registreringer og årsregnskabet (eller hvilket andet formål, der er bogføringens endemål). Fokus er her på de enkelte posteringer, f.eks. ind- og udbetalinger. Der kan således godt tænkes at være flere transaktionsspor i en virksomhed, afhængig af formålet med bogføringen. Skal der derimod ikke udarbejdes regnskaber, er det som udgangspunkt ikke nødvendigt at bogføre transaktioner, og transaktionssporet mister dermed sin betydning.

Kontrolspor

"Kontrolsporet" er summen af al den information, der dokumenterer rigtigheden af de enkelte registreringer. Udover information om de enkelte registreringer indbefatter dette begreb f.eks. også information om, hvordan en beregning (f.eks. af afgift eller rentetilskrivning) finder sted, samt hvorledes de enkelte konti er placeret i bogholderiet.

Da bogføringslovgivningen i vid udstrækning hviler på den praksis, der er fremherskende i revisionskredse, finder man en udstrakt grad af regulering gennem retlige standarder. Den vigtigste af disse er kravet om "god bogføringsskik", jf. lovens § 6. De enkeltregler, der fremgår af loven, kan betragtes som detalje-

prægede eksemplificeringer af dette overordnede begreb. Det kan imidlertid sagtens tænkes, at kravene til god bogføringsskik udfyldes og skærpes over tid, uden at dette nødvendigvis reflekteres i lovgivningen.

Se for en nærmere indføring i begrebet "god bogføringsskik", *Hasselager m.fl.* (2000), s. 63 ff. I sin vejledning nr. 17 fra maj 1990 om revision af edb-baserede brugersystemer har FSR opstillet en række krav til revisors kontrol med bl.a. transaktionssporet og kontrolsporet. Bogføringsvejledningens regler opfylder i øvrigt Europarådets rekommendation no. R (81) 20 af 11. december 1981: "Harmonisation of laws relating to the requirement of written proof and to the admissibility of reproductions of documents and recordings on computers" (1982), der i artikel 1 bl.a. opfordrer medlemsstaterne til at tillade virksomheder at opbevare bogføring på edb.

Bilagene

Et bilag er ifølge lovens § 5 enhver nødvendig dokumentation for transaktioner og hændelser, der registreres i bogføringen, uanset hvilket medium denne dokumentation befinder sig på. Bilag kan således enten være på elektroniske medier, mikrofilm, papir eller på andre medier, jf. udtrykkeligt bogføringsvejledningen (juni 1999), pkt. 6.1. Der er intet til hinder for, at et bilag overføres fra en type af medium til et andet, f.eks. fra papirform til elektronisk form eller på mikrofilm. I forbindelse med denne overførsel skal det blot sikres, at bevisværdien af det elektroniske dokument ikke forringes i en sådan grad, at bilaget ikke opfylder sin dokumentationsværdi. For en nærmere indføring i denne sikkerhedsproblematik henvises til bemærkningerne i afsnit 4.3.d. om IT-sikkerhedsrådets vejledning om digitale dokumenters bevisværdi (1999).

Da bilagene skal fungere som dokumentation for såvel de forretningsmæssige og økonomiske hændelser som for de regnskabsmæssige registreringer heraf, skal de indeholde en række oplysninger, som gør det muligt at foretage en verifikation heraf, jf. § 9, stk. 1. Sker registreringen på baggrund af elektronisk overførte data, skal den bogføringspligtige herudover dokumentere den enkelte overførsel og dens tidsmæssige placering, jf. § 9, stk. 2.

16.6.c. Systemkrav

Udgangspunkt

Bogføringslovgivningen stiller ikke udtrykkelige krav til de systemer, der understøtter registreringerne, og som muliggør kontrol- og transaktionssporene. Ansvaret herfor påhviler derfor den bogføringspligtige virksomhed, dvs. dennes ledelse. Den praktiske tilrettelæggelse af disse anliggender sker ofte i samspil med

en IT-leverandør, der tilbyder en løsning, der kan opfylde lovgivningens almindelige krav.

Systembeskrivelse

Blandt andet for at muliggøre revisionens og myndighedernes kontrol med, hvilke opgaver bogføringssystemet løser (men i sagens natur også for at give den bogføringspligtige selv et overblik over systemerne), foreskriver bogføringslovens § 14, stk. 1, at den bogføringspligtige skal udarbejde "en efter aktiviteternes art og omfang afpasset beskrivelse af registreringen af transaktioner og opbevaring af regnskabsmateriale." Denne systembeskrivelse skal gøre det muligt for en person udefra med en rimelig viden om regnskab og den anvendte teknologi til enhver tid at følge, hvorledes registreringerne foretages, og hvorledes regnskabsmateriale fremfindes og udskrives i klarskrift. Beskrivelserne skal affattes på et sprog, som er naturligt for offentlige myndigheder og med anvendelse af almindelig sprogbrug og sædvanlige fagudtryk på området.

Bogføringslovens § 14, stk. 2, giver nærmere regler om systembeskrivelsens indhold. Af størst vigtighed er her dokumentationen for, hvorledes systemerne sikrer fuldstændighed og nøjagtighed af det materiale, der danner grundlag for registreringerne (og i den forbindelse de aftaler om elektronisk udveksling af data, der foreligger). Ligeledes skal beskrivelsen indeholde en konteringsinstruks eller anden dokumentation for, hvorledes systemerne sikrer en fuldstændig og nøjagtig registrering af transaktioner. Endelig skal det fremgå, hvorledes *automatisk genererede* registreringer foretages, herunder beregningsgrundlag og -formler.

Se for en nærmere gennemgang af systemdokumentationens indhold *Hasselager m.fl.* (2000), s. 109 ff., der anbefaler en pyramideformet trelags-model: Øverste lag (overbliksniveauet) angiver her systemets formål, med moduloversigt og diagrammer. Midterste niveau (mellemniveauet) er reserveret brugervejledninger og driftsvejledning som en verbal beskrivelse af programmerne og deres struktur. Laveste niveau (det detaljerede niveau) indeholder en redegørelse for de ind- og uddata, systemet behandler, herunder med beskrivelser af programmer filer og data. Kravet om nøjagtig dokumentation af programmel kan volde vanskeligheder, hvis der er tale om standardprogrammel, der distribueres som *closed source*, altså kun i objektkodeversion. I sådanne tilfælde kan det blive nødvendigt at indgå aftale om kildetekstdeponering, jf. herom afsnit 4.4.c.

16.6.d. Elektronisk fakturering

Ifølge § 45 i *momsbekendtgørelsen* (nr. 1152 af 12. december 2003 med senere ændringer) er der indført regler om udstedelse af elektroniske fakturaer. Reglerne implementerer rådsdirektiv 2001/115/EF, der har til formål at harmonisere kravene til den elektroniske fakturering. I forhold til hidtil gældende ret indebærer de nye regler flere vanskeligheder i den elektroniske faktureringsproces.

For det første stilles det nu som et krav, jf. § 45, stk. 1, at køberen er indforstået med, at der udstedes en elektronisk faktura. Dernæst er det et krav, at fakturaens ægthed samt integriteten af dens indhold er sikret ved en elektronisk signatur, eller ved at der er gjort brug af elektronisk dataudveksling (EDI). Gør man brug af en *elektronisk signatur*, skal denne være baseret på en avanceret elektronisk signatur, der som minimum har et sikkerhedsniveau svarende til OCES-certifikatet, jf. herom bemærkningerne i tilknytning til afsnit 4.2.f. Dette fremgår af stk. 2. Gør man derimod brug af EDI, skal der forinden foreligge en aftale, som fastsætter procedurer for den elektroniske dataudveksling, som sikrer, at de i stk. 1 nævnte sikkerhedsbetingelser er opfyldte.

I tråd med de almindelige bogføringsregler opstiller § 45, stk. 5, den almindelige regel, at virksomheder, der benytter elektronisk fakturering, skal opbevare system- og procedurebeskrivelser. Denne opbevaringspligt omfatter ligeledes de indgåede aftaler (herunder om EDI-udveksling) og de certifikater, der hører til elektroniske signaturer. Om selve den elektroniske faktura fastslår § 45, stk. 6, at virksomheden skal opbevare disse i deres oprindelige form og format på en måde, der sikrer, at kravene til ægthed og integritet overholdes og sådan, at data ikke mistes på grund af fejl eller nedbrud. Disse sikkerhedskrav skal opfyldes, hvad enten lagringen sker hos den bogføringspligtige eller hos en tredje part.

I medfør af stk. 7 kan den registrerede virksomhed, som i øvrigt opfylder kravene i stk. 1 samt bestemmelsens øvrige krav, vælge at anvende en anden sikker metode til elektronisk fakturering. Se om de nye regler *Peter Nordentoft og Flemming S. Pristed* i Lov & Data nr. 78, juni 2004, s. 29 ff.

Ifølge lov om offentlige betalinger gælder der herudover en almindelig pligt for offentlige myndigheder til at sende og modtage regninger elektronisk. Se hertil afsnit 20.4.j.

16.6.e. Andre spørgsmål

Opbevaringspligt

Bogføringslovens § 10 foreskriver, at regnskabsmateriale skal opbevares på betryggende vis i 5 år fra udgangen af det regnskabsår, materialet vedrører. Opbevaringen skal ske på en måde, som i hele denne periode muliggør en selvstændig og entydig fremfinding af det, jf. stk. 1. Opbevares regnskabsmaterialet på elektronisk medium, mikrofilm eller anden lignende måde, skal det uden bearbejdning, beregninger eller tilpasninger kunne *udskrives* i klarskrift, stk. 3, hvorimod det ikke – nødvendigvis – skal *opbevares* i klarskrift. Beskrivelsen af de systemer, der skal benyttes til at hente regnskabsmaterialet frem i klarskrift, skal dog opbevares i klarskrift.

Beskrivelse

Ifølge bogføringslovens § 14, stk. 3 skal der foreligge en beskrivelse af, hvorledes regnskabsmaterialet opbevares. Denne skal i det mindste indeholde oplysninger om de metoder, der benyttes ved opbevaringen samt om hvordan materialet fremfindes og udskrives i klarskrift. Anvendes kryptering skal der foreligge oplysning om koder og dekrypteringsmetoder mv. Reglerne om opbevaring af regnskabsmateriale er de samme, uanset hvilken teknologi der er anvendt ved registreringerne, og hvilken opbevaringsform der gøres brug af, jf. nærmere *Hasselager m.fl.* (2000), s. 87 ff.

Bogføringslovens § 12 foreskriver, at regnskabsmaterialet som udgangspunkt skal opbevares her i landet. Er der tale om bogføringspligtige aktiviteter uden for landet kan opbevaring i det pågældende land dog ske i hele opbevaringsperioden (de 5 år fra regnskabsperiodens udløb). Bl.a. for at muliggøre *outsourcing* af bogføring til virksomheder uden for landet er opbevaring i udlandet dog tilladt for den indeværende og forrige måned. I så fald skal det dog sikres, at offentlige myndigheder til enhver tid kan skaffe sig adgang til det udenlandske materiale, jf. nærmere § 12, stk. 2.

16.7. Særlige problemstillinger

16.7.a. Ophavsretlige spørgsmål

Ved digitalisering af en tekst, opstår der et antal eksemplarer af den, som kan berøre en ophavsretlig eneret. Indebærer digitaliseringen en skanningsproces, indtræder første eksemplar i skannerens hukommelse. Er teksten i forvejen maskinlæsbar, opstår der

i praksis altid et nyt eksemplar, når den pågældende fil underkastes en proces, der indebærer flytning eller konvertering, f.eks. i forbindelse med lagring, udprintning, kopiering og overførsel mv.

Er der tale om en tekst, der manifesterer et litterært eller kunstnerisk værk, en database eller et fotografisk billede, vil rettighedshaveren ifølge de ophavsretlige regler som udgangspunkt kunne modsætte sig denne eksemplarfremstilling. Ophavsretsloven tager kun i begrænset omfang særligt hensyn til den offentlige forvaltning, se således lovens § 27, hvorefter ophavsretten ikke er til hinder for, at retsbeskyttede eksemplarer, der indgår til en forvaltningsmyndighed, eller frembringes inden for denne, gøres til genstand for offentlighed gennem aktindsigt. Som eksempel kan det nævnes, at teknisk prægede ansøgninger ofte vil være bilagt videnskabelige artikler mv., der kan være beskyttet af ophavsretten, se f.eks. *U 1995.782 V*, der gav beskyttelse for en miljørapport til brug for amtets teknik- og miljøudvalg. Indførelsen af det papirløse kontor ved digitalisering af værker forudsætter derfor, at der meddeles samtykke fra de berørte rettighedshavere.

De ophavsretlige spørgsmål, der opstår i forbindelse med en sådan digitalisering, beror på, om dokumentet anvendes af en offentlig forvaltningsmyndighed eller i privat regi.

Myndigheder

Ifølge ophl. § 27, stk. 1, er ophavsretten ikke til hinder for, at der i forbindelse med meddelelse af aktindsigt i dokumenter, der repræsenterer ophavsretlige værker, sker eksemplarfremstillinger heraf. Dette gælder uanset, om dokumentet er produceret i forvaltningen, eller om det modtages udefra (i hvilke tilfælde ophavsmanden typisk er en privatperson). Ligeledes tillader ophl. § 27, stk. 2, at værker gøres tilgængelige for almenheden i forbindelse med arkivering og i forbindelse med arkivlovgivningens regler herom. Bestemmelsen har alene betydning i de – hyppigt forekommende – tilfælde, hvor arkivmaterialet ikke tidligere er gjort tilgængeligt for almenheden, jf. konsumptionsreglen i ophl. §§ 19-20. Hvor arkivlovgivningen hjemler en sådan tilgængeliggørelse må der dog ikke udleveres afskrifter eller fremstilles kopier af *private* arkivalier.

Herudover giver ophl. § 28, stk. 1, nr. 2, ret til, at værker "i det omfang, som betinges af formålet" gengives i forbindelse med sagsbehandling inden for offentlige myndigheder samt institutioner, som henhører under folketinget. Bestemmelsen indebærer, at der uden samtykke fra rettighedshaveren i forbindelse med sagsbehandling de omhandlede steder kan foretages en sådan kopie-

ring, som er nødvendig for sagsbehandlingen. Denne begrænsning i den ophavsretlige eneret er begrundet med ønsket om, at nye teknologiske hjælpemidler – såsom PC'er, skannere mv. – kan blive taget i brug i stigende omfang i den offentlige sektor med henblik på det papirløse kontor. Bestemmelsen giver dog kun mulighed for at foretage den kopiering i analog eller digital form, der er nødvendig til brug for sagsbehandlingen, journaliseringen, arkiveringen og lignende. Der er således ikke hjemmel til at oprette centrale databaser, hvortil almenheden har adgang. Sådanne åbne systemer kan kun oprettes, hvis der foreligger tilladelse fra rettighedshaverne. Der er ikke indført hjemmel i ophavsretsloven for aftalelicens til en sådan anvendelse.

16.7.b. Automatiserede afgørelser

Problemstilling

Når afgørelser træffes på grundlag af en automatiseret sagsbehandling opstår en række retlige problemer som følge af, at der ikke her er nogen direkte mental "beslutning" bag den enkelte afgørelse. Modtageren af en forpligtende meddelelse har et naturligt krav på sikkerhed for, at meddelelsen kan føres tilbage til en gyldig beslutning. Problemet er her, at det systembevis, jf. herom i afsnit 4.3.d., der i almindelighed vil skulle føres herfor, beror på fakta, der ligger i hænderne på den part, der i givet fald vil anfægte meddelelsens autenticitet. Er beslutningen manifesteret i et brev, der er udskrevet på grundlag af en automatiseret tekstbehandling, kan der rejses spørgsmål ved, om brevet har den fornødne gyldighed uanset om det er forsynet med en underskrift.

U 2001.252 ØLK

Ved afgørelsen i *U 2001.252 ØLK* fandt Østre Landsret, at en begæring om tvangsopløsning af et selskab, der var meddelt ved et maskinelt udskrevet brev, ikke kunne lægges til grund for en opløsningssag uden "særlige foranstaltninger for at løse de retssikkerhedsmæssige problemer, der følger af manglende underskrift". Selv om afgørelsen umiddelbart kan være vanskelig at forene med den praksis, der generelt tillader faksimile-underskrift af stævninger, kan resultatet begrundes med, at den pågældende begæring ikke var forsynet med navnet på den *person*, der havde truffet den pågældende beslutning, og at der ikke var truffet særlige sikkerhedsforanstaltninger for at undgå utilsigtet igangsætning af opløsningsproceduren ved falsk eller ved fremsendelse af udkast mv. Resultatet ville derfor være et andet, hvis blot navnet på den ansvarlige sagsbehandler var anført.

Kendelsen i *U 2001.252 ØLK* er stadfæstet i *U 2001.1980 HK* men – i overensstemmelse med proceduren for Højesteret – under henvisning til rpl. § 261, stk. 2, se hertil afsnit 16.3.b. I betænkning 1400/2000 drøftes spørgsmålet om afsendelse af forpligtende digitale meddelelser fra offentlige myndigheder s. 155 f., hvor det konkluderes, at der vil være knyttet "betydelige retssikkerhedsmæssige betænkeligheder" ved i bekendtgørelsesform at skulle ændre lovbestemmelser, som giver borgere m.v. ret til at modtage kommunikation fra offentlige myndigheder på en bestemt måde, således at borgerne pålægges pligt til at modtage meddelelserne digitalt. Se tilsvarende kritisk *Søren Friis Hansen* i U2001B.183 ff. i en kommentar til *U 2001.252 ØLK*.

Personoplysninger

Ifølge LBP § 39 kan en registreret person gøre indsigelse mod, at den dataansvarlige lader den registrerede undergives afgørelser, der har retsvirkninger for eller i øvrigt berører den pågældende i væsentlig grad, hvis afgørelsen alene er truffet på grundlag af elektronisk databehandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold. Bestemmelsen har rod i direktivets art. 15 og gælder såvel for private virksomheder som offentlige myndigheder. Se om direktivets bestemmelse, *Lee A. Bygrave* i 17 CLSR 17 ff. (2000).

16.7.c. Virtuelle møder

Problemstillingen

Lovkrav, som fordrer en pligt til mødeafholdelse eller anden personlig tilstedeværelse, kan undertiden opfyldes ved, at de pågældende deltagere er til stede "virtuelt" – enten ved videokonference, via telefonmøder eller ved anden samtidig overførelse af det talte ord og/eller det levende billede. I tilfælde, hvor samtlige mødedeltagere er enige om at anvende en sådan fremgangsmåde i stedet for et fysisk møde, vil der almindeligvis være en formodning om, at det påbudte mødekrav kan modificeres. Men forudsættes mødet afholdt under deltagelse af personer, der ikke nødvendigvis vil kunne give et sådant forhåndssamtykke, støder man på problemer.

Rpl. § 190

Disse problemer er i stigende grad søgt løst i lovgivningen: På grundlag af artikel 10-11 i EU's retshjælpskonvention er der i rpl. § 190 givet hjemmel for anvendelse af telekommunikation i forbindelse med afhøring af vidner efter begæring af udenlandske myndigheder. Begæringer herom skal "så vidt muligt imødekommes", medmindre dette vil være åbenbart uforeneligt med landets retsorden. Ifølge § 190, stk. 2, kan afhøring fra udlandet ved anvendelse af telekommunikation uden billede (dvs. telefonmøder) kun foretages, hvis vidnet har meddelt sit samtykke hertil.

Reglerne om vidnetvang kan ikke finde anvendelse, uanset om vidnet har meddelt et sådant samtykke.

Selskabsretten

Ved lov nr. 303 af 30. april 2003 er lovene om aktieselskaber og anpartselskaber ændret for bl.a. at give hjemmel til afholdelse af elektronisk generalforsamling og elektronisk kommunikation mv. Regler herom skal udtrykkeligt fremgå af vedtægterne, jf. aktieselskabslovens § 4, stk. 2, nr. 7. Ligeledes skal vedtægterne indeholde hjemmel til, at aktiebogen skal kunne føres elektronisk, jf. aktieselskabslovens § 26, stk. 2.

Medmindre vedtægterne bestemmer andet kan bestyrelsen beslutte, at der som supplement til fysisk fremmøde på generalforsamlingen gives adgang til, at aktionærer kan deltage elektronisk i generalforsamlingen, herunder stemme elektronisk, uden at være fysisk til stede på generalforsamlingen, jf. § 65a, stk. 1. Ligeledes kan generalforsamlingen beslutte, at generalforsamlingen alene skal afholdes elektronisk uden adgang til fysisk fremmøde, jf. nærmere § 65a, stk. 2. Bestyrelsen fastsætter i så fald de nærmere krav til de elektroniske systemer, der da skal anvendes, jf. § 65a, stk. 3-4.

Supplerende litteratur

Bevisforholdene vedrørende nye elektroniske *medier* er mest indgående præsenteret af *Eivind Einersen*: Elektronisk aftale- og bevisret (1992), s. 18 ff. En god oversigt over de almindelige retsreglers anvendelse på området findes med *Susanne Karstoft*: Elektronisk dokumentudveksling – retlige aspekter (1994).

Reglerne om *elektronisk bogføring* er behandlet af *Olaf Hasselager m.fl.*: Bogføring, Regnskab og Skat – med kommentarer til Bogføringsloven og Mindstekravsbekendtgørelsen (2000), af *Lars Aggergren* i R&R nr. 7, 1990, s. 55 ff. og af *Carsten W. Heilbuth og Carsten Tjagvad*: Edb-revision (1994). Grundlaget for den første bekendtgørelse, der tillod elektronisk bogføring, ligger i Industriministeriets betænkning om revision af bogføringslovgivningen, betænkning 1140/1988. En grundig vejledning i bogføringsreglerne er udgivet af Erhvervs- og Selskabsstyrelsen (juni 1999).

Foruden de vejledninger fra IT-sikkerhedsrådet, der omtales i teksten, har Forskningsministeriet udsendt et antal vejledninger om, hvordan myndighederne omstiller sig til den digitale forvaltning, se således rapporterne Elektronisk arkivering – aktuelle muligheder og anbefalinger (1995), Statens e-post – standard for adressering (1995), I gang med digital forvaltning (1997) og Digital forvaltning – krav til systemerne (1997).

Kapitel 17. IT-KRIMINALITET

17.1. Almene spørgsmål

17.1.a. Problemstillingen

"IT-kriminalitet"

Som "IT-kriminalitet" henregner man almindeligvis sådanne forbrydelser, der enten foretages ved hjælp af IT (f.eks. udtræk fra pengeautomater, genbrug af stjålne betalingskort), eller som rettes mod IT-systemer (f.eks. indlæggelse af destruktive virusprogrammer). Hovedparten af dette IT-strafferetlige område berører delikter i den borgerlige straffelov. Med den lovgivningsmæssige udvikling er der dog kommet talrige special-delikter til i særlovgivningen, og det kan undertiden være vanskeligt at finde noget ydre fællestræk for de delikter, der henholdsvis placeres i straffeloven og i særlovgivningen. Som nævnt i afsnit 9.4.a. volder det f.eks. vanskeligheder at placere de regler, der foreskriver straf for omgåelse mv. af tekniske beskyttelsesforanstaltninger, der beskytter ophavsretlige frembringelser mv.

Beskrivelsesproblemer

Hvor IT-systemets materielle komponenter ikke giver anledning til nævneværdige strafferetlige problemer (tyveri af en PC eller en printer straffes som udgangspunkt på samme måde som tyveri af andre tekniske indretninger mv.), volder det en vis tvivl at indplacere en række IT-systemkomponenter i den sædvanlige strafferetlige ramme. Hvornår skal information betragtes som "rørligt gods"? Omfatter en "underskrift" også en digital signatur? Er en e-postmeddelelse et "brev"?

Lovrevisioner

Med lov nr. 229 af 6. juni 1985 blev der indføjet en række nye delikter om datakriminalitet i straffeloven. Ændringerne har grundlag i straffelovrådets betænkning 1032/1985 om datakriminalitet. Med lov nr. 388 af 22. maj 1996 blev strfl. § 163 ændret, således at denne bestemmelse også omfatter erklæringer afgivet "ved andet læsbart medie". En mere omfattende lovreform fandt sted ved lov nr. 352 af 19. maj 2004. Herved indførtes de forslag, der var fremsat i betænkning 1417/2002 om IT-kriminalitet. Samtidig hermed blev grundlaget skabt for en ratifikation af den "Convention on Cyber-Crime", som blev underskrevet i Budapest den 23. november 2001, og som trådte i kraft i juli 2004.

Systematik

Systematikken i dette kapitel er som følger: I dette indledende afsnit (17.1.) behandles en række problemstillinger, der hører til strafferettens *almindelige del*. De vanskelige interlegale strafferetlige spørgsmål berøres dog ikke, se hertil *Søren Hjort Christiansen*: Om lokalisering af Internet relateret kriminalitet, Justitia, nr. 6, december 2001, s. 47 ff. Herefter vendes blikket mod de tre væsentligste typer af delikter inden for IT-strafferetten: *Formueforbrydelser*, forbrydelser vedrørende *bevismidler og penge og fredskrænkelser*. Kapitlet afsluttes med en omtale af to for IT-strafferetten tilgrænsende problemstillinger: Retsstillingen vedrørende visse adgangssystemer og visse regler om ulovlig informationsspredning, der ofte sker ved brug af digitale net.

17.1.b. Analogiforbuddet

På grund af det forbud mod visse analogislutninger, der følger af strfl. § 1 (og som i hovedsagen genfindes i EMRK art. 7, stk. 1, 1. pkt.), har man på et tidligt tidspunkt overvejet og gennemført tilpasninger i den danske straffelov for at sikre en korrekt dækning af IT-kriminalitetens forskellige former. Danske domstole har dog undertiden fortolket udvidende for at ramme kriminalitetsformer, hvis strafværdighed ganske svarer til gerningsindholdet i en bestemmelse, men som pga. den teknologiske udvikling ikke har været beskrevet heri.

Analogieksempler

Et vidtgående eksempel herpå er dommen i *U 1940.156 Ø*, der straffede efter en analogi af den tidligere § 263 (der dengang kun kriminaliserede retsstridige brevåbninger) for hemmelig aflytning ved hjælp af tilkoblet lytteudstyr. Der er tale om en vidtgående afgørelse, som næppe kan opretholdes, jf. bl.a. *Stuer Lauridsen*: Pressefrihed og personlighedsret (1988), s. 187. Et andet vidtgående eksempel er *U 1996.356 Ø*, hvor Østre Landsret fortolkede forbuddet mod offentlige indsamlinger i Lov om offentlige indsamlinger ved brug af kædebreve. Tiltalte havde deltaget i et "system", hvor disketter fungerede på samme måde som kædebreve. Mod betaling af 50 kr. købte man nogle koder, som aktiverede et program til at kopiere sig selv. Kopien blev derefter sendt videre til et nyt led i kæden, som igen skulle betale 50 kr. for at aktivere det, og meningen var så, at de mange betalinger à 50 kr. skulle gøre systemet profitabelt. Landsretten fandt, at det etablerede system var opbygget i samme form som kædebreve, og at formålet var at opnå en økonomisk gevinst. Derfor var forholdet strafbart. Dette resultat forekommer omvendt noget sikrere: Den interesse i at modvirke kædebreve, der begrunder

strafbestemmelsen, gør sig så meget desto mere gældende, hvis "kædebrevet" kan genereres og videresendes automatisk.

Analogi afvist

Omvendt fandt Østre Landsret ved sin dom af 13. februar 1995 i den såkaldte *Proms-sag*, i overensstemmelse med analogiforbuddet i § 1 og med henvisning til forarbejderne til 1985-ændringen af straffeloven (jf. herom straks nedenfor), at erklæringer afgivet på diskette ikke var omfattet af strfl. § 163 eller denne bestemmelses analogi. Se i samme retning *U 1990.70 H*, hvor landsretten frifandt for dokumentfalsk i et tilfælde, hvor tiltalte havde benyttet en andens navn som underskrift på en telex.

Med lovreformen fra 2004 har man søgt at håndtere de vanskeligheder, analogiforbuddet kan give anledning til på IT-området, ved generelt at tale om "informationssystemer". Som omtalt i afsnit 2.2. (informationsteori) og 2.3. (systemteori) rammer man gennem en sådan terminologi de essentielle aspekter af IT-anvendelsen. Det er herefter f.eks. uden betydning, om et adgangsmiddel til et "ikke offentligt tilgængeligt informationssystem" fremstår som koden til en mobiltelefon, en PDA eller til lønningssystemet i en virksomhed.

17.1.c. Forsøgslæren

Ifølge strfl. § 21 straffes handlinger, som sigter til at fremme eller bevirke udførelsen af en forbrydelse, som forsøg, når forbrydelsen ikke fuldbyrdes. For visse kriminalitetsformer spiller denne straffemulighed en stor praktisk betydning, idet selve fuldbyrdelsesmomentet (f.eks. at man trænger ind i hinandens IT-system) kan være vanskeligt at konstatere, hvorimod en række forudgående skridt (f.eks. at man råder over et antal passwords med henblik på den ulovlige indtrængen) foreligger som dokumenterbare beviser. Bestemmelsen giver anledning til forskellige typer af problemstillinger.

1. Hackerværktøjer mv.

Den første type af problemer angår gerningsmandens besiddelse af adgangskoder og andre tekniske indretninger, som fremstår som midler, der alene – eller i det væsentligste – kan tjene til at udføre bestemte former for forbrydelser, f.eks. hacking eller virusangreb. Håndteringen af sådanne midler har givet anledning til indgående overvejelser, såvel i relation til det ophavsretlige område (se herom redegørelsen i afsnit 9.4.), i relation til de såkaldte piratdekodere (se herom afsnit 17.5.a.) som i relation til de andre af de midler, der ofte anvendes i forbindelse med IT-kriminalitet, se herved den indgående redegørelse i betænkning

1417/2002, s. 39 ff., der bl.a. gengiver en udtalelse herom fra IT-sikkerhedsrådet (s. 60 ff.).

Med lovreformen fra 2004 er en del af disse spørgsmål løst gennem delikter, der *fremrykker* fuldbyrdelsesmomenter for forskellige typer af forbrydelser. Reguleringen er struktureret således, at den retter sig mod forskellige typer af informationskrænkelser. Ifølge strfl. § 263a er erhvervsmæssigt salg eller udbredelse i en videre kreds af koder eller adgangsmidler til et *ikke offentlig tilgængeligt informationssystem* gjort strafbar. Bestemmelsen fremskyder den beskyttelse, der fremgår af strfl. § 263, stk. 2 ("hackerbestemmelsen"), og omtales derfor i tilknytning til denne, i afsnit 17.4.c. I strfl. § 301 er det dernæst blevet forbudt at fremstille, skaffe, besidde eller videregive visse oplysninger, der kan identificere betalingsmidler, eller genererede betalingskortnumre. Bestemmelsen lægger sig op af den strafferetlige regulering vedrørende pengemidler og omtales derfor i afsnit 17.3.c.-17.3.d. Endelig er det med strfl. § 301a kriminaliseret at skaffe sig eller videregive koder eller andre adgangsmidler til informationssystemer, hvortil adgangen er forbeholdt betalende brugere. Bestemmelsen har nær forbindelse med den særlige kriminalisering, der i forvejen er gennemført vedrørende de såkaldte piratdekodere og omtales derfor i tilknytning til disse regler i afsnit 17.5.b.

Selv om hovedparten af de vanskelige spørgsmål, forsøgslæren giver anledning til på IT-området, dermed er blevet løst gennem en fremskudt regulering (og tilmed en regulering, der befinder sig inden for samme strafferammer som de primære forbrydelser), kan der opstå situationer, der falder uden for denne regulering, og hvor man derfor må falde tilbage på den almindelige forsøgslære.

Ved *Roskilde Rets dom af 19. december 1996* i en stor hackersag fandt retten, at gerningsmandens besiddelse af et såkaldt crackerprogram til brydning af passwords ikke i sig selv udgjorde en forsøgshandling. Det var således ikke tilstrækkeligt, at besiddelsen af sådanne systemer med overvejende sandsynlighed ville blive anvendt i forbindelse med ulovlig hacking. Argumentet er, at brugere, der har glemt deres passwords, kan have en lovlig interesse i at finde det igen. Det forhold, at udarbejdelse, overladelse eller benyttelse af et crackerprogram kan indgå som et forberedende led i uberettiget indtrængen i et edb-anlæg, jf. strfl. § 263, stk. 2, indebar efter rettens opfattelse ikke et bevis for, at der var forsæt til "en nærmere bestemt uberettiget indtrængen i angivne edb-anlæg". Efter rettens opfattelse var det således ikke tilstrækkeligt, at handlingen overvejende sandsynligt var foretaget med henblik på hacking.

Det er udgangspunktet i dansk ret, at almindelige forberedelseshandlinger ikke kan straffes som forsøg, hvis de i sig selv ikke har en tilstrækkelig grov eller farlig karakter, se hertil *Waaben*: Strafferettens almindelige del I, 3. udg. (1993), s. 187 ff. Når nogen, der i øvrigt ikke kan dokumentere en legitim interesse i at benytte et hackerværktøj, besidder et sådant værktøj i en situation, hvor vedkommende ikke kan angive noget legitimt formål med besiddelsen, kan man overveje, om selve besiddelsen skal udgøre et strafbart forsøg. Herfor taler det forhold, at der ofte ikke vil være anden anvendelse for de pågældende indretninger end netop den retsstridige indtrængen mv., samt at det kan være vanskeligt at føre bevis for den fuldbyrdede forbrydelse, som den slags informationer typisk indgår i. Imod taler det, at man ved at kriminalisere rådigheden over information kan siges at gøre indgreb i selve informationsfriheden, hvilket i almindelighed bør kræve sikker hjemmel. De bevismæssige vanskeligheder – som alt andet lige bør kunne løses ad teknisk vej – kan ikke opveje denne betænkelighed.

2. Virusudvikling

For det andet kan man spørge, om det forhold, at gerningsmanden udvikler en virus, i sig selv udgør en forsøgshandling, der leder frem imod den forbrydelse, hvorved virusen sættes i omløb med et destruktivt formål. Om dette er tilfældet, beror på forholdene i den enkelte situation. Det må i den forbindelse tages i betragtning, at konstruktion af virus-programmel ikke i sig selv behøver tilsigte en retsstridig ødelæggelse el.lign. De første vira blev i sin tid konstrueret i forskningsmiljøer med det formål at finde en metode til automatisk distribution af software i netværk. Et forsøg herpå gjort i den amerikanske virksomhed Xerox endte i 1982 galt; virusen løb løbsk og gjorde netværket funktionsudygtigt. Også for de virksomheder, der forsker i "modgifte" til virusprogrammer, kan konstruktionen af en virus – med henblik på udvikling af en passende modgift – selvsagt udgøre et fuldt legitimt formål.

At man kan bevise, at den gerningsmand, hos hvem en ikkeaktiveret virus befinder sig, tidligere har foretaget tilsvarende destruktive handlinger, er imidlertid næppe i sig selv nok til at statuere, at gerningsmanden havde til forsæt at slippe denne virus. Hertil må kræves forberedelseshandlinger, der går videre end til den rene konstruktion – f.eks. oprettelse af kommunikationsveje, der gør det muligt at sende virus af sted uden at kunne identificere afsenderen.

3. Portskanning

En særlig mellemgruppe foreligger i tilfælde, hvor gerningsmanden foretager en maskinel kontrol via et offentligt kommuni-

kationsnet af, om der er "åbne indgange" til et IT-system, såkaldt *portskanning*. Viser der sig en sådan åbning, vil han herigennem kunne forsøge et retsstridigt angreb. Men portskanningen kan også have til formål at opnå en helt generel viden om, hvor sikkert systemet er – analogt til, at man kan få lyst til at tage i naboens dørhåndtag for at se, om der er låst. Det er endnu ikke afklaret, om sådanne undersøgelseshandlinger kan sidestilles med et forsøg på at skaffe sig uberettiget adgang til de pågældende systemer, jf. strfl. § 263, stk. 2. Ved den konkrete bedømmelse af forholdet må det formentlig indgå med en vis vægt, om gerningsmanden kan påvise et sagligt behov for at skaffe sig den pågældende viden, og om han i øvrigt må formodes at have et motiv eller en hang til rent faktisk at begå overtrædelser af den nævnte art.

17.1.d. Medvirkensspørgsmål

Udgangspunktet

Efter strfl. § 23 omfatter en straffebestemmelse alle, der ved tilskyndelse, råd eller dåd har medvirket til gerningen. Bestemmelsen knytter først og fremmest medvirkensansvar til tilfælde, hvor der foreligger en *forsætlig* medvirkenshandling, f.eks. at medvirkeren bestiller hovedgerningsmanden til at gennemføre en uberettiget indtrængen i et IT-system. Et eksempel herpå er *U 2001.1572 V*, hvor to unge mennesker bl.a. blev dømt medvirkensansvarlige for gennem links til ulovlige MP3-filer fra en hjemmeside at have "forøget mulighederne for, at de personer, der ønskede at kopiere musik, kunne finde musikken og foretage kopieringen på en nem og hurtig måde".

Fildeling

En tilsvarende problemstilling foreligger, når gerningsmanden ved hjælp af *peer-to-peer*-teknologien etablerer et fildelingssystem, der gør det muligt for private brugere at udveksle uautoriserede kopier af ophavsretligt beskyttede værker, se hertil *Kamilla Gibson* i Justitia nr. 1, februar 2003, s. 55 ff. (navnlig s. 64 ff.) og *Johan Schlüter & Jacob Plesner Mathiasen* i Festskrift til Mogens Koktvedgaard (2003), s. 517 ff.

Grokster-sagen

Dette spørgsmål er nu afgjort af *U.S. Supreme Court* den 27. juni 2005 i sagen *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, et al., se om underinstansens afgørelse *Koktvedgaard* (2005), s. 130. Supreme Court valgte i sin dom at lægge afstand til sin dom i sagen *Sony v. Universal Studios,* 464 U.S. 417 (1984), der antog, at videomaskiner i sig selv ikke indebar ulovlig medvirken til kopiering af beskyttede videofilm. Dommen fastslog, at Grokster befandt sig i en helt anden situation end Sony gjorde det i 1984-afgørelsen. Det lægges til grund, at "one

who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties." Dommer *Souter*, der afgav rettens votum, peger i den forbindelse på en række kritiske egenskaber ved Grokster-løsningen, herunder *at* den var kommet på markedet, efter at den tidligere Napster-løsning var blevet fjernet af samme grunde som de, der begrundede Grokster-søgsmålet, *at* man ikke havde forsøgt at indbygge teknikker, der kunne frasortere ophavsretsbeskyttet materiale, og *at* man tjente penge ved at sælge annonceplads ved brugen af løsningen. Det er sandsynligt, at tilsvarende overvejelser vil blive lagt til grund, hvis spørgsmålet skulle påkendes i dansk ret.

Medvirkenslæren gælder også i relation til særlovsovertrædelser, jf. henvisningen i strfl. § 2. Visse regler i særlovgivningen, således ophl. § 76, straffer imidlertid også overtrædelser af loven, der begås ved *grov uagtsomhed*. I sådanne tilfælde kan det blive afgørende, hvad den muligt ansvarlige *burde* have gjort. Der ses bort fra sådanne særregler i det følgende.

Når det gælder målrettede tilfælde rejser IT-anvendelsen ikke særlige problemer i relation til § 23. Sådanne problemer opstår derimod i relation til kriminalitet, der har en mindre planlagt karakter, f.eks. fordi der er afstand – i tid og rum – mellem hovedhandlingen og medvirkenshandlingen. Sådanne tilfælde kan forekomme i to hovedgrupper: Den ene drejer sig om medvirkenshandlinger, der knytter sig til retsbrud på Internet. Den anden om medvirken i forbindelse med råden over information, der kan anvendes som teknisk adgangskontrol mv.

Internet-medvirken

At spørgsmålet om medvirken i relation til Internet-kommunikation er kommet særligt i fokus skyldes Internets opbygning, der ofte ikke gør det muligt at kontrollere, hvem der har afsendt eller videresendt en retskrænkende information, jf. nærmere om denne problemstilling *IT-sikkerhedsrådets* vejledning: Privatliv på Internet (1998), s. 53 ff. Der er mange muligheder for at koble sig op på Internet via lånt udstyr, og selv i de tilfælde, hvor der kommunikeres fra et fast, abonnementsbaseret terminalpunkt, giver de protokoller, der i øjeblikket anvendes ved Internet-kommunikation, langt fra altid mulighed for at finde frem til afsenderen af en specifik meddelelse. Derfor er der – naturligt – opstået en interesse for i stedet at lade en anden (og ofte mere solid) aktør vikariere i det strafferetlige ansvar.

Personkredsen

For en nærmere oversigt over, hvilke typer af aktører der således kan tænkes at vikariere i det strafferetlige ansvar som "med-

virkere", henvises til fremstillingen i afsnit 3.3.b. Der er her navnlig de såkaldte Internet service providere (ISP'ere) og leverandørerne af Internet-information (ICP – Internet Content Provider), der står i fokus. I relation til *ISP'en* kan man f.eks. forestille sig et ansvar knyttet til selve det forhold, at man tilbyder kunderne at abonnere på en nyhedsgruppe, når der heri udspredes information af retsstridigt indhold (f.eks. børnepornografiske billeder, ulovlige kopier af ophavsretligt beskyttede værker eller PIN-koder til retsstridig indtrængen i IT-systemer). I relation til *ICP'en* kan man forestille sig et ansvar knyttet til det forhold, at der fra en hjemmeside findes en hypertekst-link til en hjemmeside, hvor der foreligger retsstridig information, f.eks. ulovligt fremstillede eksemplarer af ophavsretligt beskyttede værker.

Som påpeget i mit indlæg ved Det 35. Nordiske Juristmøde i Oslo, august 1999 (NJM 1999 I, 197 ff.), beror medvirkensansvaret først og fremmest på indholdet af den – primære – retsnorm, som medvirkenshandlingen bærer frem imod. Selvom der i den forbindelse er stor principiel forskel mellem et straferetligt og et erstatningsretligt medvirkensansvar (eftersom disse to ansvarsformer berører forskellige typer af sanktioner) fortoner forskellen sig på det praktiske plan. Dette ses f.eks. tydeligt, når det primære retsbrud har hjemmel i en særlovgivning, der foreskriver såvel erstatningsretlige som straferetlige sanktioner. Medvirkensreglerne vedrørende ophavsretlige krænkelser er et eksempel herpå.

Ansvarsvurderingen vanskeliggøres generelt af, at Internet-kommunikation i betydeligt omfang foregår maskinelt: Når en person via opkobling til en hjemmeside henter information hjem, er det maskinen bag hjemmesiden, der "afsender" denne information. For en juridisk ansvarsvurdering må det dog fastholdes, at der bag denne maskine ligger en menneskelig beslutning om ikke alene at stille informationen til rådighed, men også afsende den på anfordring, se om denne ansvarsforudsætning i edb-retten, *E&A* s. 212 ff. Terminologien om de enkelte funktioner i en Internet-kommunikation har i øvrigt endnu ikke fæstnet sig, og det bidrager til forvirringen, at de enkelte funktioner ofte ændrer sig i takt med, at nye anvendelsesformer tages i brug.

Retsgrundlag

Det gælder for alle de nævnte ansvarskategorier, at de enten kan tænkes præsteret i et aftaleforhold eller uafhængigt af aftale. Ganske ofte anvendes Internet-applikationerne uafhængigt af aftaleforholdet, f.eks. ved almindelig "surfing". Men det samme gælder for levering af selve Internet-adgangen (som ofte er mulig gennem faktisk brug af udstyr opstillet på offentlige steder, som f.eks. biblioteker el.lign.) samt for forskellige Internet-tjenester. Et eksempel på sidstnævnte er faciliteter til e-post kommunika-

tion, som i stigende omfang tilbydes vederlagsfrit (reklamefinansieret gennem såkaldte banner-annoncer på hjemmesider) fra the World Wide Web (www).

Passiv medvirken?

Det er almindeligt antaget, at strfl. § 23 i kraft af analogi kan udvides til også at omfatte visse former for passiv medvirken, hvis der er en særlig forbindelse mellem hovedmanden og den passive medvirker. For at kunne gøre et ansvar gældende for passiv medvirken kræves det dog, at den passive medvirker kan og bør indse, at der er tale om et retsstridigt forhold, og at han havde mulighed for at gribe ind og forhindre fuldbyrdelsen. Dernæst kræves det, at han havde en særlig tilskyndelse hertil i kraft af sin tilknytning til hovedmanden og den krænkede interesse. Kravene hertil er fastlagt i retspraksis, jf. nærmere *Waaben*: Strafferettens almindelige del I – ansvarslæren (1993), s. 213 ff. Tankemønsteret er principielt det samme i erstatningsretten, se hertil *von Eyben & Isager*: Lærebog i erstatningsret, 5. udg. (2003), s. 43 f. med henvisning til dommen i *U 1985.886 H:* Har den passive krænket en pligt, som må anses for relevant ud fra en erstatningsretlig synsvinkel?

Handlepligt?

Om der er en handlepligt eller ikke beror såvel på de faktiske forhold i sagen (som undertiden kan være vanskelige at oplyse) som af en retlig vurdering (hvis udfald undertiden kan være genstand for komplicerede retlige overvejelser). Et eksempel herpå er dommen i *U 1996.209 H*, hvor Højesteret antog, at udgiveren af et annoncehæfte kunne straffes for medvirken til en annoncørs retsstridige reklamering med ulovlig tilgift, jf. mfl. § 6, stk. 1, 2. pkt. Retten antog, at det ved fastsættelsen af, om udgiveren havde udvist strafbar uagtsomhed, måtte være afgørende, "... om [udgiveren] ved et umiddelbart gennemsyn af annoncerne – et gennemsyn, som det naturligt må påhvile en udgiver af et annoncehæfte at foretage som en rutine – burde have indset, at der i de pågældende annoncer utvivlsomt reklameredes med ulovlig tilgift."

Medieansvar

En særlig regulering af medvirkensansvaret gælder for den, der udgiver et periodisk skrift eller udsender en radio- eller fjernsynsudsendelse. Efter reglerne i medieansvarsloven, se herved §§ 11-24, er dette ansvar nøje knyttet til en række personer, der har at gøre med de redaktionelle beslutninger, der træffes omkring udgivelsen (men ikke med f.eks. trykning og teknisk formidling mv.). Da loven med § 1, nr. 3, også omfatter tekster, billeder og lydprogrammer, der periodisk udbredes til offentligheden, såfremt de har karakter af en nyhedsformidling, som kan ligestilles med periodiske skrifter, radio og tv (som defineret ved lovens §

1, nr. 1-2), *kan* den tænkes at omfatte visse former for Internetbaseret nyhedsformidling, der drives på denne måde (periodisk), f.eks. ved at formidle nyheder gennem *web-casting* eller *podcasting*. Ifølge lovens § 8, stk. 1, skal foretagender, der udgiver sådanne massemedier, for at være omfattet af lovens regler have indgivet anmeldelse til Pressenævnet. Ved modtagelsen af en sådan anmeldelse undersøges det ikke, om mediet er omfattet af loven.

Pressenævnet meddeler i sin årsberetning for 2004, s. 19 f., at *debatsider*, hvor udefrakommende selv kan skrive uredigerede debatindlæg, ikke er omfattet af medieansvarsloven, idet der ikke er tale om en redigeret envejskommunikation. Dette gælder også, selv om en redaktionel medarbejder på egen hånd skriver indlæg til debatsiden.

17.1.e. E-handelsloven

En række af de fornævnte medvirkensspørgsmål er nu løst ved lov nr. 227 af 22. april 2002 om tjenester i informationssamfundet herunder visse aspekter af elektronisk handel (e-handelsloven). Loven, der gennemfører direktivet om elektronisk handel, 2000/31/EF af 8. juni 2000 (EFT 2000 F L 178/1) indeholder – som allerede antydet ved titlen – en bred vifte af regler, der på forskellig vis regulerer den elektroniske handel, nærmere bestemt, jf. §§ 1-2 "tjenester i informationssamfundet". I relation til ansvarsreglerne er direktivet inspireret af den amerikanske Digital Millennium Copyright Act, se herved *Plesner Mathiasen m.fl.* (2004), s. 189 ff.

Formålet

Reglerne har til formål at trække den fine balance, der skal sikre, at leverandører af visse centrale elektroniske tjenester på den *ene side* ikke afholder sig herfra ved udsigten til at blive holdt medansvarlige for medvirken til deres kunders eventuelle retskrænkelser under en kommunikationsproces, samtidig med at man på den *anden side* forbeholder sig muligheden for et medvirkensansvar i de tilfælde, hvor leverandøren med rimelighed kunne have grebet ind. Dette formål tilgodeses gennem en regulering, der slår fast, hvornår der *ikke* kan gøres et ansvar (dvs. et erstatnings- eller strafferetligt ansvar) gældende. Om der da – uden for reglernes område – er mulighed for at gøre et ansvar gældende på andet grundlag, tager loven ikke stilling til.

Tjenester i informationssamfundet

Lovens omdrejningspunkt er som nævnt begrebet "Tjenester i informationssamfundet". Herved forstås – med de undtagelser, der fremgår af § 1, stk. 2 – "enhver tjeneste, der har et kommercielt sigte, og som leveres online (ad elektronisk vej over en vis

distance) på individuel anmodning fra en tjenestemodtager", jf. § 2, nr. 1. Det er altså enhver kommerciel *on demand online* tjeneste, der er i fokus, uanset om denne præsteres af en fysisk eller juridisk person, jf. § 2, nr. 2.

De centrale ansvarsregler fremgår af lovens §§ 14-16. Reglerne knytter sig til tre forskellige funktioner, som en leverandør af en informationssamfundstjeneste *kan* – men langt fra altid vil – levere.

Ren videreformidling

Den første situation angår "ren videreformidling". Herved forstås i medfør af lovens § 14 det forhold, at tjenesteyderen på et kommunikationsnet *transmitterer* information, der leveres af en tjenestemodtager. Normalt vil den, der alene transmitterer information, ikke kende til indholdet af denne. Dette er baggrunden for bestemmelsens almindelige princip om, at tjenesteyderen, ikke er ansvarlig for den transmitterede information. Princippet gælder dog kun, hvis tjenesteyderen (1) ikke selv tager initiativ til transmissionen, (2) ikke udvælger modtageren af transmissionen og (3) hverken udvælger eller ændrer den transmitterede information.

I tilknytning til denne afgrænsning fastslår stk. 2, at en transmission som nævnt i stk. 1 også omfatter "automatisk, mellemliggende og kortvarig oplagring af information, hvis denne oplagring udelukkende har til formål at gennemføre transmissionen, og hvis oplagringen ikke varer længere, end hvad der med rimelighed kan antages at være nødvendigt for at gennemføre transmissionen". Herved sigtes til de pakker, der lagres undervejs under forløbet af en Internet-kommunikation, jf. bemærkningerne i afsnit 3.3.a. I ophavsretlig henseende er sådanne kopier ligeledes undtaget fra eneretten, jf. ophl. § 11a, der netop fremhæver, at de pågældende eksemplarer "udelukkende har til formål at muliggøre … en mellemmands transmission af et værk i et netværk mellem tredjemænd", se hertil bemærkningerne i afsnit 6.3.b.

Bestemmelsen har først og fremmest betydning for leverandører af selve telekommunikationen, dvs. teleselskaberne. Begrebet teleselskab rummer dog i dag langt mere end leverandøren af selve kommunikationsforbindelsen. Talrige teleselskaber virker ved at "leje" kapacitet hos andre teleselskaber, som de herefter udbyder særskilt (og ofte til lavere betaling). Ifølge § 14, stk. 3, gælder bestemmelserne i stk. 1 og 2 også for sådanne tjenesteydere, der leverer *adgang* til et kommunikationsnet.

Caching

Ifølge e-handelslovens § 15 er en tjenesteyder, som på et kommunikationsnet transmitterer information, der leveres af en tjenestemodtager, ikke ansvarlig for "automatisk, mellemliggende og

midlertidig oplagring af denne information eller for indholdet af informationen, hvis oplagringen alene er foretaget med henblik på at gøre senere transmission af informationen til andre tjenestemodtagere efter disses anmodning mere effektiv". Bestemmelsen tager navnlig sigte på den type af caching, som sker på en server (også kaldet *proxycaching*). Tjenesteyderen lagrer her andre udbyderes web-sider på sin lokale server (proxyserver) med det formål at stille siderne til rådighed for sine tjenestemodtagere med så kort transmissionstid som muligt. Også denne undtagelse dækkes ophavsretligt ind af undtagelsen i ophl. § 11a. Den caching, der foretages af brugeren selv på eget udstyr i forbindelse med *browsing*, omfattes ikke af bestemmelsen, idet den ikke resulterer i et eksemplar, som leverandøren er rådig over.

Foruden disse to former for caching forekommer en tredje type, kaldet *mirror caching* i forbindelse med brugen af søgemaskiner som f.eks. <google.com>. For at effektivisere søgeprocesserne foretager udbyderne af disse systemer en kopiering af særligt populære sites på deres eget udstyr. Da udbyderen af en søgemaskine ikke er leverandør af et "kommunikationsnet", som anført i første led, er bestemmelsen uanvendelig i disse tilfælde, jf. *Plesner Mathiasen m.fl.* (2004), s. 206.

Bestemmelsen stiller imidlertid en række krav som må opfyldes, for at tjenesteyderen skal kunne påstå ansvarsfrihed.

Leverandøren må for det *første* ikke ændre informationen (og dermed gør den til sin egen). Bestemmelsen sigter altså mod en tjenesteyder, der indtager en rent passiv og teknisk funktion i kommunikationsprocessen.

Dernæst må han for det *andet* overholde betingelserne for adgang til informationen, f.eks. respektere de adgangskoder mv., som hans kunder gør brug af. Heri ligger også den, indlysende, konsekvens, at leverandøren ikke må udbyde en tjeneste, der er betalbar hos sin hjemmelsmand, uden betaling (eller mod betaling til leverandøren).

For det *tredje* skal leverandøren overholde de regler om ajourføring af informationen, der er almindeligt anerkendt og anvendt i branchen. Bestemmelsen sigter til et problem, der også er aktuelt ved linking og robottering, se herved s. 428, nemlig den tidsforskydning, der nødvendigvis vil indtræde mellem det tidspunkt, hvor værket er hentet til caching fra kilden og til det opdateres igen. Opdateres en hjemmeside hyppigt – f.eks. hvert minut – vil en caching, der foregår med et længere tidsinterval – f.eks. hver time – give brugeren en lavere informationskvalitet og dermed skabe et ringere produkt. Da caching på den anden side

er en nødvendighed ved brugen af søgemaskiner mv., er det nødvendigt at finde en balance. Og denne balance er så fundet med henvisningen til, hvad der er "almindeligt og anerkendt og anvendt i branchen".

Som et *fjerde* krav må leverandøren ikke foretage "indgreb" i den lovlige anvendelse af teknologi, som er almindeligt anerkendt og anvendt i branchen, for at skaffe sig data om anvendelsen af informationen. Bestemmelsen indeholder i hvert fald to regler, der begge beskytter den brug af bannerannoncer, der er almindelig i branchen som grundlag for finansiering af gratis nettjenester. For det første må cache-leverandøren ikke skaffe sig oplysning om, hvor mange "hits" den enkelte hjemmeside blev genstand for. Kunne han det, ville han være i stand til at få kendskab til forhold, som udbyderen normalt vil bevare som erhvervshemmelighed. For det andet må han respektere de teknologier, der måtte være indbygget i hjemmesiden for at sikre oplysning til dennes indehaver om antallet af hits på den cachede hjemmeside.

Det *femte* og sidste krav går ud på, at leverandøren straks skal tage skridt til at fjerne den information, tjenesteyderen har oplagret, eller til at hindre adgangen til den, når tjenesteyderen får kendskab til, at informationen er *blevet fjernet* fra nettet eller adgangen til den hindret, eller at en *domstol* eller en *administrativ myndighed* har krævet informationen fjernet eller adgangen til den hindret. I den ene situation er der altså tale om, at informationen er fjernet fra kilden, f.eks. efter påbud fra en domstol eller en myndighed. Den anden situation foreligger, hvor kilden af en eller anden grund (f.eks. fordi denne befinder sig i udlandet) ikke har fjernet informationen, men hvor tjenesteyderen til gengæld mødes med et krav herom fra en domstol eller en administrativ myndighed, f.eks. Datatilsynet, jf. LBP § 59, eller Forbrugerombudsmanden, jf. mfl. § 19, stk. 2, § 17, stk. 2 og 4, og § 21.

Oplagring

E-handelslovens § 16 fastslår endelig, at en tjenesteyder der har oplagret ("hostet") information på anmodning af en tjenestemodtager (typisk en kunde), der har leveret informationen, er *ansvarsfri* for den således oplagede information i to situationer.

Den ene situation foreligger, jf. § 16, stk. 1, nr. 1, hvor tjenesteyderen ikke har *kendskab* til den ulovlige eller skadevoldende aktivitet eller information. Tjenesteyderen er med andre ord i *god tro*. For så vidt angår erstatningskrav må denne gode tro knytte sig til forhold eller omstændigheder, hvoraf den skadevoldende aktivitet eller information fremgår.

Den anden situation foreligger, hvor tjenesteyderen får et kendskab som nævnt i nr. 1, og straks tager skridt til at fjerne informationen eller hindre adgangen til den.

I e-handelsdirektivets art. 15 findes en almindelig regel (som ikke er indført i e-handelsloven) om, at der ikke skal pålægges nogen generel forpligtelse til at føre tilsyn med den information, de fremsender eller oplagrer, eller en generel forpligtelse til aktivt at efterforske forhold eller omstændigheder, der tyder på ulovlig virksomhed. En sådan pligt kan vel heller ikke udledes af § 16, men begge led i § 16, stk. 1, bygger på et godtroskrav, der kan være mindst ligeså problematisk at udfylde i det praktiske liv, og som kan risikere – i strid med direktivets intentioner – at hæmme informationsspredningen på nettet: Hvornår er en racistisk udtalelse i en nyhedsgruppe f.eks. omfattet af strfl. § 266b? Er beskyttelsestiden for et ophavsretligt værk udløbet? Er der hjemmel til at opbevare en given personoplysning? I overensstemmelse med det princip, der er indeholdt i direktivets art. 15, bør domstolene ikke stille for store krav til tjenesteyderens mulighed for at ramme rigtigt i sådanne juridiske vurderinger, som kan være vanskelige selv for jurister. Det må være tilstrækkeligt, han udøver et kvalificeret skøn på grundlag af de oplysninger, han har for hånden. Han må således forventes at optræde som en *bonus pater* tjenesteyder – ikke som en retsinstans. En person, der mener sig berettiget til at få fjernet påstået ulovlig information, har omvendt en tilsvarende stærk pligt til at dokumentere sit krav.

Ansvarsfriheden gælder ikke, når tjenestemodtageren handler under tjenesteyderens myndighed eller kontrol, jf. stk. 2. Herved sigtes til omgåelseslignende tilfælde, hvor afsenderen af informationen (altså hovedmanden i det retsstridige forhold) på forhånd har aftalt med tjenesteyderen, hvilken information der skal ligge, med det formål at opnå en situation, hvor tjenesteyderen kan bibeholde denne information uden risiko for ansvar.

17.2. Formueforbrydelser

17.2.a. Tyveri

Strfl. § 276 om tyveri fastslår udtrykkeligt sit beskyttelsesfelt til begrebet "rørlig ting". Den, der tilegner sig en diskette med et edb-program, begår tyveri, hvorimod den, der ulovligt henter

programmet ned fra en hjemmeside, ikke gør det. Når data overføres, sker der en flytning (eller rettere "ommøblering") af bits, hvorimod der ikke flyttes atomer (som jo netop er "rørlige ting"). Se hertil *Christina Wainikkas* afhandling i Svensk Juristtidning 2003, s. 577 "Information som självständigt objekt".

Energimængde

At bestemmelsen tillige straffer tyveri af en energimængde, jf. andet led ("en energimængde, der er fremstillet, opbevaret eller taget i brug til frembringelse af lys, varme, kraft eller bevægelse *eller i andet økonomisk øjemed*" udhævet her) spiller ingen nævneværdig rolle på IT-området. Det tyveri af den elektromagnetiske kraft, der f.eks. indgår som et nødvendigt led ved ulovlig anvendelse af telekapacitet, må således anses for opslugt af reglerne om brugstyveri, jf. strfl. § 293 og bemærkningerne herom nedenfor.

Informationsværdi

Derimod kan det diskuteres, om den merværdi, informationsindholdet giver et datamedium, skal influere på den strafferetlige subsumption: Skal den indlæste software anses som en værdiforøgende omstændighed, der f.eks. giver hjemmel for straf i henhold til den kvalificerede strafhjemmel, jf. strfl. § 286? Eller må forholdet rettelig rubriceres som to gerningsindhold, der dels indbefatter tyveriet af mediet, dels retsstridig anvendelse af information?

Hvis originalmediet med tilhørende identificerbar manual er stjålet, mister den bestjålne formentlig retten til at udnytte denne software, idet "eksemplaret" dermed vil kunne danne grundlag for en midlertidig – og i ekstinktionstilfælde undtagelsesvis permanent – lovlig brug hos den godtroende erhverver af eksemplaret, jf. diskussionen i afsnit 12.3. Derimod opnår tyven ikke ret til at anvende programmet, allerede fordi han ikke er "lovlig bruger", jf. ophl. § 36. Forudsættes det, at der ikke indtræder ekstinktion vedrørende det bestjålne eksemplar (hvilket efter danske ejendomsretlige regler vil være den absolutte undtagelse), vil heller ikke en efterfølgende bruger have en "lovlig" adgang til at benytte programmet; men frem til det tidspunkt, hvor et udleveringskrav gøres gældende, vil der ikke kunne rettes sanktioner mod denne brug hos den godtroende erhverver. Disse betragtninger taler for at anse tyveriet af programdisketten, manualen eller andet ledsagende materiale, der signalerer en legitimation til at anvende licensen, som mere værdifuld end selve medieværdien. Tilsvarende må gælde allerede ud fra en ulempebetragtning, hvis tyveriet bevirker, at den bestjålne ikke længere kan anvende programmet – f.eks. fordi programmet er udstyret med en anordning, der forhinder geninstallation af programmet på nyt udstyr.

En enkelt amerikansk afgørelse har taget stilling til spørgsmålet, se *USA v. Darian Lyons*, 992 F.2d 1029 (1993). Appelretten for 10th Circuit kom her til, at strafferammen skulle tage højde for værdien af det bestjålne software. Som anført oven for kan resultatet tiltrædes. Se ligeledes den norske byretsdom i L&D 63/2000, s. 3 ff., der antog, at værdien af de data (forretningssensitive oplysninger), der befandt sig på et stjålet databånd skulle medregnes i vurderingen af det stjålnes værdi. Tiltalte idømtes herefter en betinget straf af 10 måneders fængsel.

Telefontidskort

Et særligt spørgsmål er, hvorledes man straffer tyveri af telefontidskort eller andre medier, der i kraft af betalingsordninger eller lignende kan give adgang til en formueforskydning. I det omfang kortet i sig selv er bærer af en værdi (som f.eks. ved Danmøntkort), er det uproblematisk at rubricere forholdet som tyveri af en tilsvarende værdi: Et Danmønt-kort med en restværdi på 500 kr. må således håndteres på samme måde som tyveri af 500 kr. Er betalingsmidlet derimod indrettet således, at det alene rummer en nøgle til at kunne gennemføre en betaling, men med mulighed for at afskære denne betaling gennem efterfølgende spærring el.lign., må forholdet vurderes anderledes. Tyveriet af kortet må her betragtes som et tyveri af selve den fysiske indretning samt – alt efter omstændighederne – som en forberedelseshandling til et efterfølgende databedrageri, der realiseres, når den kode mv., der findes på kortet, anvendes til at realisere et forbrug (f.eks. af telefontid).

Ved sin kendelse i *Rt. 1995.1872* fandt Norges Højesterett, at køb af telefonkoder tilhørende kunder hos teleselskabet AT&T måtte anses som hæleri. Højesterett lægger vægt på, at koderne ved at give adgang til teleselskabernes tjenester repræsenterede en økonomisk værdi, som der kan disponeres over og dermed havde karakter af "udbytte". Forholdet ville herhjemme umiddelbart være omfattet af bestemmelsen om databedrageri i strfl § 279a, jf. *TfK 2000.93 V*, hvor tiltalte blev straffet for "kloning" af mobiltelefonnumre muliggjort ved indbygning af et ekstra kredsløb i mobiltelefonen

17.2.b. Brugstyveri

Der findes ingen særregler om "edb-brugstyveri" i straffeloven. En del af de retsstridige handlinger, der indebærer en uberettiget anvendelse af data, vil enten kunne straffes efter strfl. § 263, stk. 2, eller efter de immaterialretlige sanktionsregler. Efter strfl. § 293 straffes den, som uberettiget bruger en "ting", der tilhører en anden, for brugstyveri. Ser man bort fra det retsstridighedskrav, der kan udledes af ordet "uberettiget", kan reglerne om brugsty-

veri anvendes i relation til de fleste IT-forbrydelser, fordi programmer og data som anden information altid vil optræde i tilknytning til et medium, som der nødvendigvis må gøres "brug" af. I overensstemmelse med denne betragtning straffede *U 1978.1003 Ø* en person efter reglerne om brugstyveri for ulovligt at have tilsluttet sig et fællesantenneanlæg. En sådan tilkobling er i sagens natur udelukkende motiveret med ønsket om at opnå adgang til det programindhold (den information), der transmitteres fra et sådant anlæg.

Når man vurderer alvoren af en sådan uberettiget brug, må man formentlig kunne skele til karakteren af den information, der er blevet brugt, jf. bemærkningerne ovenfor om tyveri. En sådan argumentation er dog ikke uden vanskeligheder. Betones den for stærkt, forvandles reglen om brugstyveri nemlig til en generel straffehjemmel for immaterialretlige krænkelser, eftersom det ophavsretlige element jo ofte vil gøre "brugen" af det medium, hvorpå programmet ligger, "uberettiget", jf. § 293.

Der vil ikke i almindelighed være grundlag for at straffe for tyveri af den elektricitet, der forbruges gennem ulovlig brug af et IT-system, sml. herved strfl. § 276, 2. pkt. Derimod kan bedragerireglen efter omstændighederne komme til undsætning i sådanne tilfælde, omend måske noget anstrengt. Se *U 1938.1113 Ø*, der straffede for bedrageri, jf. strfl. § 279, i en situation, hvor tiltalte havde installeret sin telefon på en sådan måde, at den ikke registrerede samtaler.

§ 298 nr. 4

Man kan overveje, om den, der uberettiget skaffer sig adgang til programudbud ved at omgå tekniske spærreanordninger mv., dermed omfattes af den særlige hjemmel i § 298, nr. 4, til at straffe den, der "uden erlæggelse af den fastsatte betaling tilsniger sig adgang til forestilling, udstilling eller forsamling eller til befordring med offentlig samfærdselsmiddel eller til benyttelse af anden almen tilgængelig indretning". Selv om bestemmelsen kan siges at ramme samme beskyttelsesinteresse som den, der kan begrunde en straf for brug af ulovligt dekoderudstyr mv., må det antages, at kravet om "tilsnigelse" indebærer, at gerningsmandens overværelse af den pågældende forestilling mv. sker i kraft af sin fysiske tilstedeværelse. En del af disse spørgsmål – nemlig i relation til omgang med adgangsmidler til informationssystemer, hvortil adgangen er forbeholdt betalende brugere – er nu reguleret i strfl. § 301a, se hertil afsnit 17.5.b.

17.2.c. Tingsødelæggelse

Hærværk

Angreb mod IT-systemer straffes efter den almindelige hærværksbestemmelse, jf. strfl. § 291 eller – hvis der er tale om samfundsmæssigt vitale systemer – efter strfl. § 193. § 291 er bl.a. anvendt ved dommen i *U 1987.216 Ø*, der lagde til grund, at databærende medier med indlagte data må anses for "ting". § 193 har ikke været anvendt i forbindelse med IT-betingede forstyrrelser mv. Den kan ligeledes tænkes anvendt mod en person, der bevidst spreder programvira, f.eks. via Internet. Spredes sådanne vira uagtsomt, f.eks. ved sløset omgang med inficerede programdisketter, er der derimod kun grundlag for at anvende § 291, der er undergivet almindelige forsætskrav, hvis der foreligger *dolus eventualis*, f.eks. fordi denne risiko på forhånd er indskærpet gerningsmanden (f.eks. i form af en sikkerhedsinstruks på en arbejdsplads).

Hindring af brug

Det må ligeledes anses for hærværk, at gerningsmanden manipulerer et IT-system på en sådan måde, at dets retmæssige indehaver helt eller delvis afskæres fra at bruge det, f.eks. ved såkaldte *denial-of-service*-attacks. Man kan diskutere, om et sådant angreb indebærer, at genstanden er "bortskaffet" i medfør af § 291. Dette vil utvivlsomt være tilfældet, hvis der er tale om et IT-system, som styrer indehaverens adgang til fysisk indretning (f.eks. et globalt containernetværk eller en satellit), og angrebet indebærer, at besidderen mister muligheden for at kontrollere den pågældende indretning. Men meget taler for også at anse bestemmelsen for anvendelig, hvis angrebet afskærer indehaverens adgang til at betjene et IT-system som sådant, jf. bemærkningerne ovenfor om indlagte data som "ting". En anden strafhjemmel for at ramme begge typer af tilfælde er strfl. § 293, stk. 2, som med bøde eller fængsel indtil 1 år (men med mulighed for strafforhøjelse til 2 år under skærpende omstændigheder, jf. stk. 2) straffer den, som lægger hindringer i vejen for, at nogen "udøver sin ret til at råde over eller tilbageholde en ting". Også i denne relation vil det dog være afgørende, om man – som antaget her – kan betragte digitale data i et IT-system som "ting".

I straffelovrådets betænkning 1032/1985 antages det som "mest sandsynligt", at en domstol vil anse lagrede data som "ting"; men rådet anser problemet for at have forholdsvis begrænset betydning, eftersom forholdet også kan opfattes således, at der ved sletning af data sker en beskadigelse af selve databæreren (mediet), se s. 33 f. Rådet antager ligeledes, at begrebet "slettelse" i IT-sammenhæng vil række videre end til den totale fjernelse af indholdet; men også således, at blot adgangen til lagrede data er umuliggjort.

17.2.d. Databedrageri

Strfl. § 279a straffer den, som for derigennem at skaffe sig eller andre uberettiget vinding retsstridigt ændrer, tilføjer eller sletter oplysninger eller programmer til elektronisk databehandling eller i øvrigt retsstridigt søger at påvirke resultatet af sådan databehandling. Bestemmelsen har – dette ligger vel nærmest i sagens natur – centrale lighedspunkter med den almindelige bedrageribestemmelse, der ligesom § 279a kræver, at der skal være handlet for at opnå "uberettiget vinding" for gerningsmanden eller andre. Men § 279a adskiller sig fra den almindelige bedrageriregel ved ikke at stille krav om, at *en person* skal være vildledt. Dette krav er erstattet med en betingelse om, at der skal være gjort indgreb i grundlaget for databehandlingen. I stedet for kravet om, at gerningsmanden skal "fremkalde, bestyrke eller udnytte" en vildfarelse, stiller bestemmelsen krav om, at han "ændrer", "tilføjer" eller "sletter" oplysninger (data) eller programmer.

Bestemmelsen stiller ingen krav om, hvordan dette sker. Det klassiske eksempel herpå er, at gerningsmanden ved at trænge ind i et system til kontoførelse, retsstridigt overfører beløb til sin egen konto, som efterfølgende hæves. Disse tilfælde har mange flere lighedspunkter med det klassiske tilfælde af underslæb begået ved medarbejdere. Men gerningsmanden behøver ikke befinde sig bag en almindelig computer-terminal. Med fremkomsten af elektroniske betalingssystemer er området for denne gerningstype blevet langt bredere. Også brug af misvisende stregkoder eller elektrisk påvirkning af kommunikationen kan realisere gerningsindholdet, jf. *Greve & Langsted* (2000), s. 88. Et eksempel herpå kan være manipulation af en vareautomat (f.eks. på en benzintank), der kan benyttes ved hjælp af betalingskort. Et andet eksempel er manipulationer af et Danmønt-kort, der retsstridigt sætter brugeren i stand til at "betale" for køb. Omvendt må der i en verden, hvor stort set al information på et eller andet tidspunkt passerer igennem en computer, stilles krav om en vis nærhed mellem gerningsmanden og det pågældende IT-system. Der kræves forsæt til alle led i gerningsindholdet.

Bestemmelsen om databedrageri kan i sammenhæng med forsøgsreglerne anvendes til at opsamle fremstilling af falske kreditkort eller andre redskaber, der udelukkende kan tænkes anvendt til at udvirke bedrageri. Således blev bestemmelsen anvendt i *U 2000.1881 Ø* i en situation, hvor gerningsmanden havde fremstillet 130 totalt forfalskede hævekort. Der blev tillige straffet for forsøg. Straffen blev udmålt til 1 års ubetinget fængsel under

henvisning til den ringe opdagelsesrisiko. Se ligeledes *TFK 2000.485 Ø*, der idømte 60 dages ubetinget fængsel for databedrageri i forbindelse med brug af totalforfalskede Eurocard- og Visa-kort med et udbytte på ca. 33.000 kr. Fremstilling mv. af falske elektroniske penge er i øvrigt nu kriminaliseret ved strfl. § 169a, se hertil afsnit 17.3.c.

Telefontidstyveri

Ved Roskilde rets dom af 19. december 1996 i en større sag om hacking, er det bl.a. lagt til grund, at "tyveri af telefontid" falder inden for ordlyden af strfl. § 279a, idet der er tale om at påvirke resultatet af en elektronisk databehandling. I den pågældende sag havde gerningsmændene dels udvirket telefontidstyveriet ved misbrug af frikaldsnumre, dels ved retsstridig tilegnelse af såkaldte NUI-brugerkoder, der via særlige omstillingscentraler henfører betalingspligten for en brug af datanet (Datapak-systemet) til en specifik bruger. Forholdet kunne også være henført til den mindre strenge strfl. § 293 om brugstyveri. Se nu også *TfK 2000.93 VLD*.

17.3. Forbrydelser vedrørende bevismidler og penge

17.3.a. Dokumentfalsk

§ 171

Den, der gør brug af et falsk dokument til at skuffe i retsforhold, straffes ifølge strfl. § 171, stk. 1, for dokumentfalsk. Straffen er, jf. § 172, stk. 1, bøde eller fængsel indtil 2 år. Er dokumentfalsk af særlig grov karakter, eller er et større antal forhold begået, kan straffen stige til fængsel i 6 år, jf. stk. 2.

Bestemmelsens definerer udtrykkeligt, hvad der skal forstås som et "dokument". Det er, jf. stk. 2, en "skriftlig eller elektronisk med betegnelse af udstederen forsynet tilkendegivelse, der fremtræder som bestemt til at tjene som bevis." Bestemmelsen er affattet på grundlag af forslaget i betænkning 1417/2002, se s. 104 ff. og 153 ff. Ved denne lejlighed kom henvisningen til "elektroniske" tilkendegivelser ind. Dette indebærer, at også dataoplysninger vil være omfattet af dokumentbegrebet og dermed beskyttet mod dokumentfalsk. Eksempler herpå kan være e-mail og SMS.

Det er ikke noget krav, at disse dataoplysninger fremtræder på en måde, så de "ligner" et fysisk dokument, f.eks. ved at være sat op som sådant i tekstbehandling eller i en pdf-fil. Det kræves

blot, at dokumentet fremtræder med en *udsteder*betegnelse eller i det mindste *afsender*betegnelse. At kravene formentlig må sættes relativt lavt antydes ved Østre Landsrets 5. afdelings dom af 26. september 2001 (sagsnr. 5. afd. a.s. nr. S-1974-01), altså *før* bestemmelsens indførelse. Her havde T i et enkelt tilfælde fremsendt en e-mail med en falsk afsenderbetegnelse til Diners Club, hvori han udgav sig for at være indehaver af et Diners kort, som han – svigagtigt – opgav at have mistet. E-mailen blev sendt i forlængelse af en telefonsamtale med Diners, hvor T også havde opgivet at være indehaver af det pågældende kort, som ved denne lejlighed blev meldt spærret. I e-mailen anmodede T om, at der blev fremsendt et nyt kort til kortholderen c/o T. Begge instanser fandt uden videre, at den afsendte e-mail måtte karakteriseres som en skriftlig tilkendegivelse, jf. den daværende udformning af strfl. § 171, stk. 2.

17.3.b. Urigtige erklæringer

Ifølge strfl. § 163 straffes den, som til brug i retsforhold, der vedkommer det offentlige, skriftligt *eller ved andet læsbart medie* afgiver urigtig erklæring eller bevidner noget, som den pågældende ikke har viden om, med bøde, hæfte eller fængsel indtil 4 måneder. Bestemmelsen, der som nævnt s. 725 er ændret på baggrund af Østre Landsrets dom af 13. februar 1995 i Proms-sagen, vil udvide strafansvaret for urigtige skriftlige erklæringer, således at det også omfatter tilfælde, hvor man gennem erklæringens form sikrer sig, at borgeren er klar over, at erklæringen tillægges vægt i myndighedens arbejde og eventuelt kan indgå i grundlaget for myndighedens afgørelse i en konkret sag.

Strfl. § 175

Ifølge strfl. § 175, stk. 1, straffes den, der for at skuffe i retsforhold "i offentligt dokument eller bog, i privat dokument eller bog, som det ifølge lov eller særligt pligtforhold påhviler den pågældende at udfærdige eller føre, eller i læge-, tandlæge-, jordemoder- eller dyrlægeattest afgiver urigtig erklæring om noget forhold, angående hvilket erklæringen skal tjene som bevis". På samme måde straffes ifølge stk. 2 den, der i retsforhold gør brug af et sådant dokument eller en sådan bog som indeholdende sandhed. Bestemmelsen anvender det dokumentbegreb, der er indeholdt i § 171, stk. 2. Den gælder dog også, når dokumentet eller bogen er udfærdiget eller føres på andet læsbart medie, jf. § 175, stk. 3, der blev indført efter forslaget i betænkning 1417/2002. Straffen er bøde eller fængsel indtil 3 år.

17.3.c. Falske elektroniske penge

Ifølge strfl. § 169a straffes den, der uretmæssigt fremstiller, skaffer sig eller udbreder falske elektroniske penge med forsæt til, at de anvendes som ægte. Den blotte *besiddelse* af de falske elektroniske penge er således ikke omfattet. Kravet om at pengene i givet fald er "skaffet" (hvis ikke der er tale om fremstilling eller udbredelse) markerer således et krav om en aktiv handling fra gerningsmandens side. Dermed beskyttes den, der uforvarende (f.eks. i en fremsendt e-mail) er kommet i besiddelse heraf. Ved *falske* elektroniske penge forstås midler, der uden at være ægte elektroniske penge *er egnede* til at blive brugt som sådanne, jf. stk. 2. Straffen er bøde eller fængsel indtil 1 år og 6 måneder. Straffen kan stige til fængsel i 6 år, hvis handlingen er af særlig grov beskaffenhed, herunder navnlig på grund af den måde, den er udført på, eller på grund af beløbets størrelse, jf. stk. 3.

Bestemmelsen er indsat ved IT-straffereformen i 2004 på grundlag af forslaget i betænkning 1417/2002, s. 79 ff. Baggrunden var den lovregulering af elektroniske penge, der er gennemført på grundlag af direktiv 2000/6, se hertil afsnit 20.4.g. Begrebet "elektroniske penge" skal derfor forstås i overensstemmelse med reglerne herom i § 308 i lov om finansiel virksomhed, dvs. som "en pengeværdi, som er repræsenteret ved et krav på udstederen, der er lagret på et elektronisk medium". Som nærmere omtalt i afsnit 20.4.g. er markedet for e-penge endnu ikke vokset frem. Som eksempler herpå kan nævnes Danmøntløsningen. Også løsninger, der indebærer brug af en mobiltelefon, vil være omfattet, hvis løsningen f.eks. indebærer, at pengeværdien lagres på mobiltelefonens SIM-kort.

17.3.d. Straffelovens § 301

Med bestemmelsen i strfl. § 301 er der hjemlet straf for den, der uberettiget anvender, fremstiller, skaffer sig, besidder eller videregiver (1) oplysninger, som identificerer et betalingsmiddel, der er tildelt andre, eller (2) genererede betalingskortnumre. Straffen er bøde eller fængsel indtil 1 år og 6 måneder. Formålet med bestemmelsen er at ramme visse forberedelseshandlinger, der kan føre til uberettiget brug af betalingskort og andre elektroniske betalingsmidler (herunder e-penge, jf. strfl. § 169a). Dette opnås gennem et fremrykket fuldbyrdelsesmoment, jf. bemærkningerne herom s. 726. Bestemmelsen tager således navnlig sigte på tilfælde af organiseret kriminalitet, hvor gerningsmanden dis-

tribuerer et stort antal betalingskortnumre, som så anvendes samtidigt inden det retsstridige forhold opdages og fører til en spærring af kortet. Gribes gerningsmanden, inden selve benyttelsen har fundet sted, ville det uden denne bestemmelse være vanskeligt at bevise, at han havde det fornødne *forsæt* til denne benyttelse.

De forhold, der giver grundlag for at anvende bestemmelsen, sigter derfor også bredt. Anvendelsesområdet er tilfælde, hvor gerningsmanden har foretaget sig noget aktivt i relation til de pågældende identifikationsoplysninger eller genererede betalingskortnumre, f.eks. fremstillet dem (ved hjælp af en særlig algoritme), besiddet dem eller foretaget sig noget *aktivt* for at "skaffe" dem.

Bestemmelsen straffer ikke besiddelse af "ægte" betalingskortnumre, dvs. numre som gerningsmanden har fået i hænde gennem en handling, der har bragt ham i fysisk kontakt med betalingskortet (f.eks. ved afluring af offeret). Sådanne numre vil det ofte være nødvendigt at udveksle i helt legitimt ærinde, og bestemmelsen ville dermed få en utilsigtet vid anvendelse. Derimod straffes den rene besiddelse mv. af identifikationsnumre, om hvilken der i almindelighed ikke vil være nogen tilsvarende legitim anvendelse. Dens primære anvendelsesområde er netop de tilfælde, hvor numrene frembringes "syntetisk", og hvor de dermed typisk også indgår i en organiseret kriminalitet.

Det er et fælles krav, at gerningsmanden skal have *forsæt* til at anvende de nævnte oplysninger mv. *uberettiget*. Ved anvendelsen af bestemmelsen vil disse to krav ofte spille sammen: Kan gerningsmanden godtgøre, at hans besiddelse af de pågældende oplysninger har et helt berettiget formål (f.eks. som led i en legitim forskning om IT-sikkerhed), vil det som regel være åbenbart, at der ikke er grundlag for at straffe.

17.4. Fredskrænkelser

17.4.a. Straffelovens § 263, stk. 2

IT-informationers fortrolighed nyder strafferetlig beskyttelse ifølge strfl. § 263, stk. 2, hvorefter den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem, straffes med bøde eller fængsel indtil 1 år og 6 måneder. Bestemmelsen gælder såvel for den indtrængen, der begås af *udenforstående* (ofte kal-

det "hacking"), af *ansatte* (f.eks. via et lokalnet), af *samarbejdspartnere* (f.eks. i forbindelse med vedligeholdelse eller fejlretning) eller af virksomhedens *ledelse* (i form af ulovlig overvågning mv.). Strafferammen kan stige til fængsel indtil 6 år, hvis forholdet er begået med forsæt til at skaffe sig eller gøre sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder eller under andre særligt skærpende omstændigheder, jf. stk. 3. På samme måde straffes de i stk. 2 nævnte forhold, når der er tale om overtrædelser af mere systematisk eller organiseret karakter. I gentagelsestilfælde kan straffen derudover stige til 8 år efter den almindelige regel i strfl. § 88, stk. 1.

Gerningsbeskrivelsen i § 263, stk. 2, er efter sin ordlyd ganske omfattende. I retsanvendelsen må der nødvendigvis foretages en udskillelse af de mindre alvorlige former for uautoriseret adgang (jf. forbeholdet "den, der *uberettiget* skaffer sig ..."). Dette retsstridighedskrav vil typisk være opfyldt, når tilgangen til de pågældende data eller programmer er muliggjort gennem anvendelse af passwords eller kalderutiner, som almindeligvis holdes konfidentielle, eller som i øvrigt ikke er almindeligt tilgængelige, se dog modsat *U 1996.979 Ø*.

Ved den pågældende dom blev en bankassistent frifundet for at have skaffet sig adgang til bankens IT-system og dermed til en række erhvervshemmeligheder. Dette skete ved brug af medarbejderens eget password, men uden forbindelse med sit arbejde for banken, angivelig i frustration over det personlige nederlag, han følte ved at skulle forlade sit job i banken. Retten fandt, at medarbejderen havde været berettiget til at indhente de pågældende oplysninger ved hjælp af sit password, men knytter ikke yderligere bemærkninger hertil. Dommens forudsætning om, at strfl. § 263, stk. 2, knytter sit retsstridighedskrav til, at gerningsmanden rent *faktisk* har adgang til de pågældende oplysninger, og ikke om han arbejdsmæssigt eller i øvrigt har noget *formål* med at bruge dem, fører til ganske vidtgående og næppe helt acceptable resultater. Ud fra samme betragtning måtte man f.eks. skulle anerkende, at enhver medarbejder har ret til at låse sig ind på andre medarbejderes kontorer og finde oplysninger frem, blot fordi der gjaldt en fælles nøgle til samtlige kontorer. Se tilsvarende kritikken af en lignende engelsk afgørelse, *David Bainbridge* i 13 CLSR 352 ff. (1997). Problemstillingen berøres i øvrigt ved den norske højesteretsafgørelse i *Rt. 1998.1971*, der under dissens (3-2) frifandt en ingeniør for under et tv-program om datasikkerhed at forsøge at logge sig op på Oslo Universitets computer via www ved at gætte typiske passwords. Denne brug ansås ikke i sig selv for "uberettiget".

17.4.b. Straffelovens § 263, stk. 1, nr. 1

Bestemmelsen i § 263, stk. 2, må læses i sammenhæng med bestemmelsen om brevåbning i § 263, stk. 1, nr. 1, der med samme strafferamme straffer den, som "bryder eller unddrager nogen et brev, telegram eller anden lukket meddelelse eller optegnelse eller gør sig bekendt med indholdet".

Bestemmelsen fik sin nuværende affattelse ved lov nr. 89 af 29. marts 1972 på grundlag af Straffelovrådets betænkning om privatlivets fred (nr. 601/1971), der s. 59, lægger til grund, at den også omfatter aflytning af telekommunikation (f.eks. telex) i det omfang kommunikationen ikke har karakter af samtale, og derfor falder ind under § 263, stk. 1, nr. 3). Samme opfattelse har Straffelovrådet lagt til grund i betænkning 1032/1985, som fremsatte forslaget til strfl. § 263, stk. 2, se s. 22. Tanken er altså, at en meddelelse kan være lukket i mere end fysisk forstand. Se nærmere herom mit indlæg i Vestergaard & Balvig (red.): "Med lov ..." – retsvidenskabelige betragtninger i anledning af professor Vagn Greves 60 års fødselsdag (1998), s. 53 ff., *Blume* i U 1999B.195 ff. og *Bekkevold* i Advokaten 1998.49 ff.

Efter ordlyden af denne bestemmelse og på grundlag af dens forarbejder må det antages, at "åbning" af elektroniske postmeddelelser, hvorved en udefrakommende person stifter bekendtskab med informationsindholdet heri, er omfattet, jf. *Karstoft*: Elektronisk dokumentudveksling – retlige aspekter (1994), s. 154. Hvem der er udefrakommende beror på brevets – og den elektroniske meddelelses – adressat, uanset om meddelelsen er elektronisk eller papirbaseret.

Fejladressering

Kommer man til at angive en fejlagtig modtagerangivelse på en besked (f.eks. "hansen@firma.dk" i stedet for den tilsigtede "hansen@firma.com") er meddelelsen åben i relation til den person, der modtager og åbner meddelelsen på adressen "hansen@firma.dk", jf. således *Køge rets dom af 22. marts 2000* i sag S 960/1999. Et modsat resultat ville indebære, at man skulle anse dele af en meddelelse for åbne (nemlig de indledende linjer, der bibringer modtageren forståelsen af, at der foreligger en fejltagelse), men ikke de senere. Et sådant resultat kan ikke udledes af ordlyden. At sådanne meddelelser må anses for åbne må tilsvarende antages at indebære, at modtageren frit kan råde over dem. En eventuel videresendelse kan dog være i strid med andre bestemmelser, således f.eks. strfl. § 264d om videregivelse af meddelelser vedrørende en andens private forhold, eller – hvis meddelelsen indeholder værker – ophavsmandens eneret til eksemplarfremstilling og spredning. Se endvidere afsnit 17.3.d.

Adressat-læsning

Der er næppe grundlag for at antage, at § 263, stk. 1, straffer det forhold, at gerningsmanden stifter bekendtskab med de *adressater*, hvortil og -fra en person kommunikerer. Ordene "bryder ... lukket meddelelse" forudsætter netop, at denne information (der i papirbrevets verden fremtræder på kuverten) ikke er tilgængelig for omverdenen. Tilegnelse af adressat-information kan derimod være omfattet af stk. 2.

Web-anvendelse

Det er ikke afklaret, om overvågning af en edb-terminal med henblik på indblik i de requests, der udgår herfra *uden at ske som led i en elektronisk postbesørgelse*, men for at indhente information fra web-sites el.lign., er omfattet af strfl. § 263, stk. 2. Problemet vil i praksis forekomme ved læsning af log-filer mv. Umiddelbart synes sådanne requests ikke at fremstå som *"meddelelser"*, jf. stk. 1. Vel kan man pege på, at den part, der kommunikerer med en web-site, dermed kun "taler" med web-serveren og altså ikke afgiver nogen egentlig meddelelse til en anden person. Heroverfor kan man pege på, at der i praksis altid vil være nogen, som er ansvarlig for serveren, og som til forskellige formål – f.eks. afregningsformål – kan have interesse i at få aktuelt indblik i disse meddelelser. Afgørende for fortolkningen må være de beskyttelseshensyn, der ligger bag bestemmelsen, altså først og fremmest privatlivshensynet. Og når det gælder dette, er der næppe nogen tvivl om, at der er helt samme beskyttelseshensyn at tage i relation til hypertekst-requests som overfor andre meddelelser, der har karakter af at være en *"anden lukket ... optegnelse"*. Derfor må det antages, at bestemmelsen også yder en strafferetlig beskyttelse af disse logoplysninger – uanset om de foreligger som data, lagret – med eller uden bevidsthed herom – af brugeren på eget lagermedium eller om data, der hentes udefra under den løbende web-kommunikation.

Det subjektive vurderingsprincip

Den almindelige opfattelse af, hvornår meddelelsen er "lukket", vil formentlig falde sammen med en vurdering af, hvornår det er "uberettiget" (jf. indledningsordene til bestemmelsen) at foretage den pågældende aflytning. Der må her antages at gælde et *subjektivt vurderingsprincip*, hvorefter vurderingen af, hvad der er "uberettiget", beror på, hvad en kommunikerende part i den konkrete situation *typisk* må forvente, at andre kan stifte sig bekendtskab med.

Diskussion

Når dette princip anlægges i relation til e-post er det nærliggende at sammenligne med telefoni. Hvis ikke den anvendte e-post-adresse ligefrem fremstår som den officielle kommunikationskanal for den afsendende virksomhed (på samme måde som et papirbrev på virksomhedens eller institutionens brevpapir), må

det i dag anses for almindeligt, at e-post-adressen i et vist, begrænset omfang også anvendes til privat kommunikation for den ansatte i samme omfang som virksomhedens telefon anvendes hertil. På grund af omkostningsstrukturen er en sådan kommunikation i en række henseender mere acceptabel end private telefonsamtaler (som de fleste arbejdspladser tillader i behersket omfang). Dette gælder navnlig på systemer, hvor prisen for at overføre en elektronisk post-meddelelse ikke påfører arbejdsgiveren transmissionsomkostninger, fordi den ikke beregnes i forhold til hver enkelt transmission, men som et samlet beløb pr. måned mv.

Hertil kommer, at den kommunikation, der foregår via elektronisk post, almindeligvis ikke overvåges, selv om muligheden herfor foreligger for den systemansvarlige. Hvor afsenderen af et postkort må være klar over, at postkortets indhold kan tilegnes af enhver, der lader blikket glide henover det (herunder også postbuddet), må afsenderen af den elektroniske meddelelse som udgangspunkt gå ud fra, at meddelelsen ikke overvåges af andre, medmindre han er gjort særligt opmærksom herpå. Men dette udgangspunkt kan fraviges, f.eks. hvis afsenderen må gå ud fra, at det pågældende system jævnligt overvåges eller at kommunikationen herpå i øvrigt uden vanskelighed vil kunne læses – og vil blive læst – af andre.

Sml. herved *Rt. 1990.1008*, hvor Norges Høyesterett antager, at såkaldt "overskudsinformation" fra et automatisk kamera, der overvåger trafikken som led i en automatisk trafikkontrol, trods en intern instruks om, at de pågældende fotos ikke kunne anvendes til andre formål end dem, de var indhentet for (bevis for fartovertrædelse ved bødeudskrivning) kunne indgå som bevismiddel i en straffesag: Et sådant kamera havde opfanget billedet af en biltyv, og anklagemyndigheden begærede dette foto fremlagt som bevis i straffesagen mod biltyven (men derimod ikke som bevis for hans færdselsforseelse). Både byretten og Høyesterett fandt, at beviset kunne føres. Overfor tiltaltes henvisning til "personværnshensynet" påpegede den førstvoterende højesteretsdommer, hvis votum blev afgørende, at trafikanterne ved skiltning advares om, at de vil blive overvåget, at fotograferingen kun udløses ved fartovertrædelser, og at tiltalte således har det i sin magt, om han vil fotograferes. Ved dommen i *United States v. Maxwell*, 43 F.Supp. 24 (1995), fandt retten, at en kunde hos Internet-leverandøren America Online "clearly had an objective expectation of privacy in those messages stored in computers which he alone could retrieve through the use of his own assigned password". En tilsvarende beskyttelse statuerede retten i relation til meddelelser transmitteret til andre brugere, der også havde individuelle passwords.

Klausulering

Det anførte subjektive vurderingsprincip betyder omvendt også, at det står i arbejdsgiverens magt at ophæve medarbejdernes subjektive formodning om meddelelsens lukkethed ved at give en klar instruks om, under hvilke omstændigheder meddelelser vil blive overvåget. Findes der ingen sådanne forskrifter, og ønsker ledelsen at få adgang til et lukket domæne, må den anmode om medarbejderens bistand i form af dennes udlevering af passwords mv. Nægter medarbejderen uden gyldig grund at give ledelsen adgang til sådanne områder, kan dette efter omstændighederne udgøre et sådant brud på tjenestepligten, at arbejdsgiveren opnår ret til at ophæve ansættelsesforholdet, se hertil *ET* s. 200 f. At der består en sådan misligholdelse kan dog ikke i sig selv udvide området for arbejdsgiverens ret til at gøre sig bekendt med den ansattes kommunikation. Sættes sagen på spidsen ved, at medarbejderen insisterer på ikke at åbne sin kommunikation for arbejdsgiveren, hvorefter der sker bortvisning, må arbejdsgiveren dog være berettiget til indseende, eventuelt således at der levnes den ansatte mulighed for forinden at fjerne eventuel privat korrespondance.

En tilsvarende regulering findes i bekendtgørelse om arbejde ved skærmterminaler, nr. 1108 af 15. december 1992, se herom ovenfor i afsnit 14.1.c. Bekendtgørelsens § 5 fastslår en pligt til at indrette skærmarbejdspladser i overensstemmelse med bilaget til bekendtgørelsen, og i dettes pkt. 3, litra b), findes et forbud mod at anvende kvantitativ eller kvalitativ kontrol uden de ansattes vidende.

Modifikationer

Det nævnte subjektive vurderingsprincip er underkastet visse modifikationer, når det gælder de transaktionsdata, der ledsager elektronisk post. I modsætning til den post-baserede kommunikation ved brugeren typisk også, at den systemansvarlige har i hvert fald en teoretisk mulighed for at overvåge kommunikationen og dermed gøre sig bekendt med dennes indhold. I *teknisk* henseende kan man dermed sige, at den elektroniske post er "lukket" i relation til den almindelige bruger (og dermed også den typiske kommunikationspartner), men "åben" i relation til den systemansvarlige. Selv om en i øvrigt lukket meddelelse åbnes ved en fejltagelse, f.eks. ved fejlagtig indtastning af bruger-id og/eller password, må den fortsat betragtes som "lukket", ganske som det vil gælde ved fejlagtig åbning af et brev. I disse tilfælde kriminaliserer bestemmelsen det forhold, at gerningsmanden gør sig bekendt med indholdet. Den systemansvarliges tekniske mulighed for at skaffe sig indblik i denne kommunikation, giver ham ikke også *retlig* mulighed for at gøre det, jf. dog den tvivlsomme afgørelse i *U 1996.979 Ø*. Dette er helt åbenbart i relation til bestemmelsen i strfl. § 263, stk. 1, nr. 3), om aflytning af telefon-

samtaler, hvor televirksomhederne trods deres mulighed for at aflytte abonnenter ikke har en almindelig aflytningsadgang.

Erhvervs-hemmeligheder

Ifølge § 263, stk. 3, anses det som en skærpende omstændighed, at et indgreb af den førnævnte karakter (og altså uanset om straffehjemlen findes i stk. 1 eller 2) er sket med forsæt til, at gerningsmanden skaffer sig eller gør sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder. Er gerningsmanden i et tjeneste- eller samarbejdsforhold til den pågældende virksomhed, dækkes denne gerning allerede af mfl. § 10, stk. 1, der straffer den, som på utilbørlig måde i tjeneste eller samarbejdsforhold skaffer sig eller forsøger at skaffe sig kendskab til eller rådighed over virksomhedens erhvervshemmeligheder. Da straffen for overtrædelse af denne bestemmelse dog kun er bøde, hæfte eller fængsel indtil to år, jf. lovens § 22, stk. 4, har det betydning, hvorledes forholdet subsumeres. Begge bestemmelser er uanvendelige i relation til offentlige myndigheder (på nær dog måske visse sektorforskningsinstitutioner), der som udgangspunkt ikke råder over "erhvervshemmeligheder". Sådanne angreb kan derimod efter omstændighederne straffes efter LBP § 70, stk. 2, der dog alene hjemler straf af bøde eller hæfte.

17.4.c. Straffelovens § 263a

Stk. 1

Med strfl. § 263a er den strafferetlige beskyttelse af informationssystemer i § 263, stk. 2, søgt fremrykket gennem en regel, der straffer den, der uretmæssigt *erhvervsmæssigt sælger* eller i *en videre kreds udbreder* en kode eller andet adgangsmiddel til et ikke offentligt tilgængeligt informationssystem, hvortil adgangen er beskyttet med kode eller anden særlig adgangsbegrænsning. På samme måde straffes den, der uretmæssigt videregiver et større antal af de nævnte koder eller andre adgangsmidler, jf. stk. 2. Bestemmelsen kræver forsæt til salg og videre udbredelse af de nævnte koder. Derimod skal der ikke være forsæt til deres *brug*.

Bestemmelsen bygger på den system- og kommunikationsterminologi, som er indført i straffeloven med IT-straffereformen i 2004, jf. bemærkningerne herom i afsnit 17.1.b. Den finder således anvendelse på ethvert IT-system – fra mobiltelefonens adresseliste til medicinalvirksomhedens forskningsdata på en stor mainframe-computer – der kan siges at behandle informationer, som ikke er offentligt tilgængeligt. Ved sin fremrykkelse af fuldbyrdelsesmomentet – og i nogen grad også i affattelsen – korresponderer bestemmelsen med det tilsvarende delikt, der er ind-

ført i tilknytning til offentlige informationssystemer, men hvor adgangen er forbeholdt betalende brugere, jf. § 301a.

Stk. 2

I tillæg til de regler, der findes i stk. 1-2, straffer § 263a, stk. 3, den, der uretmæssigt *skaffer sig* eller *videregiver* en kode eller andet adgangsmiddel som nævnt i stk. 1 til (1) et samfundsvigtigt informationssystem, jf. § 193, eller (2) et informationssystem, der behandler følsomme oplysninger (jf. LBP § 7, stk. 1, eller § 8, stk. 1) om *flere personers personlige forhold*. I modsætning til stk. 1 indebærer dette stykke, at selve *anskaffelsen* af disse adgangsmidler til særligt kvalificerede IT-systemer, samt den – også private – videregivelse heraf er strafbar. Væsentligt for det praktiske efterforskningsarbejde er det, at forsøg herpå vil være strafbar, jf. strfl. § 21.

Strafferammen

Straffen i henhold til strfl. § 263a er bøde eller fængsel indtil 1 år og 6 måneder. Sker den nævnte videregivelse mv. under særligt skærpende omstændigheder, er straffen fængsel indtil 6 år, jf. stk. 2. Som særligt skærpende omstændigheder anses navnlig tilfælde, hvor videregivelsen mv. sker i særlig stort omfang eller indebærer særlig risiko for betydelig skade. Udbredelse til en stor kreds via en Internet-hjemmeside, vil være et eksempel herpå.

17.4.d. "Informationshæleri"

Efter strfl. § 264c finder straffehjemlen i bl.a. §§ 263 og 263a tillige anvendelse på den, der uden at have medvirket til hovedforbrydelsen skaffer sig eller uberettiget udnytter oplysninger, som er fremkommet herved. Den, der udnytter hemmelig information, der er skaffet tilveje gennem hacking el.lign., straffes dermed på samme måde, som hvis den pågældende selv havde forestået den pågældende hacking.

Bestemmelsen er anvendt i *U 1996.1538 ØLK*, hvor et advokatfirma fik medhold i et krav om udlevering af en harddisk, som firmaet havde sendt til destruktion på en forbrændingsanstalt uden effektivt at have slettet de herpå lagrede personoplysninger. Oplysningerne kom i hænderne på en journalist, der skrev om datasikkerhed, og som ved at fremkalde disse personoplysninger ville tematisere dette emne. Afgørelsen gav ligeledes advokatfirmaet ret til at få udleveret de disketter, hvorpå oplysningerne var kopieret over.

17.4.e. Tavshedspligtregler

De førnævnte regler beskytter en privat eller på anden måde lukket sfære mod *angreb*, hvorved gerningsmanden sætter sig i besiddelse af de private oplysninger mv. henholdsvis udnytter disse oplysninger. Hertil skal føjes den regulering, der tilsigter at sikre, at en person, der *retmæssigt* er i besiddelse af visse oplysninger, ikke uberettiget videregiver disse oplysninger til tredjemand. Dette hensyn varetages gennem regler om tavshedspligt. Reglerne herom har traditionelt udviklet sig omkring offentligretlige funktioner – se navnlig de generelle regler i strfl. § 152 og §§ 152d-152f og forvaltningslovens kapitel 8 – samt for visse liberale erhverv.

I henhold til § § 13, stk. 1, jf. stk. 3, i *teleforbrugerloven* (lov om konkurrence- og forbrugerforhold på telemarkedet, jf. lovbekendtgørelse nr. 679 af 23. juni 2004) må ejere af telenet, udbydere af telenet eller teletjenester, førnævntes ansatte og tidligere ansatte ikke uberettiget videregive eller udnytte oplysninger om andres brug af nettet eller tjenesten eller indholdet til uvedkommende. De pågældende personer må heller ikke – uberettiget – videregive eller udnytte oplysninger om andres brug af nettet eller tjenesten eller om indholdet heraf, som de får kendskab til i forbindelse med det pågældende udbud af telenet eller teletjenester. Forpligtelsen er strafsanktioneret, jf. lovens § 13, stk. 2, der lader straffelovens regler om tavshedspligt (de førnævnte § 152 og §§ 152d – 152f) finde tilsvarende anvendelse for den, der er eller har været ansat hos en udbyder af et telenet eller en teletjeneste.

Sikkerhedskrav

For at understøtte den førnævnte tavshedspligt skal de nævnte teleudbydere mv. sikre, at oplysninger om andres brug af nettet eller tjenesten eller indholdet heraf ikke er tilgængelige for uvedkommende, teleforbrugerlovens § 13, stk. 3. Denne regel er i telebekendtgørelsens § 30 præciseret, således at det bl.a. skal sikres, at trafikdata vedrørende slutbrugere, som behandles ved etablering af samtaler, og som lagres af udbydere af offentlige telenet eller teletjenester, slettes og anonymiseres efter samtalens afslutning, hvis ikke der er særligt grundlag for andet, jf. bestemmelsens stk. 2-5.

17.5. Visse adgangssystemer

17.5.a. Piratdekodere

I § 91 i lov om radio og fjernsynsvirksomhed, jf. lovbekendtgørelse nr. 506 af 10. juni 2004, indsat et forbud mod "at fremstille, importere, omsætte, besidde eller ændre dekodere eller andet dekodningsudstyr, hvis formål det er at give uautoriserede adgang til indholdet af en kodet radio- eller tv-udsendelse". Annoncering eller anden form for reklame for sådant udstyr er heller ikke tilladt. Bestemmelsen rammer såvel forsætlige som groft uagtsomme overtrædelser. Den straffes som udgangspunkt med bøde, jf. § 76a. Såfremt overtrædelsen finder sted i erhvervsmæssigt øjemed, eller der er tale om udbredelse til en videre kreds (f.eks. via en Internet-hjemmeside) kan straffen dog stige til hæfte eller fængsel i indtil 6 måneder. Se f.eks. dommen i *U 2000.714 Ø*, der idømte en bøde på 16.000 kr. svarende til den anslåede fortjeneste ved erhvervsmæssigt salg af 10 dekoderkort og omprogrammering af ca. 60. Se ligeledes *U 2000.2307 V*, der idømte en bøde på 200.000 kr. (svarende til den anslåede fortjeneste) for erhvervsmæssig salg af ulovlige dekodere via Internet gennem en periode på 9 måneder.

Om det erstatningsretlige opgør i sådanne sager, se *U 2001.287 H*, hvor en virksomhed blev pålagt en erstatning på henholdsvis 15.000 kr. og 25.000 kr. for at have solgt ulovlige dekoder-programkort til to satellitkanaler.

Som det fremgår, angår bestemmelsen kun den erhvervsmæssige omsætning, og kun radio- og fjernsynsspredning. Formuleringen dækker imidlertid både piratdekodere, piratdekoderkort og andet udstyr med samme formål, herunder edb-programmer. Sælges udstyr af denne art i strid med disse regler, kan køberen i almindelighed gøre gældende, at der foreligger retsmangler, jf. sagen i *JÅF 1995.159*.

Med Europa-Parlamentets og Rådets direktiv af 20. november 1998 om retlig beskyttelse af adgangsstyrede og adgangsstyrende tjenester (98/84), EFT 1998 L 320/54, er der sket en tilnærmelse af medlemsstaternes lovgivning vedrørende foranstaltninger mod ulovlige anordninger, der giver uautoriseret adgang til tv- og radiospredning samt "informationssamfundets tjenester" (som defineret i direktiv 98/34/EF). Direktivet gør det ulovligt at fremstille, importere, distribuere, sælge, udleje eller besidde ulovlige anordninger (herunder udstyr og programmer), der er udformet eller tilpasset med henblik på at muliggøre uautoriseret adgang til tv-spredning, radiospredning og

"informationssamfundets tjenester", jf. om dette begreb afsnit 1.4.e., se herved art. 4 og 2. Forbuddet gælder ligeledes installation, vedligeholdelse eller udskiftning af sådanne ulovlige anordninger i kommercielt øjemed samt markedsføring ("kommerciel kommunikation") med henblik på et sådant salg. Direktivet har rod i forslaget i KOM(97) 6056 endelig udg.

17.5.b. Straffelovens § 301a

Parallelt med de fremrykkede delikter i strfl. §§ 263a og 301, jf. bemærkningerne herom i afsnit 17.4.c., hjemler strfl. § 301a, straf for den, der uretmæssigt s*kaffer sig* eller *videregiver* koder eller andre adgangsmidler til informationssystemer, hvortil adgangen er forbeholdt betalende brugere, og som er beskyttet med kode eller anden særlig adgangsbegrænsning. Ligesom bestemmelsen i § 169a er den rene besiddelse af de nævnte koder ikke gjort strafbar. Der kræves med andre ord et aktivt forhold fra gerningsmandens side.

Straffen er bøde eller fængsel indtil 1 år og 6 måneder. Sker den nævnte videregivelse mv. under særligt skærpende omstændigheder, er straffen fængsel indtil 6 år. Som særligt skærpende omstændigheder anses navnlig tilfælde, hvor videregivelse m.v. sker erhvervsmæssigt, i en videre kreds eller under omstændigheder, hvor der er særlig risiko for omfattende misbrug.

17.6. Ulovlig informationsspredning

17.6.a. Børnepornografi

Ifølge strfl. § 235 straffes den, som *udbreder* utugtige fotografier eller film, andre utugtige visuelle gengivelser eller lignende af personer under 18 år. Gerningsindholdet i bestemmelsen er centreret om ordet *utugtige fotografier.* Hvad der ligger her beror på de moralforestillinger, der til enhver tid er gældende i et samfund. Begrebet har derfor karakter af en retlig standard, hvis rammer ikke kan fastlægges med et præcist indhold. I bred forstand sigter det til sådanne billeder, der i repræsentative kredse vækker berettiget anstød, f.eks. i forbindelse med en udfordrende blotning af kønsorganer mv. Fokus er her primært på beskueren. Men når begrebet anvendes i relation til børn, indgår i vurderingen også en hensyntagen til det barn, der ofte ufrivilligt er stillet

Udbredelse

til skue på den nævnte vis. Denne betragtning indebærer, at begrebet her må strækkes noget videre.

Bestemmelsens formål er tveleddet. Det ene formål er at beskytte det barn, der er genstand for *overgreb* i det pågældende billede mv. Dette formål har primært betydning i de (desværre typiske) tilfælde, hvor billedet viser et barn, der er genstand for en seksualforbrydelse. Det andet formål – der primært har betydning, hvis barnet er mellem 15 og 18 år – består i at beskytte barnets personlige integritet ved selve visningen.

Ved den ændring af bestemmelsen, der fandt sted ved lov nr. 228 af 2. april 2003, blev det strafbare område udvidet, således at også trickbilleder omfattes. Denne ændring, der har grundlag i EU's rammeafgørelse om bekæmpelse af seksuel udnyttelse af børn samt børnepornografi, er ikke udtryk for nogen moralsk fordømmelse, men begrundes med bevistekniske hensyn: Ved at kriminalisere hele dette område indsnævres muligheden for, at gerningsmanden kan gøre gældende, at han troede at billedmaterialet *ikke* indebar nogen krænkelse.

Strafferammen ifølge bestemmelsen er bøde eller fængsel indtil 2 år. Under særligt skærpende omstændigheder kan straffen stige til fængsel indtil 6 år Som særligt skærpende omstændigheder anses navnlig tilfælde, hvor barnets liv udsættes for fare, hvor der anvendes grov vold, hvor der forvoldes barnet alvorlig skade, eller hvor der er tale om udbredelse af mere systematisk eller organiseret karakter.

Besiddelse mv.

Ifølge strfl. § 235, stk. 2, straffes den, som besidder eller mod vederlag gør sig bekendt med utugtige fotografier eller film, andre utugtige visuelle gengivelser eller lignende af personer under 18 år, med bøde eller fængsel indtil 1 år. Bestemmelsen suppleres med strfl. § 230, der kriminaliserer det forhold, at unge under 18 år benyttes som pornomodeller. Den omfatter dog ikke besiddelse af utugtige billeder af en person, der er fyldt 15 år, hvis den pågældende har givet sit samtykke til besiddelsen.

Bestemmelsen omfatter to forhold. For det første omfattes selve besiddelsen af de utugtige billeder, f.eks. på en harddisk eller på den statiske hukommelse i en bærbar enhed, f.eks. en iPod. For det andet omfattes det forhold, at gerningsmanden mod betaling gør sig bekendt med billedet, f.eks. i forbindelse med en biografforevisning.

Retspraksis

Der findes en omfattende retspraksis om strfl. § 235, og navnlig de seneste års praksis tyder på, at disse forbrydelser er særdeles udbredte, men at domstolene også er parate til at reagere med en håndfast strafudmåling. I *TfK 2000.456 Ø* fandtes T skyldig i

besiddelse af 5.000-6.000 børnepornografiske billeder. Straffen fastsattes til fængsel i 40 dage, som under hensyn til forholdets karakter ikke blev gjort hverken hel eller delvis betinget. Se også *U 2003.255 Ø* og *U 2003.1117 Ø*, der begge idømte 30 dages fængsel for udbredelse af børnepornografi på internettet, *U 2005.836 Ø*, der idømte 9 måneders fængsel for blufærdighedskrænkelse samt besiddelse og udbredelse af børnepornografibilleder på internettet, og *U 2005.1382 Ø*, hvor besiddelse af 360 børnepornografiske billeder, heraf 10 med gerningsmandens 4-årige datter, samt andre billeder med særdeles grov vold mod småbørn mv., blev straffet med fængsel i 1 år. Ved strafudmålingen blev der lagt vægt på, at gerningsmanden havde fortsat med sin kriminelle aktivitet, efter at der var rejst sigtelse. 13 af de nævnte filmsekvenser var blevet downloadet 301 gange over en to-dages periode. Se også *TfK 2002.322 Ø*, hvor tiltalte, der bl.a. blev straffet for at have været i besiddelse af 7 børnepornografiske billeder på sin computers harddisk, fik konfiskeret computeren med tilhørende disketter, samt *TfK 2004.273 Ø, TfK 2005.89 Ø, TfK 2005.347 V*.

17.6.b. Privatlivskrænkelser

Undertiden har Internet været anvendt som medium for chikanøs spredning af meddelelser tilhørende privatlivet. Et eksempel herpå foreligger ved dommen i *U 1999.177 V*, hvor en forsmået ægtemand fra sin hjemmeside offentliggjorde 7 nøgenbilleder af sin tidligere hustru med oplysninger om hendes personnummer, adresse og telefonnummer samt en stærkt krænkende tekst til hver enkelt billede. Denne offentliggørelse blev straffet i medfør af strfl. § 264d og § 232 med hæfte i 20 dage. Sådanne krænkelser må formodes at få øget udbredelse med den adgang, der i dag består for at optage og videresende digitale fotos ved brug af mobiltelefoni. Et eksempel herpå fra norsk retspraksis er gengivet i Lov & Data nr. 82, juni 2005, s. 34.

17.6.c. Visse nedsættende ytringer

Ifølge strfl. § 266b straffes den, der offentligt "eller med forsæt til udbredelse i en videre kreds" fremsætter udtalelse eller anden meddelelse med hvilken en gruppe af personer trues, forhånes eller nedværdiges på grund af sin race, hudfarve, nationalitet eller etnisk oprindelse, tro eller seksuel orientering. Bestemmelsen kan f.eks. anvendes, når udbredelsen sker via hjemmesider. Straf-

fen er bøde, hæfte eller fængsel indtil 2 år. Det skal ved strafudmålingen betragtes som en skærpende omstændighed, at forholdet har karakter af propaganda-virksomhed. Bestemmelsen har i enkelte tilfælde været anvendt i relation til hjemmesider, der har indeholdt stærkt racistiske udtalelser. Danmark har derimod ikke – modsat f.eks. Tyskland – noget generelt forbud mod spredning af nazistisk propaganda.

17.7. Almenfarlige forbrydelser

Efter strfl. § 193 straffes den, der på retsstridig måde fremkalder omfattende forstyrrelse i driften af bl.a. "informationssystemer" med hæfte eller fængsel indtil 6 år. Efter forarbejderne tager bestemmelsen sigte på større, samfundsvigtige IT-systemer. Når dette krav skal fortolkes i dag, må det dog tages i betragtning, at stadigt flere IT-systemer – i konsekvens af den stigende samfundsmæssige IT-afhængighed – er blevet "samfundsvigtige". Det kræves ikke, at disse systemer skal høre til den offentlige sfære. I forarbejderne antages det, at omfattende forstyrrelser også kan opstå ved angreb på f.eks. storbankers eller i øvrigt på større virksomheders IT-systemer. Der ligger dog ikke noget krav i hverken lovteksten eller dens forarbejder om, at angrebet skal rette sig mod rent erhvervsmæssige eller offentligretlige funktioner. Også angreb, der resulterer i, at et større antal private parter udelukkes fra at kommunikere, vil efter omstændighederne kunne straffes. Af andre eksempler kan nævnes angreb på centrale Internet-funktioner (f.eks. DIX- og Hostmaster-funktionen), angreb på centrale Internet-portaler eller fysiske angreb på de teleknudepunkter, der understøtter de telefoniske forbindelser.

Det er uden betydning for bestemmelsen, hvorledes de pågældende angreb gennemføres. Omfattet er såvel angreb af målrettet logisk beskaffenhed (i form af hacking mv.), mindre kontrollerede angreb i form af virus-udsendelse, som fysiske angreb i form af afbrydelse af teleforbindelser el.lign.

17.8. Strafudmåling

Domstolenes udmålingspraksis i sager om visse former for IT-kriminalitet har fra tid til anden givet anledning til diskussion. Gerningsmændene i disse sager hører ikke til kriminalretternes

"sædvanlige" klientel. Der er ofte tale om personer, der ikke tidligere har været kriminelle, som befinder sig i gode jobs eller uddannelsessituationer og for hvem anvendelsen af ubetingede frihedsstraffe derfor vil kunne få indgribende betydning. Dertil kommer, at visse gerningsmænd med held har kunnet pege på, at deres lovovertrædelser i en vis udstrækning har været motiveret af en "forskningsbetonet" interesse i at afprøve systemernes sikkerhed. Hertil kommer, som påpeget af *Ulla Høg* i Anklagemyndighedens årsberetning, 1989, s. 51, at muligheden for at begå visse IT-forbrydelser ofte fremkommer uventet, og at ofrene ofte har en anden oplevelse af den fuldbyrdede forbrydelse. De foreliggende undersøgelser viser, at IT-forbrydelser anmeldes sjældnere end klassiske formueforbrydelser – ofte ud fra en fornemmelse af, at offeret selv bærer en del af skylden ved ikke at have afskåret mulighederne for retsbrud.

Hacking

I dansk byretspraksis har man stort set altid anvendt *betinget dom* i hackersager, hvor gerningsmanden har været et yngre, ustraffet menneske. Dette skete bl.a. ved *Roskilde rets dom af 19. december 1996*, hvor samtlige seks tiltalte, hvoraf nogle var tiltalt for hacking i ganske betydeligt omfang, slap med betingede fængselsstraffe – for flere tiltaltes vedkommende dog kombineret med vilkår om samfundstjeneste. Se ligeledes *U 2000.1450 Ø*, der idømte en 20-årig betinget dom uden straffastsættelse for to tilfælde af indtrængen i en privat computer ved brug af et hackerprogram ("Back Orifice"). To dommere ville dog idømme en bødestraf. Ved landsrettens dom skete der, modsat byrettens, konfiskation af computer med tilbehør.

Muligheden for at anvende betinget straf er noget mindre, såfremt tiltaltes alder er noget højere. I *U 1996.1514 Ø* idømtes to opsagte medarbejdere bødestraf for at have taget et antal kundejournaler med hjem efter opsigelse. Også *U 1997.65 Ø* angik tyveri af erhvervshemmeligheder fra et firmas gemmer. Tiltalte, der var 49 år, og som havde udført gerningen i samvirke med en medgerningsmand, blev idømt 6 måneders fængsel, hvoraf 3 måneder under dissens blev gjort betinget. En utrykt Vestre Landsrets Dom af 30. oktober 1990 (anført i Domme i kriminelle sager 1990-92, s. 228) fastsætter straffen for uberettiget at have brudt og unddraget en lejer tre breve, hvis indhold blev fjernet og kuverterne smidt i en skraldespand, til 10 dagbøder à 50 kr. Se også *U 2002.1064 V,* som idømte betinget dom uden straffastsættelse, samt konfiskation af computer, monitor, mus og tastatur, for et tilfælde af forsøg på hacking.

Kontrolmangler

En anden årsag til at straffe mildere kan som nævnt ligge i forhold på offerets side. Hvis den angrebne ved sin passivitet eller lignende har været medvirkende årsag til, at kriminaliteten fik et så stort omfang, kan dette i visse tilfælde spille ind på strafudmålingen. I relation til underslæb er det således velkendt, at offerets svigtende kontrol efter omstændighederne kan begrunde nedsættelse af straffen, se f.eks. *U 1975.289 Ø*. Synspunktet kan dog kun anvendes i relation til gerningsmænd, over for hvem der har været en anledning til at foretage en særlig kontrol. Det kan ikke være et argument for strafnedsættelse for indbrudstyveri, at døren til ejendommen ikke var låst.

Illustrerende herfor er den norske højesteretsdom i *Rt. 1991.532*, i en straffesag mod to yngre mennesker, som næsten fik held til retsstridigt at overføre et millardbeløb til en konto i Schweiz. Byretten havde idømt de tiltalte en betinget fængselsstraf i kombination med en bøde hver på 50.000 kr., bl.a. under henvisning til, at hele projektet nærmest må have haft "et uvirkelighetens preg" og at de tiltalte "ikke burde vært utsatt for den fristelse som lå i at de hadde adgang til å endre data i databehandlingssystemet". Ved Høyesteretts dom ændredes straffen til 2 års ubetinget fængsel.

Supplerende litteratur

Reglerne om *IT-kriminalitet* er behandlet i *Vagn Greve*: Edb-strafferet (2. udg., 1986), jf. sammes kapitel om Edb-kriminalitet trykt i Bryde Andersen (1987), s. 117 ff. og af *Ulla Høg* i Anklagemyndighedens årsberetning (1989), s. 40 ff. og i Anklagemyndighedens årsberetning 1981 s. 56 ff. I 1999 er udsendt en betænkning om IT-kriminalitet, nemlig betænkning 1377/1999 om børnepornografri og IT-efterforskning og i 2002 betænkning 1417/2002 om IT-kriminalitet. En stort anlagt oversigt over disse IT-strafferetlige regler med hovedvægten på Storbritannien findes i *Martin Wasik*: Crime and the computer (Oxford, 1991). Se ligeledes – med særlig fokus på trusselsbilledet – *P.N. Grabosky & Russell G. Smith*: Crime in the Digital Age – controlling telecommunications and cyberspace illegalities (New Brunswick, New Jersey, 1998).

Problemstillingen vedrørende det strafferetlige medvirkensansvar på Internet var genstand for drøftelse ved det 35. Nordiske Juristmøde i Oslo, august 1999 på grundlag af et oplæg fra mig, se NJM 1999 I.197 ff. Se herudover *Kasper Heine* i NIR 1999.615 ff.

Kapitel 18. ERSTATNINGSANSVARET

18.1. Problemstillingen

18.1.a. IT-erstatningsansvarets kendetegn

Praktisk betydning

Risikoen for erstatningskrav efter skader forvoldt ved IT-drift mv. udgør en stærkt handlingsmotiverende faktor. Ingen IT-systemer er fejlfrie, og med nye tekniske anvendelsesformer mv. kan ingen overskue sikkerheden af forskellige løsninger mv. I takt med, at information i stigende grad stilles til rådighed via systemer, der er tilgængelige for almenheden, kommer dertil risikoen for, at en informationsfejl spreder sig som ringe i vandet og resulterer i tab, der er uforholdsmæssigt høje sammenlignet med den ansvarsudløsende årsag.

Når der i det følgende tales om IT-erstatningsansvaret, tænkes der på skadetilfælde, der skyldes fejl ved informationshåndteringen; enten således at der træffes skadevoldende beslutninger på grundlag af ufuldstændig eller fejlagtig information, eller således at et informationssystem i sig selv udvirker en skade, der skyldes informationsfejl. Her som andetsteds er en beskrivelse og afgrænsning nødvendig. Alle produkter og alle menneskelige handlingsformer rummer information, og for erstatningsretten er det velkendt, at en handling kan blive erstatningspådragende på grund af sit informationsindhold. Dette er ikke alene kernen i det informationsansvar, som professionelle rådgivere mv. er underlagt, men kan også være et led i dagligdagens handlinger, se f.eks. *U 1969.570 V*, der pålagde føreren af en bil erstatningsansvar for et misvisende tegn til en forbikørende i forbindelse med en trafikulykke.

Når IT-erstatningsansvaret skal beskrives, er det – igen – nødvendigt at sondre mellem de forskellige måder, hvorpå information og medium er knyttet til hinanden, jf. redegørelsen s. 116 ff. Ser vi først på den *fleksible* information er det nærliggende at tage udgangspunkt i den anvisning, der findes i en bog, og som påfører læseren et tab, når han disponerer efter den. Denne information adskiller sig fra den *integrerede* information, der manifesteres i selve produktet, som f.eks. i håndtag, afbryderknapper og

lignende. Herimellem finder man den *mediekompatible* information, der kendetegnes ved uden videre at kunne flyttes fra ét medium til et andet af samme slags. Et eksempel herpå er edb-programmel, som kun bliver skadevoldende i den konkrete sammenhæng, hvor det udfolder sine funktioner.

Digital information

Når det gælder den mediekompatible information, kan man karakterisere IT-erstatningsansvaret ved de egenskaber, som kendetegner moderne digital informationsanvendelse: Den digitale informations løse tilknytning til mediet, systemernes kompleksitet (*Vico-paradokset*), automatiseringsmuligheden, nutidens uforudsete anvendelsesområder, den stigende kapacitet etc. Til sammenligning rummer et skruelåg (integreret information) kun begrænsede informationer, al den stund forbrugeren kun står overfor et begrænset antal valgmuligheder, idet de pågældende informationer er uløseligt knyttet til lågets formgivning. Men selv de mest simple administrative IT-systemer rummer en mangfoldighed af procedurer og informationer, der under forskellige betingelser og omstændigheder kan sendes til og fra systemet, og som derfor i helt uventede sammenhænge kan udløse skader. Kommer kompleksiteten over et vist niveau, øges risikoen for nedbrud. Er systemet forbundet med andre systemer, stiger risikoen for, at det enkelte nedbrud får vidtrækkende følger.

Samspilsbetingelsen

Heri ligger også, at information, der isoleret set kan betegnes som "defekt" el.lign., kun opnår sin skadevoldende effekt i et samspil med noget andet. For at kunne beskrive de informationsansvarlige korrekt, må man derfor skitsere de sammenhænge, som omgiver den defekte information og giver den sin funktionalitet.

18.1.b. De enkelte tilfældegrupper

Strategi

I en første kategori kan man pege på den funktion, hvorved der fastlægges strategier for en IT-anvendelse. En IT-strategi realiseres gennem de retningslinjer, planer og regler, der styrer informationshåndteringen i en organisation eller virksomhed, og vil derfor typisk følge samme formål som organisationen. Strategien kan f.eks. fastslå, hvornår der skal – eller ikke må – anvendes IT, eller hvordan et IT-system bør anvendes af den enkelte bruger. Strategien kan også træde frem i tekniske rammer for, hvordan der overhovedet kan disponeres.

Betydningen af sådanne strategiske beslutninger træder frem på stadigt flere områder. I *IT-sikkerhedsrådets* vejledninger om digitale dokumenters bevisværdi (1998) og om praktisk brug af

kryptering og digital signatur (2000) betones nødvendigheden af, at ledelsen medvirker aktivt i dette strategiske planlægningsarbejde, netop fordi *afvejningen* af de modstående værdier spiller en så stor rolle for, hvilke risici man finder acceptable. I nogle af disse tilfælde er strategien underlagt retlige begrænsninger, se f.eks. i regnskabslovgivningen og i det regelgrundlag, der gælder for pengeinstitutters og værdipapircentralers revision. Herudover vil indholdet af den enkelte strategi ofte udmønte sig i pålæg, der håndhæves gennem ansættelsesretlige regler.

Virksomhedens IT-strategi kan ikke alene få betydning for vurderingen af, om den selv er *ansvarlig* for en skade på tredjemand for skader og tab, der kan henføres til strategien (ansvar for sikkerhedsbrist el.lign.), men også som *skadelidt*, idet et muligt erstatningskrav mod skadevoldere reduceres, fordi den valgte strategi (f.eks. om ikke at foretage sikkerhedskopiering) betragtes som udtryk for egen skyld. Et praktisk eksempel herpå er beslutningen om, hvor hyppigt der skal udføres intern henholdsvis ekstern sikkerhedskopiering af data og programmel.

Funktionsdesign

Den anden kategori af potentielt skadegørende handlinger fastlægger de funktioner, systemet udfører, dvs. bestemmer, hvilken information systemet kan modtage og afgive, og hvordan brugeren styrer denne kommunikative proces. Dette ansvar er navnlig aktuelt, når et system designes eller programmeres. I relation til den informationsspredning, der sker via Internet, knytter funktionsansvaret sig ikke mindst til den part, der træffer afgørelse om, hvilke informationer den enkelte hjemmeside udbyder.

Implementering

Med implementering menes de foranstaltninger, der gør det muligt at tage et system i brug efter hensigten. En central del heraf er den korrekte sammensætning af komponenter i overensstemmelse med de lovmæssigheder, der gælder for den enkelte komponent (funktion, kompatibilitet mv.), jf. den systemteoretiske terminologi i afsnit 2.3. Begrebets nøjagtige rækkevidde beror på, hvilket "system" man har i tankerne, om dette er under opbygning, eller om et eksisterende system vedligeholdes. I opbygningsfasen er det typisk leverandøren, der har ansvar for den tekniske sammensætning af komponenter og programmer, og brugeren, der har ansvaret for levering af data, installation af lokaler, oplæring af brugere mv. Det pågældende system behøver dog ikke have karakter af en egentlig installation. Ofte taler man om at "implementere" det ene eller andet tekniske princip i et edb-program.

Dialog

Dialogen er indbegrebet af de meddelelser, der udveksles mellem bruger og system. Indholdet af en dialog beror derfor på systemets muligheder for at kommunikere og på brugerens ønsker med kommunikationsprocessen. Hvert af de valg, brugeren træffer under systemanvendelsen, kan beskrives som meddelelser i en dialog. Én ramme for denne dialog sættes f.eks. af den indgangsmenu, hvorfra brugeren kalder et program. En anden sættes af programmets funktioner. Der vil ofte være retlige begrænsninger i, hvorledes en IT-dialog kan forme sig, f.eks., hvilke medarbejdere der må bruge hvilke programmer. Sådanne regler kan f.eks. have til formål at tilvejebringe IT-sikkerhed.

Dataanvendelse

I den femte kategori finder vi de handlinger, der udføres på grundlag af systemets data. I mange tilfælde vil brugerens dataanvendelse indgå som en del af hans dialog med systemet, f.eks. ved valg af et menupunkt i programmet. Alligevel er det nødvendigt at udskille dataanvendelsen, fordi der ingen logisk identitet er mellem dialog og handling. Man kan sagtens disponere på grundlag af data uden at stå i nogen kommunikativ forbindelse med det IT-system, der har genereret disse data.

Medvirkensansvaret

Ved siden af disse ansvarskategorier finder vi ansvaret for passiv medvirken. Denne ansvarsform, som er behandlet mere udtømmende i afsnit 17.1.d og 17.1.e, berøres ikke yderligere her. Som her nævnt giver den primært anledning til vanskeligheder i relation til passiv medvirken til visse former for Internet-baseret videreformidling, som der med e-handelsloven er indført en særlig regulering af. Ansvaret for *aktiv medvirken* giver ikke anledning til særlige retlige problemer. Udgangspunktet er her, at der anlægges samme ansvarsvurdering som for hovedhandlingen.

18.1.c. Beskrivelsesproblemet

Retskildeproblemet

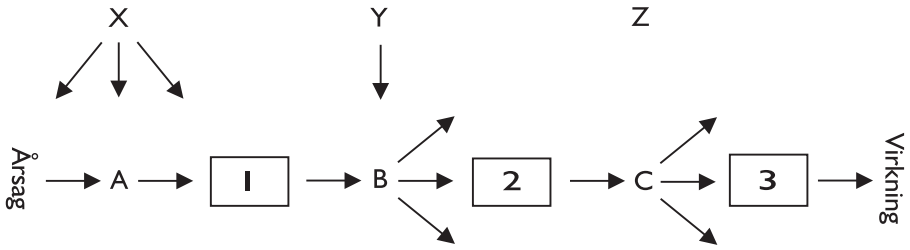
Det er kun i begrænset omfang muligt at udtale sig om gældende IT-erstatningsret. Hverken herhjemme eller i udlandet findes der almene erstatningsregler på IT-området, hvorimod man på en række specifikke områder (virksomhed som værdipapircentral, brug af betalingskort, afgivelse af digital signatur, personregistrering) har indført særlige erstatningsregler. Man må derfor tage udgangspunkt i almindelige erstatningsregler, først og fremmest culpareglen og reglerne om produktansvar. Men for begge disse regelsæt gælder det, at der hersker tvivl om deres rækkevidde på IT-området – herunder om, hvad der er god og fornuftig IT-adfærd.

Derfor står IT-erstatningsretten overfor både et faktisk og juridisk beskrivelsesproblem. Det *juridiske* beskrivelsesproblem hænger sammen med erstatningsreglernes upræcise retsfaktumbeskrivelse, der volder vanskeligheder, når de relevante erstatningsfænomener endnu ikke fremtræder som klare tilfældegrupper. Det *faktiske* beskrivelsesproblem skyldes retsanvenderens vanskeligheder ved at forstå det komplekse forløb, som IT-udvikling og -drift består af, og ikke mindst ved at udpege hvem, blandt de typisk ganske mange personer, der spiller en erstatningsrelevant rolle i et sådant forløb.

Retsfaktumbeskrivelsen

Vender vi os først til vanskelighederne ved at give nogen præcis beskrivelse af de almindelige erstatningsregler, kan det være nyttigt at flytte beskrivelsen til et niveau, der er endnu mere generelt end disse generelle regler er. Som nærmere udviklet i *E&A*, se navnlig kapitel 5, er det kendetegnende for enhver ansvarsregel (modsat regler om hæftelse), at den knytter sig til det forhold, at nogen (den ansvarlige) har *valgt* at handle på en bestemt måde. Ud fra denne beskrivelse kan culpareglens mange enkeltbetingelser sammenfattes i to grundbetingelser, der knytter sig til forestillingen om, hvorledes bonus pater "kunne" have handlet, henholdsvis "burde" have gjort det. Se ligeledes min oversigtsprægede gennemgang i FSR's årsskrift 1990 (Erhvervsret), s. 9 ff., kritikken hos *Koktvedgaard* i U1989B.268 (s. 270) og *Vinding Kruse*: Erstatningsretten, 5. udg. (1989), s. 110.

Et nærmere studium af "valgets" begrebsmæssige karakter vil afsløre, at ethvert valg fremkommer som et produkt af objektive, subjektive og sociale faktorer: en faktisk (objektiv) *handlemulighed*, en menneskelig (subjektiv) *erkendelse* heraf og et (socialt) ønske om *normharmoni*. I et samspil, hvor flere personer bærer et ansvar overfor hinanden, kan man kvalificere det enkelte valg ud fra disse tre variable og skematisere forløbet som følger:



Forklaring

I skemaet markerer den *horisontale* dimension (forløbet fra venstre mod højre) de *faktiske* grænser, der gælder i den givne situation. Hvis et IT-system (f.eks. en pengeautomat) har et givet antal muligheder, sætter dette grænserne for, hvordan brugeren kan disponere på grundlag af det. Den *vertikale* dimension markerer derimod de gældende *retlige* grænser for handlefriheden. Selv om man principielt har muligheden for at benytte det stjålne hævekort med tilhørende PIN-kode, forbyder straffeloven denne anvendelse; selv om systemet giver mulighed for en ekstra kontrol, er den ansatte operatør (f.eks. ud fra økonomiske overvejelser) tjenstligt afskåret fra at udnytte dem. I de *punkter*, hvorfra der udgår flere pile, træffes der valg. For vurderingen af disse valg har det herefter dels betydning, hvilken *information* aktøren var i besiddelse af, dels hvilke faktiske og retlige *begrænsninger* der var gældende for hans valg.

Funktion

Skemaet skitserer det samspil, der består mellem forskellige former for ansvar. En vigtig mekanisme består i det forhold, at et ansvar under visse omstændigheder kan flyttes fra en person til en anden. Har X f.eks. fastlagt nogle grænser for A's handlefrihed – det være sig normativt (f.eks. af den førnævnte tjenstlige karakter) eller faktisk (f.eks. ved at afskære visse funktioner i systemet) – betyder dette, at A kun har én mulighed for at videreføre forløbet (kasse I). Skal nogen være ansvarlig eller omvendt have æren for handlingen, må det være X (for så vidt X ikke også var undergivet en handlepligt). Valget er nemlig flyttet over på X. Er problemet, hvem der kan gøres ansvarlig, må man altså udpege X som ansvarsperson.

Når man kaster blikket på disse forskellige typer af ansvarspersoner er det vigtigt at forstå deres funktion i ansvarsvurderingen. Inddelingen tjener alene til at identificere de mulige *aspekter*, der kan have betydning for den erstatningsretlige analyse – ikke at identificere en ultimativt ansvarlig eller -medansvarlig. I en konkret skadessituation vil der ofte være tale om, at flere personer (f.eks. flere medskadevoldere samt den skadelidte) har eller kunne have haft indflydelse på skadesforløbet. I sådanne tilfælde vil udskillelsen af de forskellige typer af aktører tjene til at illustrere, hvorfor det kan være velbegrundet, at nogle af disse aktører bærer risikoen, eller ifalder ansvaret, end andre. I de fleste tilfælde vil den afgørende erstatningsretlige analyse nemlig involvere en eller anden form for medansvar fra den skadelidtes side.

18.1.d. Den relevante valghandling

Skemaet viser de vidt forskellige handlingstyper, der indgår i en kompleks sammenhæng, hvis forløb bestemmes af, at der udveksles eller behandles information. Visse af disse handlinger har retlig karakter (f.eks. meddelelsen om, at en medarbejder ikke har ret til at træffe en bestemt beslutning), andre operativ og generel karakter (f.eks. beslutningen om, at en medarbejder kun råder over et bestemt IT-værktøj), og atter andre tager sigte på udførelsen af konkrete handlinger (f.eks. en konkret beslutning truffet på et fejlagtigt informationsgrundlag). Dermed illustrerer skemaet også den måde, hvorpå forskellige handlinger kvalificeres. Jo større handlefrihed, aktøren har haft, desto mere intenst vil man fokusere på hans adfærd i henseende til såvel ansvars- som belønningssanktioner. Ved at knytte den erstatningsretlige beskrivelse til, hvorledes skadevolderen *kunne* have handlet, kan man indplacere forskellige typer af skadegørende handlinger i valghandlingsskemaet. Spørgsmålet, om der kunne være handlet anderledes i en given situation, fører derfor hen i et spørgsmål om det muliges begrænsninger.

Eksempel

Hvis en begrænsning knytter sig til det *faktiske*, at et IT-system ikke tillader, at der disponeres på en given måde eller at noget ikke kan nås inden for en tidsramme, kan der logisk set ikke være tale om noget ansvar for mulige skadevirkninger af det pågældende element af handlingsforløbet. Ansvarsvurderingen må i givet fald flyttes, således at ansvaret enten knytter sig til det tidligere tidspunkt, hvor skadevolderen valgte at bringe sig i en situation, der afskar ham fra senere at kunne disponere, eller til den person, der lagde den retlige ramme, der indebar, at der ikke var tilstrækkelig tid til handlingen.

Heri ligger også, at én og samme handlebegrænsning på forskellige planer kan tilskrives forskellige typer af faktorer: Det var kommunikative begrænsninger (den handlende kunne ikke nå at skaffe sig et dækkende beslutningsgrundlag), der var årsag til skaden, men en forpligtende vedtagelse eller et andet retsgrundlag, der lå bag denne tidsbegrænsning. Der vil typisk være grund til at sondre mellem, om reglerne er givet af den pågældende organisation eller af samfundet. Er det selve organisationen, der har givet reglerne, og er reglerne ikke i strid med retssystemets almindelige regler, vil ansvaret flytte over på organisationen efter reglerne om strategiansvar, jf. herom nedenfor. Gælder der ufravigelige regler for den pågældendes færden (f.eks. i medfør af sikkerhedsforskrifter, almindeligt gældende strafferegler el.

lign.), vil disse regler afskære alternativ handlen, hvorefter der som udgangspunkt ikke vil være ansvar knyttet hertil.

Dette princip er bl.a. lagt til grund ved PAL § 7, stk. 1, nr. 3, hvorefter producenten fritages for ansvar, når "produktet skal være i overensstemmelse med ufravigelige forskrifter udstedt af offentlig myndighed". Lovens objektive ansvar gælder altså, hvis forskrifterne efterlader producenten en valgfrihed til at bestemme produktets sammensætning og design. Tilsvarende principper gælder ifølge PAL § 7, stk. 3, om ingrediensskader: Produktet havde sin udformning, fordi det var et delprodukt i et andet (færdigt) produkt og skulle følge de anvisninger, som var givet af den, der havde fremstillet det færdige produkt.

18.1.e. Værdiafvejningen

Hvis man efter et af de førnævnte tre variable må konstatere, at skadevolderen befandt sig i en valgmulighed, altså at han "kunne" have disponeret anderledes end sket, opstår for det andet spørgsmålet, om han i så fald *burde* have handlet anderledes. Dette spørgsmål rummer basalt set en afvejning, hvor værdien af den skadegørende handling stilles overfor værdien af den handlefrihed, man vil begrænse ved at pålægge ansvar, og herunder den belastning, et ansvar vil betyde for den forpligtede: Man har som udgangspunkt ikke pligt til at gøre noget for at undgå skader på tredjemand; hensynet til skadelidte vejer altså i almindelighed mindre end hensynet til skadevolderens handlefrihed. Anderledes, hvis den skadevoldende handling kan anskues som udtryk for en vis form for hensynsløshed overfor skadelidte.

Denne afvejning falder forskelligt ud alt efter de hensyn og forventninger, der er fremherskende på forskellige områder. Det skærpede ansvar for professionel rådgivning kan f.eks. betragtes som en retlig beskyttelse af, at klienten i sine efterfølgende dispositioner kan nedsætte sin påpasselighed. Og det mildere erstatningsansvar for visse af pressens udtalelser kan anskues som et udtryk for, at informationsfriheden må prioriteres højt i et moderne demokrati, se *Stuer Lauridsen*: Pressefrihed og personlighedsret (1988), bl.a. s. 115 ff. På IT-området kan denne afvejning være vanskelig at føre ud i livet. IT-systemer er ikke blot lejlighedsvis, men som oftest behæftet med fejl, der kan føre til skader og tab. Risikoen for fejl vil alt andet lige reduceres, jo flere ressourcer der ofres på aftestning og fejlfinding. En erstatningsretlig pligt til kun at levere fejlfrit IT ville føre til færre og mere kostbare IT-systemer, som heller ikke vil være i brugernes og dermed de potentielt skadelidtes interesser. Omvendt vil IT-syste-

mer, der afgiver deres data i en dialog med brugeren, altid involvere mindst én yderligere ansvarlig: den person, der vælger at anvende dataene som led i en beslutning, og som i denne anvendelse påfører sig selv eller andre et tab.

Undertiden søger man at gennemføre cost-benefit analyser mv. for at bringe klarhed i denne afvejning. Man opstiller systematiske tankeskemaer, der sætter *værdi* i forhold til *sandsynlighed*. En beslutningsteoretiker vil f.eks. formulere spørgsmålet om pligten til at afteste et system i ét første problem om, hvorvidt det er "sandsynligt", at yderligere aftestning i givet fald vil afsløre en fejl, der kunne have ført til et tab, og i et andet problem om, hvor stort dette tab i givet fald vil være. Se *Rabbe Wrede* i NÅR 1985.13 ff. og *Gemignani* (1985), s. 353 ff. navnlig s. 356. På et tidspunkt vil den sikkerhedsmæssige marginaleffekt være så ringe, at investeringen alene giver mening, hvis der er meget store værdier inde i billedet. Efter den almindelige erstatningsret vil man derfor stille større sikkerhedskrav til programstyringssystemet for et atomkraftværk end for den grafiske brugergrænseflade til et underholdningsspil. Problemerne opstår i de "krydsende" relationer: hvor der er høje værdier på spil, men en lav sandsynlighed for, at de vil blive truet, eller hvor ringe værdier er på spil, men med en høj grad af sandsynlighed for, at de vil blive truet. Disse tilfælde finder man bl.a. i produktansvarets regler om udviklings- og systemskader. De samfundspolitiske vurderinger om beskyttelse af forbrugerens person har endnu ikke ført til nogen klar og ensartet balance. Efter dansk ret hviler risikoen for udviklingsskader som udgangspunkt på forbrugeren, sml. PAL § 7, stk. 1, nr. 4, medens andre skader udløser det objektive erstatningsansvar. Det balancepunkt, retssystemet vil falde ned på, beror på det pågældende produkt og dets placering i en innovationscyklus. Hvor man i bilens barndom måske i højere grad end nu accepterede fejl, gælder der i dag andre krav til færdselssikkerheden. I en sådan cyklus er IT-teknologien stadig i sin barndom.

Udviklingssynspunktet

Når man skal finde en erstatningsretlig balance i denne afvejning, inddrager man bl.a. samfundets interesse i den handlemåde, man overvejer at knytte sanktioner til. Dette synspunkt synes at have særlig vægt på IT-området. Et samfund, der vil profitere af teknologier, der er udviklet grundigt og samvittighedsfuldt, bør ikke samtidigt erstatningssanktionere de skader, der følger heraf, men som var ukendte efter de selvsamme teknologier. At forbrugeren bærer risikoen for "udviklingsskader" implicerer, at det langsigtede hensyn til teknologiens udvikling går forud for hensynet til skadelidte. Tilsvarende bør man i almindelighed være varsom med at knytte ansvar til fejl, der efter tidens teknologiske standard må anses som uundgåelige og dermed påregnelige. Småfejl mv. i standardprogrammel, der ikke opfylder vitale funktioner,

bør hverken udløse noget objektivt produktansvar eller give grundlag for anvendelsen af et hårdhændet professionsansvar.

Udviklingssynspunktet kan få betydning for den erstatningsretlige vurdering af fejl i systemer, som i øvrigt forventes – og med rette forudsættes – at være "sikre". De krypteringsalgoritmer, der anvendes for at skabe sikkerhed i visse systemer, anses i dag for ubrydelige efter kendte beregningsmetoder og eksisterende udstyr. Ingen kan imidlertid udelukke, at fremtidens teknologier kan ændre denne antagelse. Indtil dette er sket, må det i en erstatningsretlig afvejning antages, at strategier, der hidfører den optimale sikkerhed vurderet på grundlag af tidens højeste ekspertise, ikke skal mødes med erstatningsretlige sanktioner, hvis praksis skulle vise, at dette sikkerhedsniveau ikke er tilstrækkeligt.

Informationshensynet

Et andet væsentligt synspunkt i den erstatningsretlige afvejning er hensynet til, at information skabes og spredes til gavn for almenheden. Efter denne tanke har man i USA – hvor man ellers ikke er bleg for at statuere erstatningspligt i tilfælde, der for en europæisk tankegang kan forekomme fremmedartede – bedømt rent informationsbetingede skader på det åbne informationsmarked langt mildere end andre skadetyper. I sager, hvor kogebøger har ført til forgiftningsskader og kemi-manualer til eksplosioner, er man veget uden om det hårdhændede produktansvar. Både herhjemme og i udenlandske, ellers mere erstatningsvenlige jurisdiktioner, har domstolene været tilbageholdende med at statuere, at der forelå culpøse fejl bag producentens levering af fejlagtig information. Man frygter i nogen grad, at en for hårdhændet erstatningsretlig praksis vil kunne medføre begrænsninger i den almindelige ytringsfrihed.

Samme opfattelse ligger formentlig til grund for de lempelige regler om ansvar for passiv medvirken i e-handelsdirektivets art. 12 – 15. Se fra amerikansk erstatningsretlig praksis *Daniel v. Dow Jones & Co.*, 530 N.Y.S. 2d 334 (1987) (om en elektronisk database) samt *Walter v. Bauer*, 439 N.Y.S. 2d 821 (1981) (om kemi-sættet "Discovering Science"), *Mac Kown v. Illinois Publishing*, North Eastern Reporter, 2d Series 526 (1937), (om en metode til at behandle skaldethed) og *Winter v. G.P. Putnam's Sons*, 938 F.2d 1033 (9th Cir., 1991), hvor importøren af "The Encyclopedia of Mushrooms" blev frifundet for det strikte produktansvar overfor en bruger, der i overensstemmelse med bogens anvisninger havde indtaget en farlig svamp. Se også *Demuth Development Corp. v. Merck & Co., Inc.*, og *Cardozo v. True*, 342 Southern Reporter 2d Series 1053 (1977) (kogebog).

18.2. Strategiansvaret

18.2.a. Ansvarets karakter

Ansvaret for en strategi har rod i de beslutninger, hvorved den eller de, der er ansvarlige for en organisation, beslutter sig for at pålægge eller afskære visse handlinger eller funktioner, der skal finde sted i organisationen. Beslutningen herom kan effektueres gennem retlige påbud (A skal, hhv. må ikke, indhente denne information, inden der disponeres!) eller faktiske midler (A har ikke faktisk adgang til det domæne, hvor informationen ligger). Da virkningen af en sådan strategi ofte er adskilt i tid og rum fra den faktisk indtrådte skade, overses strategiansvaret ofte i den erstatningsretlige argumentation. Det er mere nærliggende at rette søgelyset mod dem, der fysisk/faktisk har handlet og voldt skade, og i kraft af reglerne om principalansvaret vil der almindeligvis end ikke være grundlag for at interessere sig for strategens ansvar. Derfor er der ingen tradition for at ansvarsbedømme "strategisk" adfærd i erstatningsretlige fremstillinger.

Ansvarets rammer

Som udgangspunkt står den, der er ansvarlig for en IT-strategi, frit i valget af dens nærmere udformning. De *faktiske rammer* for IT-implementering i en organisation er vide. Med den stigende standardisering bliver der stadigt flere muligheder for at tilpasse og udbygge et system. Som omtalt i kapitel 7 findes der dernæst kun et fåtal af *retsregler*, der begrænser mulighederne for at føre en IT-strategi: Børsnoterede aktieselskaber skal efter aktieselskabslovens § 56, stk. 5, (som ændret ved lov nr. 1060 af 23. december 1992) i deres forretningsorden pålægge bestyrelsen "at tage stilling til selskabets organisation, såsom regnskabsfunktion, intern kontrol, IT-organisation og budgettering." Som nærmere udviklet hos *Claus Berg & Lars Bo Langsted* i U1994B.183 ff. er der grund til at tro, at sådanne forskrifter i en forretningsorden kan virke normudfyldende ved fastlæggelsen af bestyrelsens erstatningsansvar, undertiden måske ligefrem i form af en tillempet regel om omvendt bevisbyrde, cf. *Gomard* i U1993B.146. Denne betragtning kan dog kun gennemføres med fuld konsekvens i de situationer, hvor forretningsordenen lægges frem for offentligheden og dermed kan læses af potentielle skadelidte. Ifølge bestemmelsens stk. 6 består en sådan pligt kun for statslige aktieselskaber. At bestyrelsen ikke har udarbejdet en forretningsorden kan ikke i sig selv begrunde et ansvar, jf. *Thorbjørn Sofsrud*: Bestyrelsens beslutning og ansvar (1999), s. 210.

Handling og medvirken

Det er uproblematisk at lægge til grund, at der er ansvar for den, der retligt eller faktisk *pålægger* en anden at udføre en handling, der får tabsforvoldende konsekvenser. Erstatningsretligt vil et sådant ansvar blive rubriceret som medvirken til den indtrådte skade. Denne særlige form for medvirken kan undertiden gøre det betænkeligt at statuere solidarisk ansvar også for den umiddelbare skadevolder, der er underlagt strategien; men i det praktiske liv vil den solidariske hæftelse for medarbejderen sjældent have aktualitet, sml. herved EAL § 23. Ligeledes er det uproblematisk at nå til, at en person eller virksomhed, der har pligt til at drage omsorg for andre, bliver pålagt erstatningsansvar for forsømmelig og tabsforvoldende tilsidesættelse af en sådan pligt, jf. til illustration dommen i *U 1956.1055 H*, hvor to politimyndigheder blev pålagt erstatningsansvar for ikke at have tilrettelagt en alarmprocedure "med fornøden klarhed og bestemthed" i et tilfælde, hvor dette medførte en forsinket brandudrykning.

Om e-handelslovens særlige regler om formidleransvaret

for tjenesteydere, se afsnit 17.1.e.

Aktiv handlepligt?

Strategiansvarets store problem er, om der på almindeligt eller særligt grundlag påhviler "strategen" pligt til at *modvirke*, at skader indtræder – enten ud fra synspunkter om, at den pågældende IT-virksomhed udgør en farlig bedrift, eller fordi IT-driften har en så professionel karakter, at man vil skærpe de almindelige handlepligter. Realt er dette et spørgsmål om, hvorvidt der er pligt til at føre en strategi for IT-sikkerhed. I det omfang, et system behandler data, der repræsenterer vitale formueværdier, kan trusler af denne karakter implicere et sådant faremoment, at man må *skærpe* erstatningsbedømmelsen. Skærpelsen må først og fremmest anlægges i relation til IT-brugeren selv, når spørgmålet er, om denne skal have et erstatningskrav reduceret på grund af *egen skyld*. Meget taler således for at opstille en regel, hvorefter det erstatningskrav, den skadelidte IT-bruger kan gøre gældende mod en i øvrigt erstatningspligtig skadevolder, må reduceres til et normalt tab, hvis brugeren culpøst har *undladt sikkerhedskopiering* af data. Gennem en sådan regel vil man tilskynde sikkerhedsorienteret adfærd, som i almindelighed vil have gavnlig betydning. Det nærmere indhold af brugerens pligt til at foretage sikkerhedskopiering må dog helt afhænge af, hvilke data der er tale om. Navnlig må dataenes stabilitet, omfang og vitalitet for virksomheden samt omkostningerne ved sikring, henholdsvis manuel retablering, indgå i overvejelsen. Se ligeledes afsnit 22.7.e.

18.2.b. Ansvar for IT-sikkerhed

Et særligt problem opstår, når sikkerhedsfejl hos A indebærer, at B's IT-system rammes. Et praktisk eksempel herpå kan være, at B's system inficeres med en programvirus, eller at et IT-system, der er forbundet med offentligt tilgængelige teleforbindelser pga. sin åbne arkitektur, anvendes til at skaffe uberettiget adgang til kundeoplysninger og erhvervshemmeligheder mv. Det er her vigtigt at slå fast, om erstatningsansvaret skal hentes i den almindelige erstatningsregel (culpareglen), i indgåede aftaler, eller i lovgivningen.

Culpatilfælde

Der findes ingen indarbejdet retsopfattelse af, hvornår en sikkerhedsbrist i én virksomhed kan føre til, at denne virksomhed ifalder ansvar overfor andre virksomheder efter de almindelige regler om erstatning uden for kontraktsforhold. IT-området adskiller sig også på dette punkt fra andre teknisk prægede områder af erstatningsretten, idet der ikke kan hentes støtte for den erstatningsretlige vurdering i foreliggende normer for, hvad der er god og sikker optræden, sml. til eksempel *U 1934.1104 V*, hvor tilsidesættelse af en bygningsnorm påførte en bygningsejer erstatningsansvar for en skorsten, der som følge heraf styrtede ned.

Der findes forskellige forsøg på at standardisere forskellige sider af IT-sikkerhedsarbejdet, men hovedvægten i dette standardiseringsarbejde er terminologisk/systematisk, og generelt gælder det vel, at læren om IT-sikkerhed hovedsagelig tager sigte på virksomheden som skadelidt, eller – omsat i erstatningsretlig sprogbrug – på dens tabsbegrænsningspligt. Eksempler på sikkerhedsstandarder er British Standard 7799:1995 med titlen *Code of practice for Information security management* (1995), Amtsrådsforeningens og KL's *Vejledning om Datasikkerhed* (maj 1994), EDI-rådets *Vejledning om sikkerhed i EDI-løsninger* (maj 1999). FSR's revisionsvejledninger om *revision af edb-baserede brugersystemer* (nr. 17) kan vel siges at gå skridtet videre, men vejledningens hovedsigte er at overholde regnskabs- og bogholderimæssige forskrifter.

At problemet så sjældent træder frem overfor tredjeparter skyldes, at de relevante skadetilfælde typisk også vil involvere egen skyld fra skadelidtes side. Det må f.eks. som udgangspunkt antages, at en person, der aktiverer en eksekverbar fil (angivet med efternavnet ".exe"), der uden særlig grund fremsendes ved en elektronisk postmeddelelse, handler culpøst i relation til den, der herefter rammes af konsekvenserne af en virus, der var gemt heri: Kendskabet til en sådan handlings potentielt skadevoldende egenskaber er almindeligt også uden for de IT-sikkerhedskyndiges rækker, bl.a. som følge af hyppig presseomtale af sådanne

tilfælde. Men det karakteristiske for denne type culpa er, at dens skadegørende egenskaber kun viser sig, hvis andre handler ligeså culpøst, f.eks. når de modtager den tilsvarende elektroniske postmeddelelse, som i kraft af den spredte virus rundsendes til alle, der står anført i den angrebne parts kundekartotek. Som udgangspunkt vil der derfor, så at sige pr. automatik foreligge egen skyld hos skadelidte i samme omfang, som der foreligger culpa hos skadevolderen.

Hacking

Indehaveren af et IT-system, der bruges som grundlag for ulovlig indtrængen i andre IT-systemer, er som udgangspunkt ikke ansvarlig for de tab, der måtte følge heraf, f.eks. ved kompromittering af erhvervshemmeligheder eller ved et forbrug af teleydelser, som skadelidte hæfter for. Ofte vil der være tale om, at skadelidtes egen skyld vil overstige den påståede skadevolders hovedskyld, eftersom den pågældende indtrængen mv. er gjort mulig gennem et for lavt sikkerhedsniveau. Uden for disse tilfælde vil der formentlig skulle meget til for at fastslå en særlig, erstatningsretligt sanktioneret handlepligt i henseende til den nævnte systemansvarlige. Medmindre en sådan handlepligt er hjemlet ved aftale eller har lovhjemmel, vil der efter almindelige regler om ansvar for undladelser som hovedregel end ikke være pligt til at *informere* andre ofre om et sådant angreb. Er offeret derimod den systemansvarliges aftaleparter eller en part, der har råden over det angrebne system i konsekvens af en overdragelse fra den systemansvarliges medkontrahent, vender billedet. Andre modifikationer kan tænkes i takt med, at vi får stadigt flere regler om sikkerhed for produkter og netydelser mv.

Adækvans

Når ansvaret fastlægges indgår adækvansvurderingen som et uadskilleligt element, der må tages i betragtning. Det vil således være for vidtgående at skulle antage, at simpel uagtsomhed i forbindelse med aftalte sikkerhedstiltag skulle indebære, at den pågældende driftsansvarlige skulle være fuldt erstatningsansvarlig for samtlige heraf følgende adækvate tab. De almindelige erstatningsretlige regler (culpareglen) kan med deres udgangspunkt om, at undladelse ikke pådrager erstatningsansvar, ikke begrunde et sådant resultat, der i det højeste kan overvejes inden for områder, hvor særlovgivningen pålægger en særlig handlepligt.

Aftaletilfælde

I de tilfælde, hvor relationen mellem A og B har grundlag i et *aftaleforhold*, må erstatningsansvaret søges i denne aftale. Ofte vil IT-aftaler dog snarere begrænse end udvide erstatningsansvaret. Sådanne regler er som udgangspunkt gyldige, men de må i almindelighed fortolkes således, at der ikke fraskrives ansvar for

grov uagtsomhed eller forsæt, jf. *Viggo Hagstrøm* i TfR 1996.421. Fraskrivelser for sådant ansvar vil efter omstændighederne kunne tilsidesættes som ugyldige efter aftl. § 36.

I mangel af særlige vedtagelser vil reglerne om aftaleretlig *omsorgspligt* pålægge den, der behandler data for andre, at skride ind, hvis han bliver bekendt med noget, der kan bevirke skader på disse data. Heraf følger en pligt til at føre en vis IT-sikkerhedspolitik, f.eks. med håndfaste regler om adgangskontrol, hyppig skanning og kontrol for virus-inficering af filer og løbende ændring af passwords for gæster, systemoperatører og andre ikke fast opkoblede brugere. Den pågældende branche vil ofte udvikle forventninger til et sikkerhedsniveau. Finansvirksomheder vil stille anderledes krav end universiteter.

- i kontrakt

De sikkerhedskrav, man vil stille i *kontraktsforhold*, illustreres med retspraksis i sager om *forvaring*. Denne praksis kan i nogen grad være normgivende også på IT-området i aftaleforhold, hvor der består en særlig påpasselighedspligt. Illustrativ i så henseende er dommen i *U 2000.350 H*, der (under dissens) ikke fandt et autoværksted ansvarlig for tyveri af nogle henstillede biler (Mercedes-taxaer). Tyven havde brudt en nøgleboks op, hvori ejerne af de pågældende biler – efter aftale og som led i værkstedets almindelige praksis – havde deponeret deres nøgler. Nøgleboksen var specialfremstillet med henblik på at undgå tyveri, og ifølge en syn- og skønserklæring var der ikke udvist forsømmelse med hensyn til dens opsætning og ved tilsynet med den. Flertallet i Højesteret ville ligesom landsretten uden videre frifinde værkstedet med præmisser, der lader formode, at man anså fremgangsmåden for forsvarlig, og at der ikke var ført bevis for culpa. Det samme ville den dissentierende dommer, der dog – modsat flertallet – nåede sit resultat efter en nøje efterprøvelse af, om en alternativ – og antageligvis mere sikker – boks ville have forhindret tyveriet. Flertallets votum tyder altså på, at culpareglen på dette område ikke er skærpet i retning af en "optimus vir"-standard. Se tilsvarende *U 1990.817 Ø* og senest *U 2000.432 V*, hvor tyveri af nøgler til et boligkompleks fra en VVS-installatørs bord i personalekantinen ikke fandtes erstatningspådragende i relation til det herpå følgende tab svarende til udgifterne ved omkodning af låse i boligkomplekset.

- udenfor kontrakt

Uden for kontraktsforhold kræves der som udgangspunkt særlig hjemmel for at kunne pålægge en part erstatningsansvar for den "passive medvirken", der kan siges at ligge i ikke at opretholde et sikkerhedsniveau, der *forhindrer* en hovedgerningsmand i at forrette skade via medvirkerens IT-system. Illustrerende herfor

er dommen i *U 1990.535 V*, der frifandt en murermester for de skader, der var forvoldt som følge af, at tyve havde fået adgang til noget saltsyre, som ejeren ikke havde opbevaret forskriftsmæssigt sikkert.

Bevisvirkninger

I visse tilfælde vil manglende overholdelse af sikkerhedsregler kunne vende bevisbyrden for kausalitet til skadelidtes favør. Således pålagde *U 1982.50 H* en arbejdsgiver ansvar for en arbejdsulykke ved ikke at have placeret en visirskærm på en maskinsav. Ansvaret blev pålagt, uanset det ikke var bevist, at en sådan skærm kunne have afværget ulykken.

Opfølgningsansvar

Uanset om en strategi er forsvarlig, kan der komme et ansvar på tale, når den ført ud i livet alligevel giver anledning til skader og tab pga. uregelmæssigheder mv. I disse tilfælde er det typisk enkelt at finde en umiddelbart ansvarlig: den medarbejder, der overså en ny viden, trykkede på den forkerte knap eller undlod at indsætte en påkrævet komponent. Som oftest kan man herefter konstatere, at strategien (regelgrundlaget) som sådan var i orden. Det var netop, fordi den ikke blev overholdt, at skaden indtrådte. Og undertiden vil den strategiansvarlige hæfte for den, der bryder strategien i kraft af kontrakts-, fuldmagts- eller principalansvarssynspunkter (DL 3-19-2). Spørgsmålet om et selvstændigt ansvar for overholdelsen af en strategi opstår, når disse hæftelsesregler ikke kan anvendes efter deres indhold, f.eks. fordi den umiddelbare skadevolder ikke står i principalforhold til den strategiansvarlige, fordi der foreligger abnorme skridt eller af andre grunde.

Katastrofeansvar

Behovet for et sådant ansvar føles særlig stærkt, når der er tale om ekstraordinært store tab i forbindelse med katastrofer: En olietanker havarerer og forurener store naturområder i Alaska; reaktorkernen i et atomkraftværk nedsmelter pga. forsømmelighed. I sådanne tilfælde er det almindeligvis enkelt at udpege dem, der ikke overholdt en given sikkerhedsstrategi. Spørgsmålet er imidlertid, om ikke den manglende kontrol med denne overholdelse skal give anledning til et selvstændigt ansvar. En sådan culpahæftelse er ikke ukendt. Den anses som en del af den risikofilosofi, der ligger til grund for forskellige objektive ansvarsformer, og som går ud på, at en risiko bør ligge hos den, der har haft muligheden for at styre en organisation på en måde, så skader undgås. Vor retsordning forudsætter, at erstatningsansvar må placeres på niveauer, der står i forhold til omfanget af den indtrådte skade. Det princip, der illustreres med ansvarsskemaet ovenfor, indebærer, at kredsen af mulige ansvarspersoner udvides, jo større værdier der er på spil. Er der tale om store tab og/eller vitale interesser, må blikket vendes mod de store og centrale samfunds-

aktører, selv om ansvaret for en umiddelbar betragtning måske ligger på et mere decentralt niveau. De relevante regler om erstatningsretlig hæftelse må modificeres i overensstemmelse hermed. Se nærmere *E&A* s. 218 ff.

18.2.c. Konstaterende erklæringer

En særlig form for erstatningsansvar knytter sig til den *konstaterende erklæring*, en troværdig tredjepart (f.eks. en certificerende myndighed eller et nøglecenter) afgiver om et forhold, der har betydning for andre. Værdien af sådanne erklæringer for den almindelige omsætning taler for, at retssystemet må beskytte tredjemand mod skuffelser, som certifikatudsteder bærer ansvaret for. Almindeligvis antages det, at ansvaret må bedømmes efter erklæringens egnethed til at virke bestemmende på modtagerens handlemåde i væsentlige retsforhold, den konkrete kausalitetsvurdering og graden af subjektiv skyld hos afgiveren. Se hertil *Gomard* (1958) s. 381 ff. og *Skovgaard* (1983), s. 162 ff. med henvisninger til praksis. Da certifikater netop udstedes for at indgå som tillidsgrundlag for almenheden, må der som udgangspunkt gælde et professionelt culpaansvar (udenfor aftaleforhold) for fejl i certifikatet.

Om der foreligger en fejl ved en certificeringsydelse, vil bl.a. bero på, hvor velbeskrevet certificeringsgrundlaget er. Er der ikke overladt organet noget skøn, vil det være enkelt at påvise en fejl. Ved skønsmæssige afgørelser bliver bevisbyrden vanskeligere at løfte. Som det gælder i den offentlige ret, kan skadelidtes påvisning af proceduremæssige fejl samt skødesløshed mv. lette bevisbyrden.

Forholdet belyses ved *U 1976.219 Ø* om en misvisende synserklæring fra Statens Bilinspektion. En privatperson havde købt en brugt bil for 3.200 kr. Købet var betinget af, at vognen kunne underkastes syn. Efter at bilen var fremstillet til syn nogle gange, udstedte Statens Bilinspektion senere s.m. registreringsattest. Knap 4 måneder efter blev bilen standset ved et § 13-eftersyn pga. graverende mangler, og ved et senere syn fandtes udbedringsværdien at ligge langt over købesummen. Justitsministeriet blev kendt erstatningspligtig overfor køberen under henvisning til, at bilinspektionen ved blot en overfladisk vurdering burde have indset bilens ringe tilstand, og at attesteringen uanset dette indebar, at der forelå en grov fejl. Se også *U 1990.482 V*, der frifandt en energikonsulent for ansvar i henhold til en varmesynsrapport, *U 1985.1061 H*, der under dissens frifandt en kommune for erstatningspligt for at have udstedt erklæring om lovligheden af et beboelseshus, for hvilket der senere stilledes krav om bygningsændringer og *U 2003.559 H,* der gjorde Justitsmi-

nisteriet erstatningsansvarlig for en bilkøbers tab i anledning af fejlagtig oplysning i bilens registreringsattest. Se også *U 2003.1366 V*, hvor en kommune blev erstatningsansvarlig over for køberen af en fast ejendom for ikke at have givet oplysning om et konkret anlægsprojekt i det oplysningsskema, ejendomsmægleren havde anmodet kommunen om at udfylde.

Tjenesteydelser

Det sker undertiden, at certifikatudstederen påtager sig særlige tjenesteydelser. I det omfang dette sker, handler organet som enhver anden leverandør af sådanne ydelser, sml. voldgiftskendelsen om olierørledningen i *KFE 1988.140*. I denne sag fandtes en certifikatudsteder (i kendelsen kaldet T 1) ikke at have begået fejl ved sin godkendelse af produktionen og kontrollen af rør. Kendelsen henviser til, at revner af den i sagen omhandlede art ikke tidligere havde været rapporteret, at den godkendte kontrol stemte med internationale standarder, og at erfaringerne med enderevner ved denne rørledning ikke havde ført til, at de internationale standarder var blevet ændret (s. 144). Derimod fandtes certifikatudstederen at bære et rådgiveransvar for ikke i tilstrækkeligt omfang at have advaret klienten om, at der var konstateret fejl i et enkelt rør. Ansvaret bortfaldt dog af andre grunde.

Principielt må der sondres mellem virksomhedens rådgivnings- og certificeringsopgaver. Den erstatningsretlige bedømmelse af en rådgivningsydelse præges af det noget strengere professionsansvar, hvor ansvaret for certificeringsydelsen har nøje sammenhæng med indholdet af certificeringsgrundlaget. Er certificeringsgrundlaget præcist, vil ansvaret for udstederen være let at definere. Udstedes et certifikat i strid med standarden, vil der være en formodning for erstatningspligt.

Lides tabet til trods for, at den præcise standard er overholdt, kan man overveje et ansvar mod det organ, der har formuleret certificeringsgrundlaget. Et sådant ansvar er dog næppe let at gennemføre, jf. diskussionen i afsnit 18.1.e. om hensynet til den fri spredning af informationer. Ansvar vil formentlig kun kunne komme på tale, hvis der foreligger særlige grunde – f.eks. en konkurrencemæssigt begrundet chikane.

18.2.d. Pligt til IT-anvendelse?

At en virksomhed anvender IT, forandrer som hovedregel ikke de krav om påpasselighed, man vil stille i en given sammenhæng. Efter dansk ret vil undladt IT-anvendelse som hovedregel heller ikke påføre erstatningsansvar. Dette resultat følger for det første af den almindelige hovedregel, hvorefter passivitet ikke pådrager

ansvar; men i øvrigt er den opfattelse fæstnet i vore retsordninger, at særlige risici ved komplicerede anlæg og teknologier først og fremmest imødegås ved love og forskrifter. Kun på områder, hvor gældende regler fastslår, at en given aktivitet *skal* understøttes af IT for at blive udført forsvarligt, kan man tænke sig et sådant erstatningsansvar for undladt IT-anvendelse.

Denne hovedregel modificeres dog, når IT-anvendelse er et nødvendigt element i den pågældende aktivitet. Talrige af det moderne livs handlinger – f.eks. opsendelse af satellitter, navigation af jumbo-jets samt mangfoldige skatte- og aktuarmæssige beregninger – kan ikke gennemføres uden IT. Her har det ingen realitet at diskutere, om man "bør" anvende IT eller ikke. Udføres aktiviteten, er IT-anvendelsen en nødvendig bestanddel. En sådan sammenknytning kan følge af tekniske forhold, af aftale og/eller af sædvane. En virksomhed, der ligefrem tilbyder sine kunder en IT-sikkerhedsfacilitet (f.eks. i form af et værktøj, der sikrer programmer mod infektion med virus), kan i almindelighed ikke undslå sig med, at man ikke rådede over den nødvendige teknologi hertil. Dernæst vil muligheden for gennem effektiv IT-anvendelse at forbedre kvaliteten af en ydelse kunne øge forventningerne til denne ydelses kvalitet og sikkerhed.

Hooper-sagen

Når spørgsmålet har været så indgående debatteret, skyldes det, at retsstillingen muligvis er en anden i USA, hvis IT-praksis har en vis indflydelse på vor. I amerikansk teori har dette område været domineret af et domspræjudikat fra 1930'erne, *The T.J. Hooper*, 60 F.2d 737 (1932). Her blev ejeren af to dampskibe kendt erstatningspligtig for ikke at have udstyret sine skibe med skibsradioer. Hvis skibene havde haft dette udstyr, kunne de have erfaret, at der var et voldsomt uvejr forude og dermed undgået det senere indtrufne forlis. På det pågældende tidspunkt (1928) var der kun ét dampskibsrederi, der havde radioer på sine skibe. Dette forhold indicerede i sig selv, at der ikke var tale om noget, vi ville betegne som en bonus pater-pligt. Men selv i mangel af en sådan sædvane antog dommeren – den højt ansete Justice *Learned Hand* – at visse "precautions [are] so imperative that even their universal disregard will not excuse their omission".

På grundlag af disse præmisser har man i amerikansk teori drøftet, om en tilsvarende *optimus vir*-standard eksisterer på IT-området. En sådan pligt til at anskaffe det mest avancerede udstyr, hvis dette kan reducere en skadesrisiko, må forudsætte, at den pågældende teknologi i almindelighed står til rådighed, og at den virkelig frembyder en markant bedre sikkerhed. Den øgede

sikkerhed skal med andre ord stå i et rimeligt cost-benefit-forhold til situationen uden, f.eks. således at ekstraordinære risici minimeres eller reduceres ved hjælp af den pågældende teknologi. Som nævnt er sætningen næppe dækkende for dansk ret, og dens indhold og rækkevidde har da også været omdiskuteret i USA.

Se herved gennemgangen hos *Paul DeRensis* i 25 Practical Lawyer # 4.57 (1979), p. 61 ff. og *Petras & Scarpelli*, 5 Rutgers 15 (1975). Et tilsvarende spørgsmål som det, der forelå i Hooper-sagen, opstod, da man begyndte at anvende radar-teknologien ved flynavigation. Se f.eks. dommen i *Northwest Airlines, inc. v. Glenn L. Martin Co.*, 224 F.2d 120 (1955), der frifandt, allerede fordi der "in August, 1948, ... [was] no evidence that feasible airborne radar was commercially available to operators of airlines" (p. 130).

Offentlige myndigheder

På grund af bevillingsrammer vil offentlige skadevoldere ofte være økonomisk afskåret fra at kunne minimere risiciene for skader. Spørgsmålet er da, om der kan rettes et strategiansvar mod de beslutningshavere, der træffer de fatale bevillingsbeslutninger.

Spørgsmålet belyses ved *U 1985.368 H*. En patient, der netop var blevet opereret på et provinssygehus, fik en åndedrætslammelse under opvågningen. Lammelsen blev ikke opdaget i tide, fordi patienten var ført tilbage på sengeafdelingen, hvor hun ikke var undergivet konstant tilsyn. Højesteret lagde til grund, at det tilsyn, der blev ført med patienten efter operationen, svarede til, hvad der var normalt på det sagsøgte sygehus og lignende sygehuse, og at tilsynet under de foreliggende forhold var lægeligt forsvarligt. I *Pontoppidans* kommentar U1985B.248 ff. anføres det, at det "...inden for ret vide rammer – på det foreliggende område afgrænset af det lægeligt forsvarlige – [må] tilkomme de politiske instanser at fastlægge standarden". Højesteret fandt ikke, at det kunne være domstolenes opgave gennem tilkendelse af erstatning at gribe korrigerende ind over for det serviceniveau, som er et resultat af de politiske organers beslutninger.

Ifølge kommentaren synes det som om Højesteret vil stille store krav til den culpavurdering mv., der skal føre til et strategiansvar for offentlige myndigheder, hvis ansvaret har rod i politiske beslutninger fra det kompetente forum. Man kan være enig eller uenig i betragtningen, men den harmonerer med den statsideologi, der i øvrigt er fremherskende herhjemme, hvorefter det ikke tilkommer domstolene at efterprøve politisk prægede afgørelser, der ikke er direkte i strid med loven. Et tilsvarende resultat måtte formentlig antages, hvis årsagen til skaden lå i en beslutning om at afskedige en læge for i stedet at anskaffe et medicinsk ekspertsystem. Når dette er

sagt, må det imidlertid tilføjes, at betragtningen nok bevirker, at skadelidtes erstatningsretlige beskyttelse er forskellig alt efter, om skaden sker i offentlig eller privat regi.

18.3. Funktionsansvaret

18.3.a. Problemstillingen

Begreb

Den, der fastlægger de funktioner, der gælder for betjeningen af et produkt, foregriber ved det tekniske produktdesign og ved den information (brugsanvisninger mv.), der ledsager produktet, forbrugerens anvendelse af det. De erstatningsretlige konsekvenser af en sådan funktionsfastlæggelse træder frem som to ansvarsformer. Er funktionen originært fastlagt, tales om funktionsansvar. Dette ansvar er genstand for det følgende afsnit. Fremkommer den som følge af en sammensætning af del-funktioner, der allerede er fastlagt (f.eks. af en underleverandør), tales om ansvar for implementering, jf. nedenfor under 18.4. De to ansvarskategorier har ikke skarpe grænser mod hinanden.

Det moderne forbrugsmarked florerer med produkter med nye og uventede funktioner. Talrige af disse funktioner er årsag til skader, som forbrugerne med deres flygtige kendskab til produkternes farlighed ikke altid kan forudse. I en række tilfælde skyldes skaderne forbrugerens fejlagtige anvendelse eller vedligeholdelse; men i stigende grad har produkterne selv overtaget disse funktioner. Moderne kameraer indstiller selv blænde, afstand og eksponeringstid, nutidens personvogn har automatiseret en række vedligeholdelsesfunktioner, og ikke mindst har IT-systemerne overtaget mange af de funktioner, der tidligere krævede kompliceret programmering. Dermed kan avancerede produkter anvendes uden særlig uddannelse, i takt med at produkterne selv overtager "ansvaret" for den fejlagtige håndtering mv. Tilsvarende er produktets funktion i sig selv blevet en skadesårsag.

Valghandlingen

I valget af, hvilken funktion et produkt skal have, står producenten almindeligvis frit. Den, der konstruerer en bil, træffer en lang række beslutninger, der på forskellig vis øger eller reducerer risikoen for og ved uheld. Denne frihed taler umiddelbart for at skærpe ansvarsbedømmelsen, således som det f.eks. er sket på produktansvarets område. Er der tale om et produkt med en vis kompleksitet – som det f.eks. er aktuelt på IT-området – kan designeren dog have svært ved at overskue de risici for skader mv., som produktet implicerer. Friheden til at designe produktet

får dermed til dels illusorisk karakter. Dette taler for ikke at overdrive de erstatningsretlige krav. På det trin af retsudviklingen, hvor vi i dag befinder os, er det ikke helt afklaret, hvorledes man bør fordele den erstatningsretlige risiko for skader og tab forvoldt ved det moderne industrisamfunds produkter og tjenesteydelser. Klart er det imidlertid, at tendensen går mod en stadig skærpelse af "producentens" ansvar. Med PAL blev der indført objektive erstatningsregler på væsentlige dele af dansk produktansvarsret. En lignende tendens havde allerede tegnet sig i domstolenes praksis op gennem 1970'erne og 1980'erne.

Tendens?

Man kan anskue denne retsudvikling efter forskellige betragtninger. Den væsentligste begrundelse bag udviklingen er forbrugerpolitisk. Ansvarsreglerne værner den interesse, der består i, at forbrugerne kan stole på de produkter, der erhverves i handelen, og støtter dermed den tillid til produkterne, som omsætningen i det lange løb profiterer af. På det almindelige produktmarked er det da også klart, at forbrugeren ikke forventes at skulle anstille kemiske undersøgelser af de fødevarer, han spiser. Spørgsmålet er, om denne begrundelse holder, når produktets funktioner ikke rummer en umiddelbar påvirkning af personer eller ting, men information, der er karakteriseret ved at indgå som grundlag for selvstændige beslutninger mv.

18.3.b. Produktansvaret

Dansk produktansvar har efter vedtagelsen af lov nr. 371 af 7. juni 1989 om produktansvar (PAL) fået en EU-retlig dimension. Grundlaget for loven er et Rådsdirektiv af 25. juli 1985 om tilnærmelse af medlemsstaternes administrativt eller ved lov fastsatte bestemmelser om produktansvar (85/374/EØF), EFT 1985 L 210/29, der foruden forbrugerhensynet tilsigter at harmonisere medlemsstaternes lovgivning for derved at skabe færrest mulige tekniske handelshindringer.

PAL er opbygget omkring en objektiv erstatningsregel for personskade og erstatning for tab af forsørger samt for de såkaldte "forbrugertingsskader". Herved forstås efter lovens § 2, stk. 2, skader på genstande, der efter deres art "sædvanligvis er beregnet til ikke-erhvervsmæssig benyttelse og hovedsagelig anvendt af skadelidte i overensstemmelse hermed".

Skadesbegrebet

Forbrugeres tab af data må formentlig falde under lovens forbrugertingsskade-begreb, hvis dataene befinder sig på forbrugerens eget medium. Almindeligvis defineres skade som en fysisk forandring af negativ karakter. Dette kriterium volder netop ikke

vanskelighed, hvis data befinder sig på forbrugerens eget medium. Forholdet minder i så fald om den skade, der f.eks. gør det umuligt at læse en bog, og det forekommer tilsvarende sprogligt og realt velmotiveret at antage, at en "negativ forandring" kan bestå i den tekniske uorden mv., der fjerner informationsværdien af en datamængde. Sml. herved *U 1987.216 Ø*, der lagde til grund, at databærende medier med indlagte data måtte anses som "ting" efter strfl. § 291 og *U 1991.386 H*, der tilkendte et selskab en skønsmæssigt fastsat erstatning på 160.000 kr. bl.a. for forsætlig sletning af et antal filer i selskabets IT-system. Det fremgår ikke af dommen, om selskabet havde foretaget sædvanlig backup kopiering.

Mere tvivlsomt er det, om noget tilsvarende gælder, hvis de ødelagte data befandt sig på et medium, som en tredjepart har i sin besiddelse, f.eks., hvis brugeren har data liggende på sin hjemmeside hos en Internet-leverandør. Det forhold, at brugeren i denne situation ikke har det løbende herredømme over det pågældende medium, begrunder i sig selv en ændret synsvinkel: fordi brugeren i forvejen har disponeret i tillid til, at andre end han selv sikrer de pågældende data kan det føles mere nærliggende at betragte dataene som en ren tjenesteydelse, der præsteres fra den pågældende leverandør. Det må dog erkendes, at der kan tænkes mange eksempler, hvor tjenesteydelses-analogien ikke holder stik, f.eks. tilfælde, hvor brugeren selv har det fulde sikkerhedsansvar (med heraf følgende pligt til at foretage sikkerhedskopiering af de pågældende data til eget medium). I disse tilfælde ændrer problemstillingen imidlertid karakter, idet et erstatningsrelevant tab først opstår, hvis også de pågældende sikkerhedskopier (hos brugeren selv) ødelægges.

PAL etablerer et selvstændigt ansvarssystem ved siden af det, der allerede er udviklet gennem retspraksis mv. Lovens § 13 giver skadelidte adgang til erstatning efter almindelige regler om erstatning i eller uden for kontrakt eller i medfør af regler, som er fastsat i eller i henhold til anden lovgivning. Dansk produktansvarsret kører dermed efter et to-strenget system – et forhold, der i nogen grad begrænser den tiltænkte harmonisering. En enkelt af ulemperne ved denne tve-regulering er dog afbødet ved lovens § 14 om forældelse. Her fastslås det, at der indtræder en 3-årig forældelse af såvel de krav, der kan rejses i medfør af loven som af krav "efter almindelige regler om erstatning i eller uden for kontrakt". Det samme gælder ikke for den 10-årige forældelsesfrist, § 14, stk. 2. Ved fastsættelse af erstatning for skade på ting efter PAL fradrages et beløb på 4.000 kr., se lovens § 8.

Ved kun at regulere forbrugertingsskaden er PAL umiddelbart uanvendelig for mange af de skadestilfælde, der har interesse for

nutidens IT-anvendelse, f.eks. erhvervsdrivendes tab af data som følge af "virus" eller tab ved forkerte forretningsmæssige eller driftsmæssige dispositioner truffet på grundlag af IT. Her må man principielt falde tilbage på det dommerskabte produktansvar, der var gældende ved lovens givelse. Da disse regler dog i hovedsagen anses for at være sammenfaldende med PAL's regler, udskilles de to retsgrundlag ikke i det følgende.

PAL

Efter PAL § 6, stk. 1, skal en producent erstatte den skade, der er forårsaget af en defekt ved et produkt, som er produceret eller leveret af denne. Samme bestemmelses andet stykke fastslår, at skadelidte kun behøver at føre bevis for "skaden, defekten og årsagsforbindelsen mellem defekten og skaden". Forbrugeren behøver ikke at rette sit erstatningskrav mod producenten. Efter lovens § 11 hæfter mellemhandlere direkte over for skadelidte og senere mellemhandlere i omsætningskæden for indtrådte produktskader.

"Produkt" og "producent"

PAL § 3 definerer et *produkt* som "enhver løsøregenstand, hvad enten denne er forarbejdet eller er et naturprodukt, og uanset om genstanden er indføjet som en bestanddel af en anden løsøregenstand eller en fast ejendom". Det tilføjes, at reglerne om produkter også omfatter elektricitet. *Defekt* er produktet, jf. § 5, når det ikke "frembyder den sikkerhed, som med rette kan forventes". Dette uddybes i en række kriterier, herunder produktets markedsføring, den anvendelse af produktet, som med rimelighed kan forventes, og tidspunktet da produktet er bragt i omsætning. *Producent* er ifølge § 4 den, "der fremstiller et færdigt produkt, et delprodukt eller en råvare, den, der frembringer eller indsamler et naturprodukt, samt den, der ved at anbringe sit navn, mærke eller andet kendetegn på produktet udgiver sig for at være dets producent".

Efter lovens § 7 er producenten ansvarsfri, når producenten ikke har bragt produktet i omsætning, eller hvis produktet ikke er bragt videre som led i erhvervsvirksomhed. Dernæst fritages producenten for ansvar for defekter, der skyldes, at produktet skal være i overensstemmelse med ufravigelige forskrifter udstedt af offentlig myndighed. At producenten følger en standard, der er skyld i defekten, er altså ikke tilstrækkeligt til at statuere ansvarsfrihed. Producenten af et del-produkt (f.eks. et modul til et større IT-system) er heller ikke ansvarlig, hvis han beviser, at defekten skyldes udformningen af hoved-produktet eller anvisninger, som er givet af hovedproduktets producent. Endelig er der – som vi allerede har set – gjort en særlig undtagelse for udviklingsskader, § 7, stk. 1, nr. 4. Derimod kan det være selvstændigt ansvarspå-

dragende at levere i strid med en standard, hvis aftalen henviser hertil, sml. til illustration *U 1973.53 H,* om tilsidesættelse af byggenorm.

Produktbegrebet

Afgørende for, om produktansvarsreglerne skal gælde for edb-programmel, synes umiddelbart at være, om et "programprodukt" kan betragtes som et "produkt" i lovens forstand. Lovens definition besvarer ikke dette spørgsmål, lige så lidt som Justitsministerens bemærkninger til lovforslaget eller forarbejderne til direktivet gør det. I bemærkningerne hedder det, at begrebet ikke omfatter tjenesteydelser. Der er ikke givet eksempler, der kunne give en indikation af, om information kan betragtes som et produkt eller som en tjenesteydelse. Også forarbejderne til direktivet er tavse. Problemet bliver ikke lettere af, at vi hverken herhjemme eller i udlandet rigtigt kender til "produktansvars-sager", hvor et edb-program overdrages som sådant og forvolder skade som sådant. Se nærmere herom *E&A*, s. 392 ff.

I 1985 stillede det hollandske medlem af EF-parlamentet, *Gijs de Vries* spørgsmål til Kommissionen om, hvorvidt EF-direktivet om produktansvar også gælder for edb-software. Svaret fra kommissær Cockfield var kort. Efter en gengivelse af direktivets art. 2 (definitionen af produktbegrebet) hedder det: "Som følge heraf gælder direktivet for programmel, ligesom det i øvrigt gælder for håndværksmæssige og kunstneriske produkter". Se EFT 1989 C 114/42. Svaret er næppe udtryk for nogen gennemgribende analyse af problemstillingen, jf. nærmere nedenfor.

Bortset fra mine analyser i *E&A* og i redegørelsen: Nogle IT-retlige problemer ved årtusindskiftet – en juridisk oversigt. År 2000-sekretariatet (juni 1998) er litteraturen om emnet begrænset. *Nørager-Nielsen* (1987) antager, s. 301, at standardsoftware må betragtes som "produkter" på grund af deres tilknytning til et eller andet medium, sml. ligeledes NOU 1980:29, s. 102, hvorefter "en edb-kasette i seg selv" må anses som et produkt efter den norske lov, for så vidt "feilen har karakter av en sikkerhetsmangel".

I den almindelige litteratur om produktansvaret defineres et "produkt" sædvanligvis i relation til den proces, hvormed produktets egenskaber udnyttes. Det forudsættes, at produktet anvendes af en "forbruger" under en relativt veldefineret "sædvanlig forbrugsproces", og at skaden netop indtræder under denne proces. Overfører man denne tankegang til det "produkt", en programpakke udgør, er det iøjnefaldende, at den "proces", hvorved programpakken åbnes, disketten tages ud og monteres i maskinen, er helt uden faremomenter (det skulle da lige være, hvis man tabte manualen over tæerne etc.). De produkthandlinger, der har erstatningsretlig interesse, træffes under og navnlig efter anvendelsen

af programproduktet, f.eks. ved fejlagtige beregninger, konstruktioner og heraf følgende dispositioner. Den "forbrugsproces", der ligger i sådanne dispositioner, er lige så mangfoldig som skadelidte kan disponere. I så henseende adskiller det informations-genererende produkt sig mærkbart fra de produkter, der har været inddraget i det dommerskabte produktansvar.

Det objektive produktansvar kan anskues som en erstatningsretlig beskyttelse af den tillid, der udspringer af, at vi håndterer – og "kommunikerer" med – vore produkter i overensstemmelse med deres fremtoning. Ansvaret bygger på den tanke, at produktet rummer en information om sig selv, der lægger op til, at forbrugeren skal udvise en større eller mindre grad af tillid.

Kommunikative aspekter

For både edb-programmer og bøger er det kendetegnende, at de erhverves og omsættes med henblik på, at brugeren anvender deres information under en kommunikationsproces. Produktet er dermed reelt en informationsydelse. For programansvaret fører dette til en sondring mellem, om produktet selv "disponerer", eller om det er dets bruger, der disponerer på grundlag af de informationer, produktet afgiver under denne proces, eller som fremgår af dets manual. IT-systemer, der kontrollerer forløb, som forbrugeren ikke kan indvirke på, må som udgangspunkt behandles som ingredienser i traditionelle "produkter", og ansvaret for heraf følgende fejl bedømmes efter reglerne om produktansvar. Et IT-system, der styrer en kemisk proces således, at brugeren slet ikke kan frakoble systemet i faresituationer, må derfor formodes at pådrage producenten et sædvanligt produktansvar.

Autoritetsgraden

I mange tilfælde kan der ikke sondres klart mellem disse to situationer. Dette er f.eks. tilfældet, når brugeren har en teknisk mulighed for at gøre indgreb i systemets funktionalitet (ved at påvirke opsætningsparametre el.lign.), men ikke forventes at gøre det under den almindelige brug. I det skøn, som man derfor må udøve, vil det da være graden af den *autoritet*, hvormed brugeren tilskyndes til at vise tillid til programmets funktioner, der får betydning for ansvarets hårdhed. Lægger programmet op til, at forbrugeren bør kunne "stole" på det uden at skulle gøre indgreb i dets konstruktion eller opsætning, er der en formodning for objektivt produktansvar. Med denne indfaldsvinkel kommer vurderingen af ansvarsgrundlaget til at bero på, hvorledes produktet præsenterer sig overfor forbrugeren.

Culpastandarden

I de tilfælde, hvor man må nå til, at der ikke foreligger noget "produkt", men en ren informationsydelse, opstår spørgsmålet, hvor skarpe culpakrav man bør anlægge for sådanne ydelser. Som nævnt i indledningen til dette kapitel må det spille ind, at IT

er noget, der er mangelfuldt langt hyppigere og på ganske anden vis end på det traditionelle forbrugsområde, og at der for den skadelidte bruger består en mangfoldighed af forbrugsvalg, som producenten ikke har mulighed for at tage højde for i sin konstruktion. Dette giver støtte for en regel om, at brugeren af rent informationsproducerende IT-systemer som udgangspunkt selv må anstille undersøgelser om dataenes korrekthed, før han disponerer med skaderisiko for sig selv. En sådan regel er iøvrigt i harmoni med det almindelige udgangspunkt om, at indtrådte skader bæres, hvor de falder.

For så vidt angår ansvaret for de funktioner, der styres af standard-software, kan dette synspunkt suppleres med informationshensynet, jf. herom ovenfor i afsnit 18.1.e.: Denne betragtning fører til, at standard-software bør behandles på samme måde som anden masse-distribueret information. Forholdene er formentlig tilsvarende i nordisk erstatningsret, herved den i *E&A* s. 398 ff. citerede retspraksis. Som antaget af *Gomard* (1958), s. 383 er en korttegner næppe ansvarlig overfor fly, der støder mod bjerge eller overfor skibe, der strander på skær, der fejlagtigt ikke er afsat på hans kort. Se dog muligvis modsat *Bo von Eyben* (1990), s. 137 ff.

I overensstemmelse hermed har den norske højesteret i *Rt. 1966.351* frifundet fremstilleren af et søkort (som i sin tid havde forsømt at foretage opmåling af nogle grundforhold) for erstatningsansvar ved et forlis, der kunne henføres til denne fejlangivelse. I *U 1987.985 Ø* havde en kommune givet fejlagtige oplysninger om placeringen af en gasledning. Oplysningerne medførte skade i forbindelse med et anlægsarbejde. Kommunen antoges ikke at have nogen erstatningsretligt sanktioneret pligt til at kontrollere de pågældende oplysninger. *U 1986.676 V* frifandt et vandværk for erstatningspligt for ekstra anlægsudgifter, en kommune havde måttet afholde i forbindelse med en licitation, som følge af, at vandværket havde givet fejlagtige oplysninger om vandledningens placering til brug for en kloakentreprise. Dommen lægger bl.a. vægt på, at de pågældende oplysninger var almindeligt tilgængelige. Se tilsvarende *U 1999.469 V*, hvor en kommune blev frifundet for ansvar for fejlagtige oplysninger om en kloaktilslutning meddelt i et ejendomsoplysningsskema. Frifindelsen begrundes med, at kommunen ikke havde nogen pligt til at undersøge eller kræve dokumentation for rigtigheden af de pågældende oplysninger.

Dette antyder, at også det IT-baserede "informationsansvar" må bedømmes mildere. En sådan retstilstand støttes også af reale grunde. I det klassiske produktansvar har producenten typisk lettere ved at bære skaden, end den tilskadekomne forbruger. På IT-området vil talrige software-leverandører være små virksom-

heder, der ikke vil kunne bære de omfattende erstatningskrav, der kan følge af at skulle indfri de forpligtelser, der følger af et erstatningsansvar, som rejses af en bred brugerkreds, og som derfor vil være uforholdsmæssigt store sammenlignet med produktets pris. Ved den almindelige bedømmelse må det også få betydning, at det ikke er sædvanligt at tegne forsikring mod produktskader på IT-området. Endelig vil det få betydning, at værdien af den indtrådte skade ofte står i misforhold til værdien af den informationsydelse, der i sin tid leveredes, sml. herved dommen i *U 1949.1139 Ø*, der frifandt et kreditoplysningsbureau for erstatningsansvar for fejlagtige oplysninger om en kundes solvens under omstændigheder, hvor de pågældende oplysninger kunne hentes i ubegrænset antal for et årsabonnement på 50 kr.

Modifikationer

Uanset om IT-systemer, og herunder standardprogrammel, antages at være "produkter" i lovens forstand, rummer PAL en række bestemmelser, der i alle tilfælde tager brodden af et sådant ansvar. For det første giver begrebet "defekt" anledning til vide fortolkningsmuligheder. § 5, stk. 1, nr. 2, der forudsætter en vurdering af "den anvendelse af produktet, som med rimelighed kan forventes", giver på IT-området anledning til netop de overvejelser, der er gjort i det foregående. Forudsætter systemet en selvstændig kontrol fra brugerens side, kan han ikke med "rimelighed" anvende dets uddata uden videre som grundlag for at beslutte sig til en potentielt skadegørende handling. For det andet forudsætter loven ifølge § 9 en vurdering af, om brugeren udviser egen skyld. Efter denne bestemmelse kan erstatningen nedsættes eller bortfalde, hvis skadelidte har medvirket til skaden ved forsæt eller uagtsomhed. I valghandlingsskemaet må disse undtagelser læses som udtryk for, at den, der er tættest på skaden, er nærmest til at modvirke dens indtræden.

18.3.c. Praktiske tilfældegrupper

De foregående bemærkninger om ansvaret for produktfejl kan sammenfattes som følger: Ved vurderingen af, om leverandøren af et informationsprodukt har handlet *culpøst*, må der tages hensyn til den samfundsmæssige interesse i at kunne sprede information uden for restriktive retlige bånd. Er der tale om et *fysisk produkt*, eller om et *informationsprodukt*, der i sin fremtræden helt må *sidestilles* hermed (fordi dets kommunikative funktioner ikke udspiller sig i samspil med brugeren) gælder PAL uden videre, og interessen samler sig da om, de modifikationer til det strenge produktansvar, som PAL hjemler, jf. nærmere afsnit 18.3.d.

Dette anskueliggøres ved følgende eksempler:

Fysiske produkter

I relation til klassiske produkter (som f.eks. kameraer, køleskabe, biler, videomaskiner etc.) giver den almindelige produktdefinition ikke anledning til tvivl: Hvis en bil ikke kan bremse og forårsager et sammenstød, en fryser går i stå og ødelægger fødevarer eller et kamera overeksponerer en film – alt som følge af programfejl i indbyggede halvlederchips el. lign. – foreligger der en defekt ved det pågældende produkt, som – medmindre der er grundlag for at bringe en særlig undtagelse i anvendelse – giver grundlag for et objektivt produktansvar for producent og mellemhandler. I de nævnte tilfælde kan forbrugeren "med rimelighed forvente", at produktet fungerer også i denne situation.

Standardsoftware

For så vidt angår standardsoftware, der omsættes i et stort volumen til almenheden (regneark, tekstbehandling, kartotekssystemer etc.), må man i almindelighed stille store krav for at antage et ansvar. Defekter, der består i, at programpakken sletter brugerens data pga. virus, eller fordi filødelæggende funktioner ikke er dokumenteret i den tilhørende manual eller i manualen til styresystemet, vil som udgangspunkt udløse et produktansvar. Dette udgangspunkt modificeres dog for så vidt angår skader, der indtræder straks efter systemets *implementering*. Der vil ofte foreligge egen skyld, hvis skadelidte ikke har foretaget sædvanlig back up-kopiering for så vidt angår de skader, der ville være afværget gennem en sådan foranstaltning. Egen skyld vil navnlig kunne foreligge, hvis skadelidte ikke har sikret sig en frisk back up af de data, der berøres af programmet, inden det installeres.

Et moment, der vil reducere risikoen for erstatningsansvar ved fejl i edb-programmel, vil være programfunktionernes *gennemsigtighed*. Hvis programproduktet præsenteres på en måde, der giver forbrugeren en klar bevidsthed om, hvor skadesrisiciene ligger, flyttes ansvaret for, at brugeren overså et faremoment, i vidt omfang over på ham selv. Gennemsigtighed kan f.eks. tilvejebringes gennem oplysende skærmtekster eller fejlfindingsprocedurer. Giver man derimod slutbrugeren grund til at nedsætte sin egen påpasselighed overfor fejl, flytter ansvaret tilbage til producenten.

Systemprogrammel

Systemprogrammel må som udgangspunkt behandles som andet standardprogrammel: Afgørende for ansvarsvurderingen er de funktioner, programmet udfører. Selv om et styresystem kun udfører baggrundsfunktioner for den applikation, brugeren anvender, kan disse funktioner have en umiddelbar og mærkbar effekt på de data, der behandles, f.eks. i form af sletning og ændring af data eller muliggjort indtrængen i systemet. Ansvars-

vurderingen af styresystemer til større flerbrugerinstallationer påvirkes dog af, at der for sådanne systemer typisk er udpeget en systemansvarlig, hvis opgave det bl.a. er at sikre mod fejl og uhensigtsmæssigheder. Dertil kommer, at informationshensynet spiller ind med en særlig vægt: Der er tale om programmer, der sælges i stort antal til en pris, der ikke indeholder nogen "pulveriseringspræmie" – i hvert fald ikke i relation til skader, som brugeren selv kunne afdække gennem sikkerhedskopiering. I ansvarsskemaets tankegang kan denne tanke også udtrykkes således, at der typisk er "langt" fra årsag til virkning, når der er tale om sådanne skader.

Værktøjer

Programværktøjer til programudvikling falder i en særlig kategori, selv om de fremtræder som standardprogrammel. Den, der leverer programværktøj, vil sjældent have mulighed for at vurdere, hvilke risici det færdige program kan tænkes at have. Udsættes slutbrugeren senere for tab, der kan føres tilbage til fejl eller uhensigtsmæssigheder i værktøjet, vil man almindeligvis ikke kunne sige, at leverandøren af værktøjet har været placeret i en position, hvor han har haft reel indflydelse på den opståede fejl mv. Hertil måtte i givet fald kræves uagtsomhed af en grovhed, der nærmer sig forsæt.

Teleydelser

Erstatningsansvaret for skade forvoldt ved nedbrud eller fejl på medier til telekommunikation (telefonlinjer, digitale teleforbindelser, telex o.lign.) er typisk reguleret i de abonnementsvilkår mv., der hjemler adgang til linjerne. Det er kendetegnende, at udbydere af sådanne medier (televirksomhederne, tredjepartsleverandører mv.) almindeligvis fraskriver sig ansvaret for skader forvoldt ved fejl i disse medier. Sådanne ansvarsfraskrivelser er som hovedregel gyldige.

I tilknytning til aftl. § 32 har det været overvejet, om afsenderen af en forvansket meddelelse er ansvarlig på objektivt grundlag for fejl begået af den, der transmitterer meddelelsen (f.eks. leverandøren af en teletjeneste), altså at der skulle indtræde en slags principalansvar. I motiverne til § 32 (RT 1916-17, till. A, sp. 2789) fremhæves det, at telegrafvæsenets manglende erstatningsansvar på dette område (efter de gældende regler herom) kunne tale for en sådan erstatningspligt, således at den godtroende modtager dog har en vis mulighed for oprejsning (nemlig hos afsenderen). Spørgsmålet er tvivlsomt. Efter min opfattelse er der næppe grundlag for at opstille et sådant hæftelsesansvar. Samme synspunkter som de, der begrunder en anvendelse af viljesprincippet i aftl. § 32, stk. 2, i tilfælde af transmissionsfejl mv. (i hvilke tilfælde et erstatningskrav i givet fald kan opgøres til den positive opfyldelsesinteresse) taler for heller ikke at knytte ansvar uden for kontraktsforhold for sådanne fejl (selv om erstatningen her alene kan udgøre den negative kontakts-

interesse). Se ligeledes *Ussing* (1951), s. 346 f. Sagen stiller sig derimod anderledes, hvis afsenderen har udvist culpa i forbindelse med den fejlagtige transmission. I så fald kan der gøres erstatningskrav gældende efter de almindelige regler om erstatning uden for kontraktsforhold.

18.3.d. Andre spørgsmål

Skadebegrebet

Som bestemmelsen i PAL § 6 er formuleret, er det et krav, at der er "forårsaget" en skade. Loven bygger herved på en sondring mellem de direkte økonomiske skader (f.eks. ødelæggelse af ting eller personskade) og rent økonomiske skader. Sidstnævnte, f.eks. udgifterne til afhjælpning mv., falder altså ikke inden for lovens definition. Viser det sig f.eks. gennem forebyggende vedligeholdelse eller ved aftestning mv., at et produkt lider af fejl, som vil kunne resultere i person- eller forbrugertingsskader, vil brugerens omkostninger ved at bringe produktet i sikker stand ikke kunne gøres gældende på objektivt grundlag mod producenten. I stedet må der enten rejses krav efter de køberetlige regler (hvilket forudsætter, at fristen for fremsættelse af sådanne indsigelser ikke er overskredet) eller – hvis betingelserne herfor er opfyldte – efter den almindelige culparegel. Det bemærkes, at det objektive produktansvar dog kun gælder for tingsskader, der overstiger 4.000 kr., jf. lovens § 8, stk. 1.

Producent og mellemhandler

Ifølge PAL § 10 hæfter en mellemhandler for produktansvar "umiddelbart over for skadelidte og senere mellemhandlere i omsætningskæden". Ifølge forarbejderne til bestemmelsen gælder denne hæftelse såvel i henseende til det produktansvar, der kan gøres gældende i henhold til lovens regler, som for det retspraksisbaserede produktansvar. En dansk producent af et elektronikprodukt, der pga. fejl i indbyggede halvlederchips påfører slutbrugere skade, bærer derfor ansvaret herfor, selvom produktet har passeret gennem flere forhandlerled, inden skaden sker. I sådanne tilfælde, hvor produktet passerer gennem flere led, kan skadelidte gøre sit krav gældende mod flere, jf. lovens § 11 om dette solidariske ansvar. Som anført s. 399 verserer der for tiden en sag ved EF-domstolen, der skal afgøre om det danske mellemhandleransvar er lovligt.

Forældelse

Ifølge PAL § 14 forældes erstatningskrav for produktskade – uanset om krav herom gøres gældende mod producenten eller mellemhandleren, og uanset om kravet har hjemmel i loven eller i det dommerskabte ansvar – efter to regelsæt.

Den første forældelse indtræder, når der er gået *3 år* efter den dag, da skadelidte har fået – eller burde have fået – kendskab til

skaden, defekten og vedkommende producents navn og opholdssted. Reglerne om suspension af denne forældelse følger dansk rets almindelige regler om forældelse af fordringer uden særligt retsgrundlag i den såkaldte 1908-lov.

Den anden forældelse indtræder for det *lovbaserede produktansvar 10 år* efter den dag, da producenten bragte det skadevoldende produkt i omsætning. Når det gælder dette *dommerskabte produktansvar*, gælder dansk rets 20-årige forældelsesfrist, der i relation til produktansvar også må formodes at være det tidspunkt, hvor producenten bragte det skadevoldende produkt i omsætning, sml. herved *U 1992.575 H*.

18.3.e. Særlige ansvarsregler

Visse betalingsmidler

Ifølge § 12 i lov om visse betalingsmidler er udstederen af et betalingsmiddel objektivt ansvarlig for tab hos brugeren, som skyldes fejlregistrering eller konteringsfejl. Har brugeren fået meddelelse om, at betalingstransaktionen er anerkendt, er udsteder dernæst ansvarlig for tab hos brugeren, som skyldes, at transaktionen alligevel ikke gennemføres, eller gennemføres mangelfuldt. Dette sidste gælder dog ikke, hvis der foreligger *force majeure*-lignende forhold på udstederens side. Udstederen har i så fald bevisbyrden herfor. Erstatningen kan nedsættes eller bortfalde, hvis brugeren forsætligt eller groft uagtsomt har medvirket til fejlen.

Værdipapirhandel

I henhold til værdipapirhandelslovens § 80 er en værdipapircentral erstatningspligtig for tab som følge af fejl i forbindelse med registrering, ændring eller udslettelse af rettigheder på konti i den pågældende værdipapircentral eller udbetalinger herfra, selv om fejlen er hændelig. Kan fejlen henføres til et kontoførende institut, påhviler erstatningspligten dette. Instituttet bærer således efter lovens § 81 et tilsvarende objektivt ansvar for tab som følge af egne fejl i forbindelse med indrapportering til registrering, ændring eller udslettelse af rettigheder på konti i en værdipapircentral eller udbetalinger herfra. Har skadelidte forsætligt eller uagtsomt medvirket til fejlen, kan erstatningen nedsættes eller bortfalde, se §§ 80, stk. 3 og 81, stk. 3. Den samlede erstatning kan ikke overstige 500 mio. kr. I relation til kontoførende institutter indfører lovens § 81, stk. 4, en solidarisk hæftelse for de øvrige danske kontoførende institutter, der – som stk. 5 pålægger dem – har indgået tilslutningsaftale med den pågældende værdipapircentral.

Databeskyttelse

Ifølge LBP § 69 skal den dataansvarlige erstatte skade, der er forvoldt ved behandling i strid med lovens bestemmelser, medmindre det godtgøres, at skaden ikke kunne have været afværget ved den agtpågivenhed og omhu, der må kræves i forbindelse med behandling af personoplysninger. Bestemmelsen, der har rod i art. 23 i det bagvedliggende EU-direktiv, skal ses i sammenhæng med lovens – og direktivets – krav om behandlingssikkerhed, jf. LBP § 40.

Til illustration af de krav, en overtrædelse af den slags regler kan tænkes at resultere i, kan nævnes dommen i *U 1973.190 V.* Her fik en sygeplejerske en skønsmæssigt anslået erstatning for det tab, hun led ved ikke senere at kunne opnå fast ansættelse. Årsagen var udtalelser fra en tidligere arbejdsgiver om manglende evne til at samarbejde mv. Dommen henviste bl.a. til den fremgangsmåde, man havde brugt, da man indsamlede disse oplysninger. Se ligeledes dommen i *NJA 1985.143*, der gav erstatning for ideel skade efter en fejlagtig inkassering af et tilgodehavende. Erstatningskravet, der var baseret på en særlig erstatningsregel i den svenske inkassolag, blev opgjort til 30.000 kr., heraf 5.000 kr. i arbejdsomkostninger.

Signaturcertifikater

Ifølge LES § 11 er nøglecentre, der udsteder kvalificerede certifikater til offentligheden, eller som over for offentligheden indestår for sådanne certifikater udstedt af et andet nøglecenter, ansvarlig for visse tab hos den, der med rimelighed forlader sig på certifikatet. Det erstatningsansvar, reglen tager sigte på, er gjort til genstand for en indgående analyse hos *Henrik Udsen*: Den digitale signatur – ansvarsspørgsmål (2002), s. 150 ff., hvortil i det hele henvises. Der er tale om et ansvar med omvendt bevisbyrde, idet nøglecentret kan vise ansvaret fra sig, hvis det kan godtgøre, at det ikke har handlet uagtsomt eller forsætligt. Ansvaret er gjort præceptivt, jf. stk. 4. For at understøtte ansvaret foreskriver lovens § 5, stk. 1, nr. 5, at de af loven omfattede nøglecentre (som udsteder kvalificerede certifikater), til stadighed skal have tilstrækkelige økonomiske ressourcer til bl.a. at kunne opfylde erstatningsmæssige forpligtelser i henhold til loven.

Erstatningsansvaret knytter sig til tre aspekter af certifikatanvendelsen: identitetskontrollen, oplysningerne i certifikatet og håndteringen af spærreanmodninger.

- ID-kontrol

Det ansvar, der er knyttet til første led, viser hen til LES § 7, der stiller krav om, at nøglecentret kontrollerer, at nøgleindehaveren *var i besiddelse* af den hemmelige nøgle, der korresponderer med den offentlige nøgle, der ligger til grund for certifikatet. Se hertil § 11, stk. 1, nr. 5, og henvisningen herfra til § 7.

- korrekthed

Til anden gruppe hører tilfælde, hvor *oplysningerne* i certifikatet ikke var korrekte på tidspunktet for udstedelsen af certifika-

tet, eller certifikatet ikke indeholder alle oplysninger som krævet i henhold til lovens § 4, se § 11, stk. 2, nr. 1-2.

- undladt spærring

Til tredje gruppe hører dels manglende *spærring* af certifikatet, jf. § 9, stk. 2, dels manglende eller fejlagtig *information* om, at certifikatet er spærret, hvilken udløbsdato certifikatet har, eller om certifikatet indeholder formåls- eller beløbsbegrænsninger, jf. § 9, stk. 1 og 3.

Ansvaret efter bestemmelsen er genstand for visse yderligere begrænsninger, jf. § 11, stk. 3: Er tabet opstået som følge af, at det kvalificerede certifikat er anvendt uden for de formålsbegrænsninger, som gælder for certifikatet, eller som følge af en overskridelse af de beløbsbegrænsninger, som gælder for certifikatet (såfremt disse tydeligt skal angives), er der ikke ansvar.

18.4. Implementeringsansvaret

18.4.a. Problemstillingen

Implementeringsansvaret angår i videste forstand sammensætningen af det færdige IT-system. Hvor den, der designer en funktion, står relativt frit, vil der være mere begrænsede muligheder for den, der implementerer systemet. De *tekniske rammer* for ansvaret er til enhver tid begrænset af den stillede opgave, og ansvaret er derfor mere veldefineret, al den stund de enkelte komponenters funktioner og grænseflader må respekteres. Dernæst sker implementeringen almindeligvis for at opfylde en kontraktspligt (f.eks. en aftale om installering af et IT-system eller om ydelse af konsulentassistance) eller et tjenesteforhold (f.eks. en arbejdsbeskrivelse mv.). Også kontraktsforholdet sætter grænser for, hvordan implementeringen kan finde sted.

I det følgende koncentreres opmærksomheden om den eksterne konsulentydelse. Den implementering, der sker som led i en almindelig IT-overdragelse, behandles i afsnit 21.7. i forbindelse med reglerne om overdragelse af IT.

18.4.b. Ansvaret i kontraktsforhold

En praktisk vigtig kategori af erstatningsretlige problemer angår det ansvar, der opstår i et kontraktsforhold, når IT-leverandøren misligholder sin pligt til at præstere korrekt og rettidig ydelse. At leverandøren misligholder sine aftaleforpligtelser er ikke ensbetydende med, at der indtræder erstatningspligt. Her som andet-

steds i obligationsretten skal der foreligge et *ansvarsgrundlag*, jf. nærmere herom *Bryde Andersen & Lookofsky* (2005), s. 236 ff. Men i det omfang tabet udspringer af, at leverandøren (realdebitor) ikke har opfyldt en pligt, han har påtaget sig ved aftale, skal der normalt noget særligt til, for at leverandøren kan gøre gældende, at der ikke foreligger culpa. De særlige problemer herom, der gør sig gældende på IT-området, behandles nærmere i kapitel 22.

18.4.c. Konsulentansvaret

Problemstillingen

Der er enighed om, at den almindelige culparegel – eventuelt suppleret med kontraktssynspunkter – må gælde som erstatningsgrundlag for tab forvoldt ved tekniske bistandsydelser. Se herved *Samuelsson & Søgaard*: Rådgiveransvaret (1993), *Vinding Kruse* (1989), s. 105 ff., *von Eyben & Isager* (2003), s. 80 ff., *Lars Bo Langsted*: Rådgivning I (2004), *Stig Jørgensen & Torben Wanscher* i J67.425 og *E&A* s. 395 ff. Det forhold, at rådgiveren yder sin bistand mod betaling, vil normalt bevirke, at han skal bedømmes efter en målestok, der svarer til den profession eller "stand", som rådgiveren optræder som en del af. De krav, professionen vil stille til sine udøvere (og som under en retssag dokumenteres ved sagkyndige erklæringer mv.), vil herefter danne grundlag for den erstatningsretlige vurdering af fejl ved sådanne ydelser.

Sædvanedannelsen

Dette udgangspunkt volder imidlertid problemer i sin praktiske anvendelse. Hvor anden rådgivning fremtræder som ydelser på ensartede markeder mv., findes der nemlig ingen klart defineret IT-profession. Ligeså mange IT-uddannelser, IT-anvendelsesformer og IT-anvendelser, der findes, ligeså mange mulige former for IT-ekspertise kan man tænke sig udbudt af en konsulent – og det ganske ofte i uforudsigelige kombinationer. Sager om konsulentansvar er derfor vanskelige at oplyse i henseende til indholdet af "god skik" mv. Man kan ikke uden videre falde tilbage på almene retlige overvejelser.

Systemvalg

Uanset karakteren af hans rådgivning ligger det klart, at IT-konsulenten er en professionel rådgiver, der som sådan er underlagt et professionelt rådgiveransvar. Man kan overveje, om den praksis, der gælder inden for det tekniske rådgiveransvar, se således *Jørgen Hansen* (1984), s. 225 ff. og 231 ff., kan finde anvendelse på konsulenten. På dette område har man nemlig ofte – modsat andre rådgivningsområder – kun tilladt en snæver margin for fejlskøn. Dette har navnlig vist sig ved ansvar for materialevalg mv., som byggerådgiveren ifalder et strengt culpaansvar for.

Overføres denne praksis til IT-området skulle resultatet i givet fald være, at en konsulent er erstatningsansvarlig for i sin rådgivning om, hvilket system brugeren skal anskaffe, at overse en bedre og billigere systemløsning end det anbefalede.

At drage en sådan parallel er dog ikke uproblematisk. Det hører formentlig til sjældenhederne, at en IT-konsulent opkaster sig som ekspert i alle markedets systemer til løsning af en bestemt type af funktionalitet. Typisk bevæger konsulentens ekspertise sig inden for en konkret produktgruppe, idet det fra starten ligger fast, at rådgivningen alene knytter sig til systemer af det pågældende mærke. At dette er praksis skyldes ikke mindst, at det ofte er et spørgsmål om smag og behag, hvilket system man vælger. IT-konsulentens systemvalg står ikke – som bygningsteknikerens materialevalg – mellem risikoen for langtidsvirkningerne ved nye, uprøvede, men billige teknikker overfor de eksisterende, dyrere og velkendte. Fordele og ulemper ved valget af IT-system er enten af funktionel og håndgribelig karakter eller af en så langsigtet karakter, at de ofte slet ikke har at gøre med kvaliteten af den eksisterende teknologi. Blandt disse langsigtede overvejelser kan nævnes vurderingen af, om det ene styresystem på sigt vil understøtte et større programudbud end det andet.

Når man overvejer at overføre byggeriets måske mere strikte ansvarsformer til IT-området spiller også andre forhold ind. For det første er der ikke samme veletablerede tradition for ansvarsforsikringer på det brede område af små konsulentfirmaer. For det andet vil konsulentens rådgivning sjældent – på samme måde som teknikerens – udmønte sig i tingsskader af iøjnefaldende karakter. Hovedparten af de tab, der vil indtræde som resultatet af forfejlede IT-leverancer, vil være afledede og indirekte tab, som en skadelidt udenfor kontraktsforhold efter almindelige regler anses som nærmest til at bære risikoen for.

Margin for fejlskøn

Disse forhold fører til, at man almindeligvis må give IT-konsulenterne en vis, ikke ubetydelig, margin for fejlskøn i anskaffelsesrådgivningen.

En lignende stilling synes antydet ved en ledende dom fra amerikansk IT-kontraktsret: *Chatlos Systems, Inc. v. National Cash Register*, 479 F.Supp. 738 (1979). Retten fastslog (s. 741, note 1) at "[t]he novel concept of a new tort called "computer malpractice" is premised upon a theory of elevated responsibility on the part of those who render computer sales and service. Plaintiff equates the sale and servicing of computer systems with established theories of professional malpractice. Simply because an activity is technically complex and important to the business community does not mean that greater potential liability must attach. In the absence of sound pre-

cedential authority, the Court declines the invitation to create a new tort." Se også *Triangle Underwriters v. Honeywell*, 604 F.2d 737 (1979). Nyere praksis synes dog at anlægge en mere skærpet ansvarsvurdering, se f.eks. *Diversified Graphics, Ltd. v. Groves*, 868 F.2d 293 (1989), hvor retten idømte konsulenten (et revisionsfirma) erstatningsansvar efter et professionsansvar baseret på konsulentens egne "Guidelines to Practice", der inkorporerede nogle vejledende retningslinjer for revisorer. I sagen *RKB Enterprises v. Ernst & Young*, ref. 582 N.Y.S. 2d 814 (1992), fandt retten ikke grundlag for at ikende *punitive damages* i mangel af bevis for, at der forelå en så grov uagtsomhed, der måtte være forudsætningen herfor. Sagen drejede sig om et aftaleforhold vedrørende konsulentassistance indgået med henblik på en systemanskaffelse. Se også *Hospital Computer Systems, Inc., v. Staten Island Hospital*, 788 F.Supp. 1351 (1992).

Rådgivning om enkeltsystemer

Omvendt må det antages, at konsulenten har pligt til at være informeret om de systemer, applikationer og forretningsgange mv., hans rådgivning angår. For så vidt angår disse systemer og applikationer, må han ikke alene kende produktudbuddet, men også de pågældende priser mv. Dernæst må han være orienteret om de fordele og ulemper, det valgte system har – målt i pris, ydelse og kvalitet – i forhold til de væsentligste konkurrenter. Da konsulenten imidlertid ikke forventes at kende disses produkter mv. i detaljer, kan denne rådgiving alene ydes i generelle former. Ligeledes bør konsulenten kende til – og orientere om – muligheden for at erhverve en funktionalitet som den efterspurgte som en shareware-løsning. Undlader konsulenten at informere sin klient fyldestgørende herom (f.eks. ved at erklære, at en given løsning ikke "findes" på markedet, og at den derfor må udvikles fra grunden), vil klienten efter omstændighederne kunne gøre et erstatningskrav gældende mod konsulenten svarende til sin meranskaffelsesomkostning. Konsulenten forudsættes dog ikke at være alvidende. Ej heller retspraksis om advokaters ansvar for fejlagtig rådgivning om retstilstanden kræver, at advokaten skal vide alt. Der må være en vis margin for skønsudøvelse i rådgivningen.

Alt efter opdragets karakter har konsulenten pligt til at sætte sig grundigt ind i klientens forretningsgange på en måde, så han ved, hvordan systemets funktioner vil opfylde virksomhedens behov på kort eller lang sigt. Anbefaler han et system til en kunde, må han gennemlæse dets manualer mv. for at afsløre eventuelle inkompatible grænseflader, uhensigtsmæssigheder mv. Derimod vil konsulenten almindeligvis ikke bære noget ansvar for systemfejl mv., der efter deres karakter først vil afsløre sig under almindelig brug.

Projektstyring

I det omfang konsulenten påtager sig opgaven med at kvalitetssikre en aftalt leverance, f.eks. i forbindelse med projektopfølgning og afleveringsprøver, vil man vel kunne fremholde et klart grundlag for ansvarsvurderingen: Burde der være meddelt godkendelse eller ikke? Her er problemet imidlertid, at skadelidte jo er kunden, som typisk spiller en ligeså central rolle for godkendelsen som konsulenten i det omfang han og hans folk deltager i projektarbejde og aflevering. Egen skyld-momenter får derfor ofte betydning.

Revisionskontrol

Som omtalt ovenfor i afsnit 5.2.d. har de statsautoriserede revisorer påtaget sig en del af den opgave, der ligger i at kontrollere brugerens IT-implementering. I 1989 og 1990 har FSR udsendt to revisionsvejledninger henholdsvis om revision i virksomheder, som anvender edb (revisionsvejledning nr. 14), og om revision af IT-baserede brugersystemer (revisionsvejledning nr. 17). Dermed er det blevet til en del af "god revisionsskik" at foretage en indledende vurdering af virksomhedens IT-anvendelse, bl.a. ved gennemgang af generelle kontroller (revisionsvejledning nr. 14) samt af klientens brugersystemer (revisionsvejledning nr. 17). Sidstnævnte kontrol omfatter bl.a. en gennemgang af systemets funktioner, behandling af inddata og uddata, anvendte registre, programmerede og manuelle kontroller samt en gennemgang af de transaktions- og kontrolspor, der skal være tilgængelige efter bogføringsbekendtgørelsen af 1990.

En revisor, der tilsidesætter disse krav til god revisionsskik, vil efter omstændighederne kunne blive pålagt erstatningspligt for tab, som ville være undgået med en sådan kontrol. Tab kan f.eks. tænkes at opstå ved fejl i EDI-overførsler af faktureringsdata eller ved utilsigtede afgiftsunddragelser, sml. dommen i *U 1985.831 Ø*. Ansvaret bliver dog kun aktuelt, hvis der foreligger fejl ved kontrollen. Det bygger dermed på det kendskab til systemet, revisor kunne opnå gennem sin gennemgang. Revisor har ikke noget videregående ansvar for de fejl, en IT-brugende virksomhed begår.

18.4.d. Brugerens egen implementering

Intet IT-system kan implementeres uden brugerens deltagelse. Forsømmer brugeren f.eks. at skaffe sig den nødvendige viden om systemet og dets funktioner, vil det ofte få erstatningsretlige konsekvenser. I domstolenes praksis er indsigelser om, at fejl ved IT-systemet skyldtes brugeren, hyppigt forekommende. Herudover kan tankegangen få betydning for vurderingen af, om der er

udvist egen skyld, med den virkning, at skadelidte skal bære et erstatningsretligt medansvar for en opstået skade, jf. herom oven for afsnit 18.2.b. om egenskyld-ansvaret for brugerens egen sikkerhedsstrategi.

Egen aftestning

Med grundlag i den almindelige erfaring, at IT-systemer aldrig fungerer korrekt ved første anvendelse, kan man formentlig opstille en erstatningssanktioneret pligt for brugeren til at teste et nyt system, inden det sættes til at behandle reelle data. En bruger bør med andre ord ikke stole på data fra et nyinstalleret system. En sådan procedure er forudsat ved de fleste IT-kontrakter, hvor systemerne forudsættes "afleveret" i forbindelse med en afleveringsprøve, hvor de udsættes for en gennemgribende aftestning. Se nærmere herom afsnit 21.5.e.

Afleverings-prøven

Den aftestning, der sker i forbindelse med systemets aflevering, udtømmer dog ikke brugerens erstatningsretlige pligter omkring implementeringen. I den første fase efter implementeringen af et system må brugeren foretage løbende kontroller med, at systemets uddata er som forventet. Som grundlag for denne kontrol må brugeren benytte sit kendskab til de pågældende IT-funktioner fra et tidligere system, f.eks. det eksisterende manuelle eller IT-baserede system før installeringen af et nyt program mv. Dette erstatningsansvar for brugerens egen implementering finder tilsvarende anvendelse, når brugeren under sin anvendelse af et system ændrer i de forudsætninger, der lå til grund for systemets installering. Ændringer i systemets driftsforudsætninger kan f.eks. bestå i, at systemet sættes til at behandle større datamængder eller ved at tekniske procedurer eller komponenter ændres, således at der i realiteten fremtræder et nyt system.

Sikkerheds-kopiering

Som flere gange nævnt i det foregående kan brugerens manglende sikkerhedskopiering efter omstændighederne indebære, at et erstatningskrav, brugeren ellers kunne have gjort gældende, må reduceres til det, mindre, tab, der ville være indtrådt, såfremt sædvanlig sikkerhedskopiering var sket. Om man vil betragte dette således, at tabet i disse tilfælde udmåles til et *normaltab*, om det "fulde tab" i disse tilfælde er *inadækvat* eller om der foreligger *egen skyld* fra skadelidtes side i relation til det pågældende fulde tab, synes ikke at spille nogen afgørende rolle. Afgørelsen må i alle tilfælde træffes ud fra en skønspræget vurdering, hvor tabets størrelse sammenholdes med skadelidtes og skadevolderens forhold.

18.5. Ansvar for systemdialogen

Da IT-systemer er kommunikationssystemer, ligger en del af de risici, der er forbundet med IT, i anvendelsen af digitale data som grundlag for (potentielt skadevoldende) beslutninger. Dette beslutningsgrundlag tilvejebringes hovedsagelig gennem en system-dialog, hvis indhold beror på systemets karakter. Jo flere valg, dialogen overlader til brugeren, desto større bliver brugerens ansvar for at sikre sig, at han bruger systemet korrekt. Brugerens frihedsgrader under en IT-dialog vil være en funktion af hans faktiske muligheder for at give og modtage instruktioner og hans subjektive kendskab til disse muligheder.

Tidsmomentet spiller en stor rolle for dialogansvaret. Må dialogen afvikles indenfor tidsrammer, der ikke giver mulighed for menneskelige beslutningsvalg, begrænser dette de senere kontrolmuligheder, sml. *U 1948.181 H,* der som grundlag for at frifinde en fodboldspiller for erstatningskrav for skade forvoldt på en medspiller henviste til de hastigt skiftende situationer og spillets fart, der kun levner kort tid for en spiller til at træffe beslutninger og til at overveje et angrebs farlighed for en modspiller.

Funktioner, som systemet gennemløber uden brugerens overvågning, kan alene give anledning til ansvar for brugeren, for så vidt brugeren havde mulighed for at forudsige de pågældende forløb, inden de blev initieret. Kunne han ikke det, måtte ansvarsvurderingen rette sig mod dem, der har udviklet, aftestet eller implementeret systemet med disse begrænsninger, jf. herom ovenfor.

Et særligt spørgsmål opstår, når brugeren fra sin tidligere anvendelse af systemet har kendskab til en særegen – og potentielt skadevoldende – funktion, jf. ovenfor. Undlader han i en sådan situation at tage forholdsregler mod skader, der kan forudses ved fremtidige identiske kørsler, vil dette indebære et culpøst forhold, der i givet fald falder tilbage på den arbejdsgiver, der har ansvaret for driften af det pågældende system. En sådan forholdsregel kan f.eks. bestå af uformelle advarsler til kolleger eller systemansvarlige om de pågældende risici.

18.6. Ansvaret for dataanvendelsen

Visse IT-relaterede ansvarssituationer opstår uafhængigt af selve IT-anvendelsen. Lægen modtager medicinsk information fra en kollega, der har konsulteret et ekspertsystem; bank-kunden an-

vender edb-udskrevne kontoudtog som grundlag for sine dispositioner mv. Ansvaret for dataanvendelsen har i sådanne tilfælde primært at gøre med kravene til den kontrol, retssystemet bør forlange ved dispositioner på grundlag af data fra et IT-system. Som omtalt i afsnit 18.2.d. må disse krav i dag udledes ud af en bonus pater-vurdering, der tager udgangspunkt i de livsformer, der udformer sig på det område, hvor skaden indtræder. Man må derfor se på, hvor sædvanligt det er inden for et livsområde, at man blindt stoler på de data, der udgår fra et IT-system. I det omfang der forventes en selvstændig kontrol fra brugerens side flyttes ansvarsvurderingen hen imod denne – der jo også (i overensstemmelse med den skematiske illustration i afsnit 18.1.c.) er nærmest på skaden.

Dette kan også udtrykkes således, at information knyttet til elektroniske medier ikke ansvarsvurderes anderledes end information på skriftlige medier. Synspunktet blev klart udtalt i *Daniel v. Dow Jones & Co.*, 520 NYS 2d 334 (1989), der i sin begrundelse for at frifinde en databasevært for erstatningsansvar som følge af misinformation i en database fremhæver, at "there is no reason to treat an individual who obtains information from a computer screen differently from one who obtains the same information from a printed page". Efter samme synspunkter synes det forhold, at et beslutningsgrundlag foreligger i form af en edb-udskrift, heller ikke at have påvirket domspraksis om, hvorvidt en person, mod hvem et krav om tilbagesøgning af en urigtigt erlagt ydelse gøres gældende, har udvist egen skyld. Se f.eks. dommene i *U 1988.157 H* og *U 1984.896 Ø* samt omtalen heraf i *E&A*, s. 412 f.

I en norsk dom om et tilsvarende tilbagesøgningskrav (Rettens Gang, 1982, s. 604, Halmar byret) gjorde den IT-brugende udbetaler bl.a. gældende, at en udbetalingsfejl skyldtes den pågældendes IT-system. Sagsøgeren henviste herved til, at "det er vanskelig å gardere seg mot at slike feil av og til vil oppstå". Synspunktet blev ikke behandlet i dommen, der nægtede tilbagesøgningsret. Billedet er formentlig det samme på det strafferetlige område, sml. herved dommen i *U 1985.831 Ø,* der angik strafansvaret for en virksomhed, hvis revisor havde foretaget en fejlindberetning af merværdiafgift pga. en IT-fejl.

Supplerende litteratur

Som det fremgår af teksten, behandles en række af IT-erstatningsrettens problemer i min disputats Edb og ansvar – studier i edb-erstatningsrettens beskrivelsesproblematik (1988) (*E&A*), hvortil i det hele henvises. Hvor man i den udenlandske litteratur leder forgæves efter egentlige monografier over edb-erstatningsrettens problemer, florerer tidsskriftsartiklerne. Fra det nordiske område fremhæves *Jan Hellners* lille bog Skadeståndsansvar vid dataverksamhet, ADBJ-rapport 1974-5 (1974). Problemerne om konsulentens ansvar drøftes af *Ulf Hanson* i NÅR 1984.92 og ansvaret for databasefejl i min artikel i NÅR 1989.134. Herudover fremhæves *Roy Freed*: Products liability in the computer age. 7 Jurimetrics Journal 270 (1977), *Gemignani*: Product liability and software, 8 Rutgers 172 (1981) og *Robertson*: Strict liability under the consumer protection act 1987 – some implications for producers of computer based products, 5 CLSR (January-February 1988) p. 16 (1988).

Produktansvarsloven er kommenteret af *Jens Rostock Jensen & Allan Kvist-Kristensen*: Produktansvarsloven med kommentarer (2004). Se ligeledes den grundige gennemgang hos *Børge Dahl, Vibeke Rønne, Jan Hornsberg og Marianne Levy* i J1990.145 ff.

Fra den almindelige *erstatningsretlige litteratur* fremhæves *A. Vinding Kruse*: Erstatningsretten, 5. udg. under medvirken af Jens Møller (1989), *Børge Dahl*: Produktansvar (1973), samme forfatters kommentar til produktansvarsloven i Karnovs Lovsamling og *Bo von Eyben & Helle Isager*: Lærebog i erstatningsret, 5. udg. (2003). For så vidt angår ansvaret for konstaterende erklæringer henvises til *Henning Skovgaard*: Offentlige myndigheders erstatningsansvar (1983), s. 162 ff.

Problematikken om ansvar for informationsspredning på Internet drøftedes ved Det 35. nordiske Juristmøde i Oslo, august 1999, se NJM 1999 I, s. 197 ff. Se tillige *Rosa Julià-Barcelo* i EIPR 1998.453 ff.

Kapitel 19. DIGITAL AFTALEINDGÅELSE

19.1. Beskrivelsesproblemer

19.1.a. Det digitale medium

Problemstillingen

Dette kapitel behandler de juridiske problemer, der opstår, når man anvender digitale medier som grundlag for aftalestiftelse. Centralt står spørgsmålet, hvornår der er stiftet en retlig forpligtelse ved en viljeserklæring, der er repræsenteret digitalt, hvilke eventuelle tekniske krav man vil stille til sådanne meddelelser, samt hvilke indsigelser mv. afgiveren og modtageren af sådanne meddelelser kan gøre gældende.

Hovedreglen

Der er som udgangspunkt intet til hinder for, at det digitale medium udfylder papirmediets funktion som grundlag for en aftaleindgåelse. Aftaleindgåelse og rettighedsstiftelse er ikke bundet af formregler i dansk ret, medmindre særlig hjemmel foreligger. Dette udgangspunkt er allerede fastslået i DL 5-1-1, hvorefter "Een hver er pligtig at efterkomme, hvis han med Mund, Haand og Segl, lovet og indgaaet haver". Princippet er endvidere fastslået i en righoldig retspraksis herhjemme om brugen af forskellige former for digitale bevismidler mv. ved domstole og administrative myndigheder, og den har i de senere år vundet almen international anerkendelse. Også CISG art. 11 lader aftaler være gyldige uanset deres form.

Papirets rolle

At papiret har vundet så udbredt anvendelse som medium for viljeserklæringer, og at talrige lovbestemmelser forudsætter "skiftlighed mv.", skyldes en række af dette mediums sikkerhedsmæssige kvaliteter, jf. afgrænsningen af dette begreb i afsnit 4.3.a. Som viljeserklæring betragtet henter det skrevne dokument sin styrke fra den forbindelse, der består mellem det skrevne og dets ophavsmand, og som giver en formodning for *autenticitet* (ægthed). Denne formodning er lettest at godtgøre ved håndskreven tekst, som ofte er let genkendelig, omend også den tidlige skrivemaskineteknologi (før den elektriske maskine kom til) gav ophavsmanden mulighed for at præge dokumenterne, f.eks. ved forskelle i anslagsstyrke, behandlingen af papiret o.lign. Hertil kommer den bevisværdi, der ligger i selve *underskriften*, og som

i kraft af særlige lovregler om underskriftskrav giver dokumentet en særlig status. Derudover kan papirdokumentet ubesværet gøres til genstand for faktiske *sikkerhedsforanstaltninger*: Ved at deponere dokumentet et sikkert sted kan man sikre sig bevis for dets autenticitet og integritet, således som det f.eks. er sket i tinglysnings- og arvelovgivningens regler om, at visse dokumenter tinglyses og testamenter vedkendes for notar. Sidst, men ikke mindst, må det erindres, at papiret er umiddelbart *læsbart* for alle, uanset hvilket teknisk udstyr mv. man råder over.

I kapitel 4 er redegjort for en række af de teknikker, der kan tages i brug til at understøtte digitale meddelelsers autenticitet, originalitet og fortrolighed mv. Det er fælles for disse foranstaltninger, at de forudsætter, at de kommunikerende parter råder over den *teknologi*, der gør det muligt at frembringe, afsende, modtage og læse digitale meddelelser, og at denne teknologi vel at mærke er *implementeret* på en sådan måde, at disse kommunikationsprocesser rent faktisk kan gennemføres. Netop dette hensyn til administrative papirrutiner vil ofte udgøre den væsentligste praktiske hindring for at kunne læse – og dermed anerkende – digitale meddelelser og digital signatur.

Navnlig i forbindelse med offentlige myndigheders sagsbehandling vil der opstå rutiner og procedurer, som må overholdes. Er en sådan rutine baseret på en bestemt papirgang – eventuelt ved brug af særlige skemaer, papirblanketter mv., kan man ikke uden videre digitalisere disse dele af sagsbehandlingen. Sådanne papirark kan tjene særlige informationsmæssige eller praktiske funktioner. Ganske vist kan disse funktioner ofte opnås ligeså effektivt og praktisk digitalt, men dette kræver blot, at de fornødne systemer udvikles, hvilket kan være forbundet med betydelige omkostninger. På områder, hvor sådanne forhold gør sig gældende, vil selve tilvejebringelsen af en digital *signatur* ofte repræsentere et forholdsvis begrænset problem i forhold til det problem, der ligger i at *digitalisere* sagsekspeditionen, jf. om denne problemkreds IT-sikkerhedsrådets vejledning om Digitale Dokumenters Bevisværdi (december 1998).

19.1.b. Almindelige principper

Funktionel ækvivalens

Ved UNCITRALS Model Law on Electronic Commerce fra 1996 er der etableret en række principper, som i dag synes at nyde almindelig tilslutning i den globale diskussion om digital aftaleindgåelse og om anvendelse af digitale medier til rettighedsstiftelse. Modelloven bygger på et princip om funktionel ækvivalens

(*functional equivalency*): Kan IT-systemer bringes til at udføre samme funktioner som papirmediet kan, bør det digitale medium som udgangspunkt kunne anvendes på lige fod med papirmediet. Den legislative opgave består derfor i at sikre, at disse tilsvarende funktioner understøttes med juridisk gyldighed. Dette princip gælder først og fremmest for den privatretlige aftale, men udstrækkes også til at gælde de dele af den elektroniske handel, der udspiller sig i forholdet mellem private virksomheder og offentlige myndigheder.

Ikke-diskrimination

Modellovens princip om funktionel ækvivalens følges op af et princip om ikke-diskrimination. Ifølge art. 5 fastslås den hovedregel, at information ikke skal nægtes retsvirkning, gyldighed eller mulighed for retshåndhævelse, alene fordi den foreligger i form af en digital meddelelse ("*data message*"). I relation til et retssystems krav om, at en juridisk handling skal foreligge *skriftligt* (art. 6) udmøntes denne betingelse i, at den information, der indeholdes i den ækvivalente digitale meddelelse, skal være "accessible so as to be usable for subsequent reference". *Signaturkrav* (modellovens art. 7) skal tilsvarende anses for opfyldt, hvis den digitale meddelelse er skabt ved hjælp af en metode til at identificere afgiveren og indicere dennes anerkendelse af informationsindholdet, såfremt denne metode er så troværdig, som det må anses for hensigtsmæssigt til det formål, som den digitale meddelelse var skabt eller kommunikeret til i lyset af samtlige omstændigheder, herunder relevante indgåede aftaler. Krav om et dokuments *originalitet* (modellovens art. 8) skal ifølge modelloven anses for opfyldte, hvis der foreligger en "reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise", og hvis der er stillet krav om fremlæggelse af original information, at "that information is capable of being displayed to the person to whom it is to be presented".

Direktivregulering

Et lignende princip om ikke-diskrimination følger af direktivet om elektronisk signatur (99/93/EF). Art. 5, stk. 2, heri fastslår således, at en elektronisk signatur ikke kan nægtes retlig gyldighed og anerkendelse som bevis under retssager, alene af den grund, at den er i elektronisk form eller ikke er baseret på de særlige regler, der gælder ifølge direktivet om kvalificerede certifikater, regulerede nøglecentre og avancerede elektroniske signaturer, jf. for dansk ret LES §§ 4, 5-10 og 14-15. Tilsvarende pålægger art. 9 i e-handelsdirektivet (direktiv 2000/31/EF om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked, EFT 2000 L 178/1), med-

lemsstaterne at sikre, at deres retssystem gør det muligt at indgå kontrakter elektronisk. Direktivet gør dog undtagelse for visse typer af kontrakter, herunder kontrakter om fast ejendom, kaution samt familieretlige og arveretlige aftaler.

Også i den juridiske litteratur er det almindeligt at behandle læren om digital aftaleindgåelse gennem løbende sammenligninger med papirmediet. Se til eksempel *Roger Henriksen* i J1981.285, *Agne Lindberg* (1987), s. 8 ff. og *Peter Landrock* i U1992B.176 ff. Se ligeledes Europarådets rekommendation no. R (81) 20 af 11. december 1981: "Harmonisation of laws relating to the requirement of written proof and to the admissibility of reproductions of documents and recordings on computers" (1982) henstiller bl.a., at medlemslandenes regeringer tillader anvendelsen af ikke-papirbaserede bevismidler mv., når retsforholdet ikke overstiger 728 special drawing rights (SDR) – et beløb, der løbende anbefales justeret.

Nye muligheder

Princippet om funktionel ækvivalens kan være en nyttig indfaldsvinkel, for så vidt som papiret illustrerer, hvordan man *kan* gennemføre en relativt sikker kommunikationsproces. Og det er tilmed tvingende, hvis særregler foreskriver papiranvendelse eller papirbevis, sml. dog nedenfor om fortolkningen af sådanne bestemmelser. Men papirmediet bør ikke sætte dagsordenen for de problemer, der behandles i læren om digital aftaleindgåelse. Det digitale medium kan opfylde mange andre funktioner, end papirmediet kan. Fokuserer man kun på, hvordan det digitale medium kan ækvivalere papirers funktioner, kommer man umærkeligt til at indsnævre det potentiale, mediet rummer. Blot gælder det for disse andre funktioner, at de ikke opnås uden videre. Ønsker man fuld fleksibilitet til kryptering i åbne netværk, kræves f.eks. en infrastruktur af troværdige tredjeparter. Ønsker man fuld tillid og uafviselighed til løfter afgivet som digitale meddelelser, må grundlæggende problemer vedrørende hæftelse, herunder anerkendelsen af "stærke" og "svage" indsigelser, overvejes: Den part, der vil afvise, at et forpligtende dokument bærer hans signatur, får en langt tungere bevisbyrde at løfte, end han ville have i papirets verden. Problemer som dem, der indtil nu kun har givet anledning til lovregulering på forbrugerbeskyttelsesområdet (betalingsmiddelloven mv.), får derfor stigende betydning også i relation til transaktioner med ikke-forbrugere.

19.1.c. Den digitale viljeserklæring

Udgangspunktet

Dansk aftaleret bygger på den grundlæggende tanke, at den enkelte har frihed og kompetence til at forpligte sig ved at udtrykke en vilje hertil. For at antage en privatretlig forpligtelse kræves

kun en manifestation af den forpligtedes vilje (*det subjektive krav*, viljesbetragtningen), der er egnet til at skabe en forventning hos den berettigede om, at forpligtelsen er gældende (*det objektive krav*, tillidsbetragtningen). Se hertil nærmere *E&A* s. 231 ff. og *GA* s. 45 ff. og 80 ff. Den, der "lover", "indestår" etc. ved eller bør vide, at disse ord reflekterer sig i en tilsvarende forventning om at være beføjet, berettiget etc. At sætte underskriften på et stykke papir sker ofte ud fra bevidstheden om den almindeligt gældende sædvane om, at enighed, der er opnået efter forudgående forhandling, besegles på denne vis. Gyldigheden af en forpligtelse beror dermed på, om den pågældende manifestation opfylder disse objektive og subjektive krav. Er der på det pågældende område enighed om, at noget er en manifestation, er det i princippet underordnet, hvad dette "noget" er: om det er et røgsignal, et håndtryk, et nik, en underskrift eller en digital meddelelse.

De retlige problemer opstår, når der er tvivl om, hvorvidt der *foreligger* en manifestation, og hvordan den i givet fald skal *fortolkes*. I disse tvivlstilfælde kan det få betydning, hvilke kommunikationsmedier parterne har brugt. Jo mere typisk og genkendelig, viljeserklæringen fremtræder, desto mindre krav vil man stille for at knytte gyldighed til den. Fremtræder viljeserklæringen derimod på en måde, som den anden part ikke er vant til at læse, f.eks. i form af en digital meddelelse, der kun kan læses af modtagerens IT-system, beror det på, hvordan det pågældende system er implementeret, om der rent faktisk er harmoni mellem vilje og udtryk.

Objektive krav

De objektive rammer for en digital kommunikation kan enten følge den *praksis*, der har indarbejdet sig vedrørende en bestemt teknologi (f.eks. telefax), af særlige *forskrifter* (f.eks. de regler, der gælder for VP), eller af *aftale*. Foreligger hverken aftale, forskrifter eller praksis, er der ikke grundlag for at anvende denne nye teknologi, ligeså lidt som der ville være grundlag for at knytte retsvirkning til de vink mv., der manifesterer et auktionsbud, hvis ingen af de tilstedeværende kender disses indhold. Som tidligere nævnt kan fraværet af sådanne objektive krav til viljeserklæringer indebære den største forhindring imod brug af digitale medier til aftaleindgåelse. Den aftaleretlige håndtering af disse spørgsmål behandles nedenfor i afsnit 19.1.g. om kommunikationsaftaler.

Subjektive krav

Indholdet af det subjektive krav, man stiller som betingelse for at anerkende løftevirkninger, beror på en række faktorer, herunder løftets forudsatte eller særprægede karakter, praksis på området (de objektive krav), parternes status (forbruger eller erhvervs-

drivende) og løftets indhold. I forhold til det mundtlige løfte manifesteres digitale meddelelser ofte i forløb, der er adskilt fra det moment, hvor viljen formes. I almindelig samtale kan information overføres uden ydre midler (typisk ved tale eller gestikulation); men digital informationsudveksling er kun mulig som led i komplicerede processer, der kan konvertere, fortolke, transmittere og analysere de overførte bits. Da den kommunikerende ikke har umiddelbar kontrol over disse processer, opstår risikoen for fejl og misforståelser. Denne risiko er særligt stor, når informationsudvekslingen sker i et system, der på forhånd er programmeret til ikke bare at sende og modtage information, men også at effektuere ordrer ved igangsætning af produktionsprocesser, levering af informationsmængder el.lign.

Udover denne adskillelse mellem vilje og erklæring, er digitale viljesmanifestationer udsat for en række risici, som man kun i begrænset omfang kender til fra papirets verden: Vel kan papiret brænde og teksten på det senere fremtræde uklart, men disse enkelte elementer i og trusler mod kommunikationsprocessen fremstår som noget velkendt. Dertil kommer, at hele det system, der understøtter disse kommunikationshandlinger, ofte kan antage en egen "identitet", der f.eks. kan få betydning for anvendelsen af regler om aftaleretlig "kundskab", fuldmagtslegitimation mv.

Mediets betydning

Den aftaleretlige lovgivning sondrer i et vist omfang mellem sådanne former for *middelbar* kommunikation (der på grund af det anvendte medium adskiller de kommunikerende parter i tid og rum) og *umiddelbar* kommunikation (hvor meddelelserne udveksles i en samtidig proces). CISG art. 20 taler om "øjeblikkelige kommunikationsmidler". Aftl. § 3, stk. 2, omhandler tilbud, der fremsættes mundtligt. Denne sondring mellem umiddelbar og middelbar kommunikation spiller ofte en rolle ved fortolkningen af lovkrav, der – som de citerede – knytter an til bestemte, klassiske kommunikationsformer. Man kan imidlertid stille spørgsmålet, om den generelle risiko, der består for utilsigtet afgivelse af "viljeserklæringer" ved brug af digital teknologi, generelt skal føre til en skepsis overfor sådanne erklæringer.

Utilsigtet afgivelse

Som udgangspunkt må det fastholdes, at en digital meddelelse, for at have retsvirkning, må udspringe af et kausalforløb, der kan føres tilbage til en aftaleretligt forpligtende viljeserklæring. Hvis systemet pga. en fejl eller et virusangreb pludselig afgiver meddelelser, der lader formode, at indehaveren eller andre "lover" dette eller hint, kan sådanne meddelelser som udgangspunkt ikke tillægges retsvirkninger som viljeserklæringer (løfter). I

modsat fald ville der ingen grænser være for, hvad A blev forpligtet til: Computere kan som bekendt behandle data med ekstrem effektivitet, og dermed også afgive fejlagtige data med en sådan effektivitet! Skyldes det fejl fra den systemansvarliges side, at de pågældende meddelelser er afgivet, kan disse fejl efter omstændighederne indebære, at den pågældende har handlet *culpøst*, således at han efter almindelige erstatningsregler ifalder et erstatningsansvar. Et sådant ansvar falder uden for kontraktsforhold. Der er altså ikke hjemmel til at tilkende erstatning svarende til offerets positive opfyldelsesinteresse.

Modifikationer

Dette udgangspunkt må dog modificeres i forskellige henseender. For det første må parterne have frihed til at *aftale*, at der til bestemte tekniske forhold knytter sig bestemte retsvirkninger. Dernæst må det antages, at en part, der undlader at gribe ind over for systemets "dispositioner", herunder ved at advare den eller de parter, der knytter tillid hertil, vil kunne hæfte aftaleretligt efter samme principper som dem, der ligger til grund for retspraksis om såkaldt *tolerancefuldmagt*, se herom senere.

19.1.d. Begrebet "kundskab"

Når det lægges til grund, at et IT-system ikke kan besidde nogen "vilje", der giver grundlag for nogen aftaleretlig pligtskabelse, må man tilsvarende afvise, at systemet kan besidde "kundskab", jf. aftl. § 7. Efter denne bestemmelse kan et tilbud eller svar *kaldes tilbage*, selv om det er kommet frem til adressaten, hvis tilbagekaldelsen *kommer frem* før tilbuddet eller svaret er kommet til modtagerens *kundskab*. Har A's system fremsendt en EDI-meddelelse til B's system, som A fortryder, fremtvinger aftl. § 7 en stillingtagen til, om selve modtagelsen af denne meddelelse i B's system er ensbetydende med, at B har fået kundskab til den, eller om andre faktorer skal være afgørende.

Kundskabsanalogier

Skal man opregne de tidspunkter, der kunne tillægges anvendt som kundskabsækvivalerende tidspunkt, kan man pege på tidspunktet for meddelelsens *modtagelse*, det tidspunkt, hvor modtagersystemet *bearbejder* den med henblik på behandling i og uden for modtagerens organisation, det tidspunkt, hvor der *internt hos B* foretages noget faktisk på grundlag af meddelelsen (f.eks. udfærdiges en faktura eller igangsættes en produktion), det tidspunkt, hvor der *udadtil* foretages noget faktisk (f.eks. fremsendes en faktura eller afgives en ny ordre) eller det tidspunkt, hvor en person, der tegner B, har fået *kendskab* til meddelelsen.

Der er ikke enighed i teorien om, hvilke af disse tidspunkter der skal lægges til grund, og spørgsmålet må betragtes som uafklaret. I U1994B.395 foreslår *Birgitte Kofod Olsen* et *bearbejdningskriterium*, hvorefter det tidspunkt, hvor computeren har afsluttet bearbejdningen af de indkomne data, skulle være afgørende. Se i samme retning *Susanne Karstoft*: Elektronisk aftaleret (2004), s. 64. Kriteriet volder betydelig usikkerhed (hvor sker "bearbejdningen", henholdsvis den efterfølgende "opfølgning", når vi befinder os inden for én og samme virksomhed?), ligesom det pålægger pseudo-løftegiveren risiko for uforudsete aftalepligter. *Eivind Einersen* (1992) påpeger s. 64 f., med rette, at fuldautomatiske EDI- og telebutik-systemer ofte vil effektuere bestillinger uden menneskelig indblanding, og at det her vil være mere eller mindre tilfældigt, om et menneske ser de konkrete ordrer. Denne forfatter vil derimod anerkende, at "aftaler kan afsluttes af maskiner", hvorved der drages en analogi mellem menneskelig kundskab og systemets "viden". Betragtningen er altså, at computeren betragtes som en slags "fuldmægtig" for brugeren, jf. nærmere herom nedenfor under 19.2. Problemet er ikke afklaret i UNCITRALs modellov om Electronic Commerce.

Konklusion

Er forholdet ikke afklaret ved parternes aftale, bør tilbagekaldelse formentlig kunne ske frem til det tidspunkt, hvor en person, der tegner modtageren, får kendskab til meddelelsen, f.eks. ved at modtage underretning om, at varen er på vej. Det forekommer dog velbegrundet også at antage, at der består en aftale, når en ydelse rent faktisk er præsteret og konsumeret (eller at der i det mindste er taget skridt til en sådan konsumption, der vil vanskeliggøre en tilbagelevering af varen, sml. forbrugeraftalelovens § 12, stk. 3, om tilfælde, hvor en vares forsegling er brudt). Hvis varen – af en ikke-tegningsberettiget person – sendes via posten, modtages og konsumeres, vil modtageren af varen ikke efterfølgende kunne gøre gældende, at der ingen aftale foreligger. Hans passivitet må i så fald betragtes som en *kvasidisposition*. Et sådant konsumptionssynspunkt må dog forudsætte, at *kvasiløftegiveren* har haft en subjektiv viden herom. Dette er ikke nødvendigvis tilfældet, hvis ydelsen er rent digital og leveres til et informationssystem, hvor den konsumeres (f.eks. i form af en programopdatering, der efter en automatisk opkaldsprocedure hentes hjem fra nettet).

Denne konklusion indebærer som før nævnt, at A ud fra et culpasynspunkt vil være forpligtet til at udrede B's tab ved tilbagekaldelsen (negativ kontraktsinteresse). Muligheden for at opnå en sådan erstatning tilgodeser i øvrigt de argumenter, der ellers

kunne tale for et bearbejdningskriterium: I det omfang, A som følge af et culpøst forhold, giver B indtryk af, at der foreligger en aftaleretlig forpligtelse (med den virkning, at B f.eks. disponerer i tillid hertil), vil A pådrage sig erstatningsansvar herfor efter almindelige regler. Erstatningen kan blot ikke overstige et beløb svarende til den negative kontraktsinteresse, da der netop ikke består noget kontraktsforhold.

Se i øvrigt *Erik Røsæg* i Festskrift til Karnell (1999), s. 666 ff. og *Susanne Karstoft*: Elektronisk aftaleret (2004), s. 61 ff.

19.1.e. Acceptens "fremkomst"

Retlig funktion

Et tilbud, der accepteres efter sit indhold, etablerer dermed en aftaleforpligtelse mellem parterne, såfremt accepten foreligger rettidigt til rette acceptsted og i øvrigt i overensstemmelse med de formkrav, der gælder for tilbuddet. Disse nærmere krav kan fremgå af tilbuddet selv eller bero på omstændighederne, jf. herom lovens § 3. Da accepten også forpligter modtageren (tilbudsgiveren) til at stå ved sit tilbud, udgør den et *påbud*. For at undgå, at tilbudsgiveren smyger disse forpligtelser af sig, stiller aftaleloven – her som ved andre påbud – alene krav om, at accepten er "kommet frem" til tilbudsgiveren, § 4, stk. 1. Den behøver altså ikke også være kendt af denne. Et tilsvarende princip gælder ifølge aftl. §§ 2, stk. 1, og 3, stk. 1 (om beregning af fristen for et tilbud), og § 7 (om tilbagekaldelse af tilbud). Princippet har almen betydning for påkrav i den almindelige obligationsret, jf. *Bryde Andersen & Lookofsky* (2005), s. 361 ff., omend fastsættelsen af tidspunktet for fremkomsten kan variere i relation til hver enkelt regel. Tilsvarende kan praksis om andre typer af påkrav også kaste lys over de krav, man vil stille til acceptens fremkomst.

Udgangspunktet

Reglerne om fremkomst er i hovedsagen formet efter den praksis, der kendes om udveksling af meddelelser, der foreligger på papir eller fremsiges mundtligt. En mundtlig meddelelse, der ytres overfor modtageren på en måde, der giver denne mulighed for at forstå dens indhold, er dermed også "kommet frem". Når det gælder skriftlige meddelelser er det tilstrækkeligt, at kuverten lægges på skranken i receptionen eller – udenfor kontortid – lægges i postkassen. De spørgsmål, der skal drøftes i det følgende, udspringer af, at parterne har gjort brug af andre medier end det skriftlige og mundtlige. Hvilket af den nye teknologis nye medier til kommunikation kan da anvendes, og hvordan?

1. Medium?

Når det gælder spørgsmålet om, hvilket medium man kan anvende til påkrav, må der sondres mellem om parterne tidligere har kommunikeret eller om der er tale om førstegangskommunikation.

Har parterne *tidligere kommunikeret*, kan det medium, de dengang anvendte, som udgangspunkt også genanvendes ved en senere forpligtende information, medmindre særlige forhold gør sig gældende. Mediet "gælder" således, indtil parterne klart har vedtaget et andet, eller en af parterne klart har markeret, at han nu skifter medium eller "adresse", jf. tilsvarende *Karstoft* i J 1999.117 f. og *TBB 1999.198 VLK*. Hvis A via e-post tilbyder B en vare uden nærmere angivelse af, hvilket medium B i givet fald skal anvende til accept, må B som udgangspunkt kunne forvente, at han også kan acceptere ved brug af e-post. Det samme gælder selvsagt, hvis et afgivet løfte selv angiver den form, hvorunder det skal accepteres. Sådanne angivelser er gyldige som andre typer af forbehold.

Kendelsen i *TBB 1999.198 VLK* angik en situation, hvor udlejer vidste, at den konkursramte lejer pga. fogedforbud og aflåsning var afskåret fra at komme til sin telefax. Et betalingspåkrav fremsendt pr. brev og telefax til den hidtidige adresse kunne derfor ikke anses for fremkommet ved telefaxens modtagelse. Lejer havde ikke underrettet udlejeren om den nye adresse, men han havde sørget for omadressering af sin post, hvorved påkravet først kom frem to dage senere end ellers. En enkelt dommer ville dog, ligesom fogedretten, lægge vægt på telefaxens fremkomsttidspunkt.

Har parterne *ikke tidligere kommunikeret*, må der vælges et medium for forpligtende kommunikation, der indebærer en høj sandsynlighed for, at modtageren vil gøre sig bekendt med dens indhold. Denne situation kan f.eks. forekomme, når et tilbud er afgivet via en hjemmeside. I samme kategori står de tilfælde, hvor den tidligere kommunikation har fundet sted under andre teknologiske forudsætninger end dem, der nu vil være de almindelige. Man må her se på, hvilke forventninger tredjeparter almindeligvis vil have til formen for en henvendelse *af det pågældende indhold*. Det ligger således klart, at man ikke på forhånd kan fastslå, at der i relation til en part i almindelighed må anvendes en bestemt type kommunikation. Således er praksis også på de mere klassiske aftaleområder: Skal man bestille en taxa, anvender man oftest *telefon*, evt. via tast-selv-ordninger. Bestillinger af lidt mere værdifulde formuegoder baseres ofte på *papir*, f.eks. bestillingskuponer, der forudsætter *underskrift*. Aftaler om mere værdifulde og komplekse formuegoder – f.eks. faste ejendomme og virksomheder – indgås almindeligvis efter intense

undersøgelseshandlinger, der følges op med nedfældede aftaledokumenter.

2. Terminalpunkt?

Hvert kommunikationsmedium indebærer et – og ofte flere – terminalpunkter, som markerer afslutningen på kommunikationsprocessen. En virksomhed kan have flere skranker, hvor breve og meddelelser kan afleveres, flere telefonnumre, hvortil der kan sendes telefax og flere e-mailadresser, hvortil der kan sendes elektronisk post. Det er dog langt fra sikkert, at hvert af disse terminalpunkter også vil kunne være fremkomststed for et påkrav.

Ved vurderingen af dette spørgsmål gælder i hovedsagen samme principper som de, der er nævnt ovenfor om mediet: Man må se på, hvilken praksis parterne har indført mellem sig og vurdere, om modtageren med rette kan forvente, at det således valgte medium også kan anvendes til forpligtende kommunikation. At der rent faktisk er kommunikeret mellem to virksomheder – f.eks. mellem deres respektive teknikere under et projektarbejde – indebærer således ikke nødvendigvis, at de e-mail-adresser, der herved er anvendt, kan genanvendes ved fremsendelse af påkrav. Der kan således være fornuftige tekniske grunde til at adskille afsenderfax fra modtagerfax, f.eks. for ikke at blokere for indkommende opkald.

Myndigheder og virksomheder vil ofte kundgøre fremkomststedet udadtil, f.eks. på brevpapir, i offentlige registre (telefonbog, Internet-kataloger, handelsoversigter mv.) eller ved udtrykkelig angivelse på hjemmesiden eller i aftalen. En sådan markering vil altid skabe en forventning om, at man er parat til at modtage meddelelser på disse medier/adresser. Ønsker virksomheden at skifte til et andet medium, må der derfor foretages en effektiv nedlukning af det pågældende terminalpunkt. Den, der afventer en meddelelse, bør ligeledes kunne forvente, at afsenderen anvender det officielle modtagenummer (modtagerfaxen). Har en "ikke-autoriseret" modtagerfax været anvendt tidligere i parternes *forpligtende* kommunikation (og altså ikke blot mellem medarbejdere, der har været beskæftiget med rent *driftsmæssige* opgaver), uden at modtageren har gjort indsigelse herimod, vil dette dog kunne udvide domænet for, hvilke meddelelser der skal anses for at være kommet frem.

3. Tidspunkt?

Et tredje spørgsmål drejer sig om, hvilken *informationsteknisk* begivenhed der må antages at udgøre fremkomstsituationen. Svaret på dette spørgsmål må være, at meddelelsen kommer frem, når den er placeret på et medium, hvorfra modtageren har *teknisk mulighed* for at læse den. I almindelighed vil dette krav være

opfyldt, når meddelelsen er læsbar på den server, hvorfra hjemmesiden drives, uanset om serveren er placeret hos den erhvervsdrivende selv eller hos en teknisk bistandsyder (f.eks. outsourcing-leverandør), og uanset om modtageren rent faktisk henter meddelelsen frem. Spørgsmålet er nu, hvilket tidspunkt der i *retlig* henseende skal anses for fremkomst.

- læsning?

Man kan spørge, om der indtræder fremkomst allerede, når en elektronisk meddelelse når serveren hos modtagerens tjenesteudbyder (uanset om modtageren rent faktisk har hentet sin post her), eller om modtageren rent faktisk skal have taget skridt til at læse meddelelsen. Det er her den almindelige opfattelse, at en e-postmeddelelse er kommet frem, når den er tilgængelig i modtagerens e-post-system (men dermed ikke nødvendigvis læst af denne). Se herved *Karstoft* (2004), s. 82 ff. med henvisninger.Uden en sådan regel ville man bryde med det grundlæggende princip i læren om fremkomst, at modtageren af et påkrav ikke skal kunne smyge den forpligtelse, der ligger i påkravet, af sig ved ikke at tage de skridt til læsning, som han normalt ville tage. Et tilsvarende princip ligger i øvrigt til grund for den nye bestemmelse i rpl. § 148a, stk. 3, hvorefter en digital meddelelse anses for at være *kommet frem*, når den "kan gøres tilgængelig" for retten, se hertil afsnit 16.3.a., og ved e-handelslovens § 12, stk. 2, hvorefter en elektronisk ordre og den elektroniske ordrebekræftelse, jf. bestemmelsens stk. 1, anses som modtaget, "når adressaterne har adgang til disse".

En meddelelse sendt til telefax-numre inden for en virksomhed mv., som ikke er markeret som modtage-numre i en telefonbog, på brevpapir el.lign., er næppe "kommet frem", før den rent faktisk håndteres som sådan, f.eks. af et bud el.lign., der sørger for intern videreekspedition, eller den rent faktisk kommer til modtagerens kendskab.

- konvertering mv.

Enhver elektronisk meddelelse nødvendiggør gennemførelse af nogle elektroniske processer, som kan være mere eller mindre tidskrævende. For telefax drejer det sig om den tid, der medgår ved indskanning og udprint, for elektronisk post om den tid, der medgår til opkobling til e-posthus og overførsel af postfiler. Er meddelelsen komprimeret eller krypteret medgår dernæst en vis tid til dekomprimering eller dekryptering. Som udgangspunkt må det antages, at den tid, der medgår til disse tekniske processer, ikke udskyder modtagelsestidspunktet. Hovedreglen er med andre ord, at en meddelelse er "kommet frem", når den er modtaget i en form, som det er muligt for modtageren at læse den i, uanset om dette kræver nogle øjeblikke eller minutter til gennemførel-

sen af den pågældende proces. Den passende analogi er her papirbrevet, som også anses for fremkommet, når det modtages af portneren, selvom der går nogle minutter, inden det ligger på bordet hos den pågældende medarbejder. Se tilsvarende *Røsæg* i Festskrift til Karnell (1999), s. 662.

4. Format

Selv om modtageren ikke umiddelbart er i stand til at læse meddelelsen, må der påhvile ham en vis pligt til at søge de midler bragt i anvendelse hertil, som må anses for forudsatte eller sædvanlige. Også her består opgaven i at fortolke den praksis, parterne har etableret mellem sig. Har parterne f.eks. tidligere korresponderet ved anvendelse af et bestemt meddelelsesformat (f.eks. tekster frembragt i et bestemt tekstbehandlingssystem), må modtageren også fremover betjene sig af dette; han kan med andre ord ikke uden særlig grund vise en meddelelse fra sig som ulæselig under påberåbelse af sådanne tekniske forhold. Når det gælder vurderingen af, hvornår læsbarhed anses for "sædvanlig", må der dog udvises en vis tilbageholdenhed. At et tekstbehandlingssystem nyder stor udbredelse blandt hovedparten af brugerne i et bestemt miljø godtgør ikke i sig selv, at der består en "sædvane" for brug af det pågældende format. Når det gælder brugen af de standarder, der indgår i udveksling af meddelelser via elektronisk post eller hjemmesider, består der derimod en underforstået forpligtelse til at kunne læse meddelelser, der overholder disse standarder.

- ulæselighed

Et særligt problem foreligger, hvis meddelelsen kommer frem, men efterfølgende mister sin læsbarhed. Dette problem kendes fra talrige medier: Et brev lægges i postboksen, som herefter ødelægges; en telefonbesked indspilles på en telefonsvarer, men overspilles ved en fejl af en anden telefonbesked; en telefax modtages pga. papirstop i modtagerapparatets hukommelse, men strømmen forsvinder, hvorved meddelelsen går tabt. I disse tilfælde må man formentlig drage paralleller til den brændte postboks og nå til, at der foreligger fremkomst, selv om læsbarheden siden forsvinder, se således *Hultmark* i Festskrift til Jan Ramberg (1997), s. 258 f. Dette resultat støttes ligeledes af risikooverveje-lser: Det er lettere for modtageren at afværge den risiko, der fører til meddelelsens ulæsbarhed, end det er for afsenderen at sikre sig, at meddelelsen er kommet frem. Og eftersom det står i modtagerens magt at afskære fremkomstmuligheden på særligt følsomme medier (ved f.eks. at fravælge dem aftaleretligt eller undlade kommunikation fra dem), er hensynet til den uheldige bruger af sådanne medier ikke overvældende stort.

Et spørgsmål, der ikke berøres her (se derimod afsnit 4.3.) drejer sig om *beviset* for, at meddelelsen er kommet frem. I voldgiftspraksis har man f.eks. anset den kvittering, der kan produceres af afsenderens telefax-apparat for at udgøre en fornøden kvittering, se hertil *Einersen* (1992), s. 145 f. Domstolene har dog været tilbageholdende med at knytte bevisværdi til dette dokument, når der har været tale om meddelelser med – indgribende – påkravsvirkning. Således fandt *U 1999.198 VLK*, at et påkrav, der var afgivet ved telefax, ikke var kommet frem ved telefaxens modtagelse, idet lejeren var afskåret fra at komme i kontakt med telefax-apparatet. Se omvendt *TBB 2003.492 VLK*, der lod det komme lejeren til skade, at denne ikke havde orienteret udlejeren om sin hospitalsindlæggelse. Skyldes den manglende fremkomst, at modtageren bevidst har bragt sig i en situation, hvor en henvendelse – der normalt ville være kommet frem – af praktiske grunde ikke gør det, kan man efter omstændighederne alligevel statuere fremkomst. Dette er f.eks. antaget ved *TBB 2001.457 ØLK*, hvor et påkrav og en hæveskrivelse i et lejemål ansås for at være kommet frem til lejemålets adresse (og ikke til lejerens bopælsadresse, der var angivet i lejekontrakten), uanset manglende postkasse. Retten bemærker, at lejeren tidligere uden indsigelse havde modtaget lejeopkrævninger og breve på lejemålets adresse.

Accept afgivet mod hjemmesider

De almindelige principper om fremkomst kan være vanskelige at overføre til den situation, hvor påkravet (f.eks. en accept) afsendes mod en hjemmeside. Problemet ligger i, at den kommunikation, der foregår til hjemmesider, ikke er genstand for samme, veletablerede, standardisering som kommunikation, der fremsendes via e-post. Ofte vil der kunne være begrundet tvivl om, hvorvidt meddelelsen er kommet frem – og under hvilke omstændigheder. Det retlige udgangspunkt er dog klart: Et påkrav, der afgives mod en hjemmeside (f.eks. ved indtastning direkte mod webserveren eller ved e-post afgivet ved en særlig e-mail-funktionalitet fra hjemmesiden) anses for modtaget, når hjemmesidens indehaver er i stand til at læse den, men ikke før.

E-handelslovens § 12

For at undgå tvivl af denne karakter foreskriver e-handelslovens § 12, stk. 1, at tjenesteyderen uden unødig forsinkelse elektronisk skal bekræfte modtagelsen af en elektronisk ordre. Bestemmelsen omtales i afsnit 19.2.b. om *point and click*-aftaler.

Filtrering

En særlig problemstilling opstår, hvis meddelelsen ikke når frem til adressaten, fordi den er filtreret fra af et *spam-filter*, på grund af en teknisk spærreanordning, der (med rette eller urette) har detekteret en virus i meddelelsen, eller fordi meddelelsens

størrelse (f.eks. fordi den indeholder indskannede dokumenter i pdf-format) overstiger gældende maksima for indgående e-mails. Sådanne problemer er blevet stadigt større gennem de seneste år. Langt over halvdelen af den e-mail, der transmitteres på nettet, er spam. I den praktiske brug af e-mail er det derfor nødvendigt at opsætte filtre på serveren, der efter forskellige kriterier fjerner visse typer af mails (der efter disse kriterier formodes at være spam), inden de når e-mail klienten. Jo stærkere et sådant filter sættes op, desto større er risikoen for, at en elektronisk mail ikke modtages af klienten og dermed af den adressat, mailen var tiltænkt. Derfor kan det ofte forekomme, at en meddelelse når modtagerens server, men ikke modtageren selv, dvs. dennes *klient*.

Hvis systemet i en sådan situation automatisk sender en fejlmelding til afsenderen, og hvis ikke modtageren *bevidst* har sat systemet op således, at en sådan fejlmelding vil blive afgivet (f.eks. for at undgå en uønsket påbudsvirkning), er udgangspunktet, at meddelelsen ikke anses for kommet frem, når den således er filtreret fra. En modsat regel ville være ensbetydende med, at den potentielle modtager af et påkrav, løbende måtte skaffe sig oplysning om, hvilke mails, der var filtreret fra, f.eks. fra teleleverandør eller IT-afdeling. En sådan pligt ville fjerne en væsentlig del af den fordel, der antages at være forbundet med brugen af elektronisk post. Vælger afsenderen at benytte dette medium, må han tage det, som det er.

19.1.f. "Forsvarligt befordringsmiddel"

Når man sender en meddelelse, der har karakter af påbud, er det som bekendt den almindelige regel, at påbuddets retsvirkninger indtræder ved fremkomst. Som udgangspunkt bærer afsenderen af meddelelser selv risikoen for, at meddelelsen kommer rettidigt frem. Men i relation til påkrav fastslår aftl. § 40 (og stort set i overensstemmelse hermed kbl. § 61, kommissionslovens § 3 og forsikringsaftalelovens § 33), at modtageren bærer risikoen for, at påkrav efter disse love går tabt, hvis meddelelsen er indleveret "til befordring med telegraf eller post, eller hvor andet forsvarligt befordringsmiddel benyttes". Bestemmelsen er ikke ændret siden aftaleloven af 1917 og tager derfor i sagens natur ikke stilling til, hvornår de moderne elektroniske kommunikationsmidler herefter kan betragtes som "forsvarligt befordringsmiddel". Aftl. § 40

Spørgsmålet drøftes i den svenske betænkning om elektronisk dokumenthåndtering, SOU 1996:40, der uden tøven antager (s.

124), at sådanne elektroniske befordringsmidler er "forsvarlige". Resultatet er i høj grad tvivlsomt. Der er stor forskel i henseende til driftssikkerheden og pålideligheden af forskellige elektroniske kommunikationsformer, og det er derfor ikke muligt under ét at fastslå, at f.eks. en elektronisk postmeddelelse er udtryk for en forsvarlig befordring af kommunikation, jf. § 40. Da formålet med denne bestemmelse netop er at tilvejebringe et klart retsteknisk udgangspunkt for risikofordelingen ved fremsendelse af påkrav, må man derfor nå til, at bestemmelsen er uanvendelig udenfor sit direkte anvendelsesområde. Der er imidlertid behov for en revidering af bestemmelsen, bl.a. også fordi begrebet "post", med den igangværende privatisering og deregulering af de tidligere statsmonopoler på området, givetvis vil fjerne sig fra det oprindelige udgangspunkt om en tjeneste med offentligretligt tilsnit.

Spam og sikkerhed

Vurderingen af, om elektronisk post repræsenterer et forsvarligt befordringsmiddel, må i øvrigt antages at ændre sig i takt med ændringer i den sikkerhed, der rent faktisk omgiver e-mail-teknologien. Et forhold, der i den forbindelse spiller en rolle, er sikkerheden for at den elektroniske meddelelse ikke blot modtages af e-mail-*serveren* men også af e-mail-klienten. I praksis vil brugen af såkaldte *spam-filtre* indebære vis risiko for, at dette ikke sker, jf. bemærkningerne herom oven for s. 816 f. Man kan derfor næppe udelukke, at en domstol i dag (og frem til det tidspunkt, hvor der er opnået en generelt udbredt og effektiv løsning af spam-uvæsenet) vil anse e-mail-kommunikation som uforsvarlig i relation til denne bestemmelse.

CISG

I internationale køb fastslår CISG art. 27, at en part, der har givet underretning, anmodning eller anden meddelelse i overensstemmelse med reglerne i konventionens første afsnit, og som har anvendt et meddelelsesmiddel, som under de givne forhold er forsvarligt, ikke berøves sin ret til at påberåbe sig meddelelsen, såfremt der indtræder *forsinkelse* eller *fejl* ved dens videresendelse. Reglen har et videre område end aftl. § 40 og kbl. § 61, idet den ikke alene lader modtageren bære forsinkelsesrisikoen, men også risikoen for forvanskning, som kan være ensbetydende med, at der pålægges modtageren ganske vidtgående og uventede retsfølger. Bestemmelsen viger dog for konventionens egne undtagelser om meddelelser, der befordres på afsenderens risiko, se artiklerne 47, stk. 2, 48, stk. 4, 63, stk. 2, 65, stk. 1 og 2, samt 79, stk. 4, der alle taler om meddelelser, der er "modtaget", "fået" eller "kommet frem".

19.2. Forpligtelsens indtræden

19.2.a. Tilbud og svar på tilbud

Aftalelovens kapitel 1 indeholder en række regler, der fastslår, hvornår en aftale, der bliver til gennem parternes tilbud og svar på tilbud mv., kan anses for indgået. Reglerne er deklaratoriske. Efter § 1, 2. pkt., kommer de alene til anvendelse, for så vidt ikke andet følger af tilbuddet eller svaret eller af handelsbrug eller anden sædvane.

Acceptfrist

Når loven taler om "tilbud", omfatter dette såvel mundtlige som skriftlige tilkendegivelser, jf. forudsætningsvis § 3, stk. 2, hvorefter mundtlige tilbud uden acceptfrist skal accepteres straks. Aftl. § 3, stk. 1, indeholder en særregel om, hvordan acceptfristen i mangel af særskilt angivelse skal beregnes, når et tilbud er fremsat "i brev eller telegram". Lovens henvisning til disse typer af medier må anses som eksempler på de medier for nedfældet information, der var til rådighed ved lovens givelse (1917). Det må følgelig antages, at en digital meddelelse i form af en telefax, elektronisk post-meddelelse eller EDI-instruktion kan udgøre et "skriftligt" tilbud. Sondringen bør bero på, om modtageren af tilbuddet forventes i ro og mag at kunne fordybe sig i dets indhold med henblik på mulig accept.

Opfordringer

Aftaleloven sondrer mellem tilbud og opfordringer til at gøre tilbud. Når en hjemmeside indeholder oplysning om, at forbrugeren kan aftage varer eller tjenesteydelser ved bestillinger på hjemmesiden, beror forbrugerens retsstilling på, hvornår aftale herom må anses for indgået. Hvis oplysningerne på hjemmesiden alene betragtes som en opfordring til at gøre tilbud, kommer der først en aftale i stand, når den erhvervsdrivende bekræfter forbrugerens "bestilling". Er hjemmesidens udvisende derimod i sig selv et tilbud, kommer aftalen i stand, når forbrugerens accept af dette tilbud kommer frem til den erhvervsdrivende, jf. dette begreb nedenfor. Bestillingen er dermed det aftaleskabende moment.

I dansk juridisk litteratur er det den almindelige opfattelse, at bestillingsinformation i reklamer, annoncer, kataloger og lign. alene skal anses som opfordringer til at gøre tilbud. Se herved *Lynge Andersen m.fl.*: Aftaler og mellemmænd (2001), s. 55 f., og *GA* s. 182 f. Omvendt er det opfattelsen, at den annoncering, der sker ved skiltning i et udstillingsvindue mv. i dag må betragtes som et tilbud, der som sådant accepteres ved forbrugerens bestilling. Dette resultat er for dansk rets vedkommende fastslået ved Højesterets domme i *U 1985.877 H* og *U 1991.43 H*.

Diskussion

Ved vurderingen af, om en hjemmeside i almindelighed skal betragtes som en butiksannoncering eller som et katalog, må der navnlig henses til, hvilke forpligtelser dette vil udvirke for den erhvervsdrivende, og hvad der i øvrigt vil være virkningen af at antage det ene eller det andet resultat. At man i almindelighed antager, at produkt- og prisangivelser i salgskataloger ikke skal anses for bindende tilbud, men alene som opfordringer hertil, beror navnlig på ønsket om at beskytte den erhvervsdrivende i en situation, hvor annonceringen ellers kunne fremkalde et uventet stort antal aftaleskabende accept-henvendelser, som det ville være uforholdsmæssigt bekosteligt at skulle honorere. Den erhvervsdrivendes praktiske muligheder for at tilbagekalde tilbuddet vil her være begrænset af, at kataloget nu engang var trykt og udsendt. Men når tilbud afgives via hjemmesider er situationen en anden, idet den erhvervsdrivende her vil have det i sin magt øjeblikkeligt at ændre tilbuddet, hvis der skulle vise sig at indløbe et større antal accept-henvendelser end forudsat.

Udgangspunktet

Derfor må det formentlig antages at være gældende ret allerede i dag, at hjemmeside-udbud af varer mv. som udgangspunkt må betragtes som tilbud, der altså accepteres og skaber aftaleforpligtelser efter deres indhold, når forbrugerens accept er kommet frem til den erhvervsdrivende i overensstemmelse med den foreskrevne fremgangsmåde. Dette resultat antages generelt af Forbrugerklagenævnet, se herved JÅF 1999.146, *Forbrugerredegørelsen 2002-2003.160* og *Forbrugerredegørelsen 2002-2003.210 f*. Det er imidlertid væsentligt at slå fast, at der er tale om et udgangspunkt, og at man i mange tilfælde – herunder ved en konkret fortolkning – må nå frem til andre resultater. Se herved *Karstoft* i J 2000.252 ff. og i Elektronisk aftaleret (2004), s. 41 ff.

Et grænsetilfælde er afgørelsen i *Forbrugerjura 2003.97* ff., hvor en forbruger havde modtaget en e-mail indeholdende en link til den erhvervsdrivendes *hjemmeside*. I mailen var prisen for et kamera angivet lavere end på hjemmesiden. Flertallet i Forbrugerklagenævnet fandt, at et elektronisk *nyhedsbrev* måtte anses som et tilbud i aftaleretlig forstand, når der til nyhedsbrevet var knyttet en direkte indkøbsfunktion ad elektronisk vej. Da det fremsendte nyhedsbrev imidlertid pegede hen til en hjemmeside, hvor den rigtige pris var anført, var den erhvervsdrivende ikke bundet af prisangivelsen i mailen.

Ofte vil forholdene i den konkrete handelssituation (og branche) indicere, hvordan et tilbud rimeligvis skal forstås. I *U 2003.907 V* havde en autohandler på sin Internet-hjemmeside

annonceret en brugt bil til salg til en pris af 119.900 kr. Den rigtige pris var imidlertid 349.900 kr., men inden fejlen blev rettet, havde en kunde afgivet accept. Landsretten fandt, at annonceringen af den brugte bil i det foreliggende tilfælde alene kunne anses som en *opfordring* til at gøre tilbud. Da sælgeren straks ved kundens telefoniske henvendelse gjorde denne bekendt med, at der var angivet en fejlagtig pris, var der derfor ikke indgået nogen aftale. Dommen angik en speciesydelse, som netop kendetegnes ved kun at kunne overdrages én gang – modsat den typiske genusydelse, som i elektronisk handel typisk vil blive overdraget i stort tal. Dommen tager således ikke stilling til, hvorledes retsstillingen havde været, såfremt der var tale om en standardvare. Se tilsvarende *Kim Frost* i U2003B.359 ff.

Modifikationer

Omvendt kan den erhvervsdrivende næppe være forpligtet af en accept, der afgives på hjemmesiden under omstændigheder, hvor den erhvervsdrivende ikke har haft mulighed for at opdatere hjemmesiden. Forestiller man sig, at hjemmesiden for et supermarked tilbyder salg af gær, og at der som følge af en konflikt på arbejdsmarkedet, der bliver en realitet i løbet af natten, sker et stort antal bestillinger af gær, vil man ikke rimeligvis kunne forlange af den erhvervsdrivende, at denne i løbet af natten har opdateret hjemmesiden for at undgå for mange bestillinger. I sådanne, ekstreme, tilfælde må den erhvervsdrivende dog efter omstændighederne kunne påberåbe sig *re integra*-reglen i aftl. § 39, 2. pkt. Spillerummet for, hvad der således er "muligt", må dog være forholdsvis snævert. Det forhold, at der kommer et uventet stort antal accept-meddelelser, bør ikke i almindelighed indebære, at den erhvervsdrivende kan frigøre sig fra den aftale, accepten udvirker. Det må således tages i betragtning, at den erhvervsdrivende kan undgå den slags situationer *enten* ad teknisk vej ved at spærre for accept-kvitteringer fra og med det tidspunkt, varen er udsolgt, *eller* juridisk (ved at angive, at der indenfor bestemte tidsfrister alene vil kunne leveres indenfor de grænser, der sættes af et eksisterende oplag). At det vil være forbundet med særlige omkostninger for den erhvervsdrivende at foretage en løbende opdatering af hjemmesiden med henblik på at melde varen udsolgt, må i den forbindelse spille en mindre rolle. Det kan i øvrigt ikke antages at være i overensstemmelse med god markedsføringsskik at afgive tilbud til almenheden fra Internet-hjemmesider uden løbende at opdatere disse.

Klausuleringer

Hvis dette resultat antages, opstår herefter spørgsmålet, om den erhvervsdrivende vil kunne klausulere sit "tilbud" således, at det i juridisk henseende netop ikke skal betragtes som et binden-

de tilbud, men alene som en opfordring til at gøre tilbud – f.eks. gennem klausuler herom eller om, at ydelsen kun kan leveres "så længe lager haves" el.lign. Som udgangspunkt må svaret på dette spørgsmål være ja. Ifølge § 1 i de nordiske aftalelove er det klart, at reglerne om aftalers indgåelse i lovenes kapitel 1 kun kommer til anvendelse, for så vidt ikke andet følger af tilbuddet (eller svaret herpå) eller af handelsbrug eller anden sædvane. Tilsvarende er antaget ved Forbrugerklagenævnets afgørelse i *Forbrugerredegørelsen 2002-2003.160* om en Internet-butik, som fungerede ved hjælp af en "indkøbskurv", hvori kunden kunne placere sine indkøb. Ved bestillingen afgav systemet bl.a. en meddelelse til kunden om, at "vi bliver nødt til at få din accept på, at du ikke opfatter e-mailen som en juridisk bindende ordrebekræftelse, hvorved en aftale er indgået. Men alene et elektronisk svar fra en computer til at fastslå, om det rigtige er indtastet. Du accepterer derfor at vi kan slette ordren, såfremt varen er udgået eller der er store prisfejl m.m." Fire af Forbrugerklagenævnets medlemmer fandt, at Internet-forretningen dermed på tilstrækkelig tydelig måde havde tilkendegivet, at prisangivelserne på hjemmesiden alene indeholdt en opfordring.

Modifikationer i dette resultat må dog gøres i tilfælde, hvor forbeholdet ikke fremtræder med tilpas tydelighed. At skrive et forbehold om, at "Alle tilbud på XYZ-firmas hjemmeside er først bindende, når de er accepteret af XYZ" på en særlig undermenu med oplysninger "Om virksomheden" eller "Almindelige forretningsbetingelser", er således næppe tilstrækkeligt, når den almindelige bruger af hjemmesiden ikke kan forventes at studere sådanne vilkår før aftaleindgåelsen.

Det kan ikke udelukkes, at de konklusioner, der er anført ovenfor i teksten, må modificeres indenfor bestemte brancheområder, f.eks. på områder hvor der indgås aftale efter auktionslignende vilkår, jf. ovenfor i afsnit 4.b om de såkaldte online-auktionshuse. I øvrigt bemærkes, at de situationer, hvor den erhvervsdrivende må formodes at løbe de største risici for omkostningskrævende, uforudsete aftalebindinger, efter omstændighederne kan løses efter obligationsrettens almindelige regler om umulighed og *force majeure*.

19.2.b. Point and click-aftaler

Som grundlag for de aftaler, der indgås via hjemmesider, forekommer det ofte, at den erhvervsdrivende præsenterer brugeren for et detaljeret sæt standardvilkår, som brugeren anmodes om at læse og bekræfte sin indforståelse med gennem klik på musen på en særlig "OK"-ikon. Aftaler indgået på denne måde omtales ofte

som "point and click"-aftaler. Sådanne aftaler giver anledning til spørgsmål om, hvilken aftaleretlig gyldighed der er forbundet med denne accept, navnlig når der er tale om meget omfattende og komplicerede aftalevilkår.

Sammenlignes sådanne aftaler med den form for aftaleindgåelse, der sker ved brug af standarddokumenter, vil der ofte være forskel såvel *objektivt* i omfang og detaljeringsgrad (vilkår, der trykkes på en hjemmeside, vil ofte være mere detaljerede end på papir) som *subjektivt* i henseende til den manifestation af vilje, der markerer tiltrædelsen (teknikken gør det muligt at tvinge brugeren igennem samtlige bestemmelser, inden der klikkes OK). Ligeledes kan man pege på, at den aftale, der indgås ved hjælp af et tastetryk eller aktivering af en mus, ofte vil adskille sig fra de klassiske former for aftaleindgåelse (ved håndslag, underskrivelse af kontraktsdokumenter eller andre klart forpligtende erklæringer) i henseende til *fastheden* af den viljeserklæring, der giver grundlag for den aftaleretlige forpligtelse: Om et museklik i den konkrete situation kan siges at manifestere samme grad af forpligtelse som andre pligtmanifestationer, beror på sædvanedannelsen på området, men denne er fortsat i sin vorden.

Det må i dag betragtes som usædvanligt, om *et enkelt tastetryk* fra forbrugerens side skulle blive søgt håndhævet som et bindende løfte. Almindeligvis forudsætter sådanne pligterklæringer, at forbrugeren har gennemført en flerhed af indtastninger, der blandt andet indebærer svar på udtrykkelige spørgsmål til forbrugeren om, hvorvidt han eller hun på det pågældende grundlag ønsker at forpligte sig. Det kan ikke udelukkes, at denne netpraksis vil ændre sig, f.eks. hvis – og når – det bliver almindeligt at foretage mikrobetalinger på nettet. I en situation, hvor forbrugerens betalingsforpligtelse er opfyldt, i og med at en mikrobetaling er gennemført, vil den erhvervsdrivendes incitament til at præcisere overfor forbrugeren, at der indtræder en juridisk forpligtelse, alt andet lige være mindre.

Bortset fra disse tilfælde er det dog den almindelige hovedregel, at en digital viljeserklæring, der fremkommer som svar på en meddelelse (f.eks. i form af en hjemmesidetekst), der utvetydigt fastslår forpligtelsens rækkevidde, er gældende. Det bør i den forbindelse tages i betragtning, at den part, der studerer vilkårene på en hjemmeside, ofte vil have langt lettere ved at sætte sig ind i aftalens småttrykte vilkår end den, der i en salgssituation præsenteres for et aftaledokument med henblik på underskrivelse.

E-handelslovens § 12, søger at afbøde denne risiko for retlig tvivl ved at give særlige regler om ordreafgivelse. Ifølge stk. 1 E-handelslovens § 12

skal tjenesteyderen uden unødig forsinkelse elektronisk bekræfte modtagelsen af en elektronisk ordre. En elektronisk ordre og den elektroniske ordrebekræftelse (jf. stk. 1) anses som modtaget, når adressaterne har adgang til disse, jf. stk. 2. Bestemmelsen tilsigter ikke at regulere aftaleindgåelsen. I et tidligere udkast til direktivet havde Kommissionen ønsket en sådan harmonisering, men dette ønske vandt ikke tilslutning, jf. *Jan Trzaskowski* i U2000B.648. Derfor må den primært betragtes som en markedsføringsregulering, der i tråd med de øvrige led i loven tilsigter at skabe klarhed. Således skal den afsendte ordrebekræftelse ikke (nødvendigvis) tjene til at fastslå, hvornår aftalen er indgået. Men når den er afgivet, giver den tjenestemodtageren en faktisk mulighed for at vurdere overensstemmelsen mellem ordreafgivelse og ordrebekræftelse, som herefter kan danne grundlag for aftaleretlige modtræk, hvis nærmere indhold beror på den specifikke aftalesituation.

Om elektronisk aftaleindgåelse hedder det i pkt. 4 i den fælles holdning, de nordiske forbrugerombudsmænd har afgivet i december 1998:

"Aftalefunktionen bør være klart adskilt fra andre funktioner.

Den erhvervsdrivende bør give en forsvarlig vejledning om produktets/ydelsens egenskaber, herunder brugsegenskaber, holdbarhed, sikkerhedsrisici og vedligeholdelsesmuligheder.

Inden elektronisk aftaleindgåelse bør forbrugeren have fuld klarhed over samtlige vilkår, herunder hvad forbrugeren bestiller og til hvilke priser (inklusiv transportomkostninger, skatter og afgifter mv.). Den erhvervsdrivende bør endvidere tydeligt oplyse, om forbrugeren har en aftalt eller lovbestemt fortrydelsesret.

Den erhvervsdrivende bør give en ordrebekræftelse til forbrugeren. Ordrebekræftelse bør sendes pr. fysisk post eller eventuelt pr. elektronisk post, hvis forbrugeren udtrykker ønske herom.

Forbrugeren bør have mulighed for ubesværet at opbevare alle givne informationer i fysisk eller maskinlæsbar form."

Konklusion

På dette grundlag forekommer det velbegrundet at konkludere, at gyldigheden af en "digital viljeserklæring" fra forbrugerens side er betinget af, at der forudgående er givet forbrugeren tydelig meddelelse om virkningerne af denne forpligtende meddelelse. Der kan således næppe herske tvivl om, at en forbruger i almindelighed vil have gode muligheder for at fragå en viljeserklæring, der er afgivet gennem et utilsigtet tastetryk, som blev effektueret på grund af en uklar brugergrænseflade og under omstændigheder, hvor forbrugeren ikke havde mulighed for at foretage øjeblikkelig fejlrettelse.

Der foreligger efterhånden en righoldig praksis fra USA om sådanne aftaler, og praksis er blevet stadigt mere imødekommende overfor antagelsen af sådanne aftaler. Se herved *CompuServe, Inc. v. Patterson*, 89 F.3rd 1257 (6th. Cir., 1996), *Hill v. Gateway*, 105 F.3d 1147 (1997), samt *Simon v. RealNetworks Inc.* og *Lieschke v. RealNetworks Inc.*, der begge opretholdt en klausul om voldgiftsbehandling i en *point and click*-licensaftale. En appelret i New Jersey har den 2. juli 1999 opretholdt en *click wrap*-aftale i relation til et heri indeholdt vilkår om forumvalg, *Steven J. Caspi et al. v. Microsoft Network*, 323 N.J. Super. 118, 732 A.2d 528 (1999). Afgørelsen er bl.a. begrundet med, at vilkåret – der fremtrådte på en blandt mange skærmsider – ikke i sig selv kunne rammes af en ugyldighedsgrund, idet det var "reasonable, clear and contains no material misrepresentation." Se ligeledes *Carnival Cruise Lines v. Shute*, *M.A. Mortensen Company v. Timerline Software et.al* (Washington Sup.C., May 4, 2000) samt den canadiske afgørelse fra Ontarios Superior Court of Justice af 8. oktober 1999 i sagen *Rudder v. Microsoft Corp*.

19.2.c. Inkorporering af vilkår

Problemstillingen

Som tidligere nævnt kendetegner det den information, der fremtræder på Internet-hjemmesider, at den kan befinde sig på vidt forskellige web-servere, hvis tekniske beskaffenhed og geografiske beliggenhed brugeren ikke kender: Brugeren surfer fra hjemmeside til hjemmeside ved i teknisk forstand at anmode de enkelte værtscomputere om at sende et antal bits, som brugerens computer fremviser som et skærmbillede eller et udprint med tekst og grafik mv. Men hvorfra kilden til disse oplysninger befinder sig, vil ofte fortone sig. I stedet for at lade brugeren modtage en fuldstændig informationsmængde, vil informationsleverandøren kunne nøjes med at angive en link til en database, hvor brugeren kan hente mere information, hvis dette ønskes. Denne praksis kan f.eks. understøtte aftaleindgåelse. Sådanne links kan ligefrem være teknisk nødvendige, når gældende standarder kun tillader en bestemt mængde juridisk tekst, f.eks. 64 karakterer. Dette problem gør sig gældende i relation til certifikater udstedt om identiteten af offentlige nøgler i et public key krypteringssystem efter den for dette område fremherskende *X.509*-standard.

Varianter

Der findes mange måder at inkorporere vilkår på, jf. *Chissick & Kelman* (1999), s. 86 ff. Dette kan f.eks. ske gennem *linking* til en side, hvor de fuldstændige vilkår fremgår ved etablering af en *dialogboks*, hvori vilkårene fremtræder (som et vindue ved siden af andre vinduer, som brugeren har aktiveret på skærmen), ved *udtrykkelig angivelse* nederst på selve den side, hvor brugeren

befinder sig (men uden for dennes umiddelbare synsfelt) og ved angivelse af en adresse, hvor brugeren kan lede, men *uden link* hertil.

Papirets verden

Den skitserede praksis kan anskues som en slags digital parallel til de småttrykte vilkår, som man finder på bagsiden af talrige standardkontrakter: Den inkorporerede information vil da udgøre en slags digital ækvivalent til papirdokumentets bagside. Hvis A i papirets verden tilbyder B en vare til en bestemt pris og på vilkår som anført i en *vedlagt standardformular*, bliver disse vilkår utvivlsomt en del af aftalen ved B's accept, se hertil *GA* s. 365 ff. Det samme gælder, hvis tilbuddet gives telefonisk, og A henviser til de vilkår, B på forhånd kender eller på egen hånd ubesværet kan finde, f.eks. i brochurematerialer, kataloger og prislister eller ved at læse opslag i forretningslokaler, sml. herved *U 1985.23 H* om et vilkår om afbestillingsgebyr, der var vedlagt en ordrebekræftelse. Et modsat resultat ville være ensbetydende med, at B kunne spekulere i sit ukendskab til de vedlagte vilkår og efter forgodtbefindende gøre vilkår gældende eller lade være.

Vedtagelsestærsklen sættes dog forskelligt, alt efter hvilken transaktion der er tale om, og hvilke vilkår formularen rummer, jf. nærmere *Jesper Kaltoft og Christoffer Søborg-Hansen* i Justitia, oktober 1998, s. 47 ff., *Lynge Andersen m.fl.* (1997), s. 81 f., *Torvund*: IT-kontrakter (1997), s. 262 f. (om voldgiftsklausuler) og *GA* s. 364 f. Ligeledes har det betydning, om vilkåret er sædvanligt. Ved dommen i *TBB 1999.126* henviste en underentrepriseaftale til en anden aftale, hvori AB92 var vedtaget. Retten fandt i dette tilfælde af inkorporation i "anden potens", at AB92 måtte anses for vedtaget mellem parterne, og at sagen følgelig måtte afvises fra domstolene som rettelig henhørende under voldgift. Retten begrunder ikke sit resultat; men det har formentlig spillet ind, at begge parter befandt sig i byggebranchen, hvor AB92 er både udbredt og velkendt. Se i øvrigt om problemstillingen i relation til afgivelse af digital signatur, *Stephen S. Wu*: Incorporation by Reference and Public Key Infrastructures: Moving the Law Beyond the Paper-Based World, 38 Jurimetrics J. 317-343 (1998).

Diskussion

Man kan diskutere, om anvendelsen af det elektroniske medium i sig selv indebærer, at der skal stilles skrappere vedtagelseskrav til "inkorporering" på nettet. I den retlige vurdering af dette spørgsmål bør der dog anlægges en praktisk betragtning: Når en bruger har været i stand til at identificere en hjemmeside, hvorfra han eller hun har interesse i at erhverve varer eller tjenesteydelser, må brugeren som udgangspunkt også være parat til at acceptere mediet ud fra dets egenskaber, og herunder læse, hvad der står på skærmen! En sådan regel forekommer ikke mindst velbegrundet

i tilfælde, hvor vilkårene fremstår i kort og klar form og på en måde, der uden vanskelighed muliggør udprintning. Der kan næppe opstilles skarpe kriterier for, hvornår inkorporering af vilkår må anses for aftaleretligt bindende efter nordisk aftaleret, men alene skitseres nogle retningslinjer. For en mere uddybende gennemgang af problemerne om vedtagelse af software-klausuler herunder i forbindelse med nethandel henvises til *Jesper Kaltoft* og *Christoffer Søborg-Hansens* førnævnte afhandling.

Fra amerikansk praksis foreligger bl.a. en afgørelse i *Specht v. Netscape Communications and America Online, Inc.* (306 F.3d 17), hvor brugeren af et Netscape-program som betingelse for at downloade programmet havde meddelt et accept-click på et sæt vilkår, der inkorporerede en licensaftale med voldgiftsklausul. Appelretten fandt, at kunden ikke hermed havde fået "reasonable notice" om licensaftalen og den heri indeholdte voldgiftsklausul. Heroverfor kan nævnes den vidtgående afgørelse, højesteret i den canadiske provins Ontario har afsagt den 22. februar 2002 i sagen *Kanitz v. Rogers Cable Inc*. Sagen var rejst som en class action (dvs. et søgsmål på vegne af en flerhed af brugere) mod en større canadisk leverandør af Internet-højhastighedskabelforbindelser. Under sagen gjorde Rogers Cable Inc. gældende, at der forelå en gyldig voldgiftsklausul, hvorfor sagen måtte afvises. Voldgiftsklausulen påstodes indeholdt i en brugeraftale, hvis indledende bestemmelse gav Rogers Cable Inc. ret til ensidigt at ændre aftalen til enhver tid. Dette skete i november 2000, hvor der blev indsat en voldgiftsklausul, hvorved enhver uoverensstemmelse – i mangel af udtrykkelig aftale – skulle afgøres endeligt af en enkelt voldgiftsdommer. Retten fastslog, at den indgåede aftale var bindende, hvorfor søgsmålet ved domstolene skulle afvises: "It does not seem unreasonable for persons who are seeking electronic access to all manner of goods, services and products along with information, communication, entertainment and other resources, to have the legal attributes of their relationship with the very entity that is providing such electronic access, defined and communicated to them through that electronic format."

§ 11, stk. 3, i forbrugeraftaleloven (lov nr. 451 af 6. september 2004 om visse forbrugeraftaler) kan læses som et forbud mod inkorporering af vilkår, når den fastslår, at de i stk. 1 nævnte oplysninger (om navn, varens kvalitet, pris, vilkår og fortrydelsesret mv.) skal gives i rimelig tid, inden der indgås en aftale og "skal være klare, tydelige og forståelige". På den anden side tillader bestemmelsen også, at oplysningerne skal gives på en måde, "som er egnet under hensyn til den anvendte kommunikationsteknik, og som tager særligt hensyn til umyndige personer". Bestemmelsen kan ikke siges at have gjort op med muligheden for at inkorporere vilkår. En inkorporering, der gennemføres så-

ledes, at der ikke er tvivl om indholdet af de inkorporerede vilkår (f.eks. fordi disse forventes alment kendte), kan næppe anses for stridende med denne regel. Om links, der søger at inkorporere mindre udbredte eller kendte vilkår, opfylder kravene, må formentlig bero på disses sædvanlighed og rimelighed.

Bestemmelsen er indført på baggrund af art. 4, stk. 2, i direktiv 97/7/EF om forbrugerbeskyttelse i forbindelse med aftaler vedrørende fjernsalg. I betragtning af problemets praktiske betydning må spørgsmålet forventes at finde sin afgørelse under en præjudiciel forelæggelse for EF-domstolen.

19.2.d. Automatiseringer

Teknisk mellemled

Hvis den, der ønsker at afgive en viljeserklæring, vælger at effektuere afgivelsen ved hjælp af et automatisk system, der under givne tekniske forudsætninger afgiver meddelelser til omverdenen, der er egnede til at blive opfattet som aftaleretligt forpligtende, hæfter den pågældende som udgangspunkt for erklæringen i den skikkelse, hvori den rent faktisk afgives, på samme måde som hvis den var afgivet af ham selv via masseudsendte breve eller ved brug af andre tekniske mellemled. Fejlen ligger inden for hans egen kontrolsfære, og afgiveren har selv en interesse i, at der knyttes tillid til de meddelelser, der udgår fra denne kontrolsfære. Mod sådanne forvanskninger er aftl. § 32, stk. 2, derfor uanvendelig. Afgiveren må i givet fald gå frem efter bestemmelsens første stykke, se hertil afsnit 19.3.a.

Dette resultat gælder uanset om meddelelsen afgives med eller uden digital signatur. LES foreskriver således ikke særlige regler om karakteren af den hæftelse, afgiveren af en avanceret elektronisk signatur forsynet med eller uden et kvalificeret certifikat, er underlagt. Resultatet svarer derimod til UNCITRAL-modellovens art. 13, der fastslår, at en digital meddelelse må anses for afgivet af afsenderen, hvis den er sendt af en person, som havde beføjelse til at handle på afsenderens vegne i relation til den pågældende meddelelse eller af et informationssystem, som er programmeret til at operere automatisk på vegne af afsenderen. I overensstemmelse med det almindelige princip om, at den ondtroende ikke vinder ret, se hertil *GA* s. 473 f., gøres der dog forbehold for ond tro: "The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received."

Intelligent mellemled

Som hermed antydet kan IT-systemer programmeres til at disponere med virkning for en part med sigte på, at denne bliver forpligtet på samme måde, som hvis han selv havde disponeret med

det pågældende indhold. Dette kan have praktisk betydning i fuldautomatiske EDI-systemer, der er sat op til at disponere i overensstemmelse med aftalekriterier, der på forhånd er lagt ind. Sådanne transaktioner vil typisk være baseret på forudgående aftaler (såkaldte kommunikationsaftaler). En lignende situation kan forekomme ved brug af såkaldte søgeagenter ("*search agents*") på nettet, der giver en potentiel kunde mulighed for at identificere e-handlende med henblik på at indhente det mest fordelagtige tilbud. Der er dog endnu ikke praksis for også at sætte en "contracting agent" til automatisk at afgive købsordren.

Hvis en sådan praksis bliver udbredt, hvilket ikke er usandsynligt, opstår spørgsmålet, om programmet som sådant kan udvirke en særlig type forpligtelse for besidderen af programmet, f.eks. når programmet afgiver en besked på indehaverens vegne om, at denne vedkender sig de licensvilkår, der f.eks. fremgår af en *point and click*-aftale, se hertil ovenfor i afsnit 19.2.b., hvor det antages, at aftalevilkår, som modtageren ikke forventes at have studeret i detaljer inden aftaleindgåelsen, kun bliver forpligtende i det omfang de indeholder sædvanlige vilkår. En part, der ved hjælp af en automatiseret søgeagent lokaliserer en modpart og som gennem søgeagentens mekanismer udvirker afgivelsen af en accept på sådanne web-pact vilkår, vil som udgangspunkt kun blive bundet heraf (i overensstemmelse med de foran anførte principper herfor om fejltransmission mv.), i det omfang det juridiske indhold af disse vilkår er sædvanligt og afbalanceret.

Forbrug

Principielt adskilt fra dette problem er spørgsmålet, hvornår den, der ifølge aftale har pligt til at betale for en kommunikations- eller informationsydelse efter forbrug, hæfter for et uønsket forbrug, som f.eks. udvirkes af indbudte eller uindbudte gæster eller ved utilsigtet installation af programmer, der får computeren til selv at kalde op. Dette spørgsmål må finde sin afgørelse efter en fortolkning af aftalens regler. Udgangspunktet vil normalt være, at abonnenten hæfter for ethvert forbrug – tilsigtet såvel som utilsigtet. Begrundelsen er, at abonnenten er nærmest til at gardere sig imod det utilsigtede forbrug, og at forbruget i alle tilfælde repræsenterer en udgift – eller forventet indtægt – for leverandøren. Problemstillingen er den samme, hvad enten det pågældende forbrug har kommunikativ eller fysisk karakter. Til illustration kan nævnes dommen i *U 1999.892 V*, hvor en elektricitetskunde hæftede for det forbrug, der blev registreret over hans måleapparat, selv om dette notorisk var udvirket af dennes udlejer. Omvendt hæftede ejeren af en lejlighed ikke for sin fremlejers brug af teleydelser i *JÅF 2000.106*, da ejeren ikke havde

nogen aftale med teleselskabet. Se i øvrigt om denne problemstilling *Karstoft* (2004), s. 101 ff.

19.3. Ugyldighed og tilbagetræden

19.3.a. Fejlskrift

Problemstillingen

Risikoen for fejl opstået ved udveksling af erklæringer om retlig forpligtelse er velkendt. Det skrevne ord kan være ulæseligt, f.eks. pga. typografiske uklarheder. Det talte ord kan være uklart talt og udsat for støjkilder mv. Når en part – uden at dette har kunnet bebrejdes den pågældende – herigennem bliver ophav til en "viljeserklæring", der ikke udtrykker hans vilje, opstår spørgsmålet om fordelingen af risikoen herfor. Denne risiko forstærkes, når kommunikationsprocessen foregår adskilt i tid og rum. I det omfang ingen bærer *ansvaret* for sådanne fejl (hvorved der enten kan tænkes etableret en aftaleforpligtelse ved passivitet mv. eller et erstatningsretligt ansvar), må *risikoen* for en sådan fejltagelse placeres hos enten afsender eller modtager. Denne problemstilling hører til i den basale aftaleretlige hensynslære, se hertil *GA* s. 45 ff. I denne vurdering spiller to modstående hensyn ind. Et *tillids- eller forventningshensyn* vil lægge vægt på sikkerheden i omsætningen og placere risikoen hos afsenderen, der dermed tilskyndes til at sikre kvaliteten af sine meddelelser. Efter et *viljeshensyn* lægges der vægt på afsenderens interesse i ikke at blive bundet længere end han har haft ønsker om.

Aftl. § 32

Dansk aftaleret kan ikke siges at have valgt et af disse principper frem for et andet. Aftaleloven bygger på en kombination af de to teorier. Ifølge aftl. § 32, stk. 1, er den, der afgiver en viljeserklæring, som ved fejlskrift eller anden fejltagelse fra hans side har fået et andet indhold end tilsigtet, ikke bundet ved erklæringens indhold, hvis den, til hvem erklæringen er afgivet, indså eller burde indse, at der forelå en fejltagelse. Reglen angår den form for forvanskning, der sker under selve *afgivelsen* af viljeserklæringen, f.eks. trykfejl mv., jf. ordene "fra hans side". Risikoen for en sådan forvanskning falder på afgiveren af erklæringen, og det er også ham, der skal godtgøre, at modtageren var i ond tro. Indtræder forvanskningen under erklæringens *befordring* fra afsender til modtager, gælder reglen i § 32, stk. 2, hvorefter afgiveren af erklæringen ikke er bundet af den i sin forvanskede form. Meddelelsen anses i disse tilfælde ikke for afgivet af afsenderen.

Efter sin ordlyd gælder stk. 2 kun meddelelser, der transmitteres ved brug af telegrafi eller mundtligt fremføres ved bud; men den må formentlig anvendes analogt på andre medier til telekommunikation, da de væsentligste hensyn bag bestemmelsen også gør sig gældende i disse henseender. Forvanskninger af skrevne meddelelser, der sendes i kuvert, er uden praktisk betydning. Bestemmelsens to eksempler på telekommunikation svarer til dem, der var fremherskende ved aftalelovens givelse i 1917. Derfor kan eksemplerne vanskeligt læses som udtryk for nogen udtømmende angivelse af, hvilke medier til teletransmission der kan falde ind under stk. 2.

Spørgsmålet har været indgående diskuteret; men der foreligger endnu ingen retsafgørelser om det. Den opfattelse, der udtrykkes ovenfor, er i dag den almindelige herhjemme, se herved *Einersen* (1992), s. 72, *Kofod Olsen* i U1992B.402, *Andersen & Nørgaard* (2001), s. 176, og *Karstoft* (2004), s. 106 ff. med henvisning til yderligere litteratur. I en større analyse i Festskrift til Kurt Grönfors (Stockholm, 1991), s. 403 ff., lader *Lena Sisula-Tulokas* spørgsmålet henstå som uafklaret. Holdningen er overvejende modsat i svensk ret, se således SOU 1996:40, s. 130 f., *Hultmark* i Festskrift til Jan Ramberg (1997), s. 260, note 9, og *Lindberg & Westman* (1999), s. 56 f. (der påpeger, at fejlen modsat § 32, stk. 2-situationen ikke kan henføres til en udenforstående persons fejl), men herimod *Lehrberg*: Omförhandlingsklausuler (1999), s. 45-47 i note 51. *Røsæg* i Festskrift til Karnell (1999), s. 678 ff. synes nærmest at tilslutte sig den danske opfattelse. De argumenter, der har været anført mod at anvende telegrafreglen på telefax, er, *at* fejlskrift ikke kan forekomme i telefax, og *at* telefax-transmission ikke involverer noget selvstændigt mellemled (telegrafisten), der kan begå fejl. Begge indvendinger kan tilbagevises. Når telefax-transmission sker via et såkaldt faxmodem, altså ved overførsel fra computer til computer, er der rige fejlmuligheder, f.eks. ved at karakterer ændres eller udelades. Dernæst frembyder nutidens marked for telekommunikation talrige ydelser, der – omend ikke i "realtid" – åbner risici for, at der sker fejl i overførte meddelelser. At der ikke er noget mellemled involveret i telefax-transmission er heller ikke rigtigt. Der kan påvises talrige *led* i hele det forløb, der understøtter overførsel af en elektronisk meddelelse fra A til B, som tredjeparter med hvem enten A eller B har et kontraktsforhold til, har indflydelse på. Eksempelvis kan den part, der *implementerer* en kommunikationsløsning – eller en central komponent heri – spille en sådan rolle.

Indsigelsen efter aftl. § 32, stk. 2, er en stærk ugyldighedsgrund. At meddelelsen er forvansket kan altså gøres gældende, selv om den, til hvem erklæringen er afgivet, var i god tro om, at der forelå en fejl. For at afgiveren af en meddelelse, som er forvansket på denne vis, kan frigøre sig fra den, skal han give meddelel-

se uden ugrundet ophold, efter at han har fået kundskab om forvanskningen. Undlader han dette, er han bundet ved erklæringen i den skikkelse, hvori den kom frem, såfremt modtageren var i god tro, aftl. § 32, stk. 2, 2. pkt.

UNCITRAL

UNCITRAL's modellov om Electronic Commerce tager ikke udtrykkeligt stilling til spørgsmålet om fejlskrift, men art. 13, stk. 5, regulerer følgerne af, at der indtræder fejl undervejs i transmissionen. I disse tilfælde er modtageren ikke berettiget til at støtte ret på meddelelsen, hvis modtageren vidste eller burde vide, at der var tale om en fejl i overførelsen. Er dette ikke tilfældet, kan modtageren derimod støtte ret herpå (i bestemmelsens formulering: "entitled to regard the data message as received as being what the originator intended to send"), hvilket – afhængigt af hvad man lægger i dette begreb – formentlig peger på et andet resultat end, hvad der vil følge af aftl. § 32, stk. 2.

19.3.b. Tilbagetræden

Som følge af den hastighed, hvormed edb-meddelelser udveksles, vil den kommunikerende part ofte komme til at afgive uovervejede erklæringer, som han siden ønsker sig løst fra. Dette kan i sig selv være et argument imod at lade digitalt signerede løfter ækvivalere med nedfældne og underskrevne løfter, som i og med deres fremtræden er omgærdet af en højere grad af respekt og heraf følgende uafviselighed. Udover risikoen for, at en digital signatur afgives ved en fejltagelse eller af en person, der uretmæssigt har fået adgang til den private nøgle, er risikoen for, at afgiveren fortryder sin disposition, generelt større i relation til digital teknik end i papirets verden. Indtil der har dannet sig faste sædvaner for, hvorledes digitale meddelelser afgives og signeres, vil afgiveren ikke have samme fornemmelse af at sidde med papiret foran sig, som man har i papirets verden. Netop denne til dels irrationelle forestilling om det skrevne som noget helligt, giver papirdokumentet en særlig kvalitet.

Sådanne risici ved den digitale signatur kan kun til dels imødegås gennem sikkerhedsregler. Ønsker man at anerkende en digital signatur som ligeværdig med underskriften på et papirdokument, må retsvirkningerne være de samme. Ønsker den forpligtede at smyge de forpligtelser af sig, som signaturen frembringer, må dette ske på grundlag af de almindelige aftaleretlige regler.

Re integra-reglen

Aftl. § 39, 2. pkt., giver i begrænset omfang mulighed for, at en aftalepart frigøres for sin forpligtelse kort efter, at den er etableret. Reglen giver under særlige omstændigheder hjemmel til at

tage hensyn til den kundskab, en løftemodtager har fået, inden løftet har virket bestemmende på ham, jf. nærmere herom *GA* s. 189 ff. Denne hjemmel kan afgiveren af en viljeserklæring efter omstændighederne påberåbe sig, hvis systemet i sin grænseflade ikke skaber sikkerhed for, at en disposition (f.eks. en bestilling el.lign.) er udtryk for afsenderens definitive vilje. I fuldautomatiske EDI-systemer, hvor tilbud og svar på tilbud afgives ud fra på forhånd fastsatte programinstruktioner, må spillerummet for en sådan tilbagekaldelse dog være beskeden jf. tilsvarende *Lindberg & Westman* (1999), s. 55.

19.3.c. Fjernsalg

Forbrugeraftaler

Princippet om aftalers forbindende kraft er undergivet en række modifikationer på forbrugerområdet, hvor det ofte forekommer, at forbrugeren fortryder sit løfte, f.eks. fordi han er blevet overrumplet eller ikke kunne overskue dets rækkevidde. For at værne forbrugere mod sådanne dispositioner giver lov nr. 451 af 9. juni 2004 om visse forbrugeraftaler ("forbrugeraftaleloven") forbrugeren en særlig *fortrydelsesret*. Da de væsentligste retsvirkninger af at tilsidesætte disse forpligtelser er aftaleretlige, behandles reglerne oversigtsmæssigt.

Markedsføringsforbud

Loven opstiller bl.a. et forbud mod, at erhvervsdrivende uden forudgående anmodning retter personlig eller telefonisk henvendelse til forbrugere på deres bopæl, arbejdsplads eller andet sted, hvortil der ikke er offentlig adgang, med henblik på straks eller senere at opnå tilbud eller accept af tilbud om indgåelse af aftale, lovens § 6, stk. 1. Et løfte afgivet af forbrugeren ved en henvendelse i strid med reglerne i § 6 er *uforbindende* for forbrugeren; men ønsker han det, kan forbrugeren fastholde aftalen, lovens § 7.

Selv om forbuddet mod *telefoniske* henvendelser kan siges at åbne døren på klem til en regulering af den uanmodede *telematiske* henvendelse (herunder gennem brug af elektronisk post og SMS-beskeder), er der næppe grundlag for at anlægge en sådan udvidende fortolkning. Baggrunden for forbuddet ligger primært i den psykologiske overrumpling, der gør sig gældende i en samtale. Denne risiko består ikke i samme omfang, når en henvendelse sker telematisk. Traditionelt har man ligeledes antaget, at telegrafiske meddelelser mv. falder uden for reglen.

Fjernsalg

Denne uklarhed er imidlertid nu reduceret gennem de særlige regler, der er indført om såkaldt *fjernsalg*, jf. lovens §§ 11-15. Reglerne herom, der sondrer mellem om fjernsalget angår fi-

nansielle eller ikke-finansielle tjenesteydelser, pålægger den erhvervsdrivende at fremkomme med en række yderligere oplysninger inden aftale indgås. Forbrugeren har på ethvert tidspunkt under aftaleforholdet ret til efter anmodning at få udleveret aftalevilkårene på papir, jf. § 15.

Fortrydelsesret

Som allerede antydet herved ligger fjernsalgsdirektivets centrale omdrejningspunkt i reglerne om fortrydelsesret, jf. forbrugeraftalelovens §§ 17-22. Ved fjernsalg gælder således en generel fortrydelsesret, der dog er forsynet med en række undtagelser og begrænsninger. Vil forbrugeren bruge fortrydelsesretten, skal han benytte den fremgangsmåde, der følger af § 19, stk. 1 og 2, inden for en nærmere angiven frist. *I almindelighed* er denne på 14 dage (ved aftaler om individuel pensionsordning dog inden for en frist på 30 dage), jf. § 18, stk. 1. Ved *fjernsalg af varer* udløber fristen senest 3 måneder efter den dag, hvor forbrugeren fik varen, det første parti heraf eller den første levering i hænde, jf. § 18, stk. 3. Ved fjernsalg af (ikkefinansielle) *tjenesteydelser* udløber fristen senest 3 måneder efter aftalens indgåelse, jf. stk. 3. Når der er fortrydelsesret ved fjernsalg af *finansielle tjenesteydelser*, se nærmere § 17, stk. 2, nr. 2-3, gælder den almindelige frist.

Når forbrugeren udnytter fortrydelsesretten, skal han underrette den erhvervsdrivende herom, medmindre der er tale om fjernsalg af varer, hvor den erhvervsdrivende ikke har påtaget sig at afhente varen hos forbrugeren, jf. § 19, stk.1-2. Er der det, skal forbrugeren inden fortrydelsesfristens udløb tilbagesende eller tilbagegive det modtagne til den erhvervsdrivende. Det er tilstrækkeligt for overholdelse af fristen, at underretningen (når den foreligger på papir eller et andet varigt medium, som modtageren har adgang til), er afsendt inden fristens udløb.

19.3.d. Kompetenceoverskridelser

Problemstillingen

Som nævnt ovenfor vil den digitale aftaleindgåelse ofte foregå således, at erklæring og vilje er adskilt fra hinanden på en sådan måde, at selve systemet kommer til at spille en selvstændig rolle for aftaledannelsen. Dermed opstår risikoen for, at systemet "disponerer" på en måde, der strider imod de intentioner, indehaveren havde hertil. Da systemet i sig selv blot er et teknisk mellemled, der måske kan sammenlignes med menneskelige mellemled som f.eks. fuldmægtige eller kommissionærer, er det nærliggende at betragte denne problemstilling som et spørgsmål om virkningen af en *kompetenceoverskridelse*.

Udgangspunktet

Ved vurderingen af, om et IT-system kan spille rollen som fuldmægtig, er det dog vigtigt at fastholde udgangspunktet om, at IT-systemer som sådanne aldrig kan optræde som bærere af rettigheder og forpligtelser, og derfor heller ikke kan optræde med den retssubjektivitet, som aftaleretten forudsætter, at fuldmægtigen besidder. Systemet er en ting, der som sådan ikke kan være genstand for rettigheder og forpligtelser.

Dette udgangspunkt er antaget flere gange i det foregående i relation til andre IT-retlige spørgsmål, f.eks. i afsnit 9.3., hvor det drøftes, om IT-systemet kan optræde som skaber af ophavsretligt beskyttede "værker". Hvor komplekse og menneske-lignende de end kan fremstå, er IT-funktionerne forudbestemte ved den forudgående programmering og ved de elektroniske forløb, der ligger bag. De "er" ikke andet og mere end de menneskelige beslutninger, der udtrykkes ved den programmering, der får systemet til at fungere som det gør. Det problem, man måske kan føle trang til at løse ved at tildele et IT-system en slags personlighed mv., ligger i det såkaldte *Vico-paradoks*, jf. *E&A* s. 146 ff. og oven for i afsnit 2.1.a.: Man forsøger at beskrive en teknologi, som mennesket selv har skabt, og som mennesket derfor også burde kunne forstå. Men denne teknologi er nu blevet så kompliceret, at vi ikke længere forstår den. Som anført a.st. bør Vico-paradokset søges løst ved – som sket i denne fremstilling – at fokusere på relevante tekniske aspekter og foretage en beskrivelse af disse aspekter, der er adækvat for den pågældende retsregel.

"Edb-fuldmagt"?

I Elektronisk aftale- og bevisret (1992), s. 88 ff., har *Eivind Einersen* foreslået, at systemet ("computeren") i sig selv kan optræde som beslutningstager, omend han dog ikke vil tage den konsekvens heraf, at computeren tilsvarende opnår retssubjektivitet. I konsekvens heraf opererer Einersen med begrebet "edb-fuldmagt" (se f.eks. s. 93 f.), idet han sondrer mellem sådanne fuldmagter, der har eller savner særlig tilværelse. At computeren ikke besidder retssubjektivitet spiller efter forfatterens opfattelse ingen rolle, eftersom denne egenskab primært har relevans for fuldmægtigens erstatningsansvar, der i IT-sammenhænge altid kan føres tilbage til menneskelige beslutningsfaktorer i forbindelse med programmering, implementering, brug etc.

Efter min opfattelse giver fuldmagtstankegangen et unødigt forvrænget – og til dels misvisende – billede af de problemer, der har relevans for spørgsmålet om ansvaret for systembetingede fejl i EDI-aftaleslutningen. Formålet skulle være at retfærdiggøre en friholdelse af pseudo-afgiveren, når dennes system fejlagtigt afgiver en meddelelse, som en modtager herefter støtter ret på. Men de resultater, man har behov for at udlede i så henseende, kan ubesværet nås gennem fortolkninger af den "disposition",

der ligger i systemets signal til modtageren, henholdsvis ved brug af reglerne i aftl. § 32, stk. 1, om fejlskrift og anden fejltagelse (i de tilfælde, hvor en meddelelse utilsigtet går afsted, og modtageren indså eller burde indse, at der foreligger en fejltagelse). Når et IT-system sættes til at afgive information overfor omverdenen, der giver tredjeparter grund til at tro, at indehaveren er parat til at lade sig forpligte i overensstemmelse med det således meddelte, må systemet som før nævnt betragtes som et teknisk mellemled, på samme måde som et prisskilt eller som en maskine til frankering og udsendelse af masseforsendelser. Se tilsvarende *Karstoft* (2004), s. 27.

Som omtalt ovenfor indeholder UNCITRAL-modellovens art. 13 en regel om, at en digital meddelelse kan betragtes som afsendt af den angivne afsender, hvis den hidrører fra et informationssystem, der er programmeret af eller på vegne af afsenderen med henblik på at fungere automatisk. Den, der vælger at programmere sit IT-system til at afsende en meddelelse, må altså også bære risikoen for programmeringsfejl, der fører til fejlagtige meddelelser. Bestemmelsen forudsætter, at det disponerede system rent faktisk er programmeret til at afsende den pågældende meddelelse. Indtræder der fejl, som ikke kan henføres til programmeringen, gælder artiklen ikke.

Efter dansk ret vil sådanne tilfælde formentlig skulle bedømmes efter aftl. § 32, stk. 1, eftersom der jo er tale om en fejl på afgiverside. Det føles således rigtigt, at "løftegiveren" er bundet ved fejl, som han har haft mulighed for at forhindre. Problemet er imidlertid, hvornår en fejl ligger inden for denne risikosfære. Aftl. § 32, stk. 2, hviler på et viljesprincip, for så vidt som den beskytter den person, der umiddelbart er uden skyld i den indtrådte forvanskning. Men samtidig indfører den en reklamationsforpligtelse, hvis tilsidesættelse – jf. stk. 2, sidste pkt. – indebærer, at aftale anses for indgået. En sådan reklamationsregel er ikke indbygget i UNCITRAL-modelloven, men vil efter omstændighederne kunne udledes af *aftaleretlige* loyalitetsprincipper. Derimod er det efter dansk ret et åbent spørgsmål, som UNCITRAL-modelloven heller ikke besvarer, om man kan udlede en tilsvarende forpligtelse *uden for kontraktsforhold* på alment grundlag, f.eks. ud fra reglerne om god markedsføringsskik, f.eks. fordi en sådan reklamation vil være pålagt i overensstemmelse med reglerne om "god markedsføringsskik" i mfl. § 1.

19.4. Aftaleregulering

Forud for etableringen af et forretningsforhold på grundlag af EDI træffer parterne ofte aftale om, hvordan de ønsker at effektuere deres dispositioner ved brug af denne kommunikationsform. Foruden regler om, hvordan forskellige typer af information skal håndteres ved aftaleindgåelsen og -opfyldelse (herunder ved logning, deponering, kvittering etc.), kan sådanne aftaler indeholde bestemmelser om opbevarelse og sikring af informationer, lovvalg, alternativ konfliktløsning, erstatningsansvar og om aftalens opsigelse og tilpasning. I den slags aftaler vil parterne ofte ønske at fravige de regler, der søges opstillet nedenfor. Formålet med en sådan fravigelse kan være at opnå en højere grad af *tillid* til de enkelte meddelelser på bekostning af hensynet til den *vilje*, der ikke nødvendigvis er til stede, når der viser sig fejl.

Regulering

Bogføringslovens § 3, stk. 1, nr. 2, lader aftaler om elektronisk dataudveksling være omfattet af systembeskrivelsen, jf. § 14, stk. 2, og dermed også af definitionen på "regnskabsmateriale". Dette indebærer bl.a., at sådanne aftaler er underlagt samme regler om opbevaringspligt som det øvrige regnskabsmateriale.

UNCID-reglerne

Der findes flere tilløb til internationale aftaledokumenter og -standarder, der søger at tage højde for vanskelighederne ved at udveksle løfter, betalingsanmodninger og anden handelsinformation gennem digitale medier. Det Internationale Handelskammer (ICC) vedtog i 1987 de såkaldte UNCID-regler, se ICC publication no. 452 (1988). Reglerne, der bar titlen Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission, har senere været forsøgt revideret. Et forslag til alternativt regelsæt, kaldet URGETS: Uniform Rules and Guidelines for Electronic Trade and Settlement, er blevet opgivet i 2001.

- kvitteringspligt

Det er et gennemgående krav i disse dokumenter, der forsøger at kodificere praksis omkring elektronisk kommunikation, at afsenderen af en digital meddelelse kan foreskrive, at modtageren skal fremsende kvittering for modtagelsen. Dette krav følger af UNCITRAL-modellovens art. 14 og UNCID-reglernes art. 7. Stilles et sådant krav, kan modtageren ikke handle på grundlag af den digitale modtagelse, før han har afgivet kvittering som foreskrevet af afsenderen. Har afsenderen ikke modtaget kvitteringen inden for et tidsrum, der må anses for rimeligt, eller som foreskrives, bør han tage skridt til at opnå den. Resulterer dette skridt fortsat ikke i, at der modtages en kvittering, skal afsenderen give modtageren meddelelse herom.

- notifikationspligt

Hvis en modtager-meddelelse viser sig ikke at være i orden, korrekt eller fuldstændig, er modtageren kun forpligtet til at underrette afsenderen herom snarest muligt, hvis der i forvejen består et kontraktsforhold eller andet særligt pligtforhold mellem parterne. Denne regel genfindes i de internationale instrumenter, der forudsætter, at der foreligger et kontraktsforhold, se således UNCID art. 7, litra c.

TEDIS-kontrakten

Som led i anden fase af EU-Kommissionens TEDIS-program har Kommissionen udarbejdet en EDI-standardkontrakt, som ved Kommissionens henstilling af 19. oktober 1994 om de retlige aspekter af elektronisk dataudveksling (EFT 1994 L338/98) anbefales anvendt af erhvervsvirksomheder og organisationer, der gennemfører deres handelsaktiviteter via EDI. Det kan ses som et udslag af denne aftales internationale udspring og kommissionens ønske om at reducere mulige barrierer mellem medlemsstaterne i sådanne transaktioner, at den i meget detaljeret form tager stilling til en række fundamentale spørgsmål vedrørende aftaleindgåelse, bevishåndtering, persondatabeskyttelse, tekniske krav og ansvar mv. Aftalen er ledsaget af et antal forklaringer til de enkelte bestemmelser. Dernæst er aftalen forsynet med en særlig oversigt over de artikler, der giver mulighed for eller kræver, at parterne indføjer oplysninger.

I EDI-standardkontraktens art. 3 bestemmes det bl.a., at aftaler, der indgås ved hjælp af EDI, skal anses for at være indgået på det tidspunkt og det sted, hvor den EDI-meddelelse, der indeholder accepten af et tilbud, når frem til tilbudsgiverens edb-system. Dette krav må formentlig forstås i overensstemmelse med princippet i UNCITRAL-modellovens art. 6, stk. 1, således at fremkomst kræver, at den pågældende meddelelse er tilgængelig på en sådan måde, at modtageren kan tilegne sig dens informationsindhold. Aftalens art. 5 indeholder kvitteringsregler svarende til de ovenfor nævnte ICC-regler. Herudover pålægger aftalen sine parter at indføre og opretholde sikkerhedsprocedurer og -foranstaltninger til beskyttelse af EDI-meddelelser, således at uvedkommende ikke får adgang hertil, og at meddelelserne ikke ændres, forsinkes, ødelægges eller går tabt (art. 6). Medfører sådanne foranstaltninger, at EDI-meddelelser afvises, eller at der konstateres fejl heri, skal modtageren underrette afsenderen inden for en fastsat tidsfrist. Aftalens art. 8 pålægger dernæst parterne at opretholde en log (kaldet register) over udvekslede EDI-meddelelser. Art. 10 forudsætter, at parterne etablerer et teknisk bilag, der beskriver de tekniske, organisatoriske og proceduremæssige

specifikationer og krav, der skal være opfyldt for at kunne benytte EDI i overensstemmelse med aftalens bestemmelser.

En række andre internationale fora har ligeledes indgået standardaftaler med EDI. Et væsentligt eksempel herpå er den ABA Model EDI Trading Partner Agreement med tilhørende Commentary, der er udsendt af den amerikanske advokatsammenslutning, ABA. Kontrakten og dens kommentarer udgør et af de mest gennemarbejdede paradigmaer for en EDI-handelspartneraftale. Et andet eksempel er den Interchange Agreement, der er udarbejdet af en arbejdsgruppe under *UN/ECE*. Aftalen, der (marts 2000) er under revision, kan hentes på <www.unece.org/cefact/>). Herudover kan nævnes den britiske EDI-Association's "EDI Association standard electronic data interchange agreement" (2nd edition august 1990). Senest har en arbejdsgruppe under den norske Told- og Skattestyrelse udarbejdet en "norsk EDIPRO Interchange Agreement", se herom Rolf Riisnæs i 3 EDI Law Review 165 ff. (1996).

Supplerende litteratur

Med *Roger Henriksen*s undersøgelser fra begyndelsen af 1980'erne er en række af problemerne om retlig disponeren med edb behandlet tidligt i *dansk litteratur*. Se herved hovedværket The legal aspects of paper-less international trade and transport (1982) og samme forfatters indlæg i J1981.285 og NÅR 1984.49. Det er dog først inden for de seneste år, at der tegner sig et klart billede af, hvordan de forhåndenværende teknologier vil blive anvendt i praksis, og der kan nok forventes en del litteratur om emnet i de kommende år. Problemerne om aftaleindgåelse er bl.a. behandlet af *Eivind Einersen*: Elektronisk aftale- og bevisret (1992) og af *Susanne Karstoft*: Elektronisk dokumentudveksling – retlige aspekter (1994), af samme: Elektronisk Aftaleret (2004), af *Ruth Nielsen*: E-handelsret, 2. udg. (2004), kapitel V, af *Kasper Heine m.fl.*: Internetjura (2002), kapitel 2 og af *Lars Stoltze*: Internet Ret, kapitel 5. Spørgsmålet om computerens rolle ved aftaleindgåelsen er behandlet af *C.C. Nicoll*: Can Computers Make Contracts, trykt i Journal of Business Law (1998), s. 35 ff.

Der foreligger efterhånden en omfattende nordisk og udenlandsk litteratur om emnet *digital signatur*. Af danske rapporter henvises til VTU-ministeriets hjemmeside, <www.vtu.dk>. For svensk ret, se *Christina Hultmark* i JT 1996-97, s. 876 ff. Se i øvrigt *Agne Lindberg*: Elektroniska originaldokument och elektronisk signatur. Institut för Rättsinformatik, IRI-rapport 1987:7, tekstsamlingen hos *Rolf Riisnæs (red.)*: Elektronisk betalingsform og forbrukerinteresser I. Arbeidsdokumenter til den nordiske konferansen 1990 (Complex 5/90) og indlæggene ved den nævnte konference hos samme (red.): Elektronisk betalingsform og forbrukerinteresser I. Arbeidsdokumenter til den nordiske konferansen 1990 (Complex 5/91).

Da de IT-baserede kommunikationsformer (EDI mv.) rummer kraftige besparelsesmuligheder inden for forskellige sektorer, samtidig med at deres udførelse beror på den praksis, der udfoldes i disse sektorer, findes der talrige udredninger af mere eller mindre officiøs karakter om de retlige aspekter af disse teknikker. Se herunder *Michael S. Baum & Warwich Ford*: Secure Electronic Commerce (1997) samt *Michael S. Baum*: Electronic messaging. A report of the ad hoc subcommittee on scope of the UCC. American Bar Association (1988) .

Forbrugeraftaleloven er kommenteret af Sonny Kristoffersen (2004). *Fjernsalgsdirektivet* er omtalt i *Johnny Herre*: Nordisk implementering av distansavtalsdirektivet – särskilt ur konsumentskyddssynspunkt. TemaNord 1998:532, af *Susanne Karstoft* i J2000.251 ff. E-handelsdirektivet er omtalt af *Jan Trzaskowski* i U2000B.643 ff.

Kapitel 20. DIGITALE INFORMATIONSYDELSER

20.1. Problemstilling

20.1.a. Nogle sondringer

Ydelsen

Ved "digitale informationsydelser" forstås i det følgende ydelser, der præsteres ved, at leverandøren giver en kunde mulighed for at råde over en digital informationsmængde (et antal "bits"). Det er altså snarere ydelsens form end dens funktionelle indhold, der er afgørende for definitionen. Men netop denne form giver anledning til særlige retlige problemer, når den digitale ydelse skal placeres i det formueretlige regelsystem. Hvor aftaler om køb af traditionelle real- og pengeydelser som regel indebærer en leveringshandling, hvorved en fysisk-faktisk genstand, rede penge eller et betalingsmiddel (i alle tilfælde et antal "atomer") flyttes fra sælger til køber, kendetegnes digitale informationsydelser nemlig ved at blive præsteret under en kommunikationsproces, hvor der *intet materielt* flyttes, eller hvor den genstand (det fysiske medium), der i givet fald flyttes, indtager en helt perifer rolle i den samlede transaktion. Til gengæld må den digitale informationsydelse nødvendigvis præsteres under en *kommunikativ proces*, jf. herom afsnit 2.2.b.: Begge parter må råde over teknisk udstyr, der muliggør den forudsatte tekniske leveringshandling – f.eks. en kommunikationsforbindelse og en computer eller en teknisk nøgle (f.eks. et betalingskort), der kan aktivere udstyret. Gør parterne det, kan den digitale ydelse præsteres hurtigt og effektivt, med et minimum af transaktionsomkostninger, og langt mere fleksibelt end i den fysiske verden.

I den analoge verden præsteres informationsprodukter typisk ved overdragelse af medier (bøger, aviser, grammofonplader etc.), men vel at mærke uden, at brugeren forventes at besidde særligt udstyr hertil, endsige udføre yderligere kopieringer af den præsterede information. Visse digitale informationsprodukter (f.eks. edb-programmer, CD-ROM-baserede databaser og spil mv.) præsteres fortsat med udgangspunkt i mediet; men da brugen af de heri liggende op-

havsretlige værker sker gennem kopiering, må overdragelsen ledsages af nogle rettigheder hertil, der – i mangel af anden aftale – følger af ophl. §§ 36-37.

Forsinket eller mangelfuld præstation af digitale informationsydelser kan give anledning til helt samme typer af retlige problemer som dem, vi kender i den klassiske formueret. Men behandlingen af disse spørgsmål volder beskrivelsesproblemer: På hvilket tidspunkt af den proces, hvorved de digitale bits tilvejebringes, går risikoen over på køber? Hvilke typiske kvalitetsforventninger kan brugeren stille til ydelsen? Hvad bliver konsekvenserne af en ophævelse? For at nærme sig disse spørgsmål er det nødvendigt at anlægge nogle sondringer, der placerer den digitale informationsydelse adækvat i forhold til obligationsrettens almene begrebsapparat.

Penge/realydelser

Først må man sondre mellem, om den digitale informationsydelse angår realydelser eller penge. Sondringen giver ikke anledning til nævneværdige problemer, bl.a. fordi de regler, der findes om elektroniske penge og andre elektroniske betalingsmidler, er ganske præcist afgrænset. Reglerne om elektroniske betalingsmidler behandles i afsnit 20.4.

Tjenesteydelse?

Dernæst må der ske en nærmere karakteristik af leverandørens præstationshandling. I formueretten sondrer man ofte mellem *varer* (og næsten synonymt hermed, løsøre og produkter), henholdsvis *tjenesteydelser*. Tilsvarende kan man sondre mellem *digitale informationsprodukter* (kendetegnet ved, at den digitale information, kunden sættes til at råde over, havde en i hovedsagen færdig form på aftaletidspunktet) og *digitale tjenesteydelser* (hvor den pågældende digitale information flyttes, konverteres, forandres eller på anden måde bearbejdes som led i aftaleopfyldelsen). Et eksempel på et digitalt informationsprodukt er overdragelse af et edb-program eller en MP3-fil via en hjemmeside. Disse ydelser omtales i afsnit 20.2. Eksemplerne på digitale tjenesteydelser er mere varierede, jf. nærmere afsnit 20.3.

Et tidligt eksempel på en lignende IT-baseret tjenesteydelse er den bearbejdning, et servicebureau præsterer, f.eks. i form af en lønkørsel for medarbejderne i kundens virksomhed. En sådan ydelse kan dog ikke rubriceres som *digital*, idet den præsteres ved, at resultatet af den afsluttede kørsel tilsendes kunden som et bundt papirer (lønsedlerne). I dag præsteres sådanne ydelser dog i stigende omfang digitalt, herunder som led i *facility management*-aftaler, jf. herom afsnit 21.6.

Licens?

Uanset om der er tale om at levere digitale informationsprodukter eller digitale tjenesteydelser indebærer præstationshandlingen et

element af kopiering. Dette følger som nævnt allerede af, at ydelsen præsteres i en kommunikativ proces, jf. nærmere afsnit 2.2.b. Men der er tale om andet og mere end et teoretisk aspekt. Iagttagelsen svarer helt til den praktiske virkelighed: Når køberen henter en MP3-fil fra en hjemmeside, ligger den fortsat på web-serveren, idet præstationen blot har udvirket en kopiering til køberen. Kopieringselementet indebærer, at ophavsretten får betydning, såvel inter partes som overfor tredjemand. Dernæst kan det retlige bånd, ophavsretten etablerer mellem information og medium (det forhold, at der udføres eller spredes et "eksemplar"), få betydning for, om ydelsen skal betragtes som "flytbar" (og dermed kunne sidestilles med en materiel løsøregenstand), eller om den har rent immateriel karakter. Hvilken betydning, det ophavsretlige element spiller, beror dog på den enkelte transaktion. Disse problemer omtales derfor i forbindelse med de enkelte typer af digitale informationsydelser.

Som nærmere udviklet i afsnit 7.4. sker der også kopiering under brug af edb-programmer og andre værker i digital form (brugskopiering), jf. tilsvarende afsnit 8.4. om *databaser*. Det bemærkes i den forbindelse, at den særlige programlicens i ophl. § 36 finder tilsvarende anvendelse for andre værker i digitaliseret form, hvis anvendelse styres af et edb-program, jf. ophl. § 36, stk. 3.

20.1.b. Retspolitiske spørgsmål

Selvregulering?

Den retlige og markedsmæssige håndtering af digitale informationsydelser har påkaldt sig stigende opmærksomhed gennem de seneste år. Det er i dag et væsentligt politisk tema, hvorledes man skaber de bedst mulige rammer for den elektroniske handel og dermed for præstation af digitale ydelser. Herhjemme fremlagde Forskningsministeriet i samarbejde med Erhvervsministeriet så tidligt som i 1996 et forslag til en national handlingsplan for elektronisk handel, der dog hovedsagelig havde den elektroniske aftaleindgåelse i fokus, jf. herom afsnit 19. Planen byggede i vid udstrækning på incitament-løsninger og selvregulering. Men siden er det gået slag i slag med handlingsplaner og initiativer på mangfoldige områder af den elektroniske handel, jf. nærmere afsnit 5.1.c. Foruden de mere proklamatoriske politiske initiativer har man på internationalt plan fra tid til anden gjort forsøg på at regulere den elektroniske handels rammebetingelser. Som det fremgår andetsteds i denne fremstilling, er disse forsøg gjort inden for vidt forskelligartede lovgivningssammenhænge: i relation til persondatabeskyttelsen, på det aftaleretlige område, ophavsretligt og markedsføringsretligt.

Blandt de mest fremstående internationale instrumenter, der har søgt at harmonisere denne udvikling, kan peges på *UNCITRALs* modellov om elektronisk handel fra 1996 (jf. nærmere afsnit 19.1), der dog primært søger at løse den bevismæssige, aftaleretlige og regulatoriske usikkerhed, som brugen af digitale dokumenter kan give anledning til, samt *OECD's* principper for privatlivsbeskyttelse fra 1980, hvis idé-grundlag genfindes i såvel Europarådskonventionen herom fra 1981 som i 1995-direktivet.

Når det kommer til den retlige regulering af selve den ydelse, der præsteres i åbne net – uanset hvilke markedsføringsretlige, persondatabeskyttelsesmæssige eller aftaleretlige forløb, der leder frem hertil – er der imidlertid ingen nævneværdig dansk eller international regulering. Man ledes derfor tilbage til den almene lære om ydelsen og dens præstation – suppleret med de særlige regler, der gælder om pengeydelsen, når betaling sker ved brug af betalingskort eller andre særlige betalingsmidler. IT-retten står således tilbage med de beskrivelsesproblemer, der er skitseret ovenfor.

20.2. Digitale informationsprodukter

20.2.a. Oversigt

Som nævnt i afsnit 20.1.a. kendetegnes et digitalt informationsprodukt ved, at den ydelse, kunden sættes til at råde over, havde en i hovedsagen færdig form på aftaletidspunktet. Typisk – men ikke altid – vil dette færdige produkt foreligge i form af et ophavsretligt beskyttet *værk*, f.eks. et edb-program, et andet litterært værk, eller en *database*. I begge tilfælde må der sondres mellem overdragelsen af *selve programmet/databasen*, som i nærværende terminologi rubriceres som et informationsprodukt, og *brugen* heraf, som her rubriceres som en digital tjenesteydelse (eftersom dennes nærmere karakter ikke er givet på aftaletidspunktet).

Præstationshandlingen

Et digitalt informationsprodukt kan enten præsteres, ved at data ved leverandørens hjælp *kopieres* direkte til brugerens medium i en *client/server*-struktur (f.eks. via www), eller ved at et datamedium *overdrages* af leverandøren til brugeren med henblik på brugerens efterfølgende kopiering til sit medium. Eksempler herpå kan være køb af en elektronisk bog i pdf-format via Internet eller af en ringetone til mobiltelefonen udført via en SMS-bestilling. Hvordan transaktionen tilrettelægges vil ofte bero på kapacitetsbegrænsninger: Digitale informationsprodukt-

ter stiller vekslende krav til mediet – en bog fylder f.eks. et fragment af, hvad en film gør. I takt med, at "båndbredden" udvides og teletransmissionstid (og pris) reduceres, vil stadigt flere informationsprodukter flytte over på nettet – f.eks. radio og tv i fuld kvalitet samt *video-on-demand*. Valget af præstationshandling kan få betydning for vurderingen af, hvornår risikoen for det digitale informationsprodukt overgår fra leverandør til kunde.

Retsbeskyttelse?

Når det digitale informationsprodukt karakteriseres, er det vigtigt indledningsvis at afklare, om det nyder ophavsretlig beskyttelse (og om denne beskyttelse gøres gældende af rettighedshaveren). I givet fald må aftalen nødvendigvis indebære, at brugeren som led i præstationshandlingen indtræder i nogle nærmere fastsatte rettigheder til at råde over det gennem visse former for kopiering og videreoverdragelse. Hvilke rettigheder kan enten være præciseret i en indgået licensaftale eller – for så vidt angår edb-programmer – fremgå af den legale programlicens i ophl. § 36, jf. nærmere i afsnit 7.4.b. Dette rettighedselement betyder bl.a., at der kan effektueres en tilbagegivelse af den tilståede ret til at råde over informationsproduktet, f.eks. hvis købet hæves, eller aftalen erklæres ugyldig. Er informationsproduktet derimod i *public domain*, jf. herom afsnit 7.4.b., er tilbagetagelse ikke mulig. Dette får betydning for, om produktet skal anses for omfattet af kbl. eller ikke, jf. nærmere i det følgende.

20.2.b. Retsgrundlaget

Når spørgsmålet om retsgrundlaget for salg af digitale informationsprodukter rejses, samler opmærksomheden sig først og fremmest om købeloven. Kbl. er dansk rets mest generelle formueretlige lovgivning og udtrykker en række anerkendte principper på formuerettens område. Loven gælder som udgangspunkt kun aftaler om køb og bytte af løsøre; men som udtryk for en række principper med almen gyldighed i dansk formueret kan den indirekte regulere også andre transaktioner. Omvendt viger loven ifølge § 1 for kutymer og sædvaner. Om en ydelse falder inden- eller udenfor loven har derfor ikke altid praktisk betydning. Betydningen opstår dog navnlig i to afgørende henseender: i relation til *forbrugerkøb*, hvor købeloven (ligesom kreditaftaleloven) indeholder beskyttelsespræceptive regler, og i relation til *reklamationsfristen* i § 54, stk. 1 (for forbrugerkøb, § 83), hvorefter mangelsindsigelser ikke kan fremsættes to år efter salgsgenstandens overgivelse.

Historisk grundlag

Da kbl. blev givet i 1906 kunne man selvsagt ikke forudse det marked for informationsprodukter, som vi kender i dag. Dette historiske præg træder klart frem i både systematik og terminologi. Den præstationshandling, loven beskriver, retter sig mod "salgsgenstanden" eller "varen" og en række af de retsmidler, loven udstyrer parterne med – f.eks. tilbagelevering af ydelsen, jf. kbl. §§ 57-58 – lader sig umiddelbart kun praktisere i relation til håndgribelige ting og ikke den blotte information om noget (medmindre denne information ledsages af en licens, eller man tager skridt til at fjerne den fra alle medier, hvortil erhververen har fæstnet den til). Hertil kommer, at information ikke er udsat for samme risici for mangler og undergang, som de ydelser, kbl. regulerer. Skuespillet *Hamlet* udgør i dag samme "informationsprodukt" som på Shakespeares tid. Dette *kan* tale for en anderledes vurdering af, hvornår og hvor længe en sælger skal være ansvarlig for mangler ved et informationsprodukt.

Det er det almindelige udgangspunkt i dansk køberet, at ydelser, der ikke har løsørepræg, falder uden for kbl. Dette er senest antaget af Højesteret i *U 1997.707 H*, hvor en tegningsaftale om andele i et investeringsselskab ikke kunne anses som "køb af løsøre" og derfor heller ikke for omfattet af kreditaftaleloven (hvis afgrænsning i hovedsagen anses for sammenfaldende med kbl.). Ligeledes er det fast antaget, at loven ikke gælder for entrepriseaftaler. Entreprenøren kan således ikke påberåbe sig kbl. § 54 i relation til sit ansvar for materialemangler, se *U 1975.750 H* og *U 1985.700 Ø*. Også låne- og lejeaftaler falder udenfor loven.

Teorien

Der er ikke desto mindre uenighed i teorien om, hvorvidt "køb" af information kan betragtes som løsørekøb. Spørgsmålet er genstand for indgående analyse i *Kim Frosts* ph.d.-afhandling: Informationsydelsen (2002). Frost konkluderer her, at aftaler vedrørende edb-programmer, som udgangspunkt reguleres af de køberetlige regler (herunder navnlig købeloven), for så vidt angår de maskinlæsbare instruktioner, uanset den måde, hvorpå programmet måtte blive præsenteret (se herved afsnit 4.2.4.1 med delkonklusionen s. 132). For så vidt angår fleksibel (såkaldt objektiv) information i menneskelæsbar skikkelse konkluderes det ligeledes, at købeloven finder direkte anvendelse (s. 149). Denne information kendetegnes ved at kunne verificeres, hvorved der skabes et grundlag for en mangelsbedømmelse.

Se ligeledes *Nørager-Nielsen & Theilgaard*: Købelovskommentaren, 2. udg. (1993), der antager, at levering af data via elektroniske medier må anses som løsørekøb, hvorimod *Jan Ramberg* i Köplagen (1995), s. 137 f. med note 15, afviser dette under henvisning til, at der i sådanne tilfælde ikke foreligger en "överlåtelse". Se i sam-

me retning SOU 1999: 106, s. 68 ff. og 102 ff. Spørgsmålet drøftes indgående af *Frederik Bruhn-Petersen* i specialeafhandlingen "Elektronisk præstation af digitale ydelser" (Kromann-Reumert prisopgave, 1999), s. 13 ff., der bl.a. ud fra forbrugerbeskyttelseshensynet når til, at købeloven uden videre må gælde for ydelser, der udelukkende består af information. Afhandlingen er tilgængelig på <www.jur.ku.dk/it-ret/specialer/bruhn-petersen.pdf>.

Praksis

Spørgsmålet om købelovens anvendelse i relation til digitale ydelser (herunder programmel) har endnu ikke været stillet på spidsen i dansk retspraksis. I de tilfælde, hvor der har foreligget købslignende overdragelser af informationsprodukter, har domstolene været tilbageholdende med at tage principiel stilling. At domstolene *citerer* enkelte købelovsbestemmelser i sager om programoverdragelser, rummer ingen stillingtagen til, om loven – der jo i vidt omfang kan anvendes analogt – kan anvendes.

I forarbejderne til den nye *norske* køvelov, Ot.prp. nr. 80 (1986-87), s. 50, er det forudsat, at programmer ikke anses for omfattet af købelovgivningen. I *Tyskland* har Bundesgerichthof i *NJW 1990.320* anvendt den tyske forbrugerkreditlov på et køb af et standardprogram, der "umiddelbart" blev indlagt i brugerens system af leverandøren uden samtidig overgivelse af mediet. I det omfang, information er genstand for en immaterialret, kan denne ret naturligvis overdrages og tilbagetages på helt almindelig vis ved, at licensen meddeles og kaldes tilbage. Bortfalder grundlaget for erhververens udnyttelse, kan overdrageren i kraft af retssystemets regler retablere udgangspunktet, ganske som sælgeren kan tilbagetage sin salgsgenstand. Ved dommen i *Sct. Albans City and District Council v. International Computers Ltd.* antoges det, at et standardprogram til skatteopkrævning var omfattet af den engelske Sales Act. Programmet var mangelfuldt og førte til forkerte beregninger. Retten henviser til den håndgribelige kendsgerning om, at et program "alters the contents of the hardware" (4 All ER 481-494, 1996), se i øvrigt om problemstillingen *Assafa Endeshaw* i 13 CLSR 325 ff. (1997).

Diskussion

Som flere gange påpeget i det foregående, bærer alle fysiske fænomener en mængde information i sig. Det er derfor vigtigt se på, hvordan information og medium er integreret med hinanden, når man skal vurdere, om et informationsprodukt er omfattet af kbl. Dette leder tilbage til den sondring, der er introduceret i afsnit 2.2.b. mellem integreret, fleksibel og mediekompatibel information, der ligeledes er lagt til grund ved behandlingen af de ejendomsretlige regler, jf. nærmere afsnit 12.2.

Integreret information

Ser vi først på den *integrerede* information ligger det klart, at selve dette, at der i en fysisk løsøregenstand indgår et kommunikativt aspekt, ikke i sig selv indebærer, at genstande falder uden for kbl. Var dette tilfældet ville loven aldrig kunne anvendes,

eftersom stort set alle løsøregenstande rummer et vist kommunikativt element i sig. At der i et køleskab er indbygget en processor, hvis databehandling er afgørende for den for produktet afgørende termostatfunktionalitet, fratager selvsagt ikke køleskabet dets karakter af løsøre.

I relation til den afgrænsning af begrebet "digitalt informationsprodukt", der er gjort her, kan dette resultat dog også forklares med, at der ikke er tale om et "digitalt informationsprodukt", eftersom det essentielle i ydelsen jo ikke er, at kunden skal råde over de pågældende bits.

Fleksibel information

Vender man sig til sondringens andet modstykke, må det ligeledes antages, at information, der har helt *fleksibel* karakter, ikke kan rummes i det køberetlige system. Singulære oplysninger, der leveres fra en database, vil således ikke kunne karakteriseres som løsøre i køberetlig forstand. En advokats standardiserede skatteråd er ikke omfattet af købeloven, selv om det allerede var produceret ved aftalens indgåelse i form af færdiggjorte dokumenter mv., sml. ovenfor om *U 1997.707 H*. Ej heller vil en komikers salg af en vittighed til en festtaler kunne rummes under begrebet "løsøre", selv om den så at sige lå på lager før "leveringen".

At fleksibel information falder uden for det køberetlige system betyder bl.a., at kbl. er uanvendelig, når det gælder mangler, der udelukkende kan henføres til sådanne dele af det leverede. I konsekvens heraf må det derfor antages, at mangler ved en bog, der fremtræder som forkerte eller misvisende faktuelle oplysninger mv., ikke reguleres køberetligt, medens mangler ved mediet (manglende sider eller defekt indbinding) gør det. Derimod må det antages, at mangler ved det dokumentationsmateriale (f.eks. en brugermanual), der ledsager et program, er omfattet af loven: Selv om denne information strengt taget også er fleksibel, har den for slutbrugeren kun værdi i samspil med det leverede.

Mediekompatibel information

I mellemområdet for den mediekompatible information opstår nogle vanskelige afgrænsningsproblemer. Denne information har nemlig på den ene side egenskaber til fælles med den fleksible information (risikoen for, at informationen spredes ukontrolleret som ringe i vandet), men på den anden side også egenskaber, der kendetegner den mediekompatible (den nødvendige forbindelse med medier af den pågældende art). Her er det nødvendigt at anlægge nogle sondringer.

Retsbeskyttede produkter

Hvis et digitalt informationsprodukt, der er kompatibelt med en bestemt type medium, er underkastet en ophavsretlig beskyttelse, vil det særlige bånd, ophavsretten skaber mellem information og medium, kunne begrunde, at informationsproduktet må

betragtes som et *produkt*, sml. herved *Frost* (2002), s. 114 ff., der taler om, at ydelsen i disse tilfælde besidder en *symbolværdi*. Retsbeskyttelsen indebærer, at produktet kan leveres og tages tilbage, idet et ophør af den pågældende licens vil indebære, at fortsat brug af produktet (gennem den nødvendige brugskopiering) bliver retsstridig. Da muligheden herfor består, uanset om der er overdraget et medium eller ikke, gælder denne antagelse også, når et retsbeskyttet digitalt informationsprodukt leveres over nettet i henhold til den legale programlicens i ophl. § 36, uden at det kompatible medium præsteres som et løsøreelement i transaktionen.

Licensaftaler?

Omvendt indebærer det forhold, at der består en mere kompleks ophavsretlig relation mellem parterne ikke, at man forlader det køberetlige system, hvis blot denne relation ikke forandrer transaktionen om informationsproduktet til en licensaftale: Går aftalen mellem leverandør og kunde ud på, at brugeren kun må benytte det pågældende produkt i en begrænset periode og til ganske bestemte formål, vil der ikke foreligge en sådan endelig overdragelse af en ret, som er købets kendetegn (og som i relation til løsøre indebærer, at der skal ske en overdragelse af en "ejendomsret"). Parallellen til løsøretransaktionen vil her være et låne- eller lejeforhold, hvor kbl. ikke finder anvendelse, jf. nærmere afsnit 21.4.b.

For erhververen kan en misligholdelse af disse forpligtelser give anledning til retskrav af forskellig karakter. Se herom *Koktvedgaard* i TfR 1965.571 ff., *Plesner* i J1955.201 ff., min afhandling i U1987B.121, *Hultmark* i JT 1993-94.687 ff. og – med særlig fokus på CISG – *Eric M. Runesson* i Festskrift til Karnell (1999), s. 625 ff.

Public domain

Er der derimod tale om et informationsprodukt i *public domain*, vil det være vanskeligt at anvende købelovens almindelige system. Tilbagetagelse af ydelsen vil i praksis være udelukket, eftersom den ikke kan understøttes af retlige bånd, der kan afskære "køberen" fra fortsat at benytte produktet. Det essentielle i en sådan transaktion vil typisk ligge i, at leverandøren *identificerer* det pågældende produkt for kunden og i givet fald forædler det til køberens behov. Uden en sådan bistand kan det i hvert fald være vanskeligt at se, hvilken værdi leverandørens ydelse har, eftersom produktet jo er frit tilgængeligt. En sådan bistand må siges at have karakter af tjenesteydelse. Som eksempler på produkter, der således vil falde uden for kbl., kan nævnes levering af programmel, som rettighedshaveren udtrykkeligt har opgivet sin ret til (f.eks. i relation til en *open source*-løsning), levering af informa-

tionsdele fra en database eller levering af tekniske opsætninger (såkaldte skabeloner, eller *templates*) til eksisterende produkter.

Der findes vel ingen domstolsafgørelser om sådanne produkter. Det nærmeste man kommer spørgsmålet er *U 1982.256 Ø*, der ikke ville sanktionere udebleven TV-information ("sort skærm") køberetligt. I kraft af den *public service*-forpligtelse, der påhviler DR kan man – i en argumentation som den ovenfor anførte – betragte det almindelige tv-udbud som *public domain*-information. Leveres TV-information *on demand* eller i øvrigt under en kommerciel transaktion, burde resultatet være anderledes.

Konklusionerne ovenfor har voldt mig betydelig tvivl, og i tidligere fremstillinger, herunder navnlig i *E&A* s. 323 ff., er jeg nået frem til resultater, der ikke fuldt ud modsvarer det ovenfor anførte. Spørgsmålet har været drøftet i UNCITRAL, hvis arbejdsgruppe om e-handel har næret tilsvarende forbehold, se Report of the Working Group on Electronic Commerce on its thirty-eigth session (New York, 12-23 March 2001), af 24. april 2001, afsnit B.5. I USA (jf. nedenfor om UCITA) har man valgt at regulere den digitale informationsydelse gennem særlige regler. Der er utvivlsomt et behov for håndfaste sondringer. Der er dog næppe tvivl om, at den almindelige retsopfattelse – som anført ovenfor – har vænnet sig til at betragte kommercielle informationsprodukter som køberetlige løsøregenstande.

Konsekvenser

For erhvervsmæssige køb betyder denne konklusion, at mangelsindsigelser vedrørende kommercielt standardprogrammel fortabes, hvis manglen viser sig mere end et år efter informationsproduktets overgivelse. For forbrugerkøb betyder den manglende anvendelse af kbl. først og fremmest, at leverandøren ikke kan foretage ansvarsfraskrivelser i sådanne transaktioner.

CISG

Det er uafklaret, om FN's konvention om internationale løsørekøb (CISG) omfatter aftaler om edb-programmel, se *Joseph Lookofsky*: Understanding the CISG in Scandinavia, 2. udg. (2002), s. 23 f. og *Ramberg & Herre*s kommentar til CISG (2000), s. 72 (med fyldige litteraturhenvisninger i note 33) og s. 92. Udgangspunkterne står nok rimeligt klare og svarer i hovedsagen til, hvad der ovenfor er antaget om købeloven: En programoverdragelse, der former sig som en begrænset og personlig licens til en specifik bruger, må antages at falde uden for loven. Omvendt indebærer et licenselement i en i øvrigt "flytbar" overdragelse ikke, at loven skulle være uanvendelig. CISG omhandler ifølge artikel 1, stk. 1, "løsørekøb" med undtagelse af de særlige ydelser (herunder elektricitet), der er omhandlet i artikel 2. I mellemtilfælde må

man lægge vægt på, hvilket element af transaktionen der er overvejende.

I UCC defineres løsøre som "all things (including specially manufactured goods) which are *moveable* at the time of identification to the contract for sale", § 2-105 (1). Kriteriet om ydelsens flytbarhed på kontraktstidspunktet afgrænser først og fremmest loven overfor udviklingsydelser. Herudover har det givet anledning til tvivl, om man meningsfuldt kan tale om, at information knyttet til medier "flyttes", når mediet flyttes. En god analyse af UCC's anvendelse på edb-området findes i 77 Michigan L.R. 1149 (1979) og i 9 Rutgers-Camden L.J. 303 (1977). Af interesse er desuden *Robert A. Holmes*' afhandling i 9 Rutgers 1 (1982) og den rapport, som The Committee on Computer Law under The Association of the Bar of the City of New York udarbejdede i 1985, se 40 ABCNY 756 (1985). I amerikansk retspraksis har man hidtil valgt at fokusere på, om aftalen i sin ydre fremtrædelse hovedsagelig minder om et traditionelt løsørekøb. *Triangle Underwriters v. Honeywell*, 457 F.Supp. 765 (1978) (stadfæstet ved 604 F.2d 737 (1979)) anvendte UCC på en overdragelse, der omfattede både hardware og standard- og specialprogrammel. I *RRX Industries, Inc. v. Lab-Con, Inc.*, 772 F.2d 543 (1985) blev UCC lagt til grund i en aftale om standardprogrammel til et medicinsk laboratorium. Retten udtalte, at spørgsmålet om UCC's anvendelse måtte bero på "... the essence of the agreement. ... When a sale predominates, incidental services provided do not alter the basic transaction". Ganske vidtgående forekommer afgørelsen i *Chubb Life Insurance Company of America v. Electronic Data Systems*, 817 F.Supp. 235 (1993), der lod UCC gælde for levering af servicebureau-virksomhed. Aftaler, der hovedsagelig består af udvikling, vedligeholdelse eller installation, falder herefter som udgangspunkt uden for købsbegrebet og dermed UCC, se f.eks. *Geotech Energy Corporation v. Gulf States Telecommunications and Informations Systems*, 788 South Western Reporter, 2nd Series, 386 (1990). Tilsvarende resultater må gælde efter CISG, jf. dennes artikel 3, hvorefter aftaler, hvor den overvejende del af leverandørens forpligtelser består i at levere arbejdskraft eller andre tjenesteydelser, falder uden for konventionen.

UCITA

I USA førte diskussionen om anvendelsen af UCC i relation til rent digitale ydelser i 1999 til vedtagelsen af en særlig uniform lovgivning herom, the Uniform Computer Information Transactions Act (UCITA). Oprindelig var det tanken, at disse regler skulle indføjes i et særligt kapitel i UCC (art. 2B); men da der ikke kunne opnås enighed herom, valgte man denne særskilte lovgivning, som ikke alene var ganske kompleks, men også i nogen grad kontroversiel. Loven omfattede al "computer information", herunder retsbeskyttede frembringelser som edb-programmer, bille-

der, musik, erhvervshemmeligheder, patenter og hjemmesider. Efter vedtagelsen af en første version i 1999 fortsatte de indgående diskussioner både centralt (med ændringer i 2000 og 2002) og på delstatsniveau. Emnet blev mere og mere kontroversielt, og i august 2003 blev UCITA-projektet helt opgivet.

20.2.c. Ejendomsforbehold

Udgangspunktet

Også leverandørens praktiske og retlige muligheder for at tage "ejendomsforbehold" i digital information beror på de overvejelser, der er udviklet ovenfor: Er der tale om *integreret information*, volder ejendomsforbeholdet ingen vanskeligheder. Omvendt er det som altovervejende udgangspunkt udelukket at forbeholde sig ejendomsret over *fleksibel information*, medmindre forbeholdet retter sig mod en immaterialretlig retsposition, der fastlåser brugsretten til denne information på nærmere bestemt måde (f.eks. i konsekvens af et patent).

De interessante spørgsmål knytter sig derfor igen til mellemområdet, den *mediekompatible information*. Muligheden for at gennemføre et ejendomsforhold herover beror først og fremmest på, hvilken aftale der ligger til grund for overdragelsen, og hvilket (ejendoms-)forbehold der måtte være taget. Man er her nødt til at sondre mellem to situationer:

Eksemplartilfælde

Hvis mediekompatibel information overdrages sammen med et medium eller på grundlag af en særlig kode, jf. nærmere afsnit 6.3.d., er det udgangspunktet, at råderetten knytter sig til besiddelsen af dette medium eller denne kode. Når besidderen, jf. ophl. § 19, spreder eksemplarer til andre, ophører hans egen ret til at benytte værket. Omvendt ophører besidderens ret til at benytte værket, hvis eksemplaret som følge af køberetlige regler (f.eks. fordi der efter kbl. § 28, stk. 2, er forbeholdt særskilt ret til det solgte) skal leveres tilbage til overdrageren.

Om det samme gælder, hvis eksemplaret af værket er blevet stjålet, beror på, om der er mulighed for, at tyven eller dennes godtroende erhverver kan opnå status som "lovlig" bruger af licensen. Som udgangspunkt må dette spørgsmål besvares benægtende, jf. afsnit 12.2.c.

Licensordninger

Hviler erhververens adgang til at benytte det pågældende værk derimod på en særskilt aftale med overdrageren/rettighedshaveren, beror mulighederne for at tilbagetage den beskyttede information på, hvorledes denne aftale er formuleret. I denne situation er man uden for de køberetlige regler (og dermed ikke underlagt de strenge vedtagelseskrav i kbl. § 28, stk. 2), og der vil

derfor gælde en vidtgående adgang for overdrageren til at forbeholde sig ret til det præsterede. Tværtimod vil sådanne aftaleforhold ofte skulle fortolkes til fordel for overdrageren, jf. det fortolkningsprincip, der finder udtryk i ophl. § 53, stk. 2-3.

20.2.d. Risikoovergang

Problemstillingen

Når et informationsprodukt leveres på et medium, der herefter forsendes til kunden ad fysisk vej, kan man uden videre anvende de almindelige principper for risikoovergang, der er udviklet i den fysiske handel (herunder i køberetten). Mange af de digitale informationsprodukter, der tilbydes på nettet, leveres imidlertid ved, at kunden sætter sig i forbindelse med et medium, f.eks. den server, der understøtter en hjemmeside, hvorfra han i løbet af sekunder selv kan hente den pågældende information. Hvis informationen ikke når frem, eller når frem i defekt stand (f.eks.som følge af nedbrud på et transmissionsnet), opstår spørgsmålet, hvem af parterne der skal bære risikoen herfor.

Udgangspunktet

I en analogi til den fysiske verdens leveringshandling er det nærliggende at gå ud fra, at den part, der har haft det i sin magt at træffe opfyldelsesvalget for denne leveringshandling, også bør bære risikoen for ydelsens hændelige undergang, sml. herved kbl. § 24. Dette udgangspunkt er imidlertid kun operationelt, hvis brugeren virkelig har en reel mulighed for at vælge sit medium. En sådan mulighed består kun i meget begrænset omfang for den kommunikation, der foregår via the World Wide Web, som begge parter må siges at være lige om at vælge. Det er således vanskeligt at sige, at den ene part er "nærmere" end den anden til at bære risikoen for forstyrrelser på nettet.

Med tanke på bestemmelsen i kbl. § 10, hvorefter risikoen for varen i forsendelseskøb går over, når den er overgivet "til en fragtfører, som har påtaget sig forsendelsen fra vedkommende sted", kunne det være nærliggende at anse den eller de Internetoperatører, der formidler den digitale information fra leverandør til bruger, som "fragtfører". Men heller ikke denne analogi passer. En "fragtfører" i den fysiske verden vil til enhver tid vide, hvor varen befinder sig. Han har derfor mulighed for at øve indflydelse på de faktorer, der kan udløse en risiko, ligesom han vil kunne forsikre sig. Ingen af disse kendetegn præger den digitale leveringshandling. Den Internet-leverandør, der leverer infrastruktur til levering af en digital ydelse, stiller kun en kommunikationsforbindelse til rådighed i form af en brugsret, som med vekslende sikkerhed vil være tilgængelig for hans kunder. For-

sikringer for informationsfejl på disse linjer er ukendte. Hertil kommer, at de fejlmuligheder, der kan opstå under transmissionen af digitale data, kun i begrænset omfang beror på forhold, som Internet-leverandøren har indflydelse på (protokolopsætning, tilsluttet programmel etc.).

Derfor må de juridiske resultater udledes af andre overvejelser. I den forbindelse må det tillægges betydning, at nedbrud på den teleforbindelse, der anvendes ved præstation af et digitalt informationsprodukt, ofte vil befinde sig uden for begge parters *kontrolsfære*. Lægger man i en sådan situation risikoen på *kunden*, vil dennes incitament til at få det digitale produkt leveret på denne måde derfor blive reduceret, hvilket ej heller kan være i leverandørens interesse: Kunderne skræmmes ganske enkelt væk! Lægger man risikoen på *leverandøren*, vil de økonomiske konsekvenser heraf være til at overskue: Der vil blot være tale om at skulle gentage en leveringshandling bestående af en yderligere kopiering i en situation, hvor den første kopiering ikke viste sig tjenlig til sit formål, og som derfor ikke kan være truende for afsætningen.

Konklusion

Disse betragtninger fører til, at et digitalt informationsprodukt først er leveret, når det er *kommet frem* til kunden på en måde, der giver kunden den forudsatte anvendelighed for den. Går produktet tabt undervejs i transmissionen, eller indtræder der en forvanskning, der gør produktet defekt, må det derfor antages, at leverandøren har pligt til at transmittere det på ny (eller lade det transmittere uden vederlag), og at køberen ikke har pligt til at betale, før dette er sket. Dette resultat må antages, uanset om produktet leveres gennem *uploading* eller *downloading*. Forskellen mellem disse to leveringshandlinger beror alene på, hvem der tager skridt til den pågældende leveringshandling, og hvis ellers den valgte form har den fornødne støtte i parternes aftale, bør dette ikke påvirke risikobilledet.

Kryptering mv.

Hvis informationsproduktet præsteres i komprimeret eller krypteret form, således at brugeren først får adgang til det, når han har modtaget et password (typisk mod betaling), der vil kunne gøre det læsbart og funktionsdygtigt, vil det være åbenbart forudsat, at levering først har fundet sted, når brugeren ved hjælp af dette password har kunnet gennemføre den nødvendige konvertering. Forsinkes transmissionen af dette password, vil der derfor indtræde forsinkelse med selve produktet. Fører passwordet ikke til en korrekt dekryptering, kan ydelsen ikke anses for leveret.

Modifikationer

Man kan overveje, om de skitserede resultater også gælder, når det er kunden, der – efter forudgående aftale med leverandøren – har valgt den kommunikationskanal, som ydelsen præsteres på. I en sådan situation – som vel kan forekomme teoretisk under nutidens web-anvendelse – kan det være nærliggende at anvende de almindelige risikoregler. Risikoen for informationsproduktets hændelige undergang vil da som udgangspunkt gå over på det tidspunkt, meddelelsen transmitteres ud på den pågældende kommunikationskanal. Erhververen må altså betale for den leverede information eller den realiserede brug, uanset han ingen glæde får af den. Er teleforbindelsen derimod valgt af leverandøren (f.eks. som led i en samlet systemløsning), må risikoen for, at ydelsen ikke modtages, også hvile på denne. Kommer informationen ikke frem, må den i denne situation genleveres.

20.2.e. Mangler

Et digitalt informationsprodukt kan være mangelfuldt i samme omfang som andre softwareydelser. Mangler ved selve det *medium*, hvorpå et digitalt informationsprodukt præsteres, vil almindeligvis vise sig ved, at produktet ikke er tilgængeligt, hvorved der vil foreligge forsinkelse. Ser man på det funktionelle aspekt af ydelsen, kan en ufuldstændig *dokumentation* indebære, at brugeren ikke opnår de funktioner, han er stillet i udsigt. Som nævnt i afsnit 20.2.b. må sådanne mangler betragtes som mangler ved den mediekompatible information og dermed som omfattet af købeloven i det omfang det pågældende informationsprodukt er det. Ydelsen kan dernæst være fejlbehæftet ved, at funktioner udebliver eller har en *ringere kvalitet* end aftalt eller med rette forudsat. Mangelsvurderingen af disse spørgsmål må anlægges på samme måde som i andre IT-aftaler, jf. i det hele afsnit 22.2.a.

Informationsmangler

Mangler ved information, der stilles til rådighed via et net, kan have vidt forskellige årsager. Der kan være fejl og manglende præcision i selve informationsindholdet, manglende tilgængelighed, forsinket opdatering mv. Også her knyttes mangelsvurderingen til, hvad der er aftalt eller med rette forudsat. Når det gælder "mangler" ved information i en database, er vi – som nævnt i afsnit 20.2.b. – uden for købeloven men inde i obligationsrettens almindelige mangelslære. Her må der formentlig gælde en vid mangelstolerance. Har man købt en bog, skal der formentlig foreligge helt særlige grunde for at kunne møde boghandleren med et krav om ophævelse, fordi bogens information er fejlbehæftet eller i øvrigt mangelfuld. Med en vid efterkommelse af sådanne

mangelskrav, vil de køberetlige mangelsregler medføre en begrænsning af den almindelige ytringsfrihed, sml. den tilsvarende drøftelse af produktansvarsreglernes anvendelse på informationsprodukter i afsnit 18.1.e. og 18.3.c. For visse typer af databaser kan det dog være mere nærliggende at anvende en striksere mangelsvurdering. Det gælder f.eks. databaser, som f.eks. børsdatabaser, som markedsføres med henblik på professionel, troværdig anvendelse, og for hvilke den løbende opdatering og datavedligeholdelse er en ultimativ kvalitetsparameter.

Sikkerheds-mangler

En særlig problemstilling ved ydelser i åbne net er sikkerhedsaspektet. En leverandør, der lader sine brugere lægge deres følsomme eller i anden henseende fortrolige data ligge på en server, har pligt til at sikre, at tredjemand er afskåret fra uberettiget at trænge ind og få adgang hertil. At en sådan sikkerhedsbrist realiseres afgiver i sig selv en formodning for, at der foreligger et culpøst forhold, og en påviselig risiko herfor – der ikke omgående fjernes – vil i sig selv gøre tjenesten mangelfuld.

20.3. Digitale tjenesteydelser

20.3.a. Inddeling

Som nævnt ovenfor dækker samlebegrebet "digitale tjenesteydelser" over en vid mangfoldighed af tjenesteydelser, der præsteres ved brug af digital teknologi, og som kendetegnes ved, at digital information flyttes, konverteres, forandres eller på anden måde bearbejdes. Begrebet omfatter en vid mangfoldighed af forskelligartede ydelser, der kun har dette basale kendetegn til fælles. I skalaens mere kostbare ende kan man pege på visse former for digital informationsbehandling, se hertil afsnit 21.6. Men også de tjenester, en bruger kan efterspørge på sin mobiltelefon, falder inden for, f.eks. i forbindelse med WAP-applikationer eller ved salg Internet-adgang fra en Internet-cafe.

Typisk vil denne bearbejdning ske i et system, som leverandøren på forhånd har konstrueret og stillet til rådighed for kunden. Da systemet derfor eksisterer, inden aftalen indgås, kan det være nærliggende at rubricere den digitale tjenesteydelse som et eksempel på en brugsrettighed. Denne karakteristik forekommer dog mindre nærliggende i de – talrige – tilfælde, hvor ydelsens endelige udformning for kunden først hidføres, når kunden præsenterer sit behov i en kommunikationsproces med det pågældende system, f.eks. ved søgning i en database, eller adgang til en

funktionalitet, der fremkaldes af kunden. I så fald vil der nemlig indgå vekslende elementer af *licenselementer* i ydelsen, ligesom der kan være tale om præstationshandlinger, der nærmest har karakter af *resultatforpligtelser*. Det lønner sig næppe at foretage nogen mere eksakt inddeling mellem disse forskellige typer af ydelser. I stedet kan man i tilslutning til det definitoriske krav om, at ydelsen præsteres ved en digital bearbejdningsproces, anføre et supplerende krav om, at denne brug er afgrænset i tid, og at den ikke involverer overdragelse af det pågældende produkt.

I afsnit 3.3.b. findes en kort præsentation af de virksomheder, der fungerer som mellemled mellem de kommunikerende brugere på nettet, de såkaldte Internet-leverandører. Det drejer sig om leverandører af Internet-adgang (*Internet Access Providers*), leverandører af Internet-tjenester (*Internet Service Providers*) og leverandører af Internet-informationsindhold (*Internet Content Providers*). En del af disse ydelser betegnes i den sprogbrug, der anvendes på teleområdet, som "tjenester". Begrebet er næppe sammenfattende med det juridiske residualbegreb "tjenesteydelse", der almindeligvis anvendes om forpligtelser, der indebærer en aktiv handlen.

Kontrakt?

Når retsstillingen mellem leverandøren og brugeren af sådanne tjenesteydelser skal lægges fast, må det indledningsvis præciseres, om ydelsen præsteres i et kontraktsforhold eller ikke.

- vederlagsfri brug

Mange af de digitale tjenester, der tilbydes på nettet – og som gør dem profitable – vil ikke udspringe af en sædvanlig udveksling af ydelser. Brugeren betaler i en vis forstand ved at lade sig eksponere for en annoncering eller blot – ved f.eks. at hente et gratis certifikat fra en CA-virksomhed – at blive introduceret til en udbyder, hvis tjenester, han efterfølgende kunne tænkes at blive betalende bruger af. I disse tilfælde vil brugeren alene kunne hævde et kontraktsforhold, hvis der fra leverandørens side er afgivet en utvetydig pligterklæring, der opfylder betingelserne for at være aftaleretligt forpligtende. En klausulering, der signalerer, at leverandøren ikke er parat til at indestå for det leverede, vil derimod bekræfte formodningen for, at der ikke tilsigtes etableret en sådan kontraktsrelation.

Som almindelig regel må det antages, at der *ikke* etableres noget kontraktsforhold i tilfælde, hvor brugeren ikke forpligtes til at foretage nogen betaling og ej heller optræder i en identificeret form overfor leverandøren af den pågældende tjeneste. Et kontraktsforhold er en retlig ramme om en relation mellem to parter, der har ønsket at forpligte sig overfor hinanden. Det er i disse tilfælde vanskeligt at udpege et sådant katalog af gensidige forpligtelser. De vilkår, som ofte fastsættes af de pågældende udbydere, tegner ligeledes et klart billede af, at der ikke er noget ønske

om at påtage sig videregående forpligtelser af juridisk karakter. Tjenesten må da betragtes som en faktisk brugssituation, som etableres på fritstående grundlag og som alene er reguleret af retssystemets almindelige regler, herunder reglerne om erstatning uden for kontraktsforhold.

- aftaletilfælde

Heroverfor står de tilfælde, hvor en ydelse præsteres som led i et forudgående aftaleforhold, f.eks. i forbindelse med såkaldt *servicebureauvirksomhed*. Ligesom i et forhandlerforhold, se hertil *ET*,s. 352 ff., vil der her være tale om, at parterne forinden har indgået en aftale om, hvad der skal leveres, og under hvilke vilkår. Som led i en aftale om *facility management*-virksomhed, kan det f.eks. være bestemt, at parterne lejer en telelinje, der forbinder deres IT-systemer med hinanden. De nærmere krav til ydelsen vil da typisk være reguleret i denne aftale.

I det følgende omtales kun digitale informationstjenester, der baseres på et aftaleforhold. Blandt de væsentligste af disse fremhæves følgende:

Transmission

En transmissionsydelse giver kunden ret til at transmittere digitale data over en netforbindelse. Når der er tale om at transmittere digitale data, udtrykkes kravene til ydelsen almindeligvis i, hvilket antal kilobit pr. sekund (kbit/s) den præsterede teleforbindelse kan transmittere. Sådanne funktionsbeskrivelser må – medmindre andet er aftalt – som udgangspunkt fortolkes som cirkabeskrivelser. Om en tilsagt transmissionskapacitet kan præsteres til enhver tid beror på, hvilken belastning nettet er udsat for på det tidspunkt, den pågældende tjeneste efterspørges. En 100 procent garanti for, at kapaciteten er tilstede, vil være meget vanskelig at leve op til og ligger formentlig udenfor parternes typeforudsætninger, sml. i øvrigt *U 1982.256 Ø*. Aftaler om teletransmission er dermed i familie med aftaler om energimængder (f.eks. el og vand), der ligeledes kan være påvirket af spidsbelastninger.

Transmissionsydelsens retlige problemer er ikke gjort til genstand for nyere retsvidenskabelige studier herhjemme. Fra norsk litteratur kan henvises til redegørelsen hos *Bing m.fl.*: Innføring i telekommunikasjonsrett (2001), kapitel 9 (s. 241-261).

Servertjeneste

En anden væsentlig informationsydelse er levering af serverfunktionalitet: Her opnår kunden ret til at anvende den digitale tjeneste, som en computer ("server") er programmeret til at udføre. Eksempler herpå kan være lagring af data (f.eks. i forbindelse med web-hoteldrift) eller e-mail service. For sådanne tjenester vil beskrivelsen som regel være præciseret med et maksimeret lagerareal el.lign.

Databaser

En tredje digital informationsydelse giver kunden ret til at hente en informationsmængde, som leverandøren har eller – i kraft af en maskinel bearbejdning – kan bringe til verden i et informationssystem. Er der tale om eksisterende informationer beskrives sådanne ydelser almindeligvis som databaseydelser. Når en database markedsføres som tjeneste vil det typisk ske ved, at at kunden tilsiges en vis *on-line* adgang. Databasen befinder sig på et centralt medium, som brugeren kan koble sig op til (f.eks. via Internet). Præstation af en *off-line* database på CD-ROM må derimod betragtes som et digitalt informationsprodukt. Da den mangelsvurdering, der skal foretages i tilfælde, hvor databasens indhold viser sig fejlagtigt, i begge tilfælde sker uafhængigt af købelovens regler, har denne forskel dog sjældent stor praktisk betydning.

Licensrettigheder

I begge tilfælde er der behov for en aftalemæssig licensregulering af, hvordan brugeren må anvende databasen i tillæg til de andre forhold vedrørende dennes kvalitet mv. Denne regulering adskiller sig ikke fra andre licenselementer i en IT-overdragelse. I det omfang de pågældende data er undergivet en ophavsretlig eller anden immaterialretlig beskyttelse, der lægger retlige begrænsninger i de handlinger, kunden må foretage, indgår der i aftalen et element af licens. Frem til december 2002, hvor Infosoc-direktivet blev indført i dansk ret, fulgte denne regulering direkte af ophl., idet den dagældende § 36, stk. 3, lod reglerne om den legale programlicens finde tilsvarende anvendelse på "andre værker i digitaliseret form, hvis anvendelse styres af et edb-program." Da afløseren for § 36, stk. 3, nemlig ophl. § 11a, alene giver hjemmel for en begrænset, ikke-økonomisk, udnyttelse af det digitale værk, må brugerens ret til at benytte det digitale værk søges på rent aftaleretligt grundlag. Foreligger der ikke en udtrykkelig licensaftale, må man hense til hvilken benyttelse, der må *formodes* at være tilladt af rettighedshaveren, givet det digitale værks egenskaber og funktioner samt praksis på området.

Ifølge § 36, stk. 2, må den, der har ret til at benytte en database, i øvrigt foretage sådanne handlinger, som er nødvendige for, at den pågældende kan få adgang til databasens indhold og gøre normal brug af denne. Man må derimod ikke rette fejl i databasen. En sådan ret består heller ikke for "andre værker i digitaliseret form".

20.3.b. Retsgrundlag

Almindelige regler

Foruden de regler, der kan udledes af parternes aftale, må retsgrundlaget for digitale tjenesteydelser udledes af obligationsrettens almindelige regler om kravene til realydelsen. Se hertil *Bryde Andersen & Lookofsky* (2005), kapitel 2. Som antydet ved bemærkningerne ovenfor må disse almindelige regler dog på visse punkter modificeres, når ydelsen præsteres digitalt.

Telebekendtgørelsen

Er den digitale tjenesteydelse en *teletjeneste,* må leverandøren herudover opfylde de særlige pligter, der følger af telelovgivningen. Af særlig betydning er her reglerne i *telebekendtgørelsen,* bekendtgørelse nr. 639 af 20. juni 2005. Bekendtgørelsen, der gennemfører en række direktiver på teleområdet, foreskriver, at udbydere af offentlige elektroniske kommunikationsnet eller -tjenester skal sikre, at der foreligger en kontrakt som grundlag for ethvert kundeforhold med en slutbruger, der indeholder en række oplysninger (§ 5). Udbyderen er forpligtet til at lade de takserings-, debiterings- og faktureringssystemer, der er knyttet til udbuddet, være certificeret i henhold til ISO 9001-standarden eller tilsvarende anerkendte standarder (§ 9, stk. 2). Der opstilles krav til, hvordan klager skal ekspederes (§§ 11-13), og en række tjenester er gjort pligtmæssige for visse tjenester (telefoni via faste net, ISDN-tjenester og mobilkommunikation), herunder saldooplysning, spærring og henvisning – se nærmere bekendtgørelsens §§ 14-24.

20.3.c. Risikoovergang

Når en digital tjenesteydelse præsteres via telekommunikation opstår ikke helt samme problemer om risikoovergang som ved præstation af digitale informationsprodukter. I det omfang der er tale om en *løbende ydelse*, vil et nedbrud på transmissionsforbindelsen resultere i, at der slet ikke iværksættes nogen leveringshandling. Men i det omfang en leveringshandling rent faktisk sættes i værk uden at føre til en færdig præstation – et opslag mod en database fører til, at der afsendes en datamængde, som dog går tabt undervejs på telelinjen – bør samme principper som de, der er anført i afsnit 20.2.d. finde anvendelse. Selv om den manglende tilgængelighed skyldes forhold på selve kommunikationsforbindelsen (f.eks. overbelastning af net mv.) og dermed udgør en opfyldelseshindring uden for leverandørens kontrol, vil reale betragtninger føre til, at ydelsen først er præsteret, når den er kommet frem til kunden i brugbar skikkelse.

I den noget specielle afgørelse i *U 1982.256 Ø* nægtede en seer at betale en forholdsmæssig andel af sin TV-licens svarende til den tid, hvor der som følge af en arbejdsnedlæggelse havde været sort skærm. Danmarks Radio frifandtes, bl.a. med den begrundelse, at kontraktsretlige grundsætninger ikke skulle være afgørende for forholdet mellem seeren og radiofonien. Dette synspunkt kan – som nævnt i afsnit 2.2.b. – hænge sammen med, at indholdet af DR's programudbud ikke forudsættes påvirket af aftalegrundlaget med seerskaren, men derimod gennem den demokratiske procedure, der er lagt fast i lovgivningen om DR. Afgørelsen knytter sig til det særlige regelgrundlag, der gælder for TV-licens og kan næppe overføres til informationsydelser, der hviler på et rent aftaleretligt grundlag. Når skrevne medier som f.eks. aviser er afskåret fra at udkomme pga. faglige aktioner mv., er der sædvane for at kreditere abonnenterne et beløb svarende til betalingen for deres abonnement i den tid, avisen ikke er udkommet.

20.3.d. Særlige reguleringstemaer

Der har – endnu – ikke udviklet sig nogen veletableret aftalepraksis for aftaler om forskellige typer af digitale tjenesteydelser, herunder databaseanvendelse, Internet-adgang og teletransmission. Transaktionen kan derfor siges at lide af samme børnesygdomme som andre IT-aftaletyper: Parterne skriver under uden noget klart kendskab til de risici, der kan tænkes realiseret ved transaktionen, og det bliver så op til den efterfølgende retsudvikling – under anvendelse af de relevante retskildefaktorer – at finde rimelige og afbalancerede resultater i praksis. Blandt de problemer, der ofte forekommer, er følgende:

Domænerettigheder

Erfaringsvis har ganske mange Internet-leverandører, som har registreret domænenavne for deres kunder, efterladt kunden i en retlig usikkerhed om det registrerede domænes tilhørsforhold. I mangel af anden aftale er udgangspunktet her, at det er kunden, der optræder som *registrant* for det registrerede domænenavn: Det er i kundens interesse, domænenavnet benyttes, og også ham, der har finansieret erhvervelsen. Tilsvarende må udgangspunktet også være, at kunden har ret til at optræde som registrant i den pågældende hostmaster-database i overensstemmelse med de forskrifter, der til enhver tid er gældende for det pågældende toplevel-domæne.

Formidlingsansvar

Som anført andetsteds i denne fremstilling er der righoldige muligheder for, at den informationsudveksling, der formidles via en database eller via en hjemmeside der "hostes" af en Internetleverandør, realiserer retsbrud (f.eks. inden for markedsførings- og databeskyttelseslovgivningen) eller påfører tredjeparter øko-

nomiske tab (f.eks. ved krænkelse af tredjeparters immaterialrettigheder). Risikoen for, at sådanne krav rettes mod den part, der har stillet hjemmesiden til rådighed (f.eks. fordi "hovedgerningsmanden" ikke er inden for rækkevidde) har ført visse Internet-leverandører til at lægge klausuler i adgangen til at anvende hjemmesiden til bestemte former for informationsspredning. Også her gælder det almindelige udgangspunkt om aftalefrihed. I aftaleforhandlingen er det op til den Internet-leverandør, der stiller hjemmeside-funktionalitet til rådighed for sine kunder, at lægge kriterier for, hvilken form for information der skal være adgang til at formidle herfra.

Trafikmålinger

Som nævnt i afsnit 20.3.a. vil brugerens "betaling" for brug af visse Internet-tjenester ske ved annonceeksponering. Dette betalingskrav kan være baseret på forskellige former for eksponering, f.eks. at brugeren har *set* en bannerannonce (f.eks. undervejs i en søgning), at han har *klikket* på den ("CPC" – *cost per click*), eller at han rent faktisk har *reageret* på den ved at lade sig registrere hos annoncøren ("CPL" – *cost per lead)* eller købt en ydelse hos denne ("CPA" – *cost per action*). Sådanne betalingsordninger bør altid baseres på troværdige trafikmålinger, der gennem logning registrerer den kommunikation, der sker fra og til den pågældende hjemmeside. Det er derfor nødvendigt at underkaste tjenesteudbyderen visse kontrolforanstaltninger, der gør det muligt for annoncøren at forvisse sig om rigtigheden af disse logs.

20.4. Elektronisk betaling

20.4.a. Problemstillingen

Begreber

Et særligt problem ved at præstere ydelser i åbne net – og i sig selv en "digital ydelse" af særlig art – er *betalingen*, dvs. den handling, hvorved debitor ad digital vej fyldestgør sig for en pengeforpligtelse ved at give kreditor rådighed over rede penge eller hvad der i likviditet og betalingsevne svarer dertil. For en almindelig gennemgang af betalingsydelsens retsforhold henvises til den almindelige fremstilling hos *Bryde Andersen & Lookofsky* (2005), kap. 3. De spørgsmål, der behandles i det følgende, drejer sig om *hvordan* en pengeydelse kan præsteres digitalt, og *hvilke* retlige begrænsninger der gælder herfor.

Systemerne

En oversigt over de midler, hvormed betaling kan effektueres via nettet eller på anden måde, ville helt sprænge rammerne for denne fremstilling. Selv hvis man afgrænser feltet til de rene

Internet-betalinger, findes der et væld af forskellige løsninger, danske såvel som internationale, og af større eller mindre udbredelse. Ingen af disse løsninger har til dato opnået en sådan udbredelse, at der er grund til fremhævelse. Når dertil kommer, *at* det danske betalingsmarked er domineret af de betalingstjenester, der udbydes via PBS, og *at* adgangen til at benytte betalingssystemer herhjemme er underlagt væsentlige retlige begrænsninger i lovgivningen, er det hensigtsmæssigt at systematisere en fremstilling af dette område efter strukturen i den særlige lovgivning herom.

LVB

En væsentlig del af den elektroniske betalingshandling er undergivet en særlig, til dels offentligretlig, regulering ved lov nr. 414 af 31. maj 2000 om visse betalingsmidler, jf. lovbekendtgørelse nr. 1501 af 20. december 2004 med senere ændringer.

LVB er gennemført på grundlag af den betænkning, et udvalg under Forbrugerstyrelsen har afgivet i april 1999 om "regulering af visse betalingsmidler og adgangskoder". Til loven hører et antal bekendtgørelser. Lovens forgænger, *betalingskortloven*, hvorfra hovedparten af dens bestemmelser stammer, blev i sin tid gennemført på grundlag af Industriministeriets rapport om betalingskort, betænkning 965/1982. Den oprindelige lov blev dog revideret flere gange senere, bl.a. på grundlag af et forslag i betænkning 1255/1993 om *home banking*.

LVB's hovedformål

Lovens formål er at sikre, at betalingsmidler, der er omfattet af loven, er sikre og velfungerende, jf. § 4, stk. 1. Denne generalklausul følges op af en række særlige regler, hvorefter et betalingssystem skal indrettes og virke således, at der sikres brugerne *gennemsigtighed*, *frivillighed*, *beskyttelse mod misbrug* samt *fortrolighed* om brugerens anvendelse af betalingsmidlet. De tre målsætninger om overskuelighed, frivillighed og beskyttelse mod misbrug er bærende for loven og udtrykkes i en række af dens enkelte materielle regler og tilsynsbestemmelser. I et generelt perspektiv skal der bl.a. løbende træffes de juridiske, organisatoriske, driftsmæssige, tekniske og sikkerhedsmæssige foranstaltninger, som er nødvendige for, at der er tale om et sikkert og velfungerende betalingssystem, jf. § 4, stk. 2.

Elektroniske penge

Ved siden af LVB gælder kapitel 19 i lov om finansiel virksomhed, jf. nærmere i afsnit 20.4.g. Hvor LVB primært søger at regulere brugerens beskyttelse mod uønskede sikkerhedsmæssige og markedsføringsmæssige hændelser, angår kapitel 19 primært sikkerheden for udstederens soliditet, når der er tale om udstedelse af elektroniske penge i snæver forstand.

20.4.b. Betaling og løfte

Jus og faktum

Når man nærmer sig den digitale betalings retsspørgsmål er det vigtigt at slå fast, at en betalingshandling såvel har en faktisk som en retlig side, jf. nærmere *Bryde Andersen & Lookofsky* (2005), s. 129 f. De to sider er forholdsvis indlysende i den fysiske verden (illustreret ved forskellen mellem en pengeseddel og en gældspost), men kan fortone sig i den digitale, hvor der i alle tilfælde er tale om overførsel af bits via en eller flere troværdige tredjeparter. Som nærmere præciseret det anførte sted er en betaling i sig selv en faktisk handling: Ganske som selve gælden mellem to parter har faktisk/økonomisk karakter, er det i sig selv et faktisk forhold, at sedler og mønter skifter hænder, eller at konti udjævnes. Men når betaling sker, er dette udtryk for en "vilje" til at indfri en skyld, som i sig selv kan være genstand for fortolkning.

Denne dobbelthed mellem det faktiske og det retlige træder navnlig frem ved betalingsoverførsler. Det første, nødvendige, led heri er *meddelelsen* fra debitor til kontoføreren om, hvilket beløb der skal overføres og til hvem. Overførslens *faktiske side* fremtræder ved, at kontooverførslen posteres. I en dankortbetaling udgøres det faktiske element ved dankortets fysiske kontakt med betalingsautomaten (og den heraf følgende kontering), medens det juridiske element træder frem ved betalerens indtastning af PIN-kode og efterfølgende tryk på "godkend"-knappen.

De to aspekter af betalingshandlingen er forbundet med forskelligartede retlige problemer. Den del af betalingshandlingen, der rummer betalerens *viljeserklæring*, er genstand for fortolkning og udfyldning som enhver anden viljeserklæring. Er betaling erlagt i urigtig formening om skyld, spiller det således en væsentlig rolle for retten til tilbagebetaling, hvilken bevidsthed den betalende havde om forpligtelsen: Kendte han, eller burde han kende, til de forhold, der begrunder den manglende pligt til at betale, er det nærliggende at anse betalingshandlingen som en viljestilkendegivelse og dermed nægte tilbagesøgning. I tilsvarende omfang må en sådan betaling betragtes som "æresgæld", som betaleren frafalder sin ret til at bestride, når den er gennemført, sml. DL 5-14-55. Er betalingsmodtageren derimod i ond tro om betalingens pligtmæssighed, taler dette – ganske som i løftetilfælde – for ikke at lade betalingen være endelig og gyldig. Den faktiske side kan i sig selv udløse pligter og rettigheder i henhold til et nærmere angivet retsgrundlag, f.eks. afbrydelse af en forældelsesfrist.

Omkostningssiden

Enhver betalingstransaktion er forbundet med omkostninger af økonomisk eller anden art. Valget af betalingsmetode beror til

enhver tid på en afvejning, hvor *omkostningerne* ved at gennemføre betalingstransaktionen (f.eks. betale et checkgebyr) sammenholdes med størrelsen af den *risiko*, parterne løber, hvis denne slår fejl (f.eks. muligheden for at afvise en check, der indløses af en falskner). Betaling med mønter og sedler er velegnede til småpengebetalinger (også kaldet "mikrobetalinger") som f.eks. køb af dagligdagens livsfornødenheder, men upraktiske ved større betalinger (også kaldet "makrobetalinger") som f.eks. køb af motorkøretøjer og fast ejendom. Omvendt er det upraktisk at skulle gennemføre det papirarbejde, der består i at skrive en check eller påtegne en betalingsslip via et kreditkort, hvis det drejer sig om ørebeløb.

20.4.c. Betalingsmidler og betalingssystemer

De systemer til elektronisk betaling, der findes i øjeblikket, kan inddeles efter forskellige kriterier: Hvem står bag systemet? Hvilke betalingstransaktioner understøtter det? Er systemet baseret på hardware eller software? Anvender det troværdige tredjeparter? I en bred karakteristik kan man sondre mellem to typer af betalingssystemer:

Konto-til-konto

Den første kan beskrives som den digitalt initierede *konto-til-konto-betaling*. Ved denne betalingsform flytter debitor et beløb fra sin konto til kreditors ved hjælp af en digital meddelelse. Betalingsformen kendetegnes ved, at debitor på forhånd råder over et beløb eller en trækningsret hos sit kontoførende pengeinstitut, der kan fyldestgøre kreditor, og at også betalingsmodtageren indgår i et kontoforhold, der sætter ham i stand til at modtage betalingen. I det omfang betalingen ikke indebærer noget særligt "betalingsmiddel" (overførslen igangsættes f.eks. ved en telefonisk eller skriftlig anmodning uden brug af kode eller lignende middel), er den alene underlagt almindelige regler. LVB gælder således ikke.

Betalingsmidler

Den anden type indebærer derimod et *betalingsmiddel*. Som almindelig regel vil dette betalingsmiddel tjene til at igangsætte en konteringsproces af mere eller mindre anonym beskaffenhed. Det er disse tilfælde, der er omfattet af LVB. I sin oprindelige skikkelse var betalingskortloven alene afgrænset til "betalingssystemer med betalingskort"; men i overensstemmelse med den almindelige IT-retlige lovgivningsudvikling hen imod en teknologineutral begrebsanvendelse er LVB afgrænset omkring det generelle begreb "betalingsmiddel". Herved forstås, jf. § 1, stk. 2, fire typer af betalingsmidler:

- hævekort mv.

I en første undergruppe finder man hævekort og betalingskort, som er knyttet til bestemte brugere, jf. § 1, stk. 2, nr. 1. Med dette begreb markeres en afgrænsning mod betalingsmidler, der kan gøres gældende af indehaveren, og som følgelig ikke anvendes som *legitimationsbevis* ved betalingen. I det omfang sådanne ikke-brugerbestemte betalingsmidler er bærere af en økonomisk værdi, gælder reglerne om e-penge i lov om finansiel virksomhed, kapitel 19, jf. LVB § 1, stk. 3, nr. 1.

Retspraksis ifølge betalingskortloven har forstået dette begreb ganske vidt, se således *U 1992.29 SH* om den såkaldte "VEKO"-check. Checken, der var udstedt af en kæde af lokale forretningsdrivende med en gyldighed på 14 dage og gav adgang til at få udleveret varer, blev betragtet som et betalingskort. Allerede med denne afgørelse lå det klart, at der ikke nødvendigvis skal være tilknyttet et plastikkort til betalingssystemet. Det afgørende kriterium er, at kortet anvendes som et legitimationsbevis af særlig karakter i betalingsøjemed, jf. FT fra 1983/84, 2. samling, spalte 789 ff.

- andre legitimationsmidler

I en anden undergruppe finder man andre fysiske legitimationsmidler, som er knyttet til bestemte brugere, og som er beregnet til *elektronisk* aflæsning, jf. § 1, stk. 2, nr. 2. Praktiske eksempler herpå er de "brobizz"-systemer mv., der anvendes til at præstere betaling ved passage af broer eller færgeanlæg.

- koder mv.

Som et logisk modstykke til den førnævnte gruppe omtaler § 1, stk. 2, nr. 3, for det tredje "koder og biometriske værdier, som er beregnet til at legitimere brugeren." Herved sigtes f.eks. til de passwords eller andre koder, som kan anvendes i forbindelse med Internet-handel. Således vil en digital signatur, der anvendes til at effektuere en betaling med, være omfattet, jf. LES § 11, stk. 5, der med sin tilbagevisning til LVB's erstatningsregler forudsætter en sådan anvendelse. Ligeledes vil man her kunne placere de betalingssystemer, der i disse år er under opbygning omkring GSM-mobiltelefonen: Gennem den identifikation, SIM-kortet knytter til kunden, og som kan verificeres gennem en besked, der transmitteres via GSM-nettet, kan der udvirkes en debitering af abonnentens konto.

- e-fordringer

Den sidste undergruppe er de elektronisk registrerede fordringer, som udsteder er forpligtet til at indfri på brugers anmodning, jf. § 1, stk. 2, nr. 4. Med denne bestemmelse regulerer loven elektroniske penge i bred forstand (sml. om det snævrere begreb LVB § 1, stk. 3, nr. 1), forstået som elektronisk registrerede fordringer på en udsteder, som kan benyttes til køb af varer eller tjenesteydelser hos udstederen eller andre. Bestemmelsen er anvendelig, uanset hvor den pågældende fordring opbevares. Den

gælder således også, selv om opbevaring sker på brugerens eget udstyr. Eksempler herpå er forudbetalte telefontidkort. Se nærmere hertil: *Helen Holdt:* Elektroniske betalinger i forbrugerforhold, TemaNord 1998:560 (Udgivet af Nordisk Ministerråd), 1998, 234 ff.

Aktører

De nævnte typer af elektroniske betalingssystemer involverer en fast kreds af aktører:

- betaleren

Den første – og væsentligste – aktør er *betaleren*, dvs. den, der anvender betalingsmidlet til at præstere en betaling overfor en kreditor. I LVB's terminologi defineres denne part almindeligvis som *brugeren*. Herved forstås, jf. lovens § 3, stk. 1, den, der indgår aftale med udsteder om brug af et betalingsmiddel, eller den, der i forhold til udsteder er retmæssig bruger af et forudbetalt betalingsmiddel.

- betalings-modtager

Den anden – og umiddelbart ligeså iøjnefaldende – part, er *betalingsmodtageren*, f.eks. den, der indgår i et retsforhold til betaleren. Denne part defineres i LVB § 3, stk. 4, som "den, hos hvem brugeren kan anvende betalingsmidlet til at erhverve varer eller tjenesteydelser, foranledige overførsel af beløb eller foretage andre betalingstransaktioner." Betalingsmodtageren behøver ikke være erhvervsdrivende. Der kan f.eks. også være tale om en privatperson eller institution eller en offentlig myndighed.

Mellem betaler og betalingsmodtager optræder nu de tekniske mellemled, der indebærer, at betalingshandlingen efter LVB adskiller sig fra kontant- og checkbetalingen mv.

- indløser

Indløseren er det ene mellemled, der optræder som mellemmand mellem betaleren og medkontrahenten. Indløseren defineres i LVB § 3, stk. 3, som "den, som indgår aftale med betalingsmodtageren om tilslutning til betalingssystemet". En købmand, der ønsker at kunne modtage Dankort-betalinger, vil således indgå aftale med Dankort A/S (et datterselskab til PBS A/S, udskilt i 2000) om at kunne indløse Dankort-betalinger hos denne indløser. Dankort A/S vil herefter i kraft af aftaler med de brugere (kortindehavere), der anvender systemet til betaling, foretage den fornødne opkrævning eller debitering hos den enkelte betaler.

- udsteder

Endelig er *udstederen* den part, som brugeren indgår aftale med om udstedelse og anvendelsen af betalingsmidlet. Af de netop nævnte grunde (mange udstedende pengeinstitutter; én indløser) vil udstederen ikke være identisk med indløseren: Et Dankort, der anvendes i Danmark, er udstedt af et pengeinstitut, men indløses f.eks. af PBS.

Dankort på nettet

I forbindelse med den lovændring til betalingskortloven, der skete ved lov nr. 217 af 13. april 1999 med henblik på at sikre

muligheden for at anvende Dankort på Internet, jf. nu LVB § 14, har PBS siden april 1999 udbudt to løsninger til betaling med Dankort på Internet.

- SSL-baseret

Den ene løsning er SSL-baseret: Betalingen initieres ved, at brugeren logger sig op på en hjemmeside, hvor han udfylder en formular i browseren. Heri indtastes bl.a. korttype, kortnummer, udløbsdato, navn og adresse. Brugeren bekræfter derefter ordren ved at sende formularen fra browservinduet til Internet-forretningen. Da denne kommunikation foregår via SSL, er brugeren beskyttet mod kompromittering af oplysningerne undervejs. Det er imidlertid kun forretningsstedet, ikke kunden, der er udstyret med et certifikat. Forretningsstedet kender derfor ikke (nødvendigvis) den part, der indtaster oplysninger.

Ved modtagelsen af denne meddelelse sender forretningsstedet de relevante betalingssegmenter videre til PBS, der herefter – hvis ikke kortet er spærret mv. – afsender en bekræftelse på transaktionen. Denne bekræftelse fremsendes i form af en særlig *token*, og ved modtagelsen af denne bekræfter forretningsstedet overfor brugeren, at kortet og handlen er godkendt. Først når forretningen effektuerer ordren og sender varen til kunden, må forretningen trække pengene på brugerens kort. Dette sker ved, at brugerens data sammen med den fremsendte token videresendes til PBS, der herefter sørger for, at pengene bliver overført fra brugerens konto til forretningens konto.

- SET-baseret

Den anden løsning er baseret på SET-standarden og sikrer dermed betalingernes integritet og konfidentialitet gennem kryptering af alle elementer i transaktionen. Systemet forudsætter, at både betalingsmodtageren og kortholderen (kunden) er udstyret med et certifikat. PBS optræder som troværdig tredjepart, der certificerer identiteten af de personer, der optræder under krypteringsnøglen eller – ved public key-kryptering – den offentlige nøgle i nøgleparret. Af samme grund kan denne betaling kun ske til særligt udnævnte web-butikker (f.eks. forsikringsselskaber, boghandlere og rejsebureauer), der udbyder deres varer og tjenester fra særlige web-servere. Betalingen sker via kundens pengeinstitut og med PBS som mellemled. Det teknologiske grundlag for dette projekt er et software-produkt ved navn *Net.Wallet*. Clearingen sker via programmet Net.Registry, der ligger hos PBS, som registrerer transaktionen og som overfører de beløb, der skal betales.

20.4.d. Offentligretlig regulering

Efter dansk lovgivning er der flere kontrolinstanser, der fører tilsyn med den måde, hvorpå de pågældende systemer *markedsføres*, henholdsvis den *soliditet*, hvormed brugerne sikres mod at lide økonomiske tab gennem brugen af systemerne.

Primært forbrugere

LVB søger først og fremmest at beskytte forbrugere i rollen som betalere. Erhvervsdrivende betalere er principielt ikke omfattet. Imidlertid har man ønsket at beskytte den forbruger, der anvender et betalingsmiddel, der er etableret med sigte på anvendelse i erhvervsforhold. Dette har ført til den afgrænsning, der fremgår af lovens § 1, stk. 4: LVB gælder ikke for betalingsmidler, der *udelukkende* udbydes til erhvervsdrivende. Udstederen skal dog godtgøre, at brugeren i tilslutningsaftalen har forpligtet sig til udelukkende at anvende betalingsmidlet erhvervsmæssigt, og udstederen må ikke efterfølgende acceptere, at betalingsmidlet anvendes på anden måde (altså til forbrugsbetalinger). Betalingsmidler, som udbydes med henblik på såvel erhvervsmæssig som ikke-erhvervsmæssig anvendelse, er derimod fuldt ud omfattet af loven, jf. § 1, stk. 5, der dog modificerer dette udgangspunkt i relation til visse beskyttelsesregler.

Den offentligretlige regulering indebærer dels, at udstedere af betalingssystemer er underkastet et offentligretligt tilsyn ved Forbrugerombudsmanden, dels at de er underlagt visse oplysningsforpligtelser

Anmeldelse

Inden for lovens område gælder en række forpligtelser, som søger at tilgodese lovens overordnede formål, jf. § 4. Udstedere af betalingsmidler skal anmeldes til Forbrugerombudsmanden, jf. § 6, under angivelse af en række detaljerede oplysninger om udstederens identitet og informationsmateriale. På grundlag af denne anmeldelse fører Forbrugerombudsmanden et tilsyn med de anmeldte udstedervirksomheder, jf. nærmere § 18. Tilsynet indebærer bl.a., at Forbrugerombudsmanden kan søge kritisable forhold ændret gennem forhandling, jf. nærmere § 4, stk. 3.

Oplysningsforpligtelser

De oplysningsforpligtelser, betalingssystemudbyderen er underlagt, knytter sig dels til *markedsføringen* af selve systemet, dels til forholdene omkring den *enkelte transaktion*: I forbindelse med indgåelsen af en aftale om anvendelse af et betalingsmiddel skal udstederen stille et informationsmateriale til rådighed, jf. nærmere § 7, stk. 1. Materialet skal i et let og forståeligt sprog sætte brugeren i stand til at anvende betalingsmidlet på en sikker og hensigtsmæssig måde og give oplysning om typiske omkostninger ved anvendelse af betalingsmidlet. Det skal særligt gøre

opmærksom på de sikkerhedsmæssige krav, som brugeren skal efterleve, samt hvilket ansvar brugeren kan ifalde ved tredjemands misbrug af betalingsmidlet. Ifølge LVB § 8 har brugeren krav på kvittering ved enhver transaktion, som iværksættes med betalingsmidlet, medmindre han på anden måde har let adgang til oplysninger om, hvorvidt og hvornår den pågældende transaktion er gennemført.

Kontantbetaling

Ifølge lovens § 10 er betalingsmodtager forpligtet til at modtage kontant betaling, hvis betalingsmodtageren modtager betalingsmidler, der er omfattet af denne lov, f.eks. betalingskort-betalinger. Denne pligt gælder dog ikke ved fjernsalg (f.eks. ved e-handel) eller ved betalingstransaktioner i ubemandede selvbetjeningsmiljøer (f.eks. på benzin-tankstationer).

20.4.e. Ansvar og misligholdelse

Udsteders ansvar

Ifølge LVB § 12, stk. 1, er udstederen af et betalingsmiddel ansvarlig overfor *brugeren* og *betalingsmodtager* for tab, som skyldes fejlregistrering, konteringsfejl, teknisk sammenbrud eller andre lignende omstændigheder, selv om fejlen er hændelig. Har brugeren fået meddelelse om, at betalingstransaktionen er anerkendt, er udsteder endvidere ansvarlig for tab hos brugeren, som skyldes, at den pågældende betalingstransaktion ikke gennemføres eller gennemføres mangelfuldt.

Der er altså tale om et objektivt ansvar; men loven modificerer det i to henseender. For det første gælder ansvaret kun inden for udstederens *kontrolsfære*. Hvis udstederen godtgør, at han ikke har haft mulighed for at gennemføre betalingstransaktionen pga. "ekstraordinært indgribende omstændigheder, som udstederen ikke har nogen indflydelse på, og som udstederen ikke burde have taget i betragtning", da brugeren modtog meddelelsen om, at betalingstransaktionen var anerkendt, er han ansvarsfri. Dernæst kan erstatningen nedsættes eller bortfalde, hvis brugeren forsætligt eller groft uagtsomt har medvirket til fejlen. Udsteder og indløser har bevisbyrden for, at et tab ikke skyldes de nævnte forhold, jf. § 12, stk. 5.

Indløsers ansvar

Ifølge LVB § 12, stk. 3 er indløser ansvarlig for tab hos betalingsmodtager, som skyldes fejlregistrering eller konteringsfejl, selv om fejlen er hændelig. Indløser er dog ikke ansvarlig for tab, som skyldes forhold hos betalingsmodtageren.

Misligholdelse

LVB § 12, stk. 2, regulerer den kontraktsretlige virkning af, at en betaling er udeblevet eller forsinket som følge af systemfejl. En betaling, der er udeblevet eller forsinket som en følge heraf,

giver ikke ret til at gøre misligholdelsesbeføjelser gældende overfor brugeren, bortset fra krav på rente. Er der sket træk på brugerens konto, anses betalingen dog for sket med frigørende virkning for brugeren.

20.4.f. Hæftelse for uberettiget brug

En væsentlig risiko ved at anvende elektroniske betalingsmidler er risikoen for, at betalingsanmodningen uberettiget forvanskes undervejs eller at der opstår tvivl om, hvorvidt betalingshandlingen er gyldigt igangsat. Risikoen for transmissionsfejl på linjen kan i den digitale verden løses ad teknisk vej, f.eks. gennem kryptografiske teknikker. Men uanset hvor pålidelige systemer der opbygges for at understøtte sikker identifikation, vil kædens svageste led stedse være det forløb, hvormed systemet sættes i gang med at gennemføre betalingen eller udvirke et forbrug (f.eks. via en mobiltelefon), der tilsvarende etablerer en betalingspligt. Hvis andre end den berettigede opnår kontrol med dette forløb, kan der gennemføres uberettigede hævninger, jf. strfl. § 279a, og påføres betalingsmidlets indehaver tab. Spørgsmålet er nu, hvem af de parter der indgår i betalingssystemet, der i sidste ende skal bære sådanne tab.

Udgangspunktet

LVB § 11 opstiller et kompliceret regelsæt, der fastlægger brugerens hæftelse i tilfælde, hvor et betalingsmiddel anvendes uberettiget. Reglerne gælder både for betalingsmidler, der umiddelbart opfattes som sådanne – f.eks. betalingskort – og får midler, der fremtræder som integreret i en ydelse, f.eks. SIM-kortet i en mobiltelefon, se herved til illustration *JÅF 1999.163*, hvor forbrugeren hæftede for forbruget fra en mobiltelefon, som var stjålet fra en aflåst bil.

Se ligeledes Forbrugerklagenævnets afgørelse i *Forbrugerjura 2003.65,* hvor forbrugeren først havde spærret sin mobiltelefon tre dage efter, at telefonen var stjålet, idet forbrugeren troede, hun havde forlagt telefonen, eller at hendes små børn havde gemt den. Først tre dage senere spærrede hun mobiltelefonen, der på dette tidspunkt var misbrugt for ca. 7.000 kr. LVB § 11, stk. 2 fandt anvendelse, da telefonen var tændt, hvorfor den til SIM-kortet hørende personlige kode var aktiveret. Forbrugeren hæftede derfor for op til 1.200 kr. for det uberettigede forbrug. Da det store forbrug imidlertid havde fundet sted ganske kort tid efter tyveriet, fandt nævnet ikke, at forbrugeren skulle hæfte for mere end selvrisikobeløbet.

Hovedreglen er, jf. LVB § 11, stk. 1, at udsteder i forhold til brugeren hæfter for tab som følge af andres uberettigede anvendelse af et betalingsmiddel, medmindre andet følger af stk. 2-6.

Og i alle tilfælde hæfter brugeren kun, hvis transaktionen er korrekt registreret og bogført. Men denne almindelige regel suppleres med forskellige hæftelsesregler for forskellige niveauer af uberettigede brugssituationer, der bl.a. beror på, om den personlige, hemmelige kode (PIN-kode) har været anvendt i forbindelse med den retsstridige brug.

Kodemisbrug

Har den hemmelige kode været anvendt, og foreligger der *ikke særlige forhold*, jf. herom i stk. 3, hæfter brugeren med op til 1.200 kr. for tab som følge af andres uberettigede brug. Da brugeren hæfter uanset årsagen til at koden er anvendt, kan man betragte bestemmelsen som en selvrisiko, der knytter sig til disse objektivt bestemte tilfælde. Teoretisk set åbner dette mulighed for, at gerningsmanden ved at gætte sig til PIN-koden (et forhold, der er forholdsvis usandsynligt givet de 10.000 muligheder, hvorpå koden kan sammensættes) påfører indehaveren en hæftelse op til dette maksimum. At man har gjort denne hæftelse objektiv skyldes en antagelse om, at brugeren må formodes at bære en del af skylden for, at koden er anvendt (f.eks. fordi brugeren ikke har sikret sig mod afluring i forbindelse med indtastning til en betalingsterminal).

Hvis koden har været anvendt ved den uberettigede brug, og en af de i stk. 3 omhandlede *kvalificerede forhold* foreligger, kan brugerens hæftelse stige til 8.000 kr. De kvalificerede forhold, der udløser en sådan hæftelse, kendetegnes ved, at den uberettigede brug vil kunne henføres til brugeren. Det påhviler i alle tilfælde udstederen at godtgøre, at det angivne forhold kan tilskrives indehaveren af betalingsmidlet.

Det kan for det første tænkes, at brugeren har *undladt at underrette* udsteder snarest muligt efter at have fået kendskab til, at koden er kommet til den uberettigedes kendskab, jf. nr. 1.

Der foreligger en vis praksis hos domstolene, Forbrugerklagenævnet og Pengeinstitutankenævnet, der belyser disse regler. Se hertil *Karstoft* (2001), s. 95 ff. Ved dommen i *U 1995.796 Ø* kunne kortindehaveren ikke finde sin pung om torsdagen. Han regnede med at have forlagt den, men først lørdag blev han positivt klar over, at den var væk. Han underrettede herefter pengeinstituttet mandag. Retten fandt, at han hæftede ifølge den daværende (tilsvarende) betalingskortlovs § 21, stk. 3, nr. 2, for beløb trukket søndag og mandag ved anvendelse af den korrekte PIN-kode. Omvendt fandt Pengeinstitutankenævnet ved sin afgørelse 715/1993, at kortindehaveren kun hæftede med selvrisikoen i en situation, hvor kortet og PIN-koden var blevet stjålet. Kortindehaveren havde underrettet pengeinstituttet, så snart han opdagede, at betalingskortet var væk, og nævnet lagde

ikke vægt på, at han i forbindelse med tyveriet dagen før kun overfladisk havde checket, at alt var tilbage i pungen, da han fik den tilbage. I *JÅF 2000.108* fandt Forbrugerklagenævnet ikke, at det havde været groft uagtsomt af en forbruger at opbevare en tændt mobiltelefon i lommen på en jakke, der befandt sig i en bevogtet garderobe. Forbrugeren opdagede først tyveriet af mobiltelefonen dagen efter, og spærrede først 5 timer herefter telefonen. Han hæftede derfor kun for det forbrug, der var sket fra opdagelsestidspunktet og til spærring fandt sted. Se i øvrigt om praksis vedrørende betalingskortlovens § 21, stk. 3, nr. 2 og 3, *Peter Blok*s redegørelse i Pengeinstitutankenævnets årsberetning fra 1996, s. 11 ff.

For det andet kan der foreligge et *betroelsestilfælde*, idet brugeren har overladt koden til den, der har foretaget den uberettigede brug, jf. § 11, stk. 3, nr. 2. Bestemmelsen må afgrænses overfor § 11, stk. 6, hvor der er tale om, at såvel kortet som den hemmelige kode er overladt til gerningsmanden.

Den tredje mulighed er, at brugeren (eller nogen, som han har overladt kortet til) har udvist "groft uforsvarlig adfærd", der har *muliggjort* den uberettigede brug, jf. § 11, stk. 3, nr. 3.

Kortmisbrug

Brugeren hæfter med op til 8.000 kr. for tab som følge af andres uberettigede anvendelse af betalingsmidlet, når betalingsmidlet har været *aflæst fysisk eller elektronisk* og den uberettigede i tilknytning hertil har anvendt en *falsk underskrift*, og udsteder godtgør, at et af de to følgende forhold foreligger. For det første at brugeren eller nogen, som brugeren har overladt betalingsmidlet til, har *undladt at underrette udsteder* snarest muligt efter at have fået kendskab til, at betalingsmidlet er bortkommet. Eller for det andet, at brugeren eller nogen, som brugeren har overladt betalingsmidlet til, ved *groft uforsvarlig adfærd* har muliggjort den uberettigede anvendelse.

Legitimationstilfælde

Ifølge § 11, stk. 6, hæfter brugeren uden beløbsbegrænsning for tab, der opstår som følge af andres uberettigede anvendelse af betalingsmidlet, når den til betalingsmidlet hørende personlige, hemmelige kode er anvendt, og udsteder godtgør, at brugeren har oplyst koden til den, der har foretaget den uberettigede anvendelse. Det er dernæst et krav, at den uberettigede brug er sket under omstændigheder, hvor brugeren indså eller burde have indset, at der var risiko for misbrug. Denne regel er udtryk for et almindeligt princip om, at den, der har skabt en legitimation for en anden, hæfter for dennes dispositioner overfor godtroende (jf. stk. 7) tredjeparter. I så fald fører almindelige aftaleretlige principper til, at hovedmanden hæfter, som om han selv havde disponeret.

- modtagers forhold

De nævnte regler finder ikke anvendelse, hvis betalingsmodtageren (forretningsstedet) vidste eller burde vide, at brugeren var uberettiget til at benytte kortet, jf. LVB § 11, stk. 8.

I medfør af den tidligere betalingskortlovs § 12a og mfl. § 17 har Forbrugerombudsmanden i december 1996 udstedt retningslinjer vedrørende fjernsalg mv. i betalingssystemer med betalingskort. Retningslinjerne, der fortsat er gældende, finder anvendelse ved fjernsalgstransaktioner, hvorved forstås betaling uden en aflæsning af betalingskortet kombineret med brugerens autorisation i form af en underskrift eller angivelse af PIN-kode. I retningslinjerne hedder det bl.a., at kortudstedere ikke må gøre kortindehaveren ansvarlig for, at kortindehaveren har videregivet det *ikke-hemmelige* nummer på betalingskortet (pkt. 4). Det er altså lovligt at anvende selve kort- eller kontonummeret på et betalingskort. Gør kortindehaveren gældende, at en fjernsalgstransaktion hverken er foretaget eller bemyndiget af ham, at debiteringen overstiger det beløb, der er aftalt med betalingsmodtageren, at den bestilte ydelse ikke er leveret, eller at kortindehaveren eller den angivne modtager har udnyttet en lovbestemt eller aftalt fortrydelsesret ved at undlade at modtage eller afhente den bestilte ydelse, skal kortudstederen stille opkrævningen i bero, medens indsigelsens rigtighed undersøges. Kan indsigelsen ikke umiddelbart tilbagevises som uberettiget, må kortudstederen alene opkræve det beløb, som kortindehaveren kan vedkende sig. Kortindehaverens ret til at fremkomme med disse indsigelser må ikke begrænses ved reklamationsfrister i kortindehaverreglerne, ligesom kortindehaverens indsigelse imod en fjernsalgstransaktion ikke i sig selv må medføre, at kortudsteder inddrager kortet eller opsiger aftalen med kortindehaveren. Se nærmere hertil *Karstoft* (2001), s. 91 ff.

20.4.g. Særligt om elektroniske penge

Begreb

Udtrykket "elektroniske penge" (eller e-penge) anvendes almindeligvis om betalingsværdier, som er oplagret elektronisk på et elektronisk medium, f.eks. et chipkort eller en computer, som anerkendes som betalingsmiddel af andre foretagender end det udstedende institut, som skabes med det formål at blive stillet til rådighed for brugerne som elektronisk erstatning for mønter og sedler, og som skabes med henblik på elektroniske betalingsoverførsler af begrænset værdi, se herved definitionen i art. 1, stk. 3, litra b) i direktiv 2000/46/EF af 18. september 2000 om adgang til

at optage og udøve virksomhed som udsteder af elektroniske penge, EFT 2000 L275/39.

Ud fra den angivne definition kan man sondre mellem hardwarebaserede og softwarebaserede elektroniske penge. En tilsvarende sondring ligger til grund for LVB § 1, stk. 2, nr. 3 hhv. 4. I *hardware*-baserede systemer ligger den økonomiske værdi på et kort, som brugeren bærer på sig (typisk et magnetkort eller chipkort). De *software*-baserede systemer knytter sig til en kode, som udveksles mellem betaler og betalingsmodtager med henblik på efterfølgende at blive clearet via en konto.

Softwarebaserede

Fordelen ved softwarebaserede e-penge er, at metoden er enkel at implementere for brugeren. Den software, der styrer systemet, kan ubesværet hentes ned over Internet og installeres umiddelbart med et minimum af omkostninger. Ulempen kan være, at brugeren låses fast til den terminal, hvor programmet er installeret, når han skal betale. Da brugeren ikke kan forventes at befinde sig ved sin terminal altid, består der dernæst en risiko for, at tredjeparter uberettiget gør brug af systemet – et problem, der dog kan reduceres ved brug af forskellige sikkerhedsmekanismer (f.eks. password-beskyttelse).

Hardware-baserede

Fordelen ved hardware-baserede e-penge ligger først og fremmest i deres fleksibilitet. Besiddelsen af chipkortet er nødvendig for at kunne betale. Dette er på den ene side besværligt, men på den anden side også chipkortets styrke: Ikke blot tillader denne portabilitet betaling fra forskellige terminaler, f.eks. såvel fra brugerens egen PC (udstyret med chipkort-læser) eller fra en betalingsautomat (f.eks. en telefon); ved at sikre sig rådighed over chipkortet undgår man risikoen for tyveri – en risiko, der alt andet lige er større, når man betjener sig fra en enkeltstående terminal, som andre – i ens eget fravær – kan tænkes at bemægtige sig adgang til.

Der findes to former for chipkort, et hukommelseskort, der kun kan oplades med værdi én gang og som derefter løbende kan holde rede på forbruget af denne værdi, og et processorkort, som kan genoplades, og som dernæst kan forsynes med andre funktioner (f.eks. digital signatur el.lign.).

Idé

For begge typer af løsninger er der tale om, at betaleren lader et informationssystem op med *pengesymboler*, som herefter sendes videre til en betalingsmodtager under omstændigheder, hvor denne på et tidspunkt kan erstatte disse pengesymboler med kontante penge eller betalingsoverførsler. Denne grundlæggende idé varieres på forskellig vis i de systemer, der findes på markedet. Nogle systemer er opbygget således, at brugeren forud for sin

betaling anmoder sit pengeinstitut om en digital pengeseddel. Meddelelsen fastslår sin egen værdi samt navnet på den bank, som har afgivet den. Herudover indeholder meddelelsen en unik, krypteret datamængde. Meddelelsen lagres på kundens harddisk, hvorfra den ved hjælp af et program kan udvirke krypterede informationer, der modsvarer de beløb, kunden ønsker overført til kreditor. Når kreditor herefter præsenterer meddelelsen for banken (første gang), honoreres den. Andre systemer indebærer, at der sker en løbende overvågning og beregning af et forbrug, som efterfølgende debiteres brugeren, f.eks. ved at beløbet – efter aftale med en Internet-udbyder – blot lægges på månedsregningen, principielt på samme måde som checkkontoen løbende belastes for de udstedte checks

Anonymitet

En central ingrediens – og kvalitetsparameter – ved et elektronisk betalingssystem er den grad af anonymitet, der sikres brugeren. På den ene side har brugeren en iøjnefaldende interesse i at kunne optræde anonymt ved indkøb af bestemte ydelser (at opgive sit navn er generelt ensbetydende med en risiko for efterfølgende markedsføringshandlinger; dertil kommer, at visse ydelser kan rumme oplysninger af følsom art, f.eks. medicinalindkøb). Et middel til at opnå denne anonymitet er at gennemføre betalingen således, at betalingsmodtageren blot verificerer, hvilken bank der står bag den elektroniske pengeseddel. Det er altså kun betalerens identitet, der er skjult.

For at kunne anvendes som betalingsmiddel må der være sikkerhed for, at de digitale penge kun kan bruges en gang. Dette sker ofte således, at den enkelte "mønt" i forbindelse med betalingshandlingen fremsendes til den udstedende bank, hvor den verificeres on-line og "logges" (dvs. registreres). Gennem denne clearing sikres det, at en digital "mønt" vil blive afvist, hvis den præsenteres til betaling en gang til. Den udstedende bank kender altså den totale værdi af udstedte digitale mønter. Når betalingen er gennemført, krediteres modtagerens bankkonto.

Danmønt

Danmønt-kortet er et dansk småpengekort, som er blevet til i et samarbejde mellem TeleDanmark A/S (tidligere KTAS) og PBS og udbudt siden 1992. I sin oprindelige skikkelse deltog også Hovedstadsområdets Trafikselskab i projektet. Baggrunden for projektet var, at der var udviklet en række kort-baserede betalingssystemer, der udelukkende understøttede bestemte typer af ydelser (HT-rabatkort, telefonkort mv.), men som anvendte den samme teknologi (chipkort, kryptering mv.). Den praktiske afvikling af systemet varetages af selskabet Danmønt A/S, der står

såvel for planlægning og koordinering (vedtagelse af standarder og specifikationer for kort og terminaler mv.), for den driftsmæssige afvikling og overvågning som for selve betalingsclearingen.

Systemet forudsætter, at en betalingsmodtager (et pengeinstitut, et telefonselskab eller et benzinfirma) fungerer som *kortudsteder*. Når kortet produceres, indbetaler kortudstederen dets pålydende til Danmønt, der herefter registrerer og krediterer forbruget af varer og tjenester på grundlag af kortet.

Regulering

Med reglerne i kapitel 19 i lov om finansiel virksomhed, jf. lovbekendtgørelse nr. 613 af 21. juni 2005, foreligger en tilsynsregulering af nogle af de brugerrisici, der er forbundet med elektroniske penge, hvilket med lovens § 308, stk. 1, forstås som "en pengeværdi, som er repræsenteret ved et krav på udstederen, der er lagret på et elektronisk medium". Elektroniske penge må ikke udstedes til *overkurs* og skal være *anerkendt* som betalingsmiddel af andre foretagender end udstederen. De må ikke udstedes med en højere værdi end 300 euro, jf. § 309.

Om forholdet mellem indehaveren og udstederen af elektroniske penge bestemmer lovens § 311, stk. 1, at ihændehaveren i op til *1 år efter* gyldighedsperiodens udløb kan anmode udstederen (eller det udstedende pengeinstitut) om at få restbeløbet *indløst* til pålydende uden andre omkostninger end dem, der er nødvendige for at gennemføre transaktionen. Betingelserne for genindløselighed i henhold til stk. 1 skal klart fremgå af aftalen mellem udstederen og ihændehaveren. I aftalen kan fastsættes, at beløb under 25 kr. ikke kan genindløses, jf. stk. 2.

Elektroniske penge kan kun udstedes af pengeinstitutter eller af virksomheder, der har opnået en særlig tilladelse hertil, jf. lov om finansiel virksomhed § 312. En virksomhed, der søger om tilladelse efter stk. 1 uden at være et pengeinstitut, skal have en aktiekapital, der mindst udgør et beløb svarende til 1 mio. euro, jf. § 308, stk. 4. Lovens tilsynsregler afhænger i øvrigt af, om de elektroniske penge udstedes med et pålydende over eller under 150 euro, se § 308, stk. 5.

20.4.h. Bevis- og sikkerhedsspørgsmål

Uberettigede hævninger

Den fundamentale forudsætning for opbygningen af et elektronisk betalingssystem er sikkerheden for, at overførte beløb bogføres korrekt, og at der ikke sker uberettigede hævninger mv. Uden en sådan sikkerhed vil brugerne ikke kunne udvise den tillid, der er nødvendig for at betjene sig af disse systemer. Som det gælder for andre sikkerhedsspørgsmål, beror graden af den

sikkerhed, man vil forvente, på en afvejning mellem omkostningerne ved at tilvejebringe et højt sikkerhedsniveau på den ene side og på den anden side størrelsen af det potentielle tab, som en sikkerhedsbrist vil realisere.

LVB indeholder ingen regulering af dette problem. Forbrugerombudsmanden har udtalt, at den tidligere betalingskortlovs § 22, stk. 4 (nu LVB § 12, stk. 5) – der efter sin ordlyd alene pålægger kortudsteder bevisbyrden for, at en transaktion ikke skyldes systemfejl (fejlregistrering, konteringsfejl, teknisk sammenbrud o.lign.) – indebærer, at kortudsteder skal kunne føre bevis for, at enhver betalingstransaktion, der fremgår af kontoudtog el.lign., faktisk har fundet sted, se f.eks. *JÅF 1990.7 ff.* Dette indebærer navnlig et bevis for, at betalingsmodtager har modtaget betalingen, og at konteringen har været korrekt. Det er imidlertid uklart, hvilke krav man skal stille til dette bevis, herunder om en udskrift af betalingsterminalens kontrolregister med angivelse af en korrekt indtastet PIN-kode vil opfylde beviskravene. LVB indeholder derimod ingen udtrykkelige regler om bevisbyrden i tilfælde, hvor det er omtvistet, om det er brugeren selv eller en uvedkommende tredjemand, der har gjort brug af kortet.

Finansrådet har den 30. august 1996 vedtaget et Kodeks om IT-sikkerhed i home-banking-systemer. Kodekset indeholder bl.a. krav om, at der som teknisk sikkerhedsløsning skal anvendes public key kryptering, således at forbrugerens hemmelige nøgle kan anvendes til at fremstille en elektronisk underskrift (digital signatur). Adgangen til den hemmelige nøgle skal beskyttes af et af forbrugeren valgt password, og forbrugerens offentlige nøgle må kunne anvendes til at verificere denne signatur. Systemet skal sætte signatur på transaktioner, der indeholder økonomisk forpligtende ordrer fra forbrugeren og i øvrigt give mulighed for, at oplysninger udveksles i krypteret form. Som minimum skal personlige oplysninger samt oplysninger vedrørende saldo og beløbsoverførsler udveksles i krypteret form. Videre hedder det, at systemet skal fremstille det kryptografiske nøglepar på en sådan måde, at den hemmelige nøgle ikke kan genskabes. Det skal sikre, at den hemmelige nøgle opbevares i krypteret form, når den ikke anvendes. Adgangen til at anvende forbrugerens hemmelige nøgle skal være beskyttet af et password bestående af mindst otte tal/bogstaver, som ikke må anvendes til andre formål. For så vidt angår kravene til skærmdialog og informationsindhold hedder det, at forbrugeren "ved programmets virkemåde" tydeligt skal gøres opmærksom på, når der sendes økonomisk forpligtende transaktioner til pengeinstituttet. Ligeledes skal forbrugeren kunne kontrollere de seneste økonomiske forpligtende transaktioner, der er afsendt til og modtaget af pengeinstituttet. Forbrugeren skal kunne spærre sin deltagelse i systemet døgnet rundt, og pengeinstituttet skal skriftligt bekræfte spærringen med angivel-

se af modtagelsestidspunktet. Ved mistanke om misbrug skal pengeinstituttet spærre for forbrugerens deltagelse i systemet. Maksimalt fem på hinanden følgende forkerte adgangsforsøg skal medføre automatisk spærring af adgang til systemet. Pengeinstituttet skal skriftligt underrette forbrugeren om, at spærring har fundet sted.

20.4.i. International regulering

I EU-retlig sammenhæng er en betalingstransaktion i sig selv en finansiel tjeneste, der ligesom andre finansielle tjenester bør kunne udbydes uden restriktioner på tværs af landegrænser. Det grænseoverskridende element spiller en særlig markant rolle i relation til sådanne betalingstjenester, der kan udnyttes via åbne digitale net. Da elektroniske betalingstjenester i stigende omfang anvendes af forbrugere, kan der også være et behov for at beskytte forbrugeren overfor udbyderen. Dette er baggrunden for, at Kommissionen på et tidligt tidspunkt har søgt at påvirke den måde, hvorpå elektroniske betalingstjenester udbydes. Hidtil er denne regulering søgt gennemført gennem "soft law".

1988-henstillingen

Den 8. december 1987 vedtog Kommissionen en henstilling om en europæisk adfærdskodeks for elektronisk betaling (forbindelse mellem penge- og finansieringsinstitutter og handlende/tjenesteydere samt forbrugere), se EFT 1987 L 165/72. Henstillingen formulerer en række minimumskrav til indholdet af de aftaler, der indgås mellem brugere og udbydere, samt om kompatibilitet, adgang og datasikkerhed: Aftaler mellem kortudstedere og kortindehavere bør f.eks. være skriftlige og indeholde klare regler om opsigelse og databeskyttelse, og gebyrfastsættelsen skal være gennemsigtig. Den suppleres med en henstilling af 17. november 1988 om betalingssystemer, herunder navnlig forholdet mellem kortindehaver og kortudsteder (88/590/EØF), EFT 1988 L 317/55.

1997-henstillingen

1988-henstillingen er senere afløst af en henstilling af 30. juli 1997 (97/489) om transaktioner med elektroniske betalingsmidler. Henstillingen er afgivet på grundlag af Kommissionens meddelelse om "Fremme af forbrugerens tillid til elektroniske betalingsmidler inden for det indre marked", KOM(97) 353, endelig udg., hvori der udpeges fire hovedområder, hvor der er behov for et betydeligt bidrag fra de offentlige myndigheders side inden for elektroniske betalinger: Passende overvågningsrammer for udstedelsen af elektroniske penge, retningslinjer mht. gennemsigtighed, ansvar og klagemuligheder, konkurrenceretlig klarhed samt sikkerhed mod misbrug og forfalskning.

Selv om også denne henstilling i sig selv er uforpligtende, er tonen skærpet. Det fremgår af præamblens pkt. 12, at Kommissionen nøje vil føre tilsyn med dens gennemførelse og eventuelt – hvis den finder gennemførelsen utilfredsstillende – vil stille forslag til den fornødne bindende lovgivning om de spørgsmål, der er omhandlet i henstillingen. Som frist herfor sættes 31. december 1998.

Ifølge artikel 1 finder henstillingen anvendelse på pengeoverførsler med elektroniske betalingsmidler (bortset fra pengeoverførsler, som finansielle institutioner giver ordre til og gennemfører) samt kontanthævninger med elektroniske betalingsmidler samt opladning og tømning af elektroniske pengeinstrumenter (f.eks. forudbetalte kort eller elektroniske værdienheder lagret i computere). Såvel dens anvendelsesområde som det væsentligste indhold af dens forpligtelser er stort set sammenfaldende med LVB.

Henstillingen pålægger udbyderen i god tid før udstedelsen af et elektronisk betalingsmiddel at give indehaveren meddelelse om kontraktsvilkårene for det pågældende betalingsmiddel. Meddelelsen skal foreligge skriftligt, eventuelt elektronisk, i letforståeligt sprog, i en lettilgængelig form og i den pågældende medlemsstats sprog. Nærmere regler om indholdet af denne oplysningsforpligtelse fastsættes i artikel 3. Herudover skal udstederen give indehaveren oplysninger om transaktioner, der er gennemført med et elektronisk betalingsmiddel. Blandt andet skal der som minimum gives en reference, der gør det muligt for indehaveren at identificere transaktionen samt det transaktionsbeløb, der debiteres indehaveren i faktureringsvalutaen. Herudover skal eventuelle provisioner og gebyrer angives tillige med den valutakurs, der er anvendt ved omregningen af valutatransaktioner. Disse regler fremgår af henstillingens artikel 4. Artikel 5 pålægger indehaveren (betaleren) at anvende det elektroniske betalingsmiddel i overensstemmelse med vilkårene for udstedelse og anvendelse af et betalingsmiddel. Indehaveren skal især træffe alle rimelige foranstaltninger for at garantere sikkerheden i forbindelse med det elektroniske betalingsmiddel, og de midler (f.eks. PIN-kode), der gør det muligt at bruge det. Opdager indehaveren, at det elektroniske betalingsmiddel er blevet kompromitteret, skal han omgående give udstederen besked. Det siges udtrykkeligt, at indehaveren ikke må notere sit personlige identifikationsnummer på letgenkendelig måde (f.eks. ved at skrive en PIN-kode på et betalingskort). Disse regler fremgår af artikel 5. Regler om indehaverens ansvar følger af henstillingens artikel 6. Indtil indehaveren har meddelt udstederen, at et elektronisk betalingsmiddel er blevet kompromitteret, skal indehaveren bære det deraf følgende tab op til en grænse på højest 150 ECU. Denne grænse gælder dog ikke, såfremt indehaveren har handlet svigagtigt, groft uagtsomt eller i strid med de førnævnte sikkerhedsregler. Herom handler henstillingens artikel 6. I artikel 7 er

der givet regler om udstederens ansvar. Foreligger der ikke en situation, hvor indehaveren har tilsidesat sine forpligtelser eller har handlet groft uagtsomt mv. er udstederen ansvarlig for transaktioner, der ikke gennemføres eller gennemføres mangelfuldt. Ansvaret gælder også, selvom en sådan transaktion indledes på terminaler eller andet udstyr, der ikke er under udstederens direkte kontrol eller enekontrol, blot udstederen har godkendt det pågældende udstyr. Ansvaret dækker beløbet for den transaktion, der ikke er udført, eller som er udført mangelfuldt, eventuelle rentedage samt det beløb, der er nødvendigt for at sætte indehaveren i samme situation, som før den pågældende transaktion fandt sted. Udstederen er ansvarlig overfor indehaveren af et elektronisk pengeinstrument (f.eks. et Danmøntkort) for tab af værdienheder lagret i pengeinstrumentet, hvis tabet skyldes, at det pågældende pengeinstrument eller den godkendte terminal mv. har fungeret forkert. Der er dog ikke ansvar, hvis indehaveren var bekendt med den pågældende fejl. Disse regler følger af henstillingens artikel 8.

20.4.j. Lov om offentlige betalinger

Loven

Ved lov nr. 1203 af 27. december 2003 om offentlige betalinger mv. er der gennemført en regulering, der må formodes at sætte standarden for, hvorledes der faktureres for og betales, når en offentlig myndighed er debitor. Loven er udformet som en rammelov, der udfyldes gennem bekendtgørelser udstedt af Finansministeriet. Således indfører bekendtgørelse nr. 991 af 7. oktober 2004 en almindelig pligt for offentlige myndigheder til at sende og modtage regninger elektronisk, medmindre det er enklere og billigere at udarbejde og sende regninger på papir, eller debitor ikke kan modtage regningen elektronisk eller ikke ønsker at modtage regningen på papir, se §§ 1 og 3. En faktura modtaget i strid med lovens regler er myndigheden ikke forpligtet til at betale. Loven er gradvis sat i kraft ved bekendtgørelser fra Finansministeriet, se herved ved bekendtgørelse nr. 993 af 7. oktober 2004, der sætter bestemmelserne i §§ 6, 7 og 12 i kraft.

Fakturering

Den elektroniske fakturering kan ske på forskellige måder. Vælger kreditor selv at producere fakturaen, skal fakturaen udskrives i en fil, der overholder et elektronisk format, myndigheden kan modtage. Man anvender her det såkaldte OIOXML-format, se herved bekendtgørelsens § 6 og de detaljerede regler i bilaget til bekendtgørelse nr. 1075 af 11. november 2004. Kreditor kan dog også vælge at gøre brug af en såkaldt *fakturaportal*, dvs. en tjeneste udbudt af en privat virksomhed. Her indtastes fakturaoplysningerne for derefter at blive videresendt af portalen til debitormyndigheden. Den tredje mulighed består i at gøre brug af

såkaldte "*læs ind"-bureauer*, jf. herom nærmere bekendtgørelse nr. 37 af 14. januar 2005. Bekendtgørelserne trådte i kraft "eDag2" (se herom s. 698), dvs. den 1. februar 2005. Virksomheden skal i så fald indgå en særlig aftale med dette bureau. For små og mellemstore virksomheder (som nærmere defineret i § 4 i bekendtgørelsen) yder det offentlige tilskud til denne "læs ind"-service, således at den kan være gratis. Dette forudsætter, at tjenesten leveres af et certificeret "læs ind"-bureau.

Betaling

Loven har også til formål at gøre offentlig betalingsforvaltning nemmere for borgere såvel som for virksomheder og myndigheder. Til opfyldelse af dette formål indfører den tre initiativer, hvoraf det i sammenhængen væsentligste er etableringen af et system med såkaldt NemKonto og NemBetalinger, se nærmere <www.nemkonto.dk>: Personer over 18 år, som i henhold til lov om Det Centrale Personregister er tildelt et personnummer, og som ikke er registreret som udrejst af Danmark, skal således i medfør af lovens § 1, stk. 1, anvise en konto i et pengeinstitut (en NemKonto), hvortil offentlige myndigheder *med frigørende virkning* kan foretage udbetaling af pengebeløb. Det samme gælder personer under 18 år, der i henhold til lov om Det Centrale Personregister er tildelt et personnummer, og som modtager betalinger fra offentlige myndigheder, samt juridiske personer (eller fysiske personer, der er arbejdsgivere), som er tildelt et CVR-nummer ifølge lov om Det Centrale Virksomhedsregister.

Betalingsstedet

Foruden det væsentlige princip, at betalinger til en NemKonto sker med frigørende virkning, jf. lovens § 1, stk. 1, vil de obligationsretlige retsvirkninger af konteringerne på denne konto blive fastlagt ved en række ministerielle bekendtgørelser, der vil blive udstedt på grundlag af loven. Heri vil der bl.a. blive givet regler om offentlige myndigheders ret til med frigørende virkning at foretage udbetalinger til fysiske og juridiske personer omfattet af § 1, som ikke har anvist en NemKonto.

NemKonto

I praksis vil NemKontoen være en helt almindelig bankkonto, som borgeren eller virksomheden bruger i forvejen. Ved at blive udpeget som NemKonto bliver denne konto rette betalingssted for alle udbetalinger fra staten, kommunerne og amterne. Nærmere regler om NemKontoen er fastsat ved bekendtgørelse nr. 316 af 6. april 2005. Den løbende opdatering af NemKonti forudsættes primært foretaget via pengeinstitutter på vegne af borgere og virksomheder eller via borgeres og virksomheders egen indberetning via NemKonto-systemets hjemmeside. Offentlige myndigheder kan dog på vegne af borgere og virksomheder foretage løbende opdateringer af NemKonti og specifikke konti, jf. §

18. Efter et afholdt EU-udbud er der den 30. juni 2004 indgået aftale med KMD A/S om etablering og vedligeholdelse af NemKonto og NemBetalinger. Når loven er fuldt implementeret, kan offentlige udbetalinger som følge af NemKonto og NemBetalinger overføres elektronisk som konto-til-konto-overførelser. Offentlige udbetalinger ved checks kan herved afskaffes, og antallet af kontantkasser begrænses.

Supplerende litteratur

I *E&A* har jeg analyseret en række principielle problemer om anvendelsen af *de køberetlige regler* i relation til digital information, se bl.a. s. 320 ff. De synspunkter, jeg har fremlagt i *E&A*, har givet anledning til en del efterfølgende debat, se f.eks. *Ellen-Kathrine Thrap-Meyer* i Complex 5/89, samme & *Robin Thrap-Meyer* i Complex 1/90, s. 26 ff. og *Nørager-Nielsen* i NJM 1990 I.287 ff. Problemerne om ophavsretlige retsmangler er desuden behandlet af mig i U1987B.121 ff. og af *Magnus Stray Vyrje* i NÅR 1986.99 ff. henholdsvis i Complex 12/85.

I *Frederik Bruhn-Petersens* specialeafhandling "Elektronisk præstation af digitale ydelser" (Kromann-Reumert prisopgave, 1999), s. 13 ff., findes en god beskrivelse af de særlige problemer, der opstår ved præstation af digitale ydelser. Afhandlingen er tilgængelig på <www.jur.ku.dk/it-ret/specialer/bruhn-petersen.pdf>. Se også *Susanne Karstoft*: Elektronisk Aftaleret (2004).

Problemerne om *forbrugerbeskyttelse* på Internet er bl.a. behandlet i Erhvervsministeriets rapport om Forbrugerens retsbeskyttelse i grænseoverskridende digitale net (juni 1997), i Nordisk Ministerråds rapport "Shopping på Internet" (1999) og i den svenske rapport "Konsumenterna och IT", SOU 1999:106.

Lov om Visse Betalingsmidler er kommenteret af *Susanne Karstoft* (2001). I TemaNord 2004:549 har *Anne-Dorte Bruun Nielsen* afgivet en redegørelse om Mikrobetalinger og Forbrugerbeskyttelse.

En praktisk vejledning om aftaler vedrørende udvikling af hjemmesider er udsendt af Dansk Dataforening i 2000.

Kapitel 21. IT-OVERDRAGELSE

21.1. Afgrænsning

21.1.a. IT-aftalens kendetegn

En IT-overdragelse kan karakteriseres som en transaktion, hvorved en part – IT-leverandøren – overdrager et IT-system, en IT-komponent eller IT-relaterede tjenesteydelser eller brugsrettigheder til en anden part, brugeren. Transaktionen kan afgrænses i *faktisk* henseende gennem dens fysiske komponenter (f.eks. medier, information eller tjenester og anden bearbejdning) og i *retlig* henseende ved dens struktur af præstationshandlinger (f.eks. som køb, leje, tjenesteydelse eller licens).

Faktiske kendetegn

I faktisk henseende kendetegnes IT-overdragelsen ved de *komponenter*, *funktioner*, *lovmæssigheder* eller hele *systemer*, der indgår i leverandørens ydelse, jf. nærmere afsnittene 21.4.-21.7. Vanskelighederne ved at beskrive disse aspekter af ydelsen skyldes her – som i de transaktioner, der er behandlet i kapitel 20 – det element af information, der indgår i det leverede. Disse elementer af transaktionen vil ofte præsteres på en anden måde end de fysiske elementer, f.eks. ved at information kopieres, genskabes eller gøres til genstand for en særlig bearbejdning. Dette giver anledning til beskrivelsesproblemer, bl.a. ved anvendelsen af reglerne om overdragelse og risikoovergang og i mangelsvurderingen.

Retlige kendetegn

I retlig henseende kan man sondre mellem forskellige overdragelsesformer: Udover den egentlige *overdragelse* af komponenter, systemer eller tilbehør hertil, kan IT overdrages ved, at leverandøren meddeler brugeren en *brugsret* til f.eks. komponenter, ledningsnet eller rettigheder. Dernæst kan der være tale om, at brugeren tilstås en *licens* til at indtræde i immaterialretlige retspositioner (f.eks. ophavsretlige værker eller patenterede opfindelser). Der kan også være tale om at give tilladelse til brug af personoplysninger. Hertil skal føjes aftaler om hertil hørende tjenesteydelser, herunder *vedligeholdelsesydelser* og *konsulentydelser*. I den enkelte transaktion vil disse enkeltydelser ofte indgå i samspil med hinanden. Et sådant samspil ses f.eks. ved aftaler

om såkaldt *facility management*, *outsourcing* og i de såkaldte *ASP-kontrakter*.

Da de formueretlige regler ikke altid tager højde for samspillet mellem de forskellige komponenter i sådanne transaktioner, og da de særregler, der findes om enkelte af disse komponenter, heller ikke tager højde for dette samspil, er der et stort behov for, at parterne aftaler sig til rette. Derfor er det nødvendigt at fremstille IT-overdragelsens problemer i nær forbindelse med aftaleproblemerne, ligesom studiet af de foreliggende aftaleformularer på området spiller ind.

21.1.b. Typer af IT-ydelser

Produkt-overdragelse

Produktoverdragelse taler man om, når den præsterede ydelse eksisterer på aftaletidspunktet. Sådanne IT-transaktioner adskiller sig ikke nævneværdigt fra overdragelse af andre komplekse løsøreydelser, f.eks. kontorudstyr, husholdningselektronik el.lign. En væsentlig forskel kan dog ligge i, at IT-komponenter i højere grad end andre elektroniske komponenter indeholder digital information, herunder edb-programmel, som er underlagt ophavsretlige begrænsninger.

System-overdragelsen

En systemoverdragelse taler man om, når leverandøren skal sammensætte det leverede ud fra komponenter, som enten findes i forvejen eller som bringes til verden som led i aftaleopfyldelsen. "Systemet" findes altså ikke på aftaletidspunktet (hvilket komponenterne dog gør), men skal først sammensættes og typisk også implementeres. Dermed minder systemoverdragelsen om den klassiske entrepriseaftale. Entrepriseretten har da både haft indflydelse på aftalepraksis, ligesom entrepriseretlige grundsætninger indgår i den retlige vurdering af problemerne om aftaleopfyldelse og misligholdelse. I takt med, at IT-systemerne er blevet mere standardiserede og har nået et bredere marked (med lavere priser), har systemoverdragelsen mistet en del af sin selvstændige betydning. En betydelig del af den klassiske systemudvikling er dermed overtaget af individuelt tilpassede løsninger (på engelsk "*customised systems*"). Et praktisk eksempel herpå er det såkaldte *standardramme-system*, hvor et standardsystem – som enten er udviklet af leverandøren selv, eller forhandlet af denne – tilpasses den enkelte brugeres behov. Leverandørens forpligtelse vil da dels bestå i at skaffe brugeren en *licens* til det pågældende system, dels at udføre en *opsætning*, der svarer til brugerens behov.

Konsulentopdrag

Mange brugere, private såvel som erhvervsmæssige, har brug for IT-løsninger, men ved ikke rigtigt hvordan de har brug for

dem. Dette gælder, hvad enten løsningerne tænkes anskaffet som standardprodukter eller som udviklingsydelser. Sådanne vidensspring kan reduceres gennem *konsulentrådgivning*. Man sondrer undertiden mellem *uegentlig* konsulentrådgivning, som ydes af den virksomhed, der også leverer selve løsningen, og *egentlig* konsulentrådgivning, som forestås af uafhængige virksomheder. De sidstnævnte konsulenter udbyder deres tjenester på et heterogent marked for mindre og mellemstore virksomheder samt for de offentlige myndigheder, jf. herom afsnit 21.7.

Implementering

Komplicerede IT-systemer fungerer ikke ved blot at blive sat i stikkontakten. Systemets komponenter skal kunne kommunikere med hinanden. Dernæst må de *ydre rammer*, f.eks. pladsforhold, elektricitetsforsyning, elektromagnetisk afskærmning, ventilations- og varmeforhold, være i orden. Aftaler om overdragelse af IT-systemer fordeler typisk implementeringsopgaven funktionelt, således at brugeren står for klargøringen af de lokalemæssige forhold (el-installationer, ventilation, bygningsindretninger mv.), medens leverandøren står for de tekniske og immaterielle aspekter (teknisk klargørelse, instruktion, uddannelse mv.). Begge dele af implementeringen må være tilpasset, hvis systemet skal fungere.

Datakonvertering

Ved overdragelse af IT-systemer, der erstatter eksisterende systemer, aftales det ofte, at leverandøren – eller en af ham udpeget tredjepart – skal *konvertere* data fra det gamle til det nye system. Aftaler om konvertering indgås ofte adskilt fra den egentlige overdragelse. En konvertering kan efter omstændighederne ske ved, at brugeren udstyres med et værktøj hertil af leverandøren. Sådanne bistandsydelser ligger meget nær de aftaler om bearbejdning, der kendes fra det industrielle område, se hertil *ET* s. 281 ff. Særlige problemer kan her opstå om de rettigheder, der kan bestå til konverteringen, sml. bemærkningerne herom ovenfor i afsnit 7.4.c.

Uddannelse

Til implementering hører også den nødvendige *uddannelse* af operatøren i systemets brug. Sådanne implementeringsydelser tilbydes ofte af kursusvirksomheder mv. Implementering udført ved tredjemand har i øvrigt praktisk betydning i tilfælde, hvor en uafhængig konsulent helt eller delvis står for den tekniske klargøring af systemet.

Internet-ydelser

Med den tiltagende anvendelse af Internet-kommunikation som grundlag for markedsføring af ydelser, aftaleindgåelse og -opfyldelse, er der opstået et voksende marked for hertil relaterede digitale produkter og tjenesteydelser. Problemerne herom be-

handles i afsnit 20.2. og 20.3. En oversigt over forskellige typer af Internet-tjenester er givet i afsnit 3.3.f.

Andre ydelser

I tillæg til de ovennævnte ingredienser vil en række andre ydelser ofte indgå i en IT-overdragelse. Flere af disse er omtalt andetsteds i denne bog. Foruden de allerede nævnte *digitale ydelser* og *licenser* mv. kan nævnes de *sikkerhedsydelser*, der tegnes som vedligeholdelses-, sikrings- og forsikringsordninger, og som omtales i afsnit 4.4., samt de *accessoriske pligter*, som parterne enten påtager sig udtrykkeligt, eller som de efter almindelige formueretlige regler er forpligtet til at varetage for at tilgodese hinandens interesser (rådgivning i konsekvens af den loyale oplysningspligt mv.).

21.1.c. Udviklingslinjer

De tidlige år

IT-aftalepraksis har udviklet sig i takt med de forskellige anvendelsesformer, der har præget teknologiens udviklingsaldre. Da en "datamaskine" var et monstrum, som det krævede stor teknisk ekspertise at beslutte sig for, millioner af kroner at købe og omfattende ændringer i de ydre omgivelser at installere (sml. til illustration dommen i *U 1976.531 H*), tog IT-aftalen primært sigte på selve opfyldelseshandlingerne. I den periode, hvor IT alene blev anvendt i forskningsmæssige miljøer, opstod der sjældent retlige problemer omkring aftaleindgåelse og -opfyldelse. Begge parter vidste lige meget om teknologien og havde dermed sammenfaldende kvalitetsforventninger. Ved systemets levering stod brugerens kreds af eksperter klar til at tage imod. Kontrakterne lignede dem, vi kender fra de tekniske videnskabers verden ved forskeres indkøb af laboratorieudstyr mv.

Gennem 1950'erne var det almindeligt, at leverandørerne alene leasede systemerne til kunden, for dermed at afskære et marked for brugt udstyr fra at opstå. Leverandørernes fordele ved kun at udleje var indlysende. Længe efter, at salgsværdien reelt var erlagt, fortsatte de månedlige ydelser med at forfalde til betaling. Dette gav anledning til konkurrenceretlig indgriben, jf. nærmere herom *E&A* s. 303 ff. Da denne praksis var fjernet, forelå grundlaget for et marked for modulopbyggede systemer, hvor den enkelte bruger kunne vælge sin egen løsning på grundlag af et veldefineret udbud af standardiserede komponenter. Hermed var kimen lagt til den senere udvikling af "åbne systemer", der senere er blevet understøttet af den stigende *standardisering* på IT-området og heraf følgende prisfald. Prisfaldet har dog også været ensbetydende med, at brugere ofte erhverver IT uden den

forberedelse, der tidligere ledsagede de langt mere kostbare transaktioner. Det uundgåelige vidensspring mellem leverandør og kunde resulterede ofte i juridiske konflikter bl.a. om leverandørens pligt til at oplyse og vejlede mv. Det retlige grundlag for disse konflikter lå typisk i den aftalepraksis, der var nedarvet fra dengang, leverandøren var bundet tæt sammen med sin kunde. Når systemerne skulle sælges på et åbent marked, hvor der ikke længere var løbende kontrol med dets efterfølgende skæbne, krævede leverandørerne ofte ansvarsfrihed.

Det offentliges rolle

Det offentlige har altid været den største IT-bruger og dermed største IT-køber. Derfor har myndighedernes kontraktspraksis sat mærkbart præg på dansk IT-aftalepraksis. Efterhånden som stigningen i statens IT-anskaffelser tog til i løbet af 1960'erne, øgedes behovet for at skabe ensartede og rimelige handelsvilkår for statens styrelser og institutioner. Staten har en forståelig pligt til at vælge de bedste og billigste løsninger, og standardisering var bl.a. nødvendig for at kunne sammenligne forskellige leverandørers tilbud og opbygge systemer af produkter fra forskellige leverandører. Allerede i begyndelsen af 1970'erne førte dette Finansministeriet til at udarbejde et sæt standardbestemmelser (standardkontrakter) om henholdsvis køb, leje og vedligeholdelse af IT-udstyr. I det følgende tiår blev kontrakterne genoptrykt af det nu nedlagte EDB-råd som "EDB-rådets Standardkontrakter". Selv om alle var enige om, at disse aftaler var stort set utjenlige til deres formål, anvendtes de hyppigt i løbet af 1980'erne, bl.a. fordi leverandørerne gjorde brug af standardtilføjelser, der reelt gjorde "standardkontrakten" til en ramme for en ensidigt fastsat IT-aftale.

K18 og K33

De aftaleformularer, der i dag er toneangivende (K18 og K33), prætenderer ikke at være gældende for enhver form for systemoverdragelse. For det første tager de sigte på specifikke leverancer; for det andet har de et langt større omfang, end IT-rådets kontrakter havde. K33 blev udsendt i september 1987 og er opkaldt efter ophavsmanden (Kammeradvokaten) og det forventede – men ikke realiserede! – sidetal. Kontrakten, der binder leverandørerne hårdt op i henseende til at levere det, brugeren forventer at få, har primært betydning for større systemer, hvor der forudsættes mere detaljerede kontraktsforhandlinger. Kontrakten suppleredes i 1990 med en noget mindre kontrakt for "standardiserede edb-systemer" (K17), se herom *Henrik Berg*, R&R 1990, nr. 6, s. 25 ff., der i 1992 blev revideret på enkelte punkter og udsendt som K18 med samme undertitel. Efter et nu ophævet cirkulære nr. 58 af 11. april 1975 havde offentlige myndigheder pligt

til at anvende de første aftaler om køb, leje og vedligeholdelse af IT. En sådan pligt gælder ikke længere, jf. cirkulære nr. 200 af 15. oktober 1990 og cirkulære nr. 142 af 3. august 1992. I dag er K18 den mest udbredte danske standardformular på IT-området, omend denne udbredelse som regel finder sted i en modificeret form tilpasset den enkelte transaktions tekniske omstændigheder.

I Sverige og Norge har man udviklet egentlige agreed documents på IT-området. I Sverige er "Avtal 90" resultatet af forhandlinger mellem den svenske IT-brancheforening (SITO), den svenske dataforening og Sveriges Inköps- och Logistikförbund (SILF), medens formularen EDEL 90 er udsendt af Föreningen Svensk Programvaruindustri. En god og grundig oversigt over disse kontraktsformularer findes hos *Lindberg & Westman* (1999), s. 287-386. I Norge har det statslige rådgivningsorgan Statskonsult udarbejdet serien "Standardavtaler og veiledninger om anskaffelse av informasjonsteknologi" herunder om køb og vedligeholdelse. Ligeledes har Kontor og Datateknisk Landsforening (KDL) udsendt en "KDL's standardavtale om køjp av utstyr og tjenester / Disposisjonsrett til programmer", henholdsvis om "Vedlikehold og programservice". De nævnte kontrakter er optrykt hos *Torvund* (1997), s. 267 ff.

Nyere tendenser

Gennem de seneste år har der vist sig et behov for standardaftaler, der tillader en videre grad af fleksibilitet, dvs. mulighed for at tilpasse parternes pligter til de ændrede omstændigheder, der ofte viser sig under IT-udviklingsforløb. Allerede i 2002 udsendte IT-Brancheforeningen et sæt standardforbehold til K18, der lagde afstand til den meget faste regulering i K18. Forbeholdene angår bl.a. leverandørernes pligter ved markedsføring af udstyr (aftalens pkt. 2.3), pligten til installation og kontrol af lokaler (pkt. 3), vedligeholdelsespligten (pkt. 4), pligten til at gennemføre prisnedsættelser over for kunden, såfremt der efter aftaleindgåelsen indtræder generel prisnedsættelse (pkt. 8.2), ansvarsfraskrivelse (pkt. 16) samt retten til specialdesignet programmel (pkt. 21). De blev godkendt af Konkurrencerådet den 24. april 2002. Som nævnt i afsnit 21.4.c. er der også kommet senere standardaftaler til. Ønsket om fleksibilitet er i nogen grad blevet efterkommet med den såkaldte K01-kontrakt, der på flere centrale punkter markerer en bevægelse bort fra de rigoristiske K18 og K33-kontrakter, herunder ved reglerne om "afklaringsfase" og om ændringsanmodninger.

Brancheformularer

De standardkontrakter, der konciperes af IT-leverandørerne, har traditionelt været domineret af ansvarsfraskrivelser, jf. ovenfor. Denne tradition har rødder i maskinindustrien og i virksomheder, der leverer information, jf. *Günther Petersen:* Ansvarsfraskrivelse (1957), s. 25 f. På dette punkt er praksis dog ved at

vende. Teknologien har skabt mere driftssikre systemer, og kvalitet er blevet et konkurrenceparameter, jf. allerede omtalen i *E&A* s. 309 ff. Problematikken omkring årtusindskiftet har ligeledes sat leverandørsiden under pres for også aftalemæssigt at leve op til, hvad der loves i salgsannoncerne.

21.1.d. Kvalitetsparametre

Problemstillingen

Det er ikke muligt at opstille et udtømmende katalog over de egenskaber, der kvalificerer et godt IT-system. Hvad der er "godt" beror på subjektive forestillinger. Derimod kan man inddele en række tekniske aspekter, som der kan knytte sig kvalitetsforestillinger til.

ISO har forsøgt at karakterisere kvalitetsegenskaber ved edb-software og -dokumentation i ISO 9126 (EN 29.126) fra 1990: "Information technology – software product evaluation – quality characteristics and guidelines for their use" og ISO 9127 (EN 29.127) fra 1989: "Information processing systems – user documentation and cover information for consumer software packages". ISO 9126 definerer softwarekvalitet som "the totality of features and characteristics of a software product that bear on its ability to satisfy stated or implied needs", og denne generelle angivelse udmønter standarden herefter i en række karakteregenskaber. Med *funktionalitet* menes tilstedeværelsen af en række funktioner. *Driftssikkerhed* bestemmes i relation til programmets evne til at bevare sin funktion under givne vilkår og i et givet tidsforløb. Programmets *brugbarhed* defineres efter de krav til operatøren, som det kræver. Dets *effektivitet* måles i forholdet mellem systemets egenskaber og de hertil nødvendige ressourcer. Dets *vedligeholdelsesevne* (maintainability) består i mulighederne for at ændre systemet og dets *portabilitet* i muligheden for at flytte programmet fra et miljø til et andet. I IT-litteraturen synes hver forfatter at lægge sin indfaldsvinkel til grund. *Rolf Molich* (1986) sondrer – som nedenfor – mellem drift, vedligeholdelse og omlægning, men supplerer samtidig med en række underinddelinger, der slører overblikket. *Egebjerg Johansen m.fl.* (1986), s. 99 fremhæver egenskaberne brugervenlighed, dokumentation, integrationsmuligheder, transportabilitet og fremtidssikring. Se også *Duncan M. Davidson*, 24 Jurimetrics Journal 129 (1984): "speed", "accuracy", "cost", "flexibility" og "commercial feasibility" samt *William E. Perry* (1982, 1984), s. 208.

Tilgængelighed

Den mest iøjnefaldende kvalitetsparameter består i, at systemet er tilgængeligt, dvs. at brugeren kan benytte det, når han vil. Manglende tilgængelighed kan skyldes fejl ved både software og hardware (f.eks. fejl i belægningen af det magnetiske materiale, kabelfejl, løse forbindelser eller lodningsfejl); men oftest ligger forklaringen i mangelfuld eller manglende dokumentation. Et

særligt problem består i, at systemet ikke afgiver sine svar inden for de tidsmæssige grænser, hvor brugeren har brug for den pågældende information. Manglende tilgængelighed kan også skyldes, at en funktion vel kan gennemføres, men på en anden – og besværligere – måde end forudsat i manualen, f.eks. med hyppige nedlukninger og opstarter, med ekstra indtastninger eller på tvungne arbejdstider. I IT-aftaler formuleres kravene til tilgængelighed ofte i en driftseffektivitet, der måles i en procentsats, hvor "oppetid" sættes i forhold til "nedetid".

Korrekthed

Når systemet er tilgængeligt ligger der et andet væsentligt kvalitetsparameter i, at dets *funktioner* modsvarer brugerens berettigede forventninger. De færreste IT-systemer er fejlfri. "Fejlfrihed" vil forudsætte, at samtlige del-elementer af systemet er i total harmoni. Derfor er driftssikkerhed ikke et spørgsmål om et enten/eller, men snarere om et mere eller mindre.

Der må her ske flere grænsedragninger. For det første må det afklares, om en teknisk egenskab overhovedet har karakter af fejl: Det kan f.eks. tænkes, at egenskaben nødvendigvis *er* tilstede i systemer af den pågældende art (f.eks. pga. det tekniske udviklingstrin), eller at egenskaben ikke *burde* være tilstede, men fremkommer som følge af brugerens fejlbetjening. Leder disse betragtninger til, at der er tale om en fejl, må det dernæst afklares, om leverandøren har en forpligtelse til at præstere ydelsen uden denne fejl. Må også dette spørgsmål besvares bekræftende, må der for det tredje afklares, om fejlen giver køberen ret til at gøre et retligt krav gældende. Svaret på de to sidstnævnte spørgsmål beror på almindelige obligationsretlige overvejelser, herunder først og fremmest den indgåede aftale, almindelige typeforudsætninger, produktoplysninger mv., jf. nærmere *Bryde Andersen & Lookofsky* (2005), afsnit 2.3. og kapitel 5-6.

Sikkerhed

Et tredje driftskrav angår systemets evne til at yde sikkerhed mod skader på maskinel, programmel eller data forvoldt af systemet selv eller ved udefra kommende angreb. De tekniske muligheder for at opnå fysisk og logisk sikkerhed behandles nærmere i kapitel 4. I afsnit 22.1.b. drøftes de forpligtelser, leverandøren på alment grundlag har til at tilvejebringe et sikkert system for kunden.

Brugervenlighed

En vanskeligt definerbar kvalitet, der nærmest har residuel karakter, angår systemets brugervenlighed. Begrebet er svært at håndtere pga. dets subjektive karakter. Brugeren af selv det mest besværlige system vil med tiden vænne sig til det og opfatte det som det bedste til hans behov. I forsøget på at objektivisere begrebet sigter man for det første til den lethed, hvormed brugeren

kan lære (henholdsvis genindlære) et system at kende, for det andet til hans æstetiske oplevelse af at anvende systemet.

Modularitet

Systemets *modularitet* er dets evne til at lade komponenter *udskifte* med andre, at *tilføje* nye enheder eller at *tilpasse* det til nye anvendelsesområder. Indenfor rammerne af den enkelte PC består det "modulære" i muligheden for dels at udskifte de kort, der påsættes bussen for at understøtte CPU'en i særlige funktioner, dels at udskifte selve CPU'en (PC'ens såkaldte "motherboard") og de periferienheder, der er knyttet til den (diskettestationer mv.). Modularitet og kompatibilitet har nær forbindelse med hinanden. Med begrebet kompatibilitet beskrives en systemenheds evne til at kommunikere med en anden systemenhed (i kommunikationsteorien, dens evne til at tale samme sprog). En af forklaringerne på den eksplosionsagtige udvikling af PC-markedet ligger netop i disse to nøgleord. PC'er kan genbruges som moduler i andre IT-sammenhænge (f.eks. som terminaler til telekommunikation) eller anvendes til varetagelse af nye IT-opgaver i takt med, at eksisterende opgaver overtages af nyere og stærkere udstyr. I et overordnet perspektiv kan den enkelte PC udgøre et modul i et større system, der kan udskiftes, suppleres og opgraderes.

I praksis vil kun kopier være 100% "kompatible", og er der tale om en sådan, mister kompatibilitetsbegrebet sin betydning. Betegnelser som f.eks. "99% kompatibel" er ikke tjenlige uden en præcision af, hvad procentdelen beregnes af (markedets samlede programudbud, enkelte funktioner eller andet). Standarder for kompatibiliteten kan i øvrigt være vanskelige at indfri, hvis kompatibiliten knytter sig til en immaterialret, f.eks. retten til Windows-styresystemet. Se i øvrigt til illustration om begrebets køberetlige aspekter, *JÅF 1995.159*, hvor en pc ikke kunne udvides med yderligere RAM-hukommelse som angivet i manualens tekniske specifikationer. Forbrugerklagenævnet fandt, at det var en typeforudsætning for en pc-køber, at en pc kunne udvides med yderligere hukommelse og gav køberen ret til at hæve.

Udbygningsmulighed

Et administrativt IT-system vil umærkeligt blive en del af brugerens infrastruktur. Derfor er det vigtigt, at systemet kan bygges ud i takt med, at brugerens organisation ændrer sig. Kan det ikke det, kan selve systemet nemlig blive en afgørende hindring for et ellers nødvendigt udviklingsforløb. Dette tilpasningsbehov kan være større eller mindre. Et fælles, samfundsmæssigt behov for udbygning af talrige systemer opstod, da man passerede årtusindskiftet, og talrige – hovedsagelig ældre – systemer skulle tælle fra 99 til 00, se hertil *Bryde Andersen*: Nogle IT-retlige problemer ved årtusindskiftet. År 2000-sekretariatet (1999). Et

andet tilsvarende eksempel på et bredt behov for udbygning er systemernes overgang til betaling i *euro*. Som hermed antydet kan den kvalitetsparameter, som muligheden for at udbygge et system repræsenterer, være mere eller mindre individuel.

21.1.e. Udfordringer

Problemstillingen

Foruden sine særlige beskrivelsesproblemer er det kendetegnende for mange IT-transaktioner – og herunder navnlig de, der indebærer et element af produktudvikling – at leverandøren ikke med sikkerhed kan hidføre de funktioner, kunden forventer, selv om han med sin særlige kyndighed ofte vil have lettere ved at overskue sine muligheder herfor end kunden. Dette vidensspring kan give en risiko for, at leverandøren misbruger sin teknologiske overlegenhed til at sælge kunden mere, end denne har brug for, eller garderer sig mod følgerne af teknologisk inkompetence gennem vidtgående ansvarsfraskrivelser, der råder bod på, at det solgte ikke lever op til kundens måske berettigede forventninger.

Bl.a. foranlediget af nogle sager, hvor offentlige myndigheder har mødt betydelige problemer med at opnå forventet funktionalitet i større IT-leverancer, har denne problematik herhjemme ført til en debat om kvaliteten af offentlige IT-anskaffelser: Hvordan kan anskaffelsesforløbene forbedres, så skattekronerne fører til de optimale løsninger?

Bonnerup-rapporten

Som nævnt i afsnit 3.2.d. førte de uheldige erfaringer i nogle store IT-udviklingsprojekter Teknologirådet til i 2000 at nedsætte et sagkyndigt udvalg, Bonnerup-udvalget, der i marts 2001 afgav rapporten "Erfaringer fra statslige IT-projekter – hvordan gør man det bedre". I rapporten anføres det bl.a. (se nærmere kapitel 3), at de offentlige myndigheder ikke har været modne til at gennemføre meget store projekter på en tilstrækkeligt professionel måde. Samtidig stilles det spørgsmål, om de professionelle parter har gjort nok for at advare om og forebygge de problemer, projekter løber ind i – et problem, der i øvrigt vanskeliggøres ved en ukritisk brug af private konsulenter og et ikke altid klart samspil mellem køber, leverandør og konsulent (kapitel 4.). Vedtagelsen af K01, se herom afsnit 21.1.c., kan bl.a. ses som udslag af sådanne overvejelser.

21.2. Baggrundsretten

21.2.a. Problemstillingen

De regler, der regulerer en IT-overdragelse, beror på, hvilke ydelser den omfatter. Pga. det samspil mellem forskellige typer af ydelser, der typisk vil præge en IT-transaktion, vil en og samme aftale typisk være reguleret af forskelligartede retsgrundlag. I det omfang, leverancen rummer elementer af løsøre, anvendes købeloven *inter partes*, f.eks. ved fastlæggelsen af stillingen ved misligholdelse mv. Indgår der rettighedselementer, må man søge vejledning i de relevante immaterialretlige regler, f.eks. om konsumption og overdragelse, og i det omfang, den inddrager en arbejdspræstation, må reglerne om tjenesteydelser, værksleje eller entreprise inddrages. Hertil kommer, at regulatoriske regler, bl.a. i lovgivningen om teknologisk våbenkontrol mv. kan spille ind samt andre regler af offentligretlig art, der på forskellige måder begrænser parternes aftalefrihed.

21.2.b. Den almindelige obligationsret

Anvendelsen af købeloven på aftaler om overdragelse af IT volder vanskeligheder i flere henseender. Nogle af disse problemer er behandlet i afsnit 20.2.b., hvor det gøres gældende, at rene informationsprodukter alene vil være underlagt købeloven, hvis de pga. en tilhørende licens er "flytbare". Derudover volder loven vanskeligheder i relation til enkelte af de komponenter, der indgår i en IT-overdragelse, og som præsteres under forhold, der for en ydre betragtning minder om *entreprise* eller *værksleje* mv. Udgangspunktet er generelt, at loven gælder for *varer* (løsøre), men ikke – eller kun i kraft af analogi – for *tjenesteydelser*.

Disse problemer behandles nærmere i tilknytning til hver enkelt delydelse, jf. afsnittene 21.4 – 21.7. På dette sted kan der dog være grund til at fremhæve, at der intet klart skel er mellem vare- og tjenesteydelsesbegrebet. Sondringen tjener kun som et generelt og alment udgangspunkt: Tjenesteydelser betragtes kort fortalt som de grupper af ydelser, der ikke har karakter af varer, altså en negativ afgrænsning. Imidlertid ligger det klart, at talrige tjenesteydelser kan optræde som bestanddele af løsørekøb, f.eks. som accessoirer til et varesalg. Den loyale oplysningspligt, som enhver sælger er undergivet, vil f.eks. implicere et rådgivningselement. Varens indpakning og afsendelse rummer et forarbejdningselement.

21.2.c. Immaterialretlige regler

Eksemplarer

Fordi brugen af softwarekomponenter typisk kræver en løbende tilladelse for brugeren til at foretage sig visse handlinger, der dækkes af en immaterialret, spiller immaterialrettens regler – og herunder navnlig ophavsretten – en central betydning for IT-overdragelsen. Navnlig spiller reglerne om den *legale programlicens*, jf. ophl. § 36, om *reverse engineering*, jf. ophl. § 37 (se hertil afsnit 7.4.), og om konsumption, jf. ophl. § 19 (se hertil afsnit 6.4.d.), ind. Disse regler fungerer – undertiden med præceptiv kraft – som udfyldningsregler i aftaleforhold, der ikke tager sigte på disse immaterialretlige aspekter og tjener for så vidt en aftaleretlig funktion. Som anført i afsnit 20.2.b. indebærer det forhold, at der består en mere kompleks ophavsretlig relation mellem parterne, dog ikke i sig selv, at man forlader det køberetlige system, hvis blot denne relation ikke forandrer transaktionen om informationsproduktet til en licensaftale.

Licensaftaler

I relation til egentlige licensaftaler har ophl. kap. 6 dernæst betydning som udfyldningsregler for aftaler, der indebærer overdragelse af en ophavsret. Det antages således, at ophl. § 53, stk. 3, giver støtte for en generel fortolkningsregel, hvorefter ophavsretlige licensaftaler – i tilfælde af tvivl om deres forståelse – skal fortolkes til fordel for ophavsmanden (eller den rettighedshaver, der i henhold til aftale med denne, træder i ophavsmandens sted). Har denne overdraget en ret til at udnytte værket på en bestemt måde eller ved bestemte midler, giver overdragelsen ikke erhververen ret til at udnytte værket på andre måder eller ved andre midler.

21.2.d. Offentlige udbudsregler

Udbudscirkulæret

Offentlige myndigheder står ikke frit i deres valg af leverandører af varer og tjenester. Nationalt er de bundet af forvaltningsrettens principper om ligelighed mv. Hertil føjer sig en pligt til med passende mellemrum at gennemføre udbudsrunder efter reglerne i Finansministeriets cirkulære af nr. 159 af 17. december 2002 om udbud og udfordring af statslige drifts- og anlægsopgaver. Denne pligt gælder opgaver, som er "udbudsegnede", jf. § 2, stk. 2-3, og som har en forventet kontraktsum over 500.000 kr., jf. § 4. Hvis institutionen godtgør, at det ikke er muligt at udbyde opgaven eller nogen del heraf i konkurrence, eller hvis den godtgør, at udbuddet af opgaven medfører uforholdsmæssigt store

omkostninger eller administration, skal myndighederne dog ikke sende opgaven i udbud, jf. § 5.

Standarder

Alle offentlige myndigheder – dvs. også amter, kommuner og andre forvaltningssubjekter – har ved anskaffelse eller indførelse af IT pligt til at følge de regler, der fremgår af bekendtgørelse nr. 132 af 28. februar 1991 om anvendelse af standarder ved offentlige indkøb af informationsteknologi og ved fastsættelse af visse tekniske forskrifter. Bekendtgørelsen implementerer de regler om standardisering inden for informationsteknologi og telekommunikation, der er fastsat ved Rådets beslutning 87/95/EØF af 22. december 1986 (EFT 1987 L 36/31).

Sml. herved *U 2002.1277 V*, der efter en præjudiciel forelæggelse for EF-domstolen fandt, at EF-traktatens art. 28 var til hinder for, at der i udbudsbetingelserne indsættes en bestemmelse, hvorefter der til opfyldelse af den pågældende kontrakt skal anvendes et bestemt fabrikat, såfremt bestemmelsen ikke ledsages af bemærkningen "eller dermed ligestilles".

EU-udbudsregler

EU's regler om offentlige myndigheders indkøb af varer og tjenesteydelser har central betydning for enhver offentlig myndigheds anskaffelse af varer og tjenesteydelser. Da de offentlige myndigheders indkøb udgør 10-15% af medlemsstaternes BNP, er der ikke blot juridisk, men også politisk interesse i at sikre fri konkurrence og at modvirke national særbehandling (statsstøtte mv.). Ligeledes giver udbudsreglerne mulighed for at kunne udbrede vedtagne standarder mv., jf. bemærkningerne straks ovenfor og i afsnit 1.4.e. Det offentlige indkøbsområde er derfor på et tidligt tidspunkt blevet genstand for EU-regulering.

Den 31. marts 2004 blev der gennemført en reform af direktiverne om offentlige udbud. Udbudsregimet består nu af to direktiver, der angiver hvilke udbudsformer, der kan benyttes inden for de områder (og tærskelværdier), hvor der er pligt til at gå i udbud. Det ene direktiv angår Samordning af fremgangsmåderne ved indgåelse af offentlige vareindkøbskontrakter, offentlige tjenesteydelseskontrakter og offentlige bygge- og anlægskontrakter (2004/18, almindeligvis kaldet *udbudsdirektivet*); det andet Samordning af fremgangsmåderne ved indgåelse af kontrakter inden for vand- og energiforsyning, transport samt posttjenester (2004/17, almindeligvis kaldet *forsyningsvirksomhedsdirektivet*). I det følgende henvises alene til reglerne i udbudsdirektivet.

Reglerne er særdeles komplicerede, og litteraturen om udbudsdirektiverne er tilsvarende overvældende, både herhjemme og når blikket vendes uden for Danmark. Konkurrencestyrelsen har den 20. december 2004 udarbejdet en god og instruktiv vejledning til direktiverne, der sammen med alle relevante retsregler findes på <www.ks.dk/udbud>. Hos *Dragsted m.fl.* (2004), s. 273 ff. findes en instruktiv oversigt over reglerne med særligt sigte på IT-anskaffelser. En samlet redegørelse over de nye direktiver foreligger med *Simon Evers Hjelmborg m.fl.*: EU-udbudsretten (2005).

Ifølge de nugældende direktiver findes der følgende udbudsformer, der – efter forskellige kriterier – kan anvendes, når en offentlig myndighed skal indkøbe IT.

1. Offentligt udbud

Et offentligt udbud er en procedure, hvorved alle interesserede leverandører indbydes gennem en licitation i EF-tidende, jf. art. 1, stk. 2, nr. 11, litra a. Denne udbudsform, indebærer – hvis den gennemføres gennemsigtigt og ikke-diskriminatorisk – den største garanti for fri konkurrence og kan derfor altid anvendes.

2. Begrænset udbud

Begrænset udbud er en procedure, som enhver økonomisk aktør kan ansøge om at deltage i, men hvor kun de økonomiske aktører, der af de ordregivende myndigheder modtager opfordring dertil, kan afgive tilbud, se art. 1, stk. 2, nr. 11, litra b. Myndigheden inviterer således en begrænset kreds – f.eks. 4-6 leverandører – til at give bud. Ved brugen af denne udbudsform er det særligt væsentligt, at myndigheden overholder de principper om gennemsigtighed og ikke-diskrimination, der ligger til grund for udbudsreguleringen.

Både ved offentligt og begrænset udbud gælder der et forbud mod, at den ordregivende myndighed forhandler enkeltvis med de bydende under og efter udbudsforløbet, se hertil *Dragsted m.fl.* (2004), s. 277. Reglerne herom fremgår ikke direkte af udbudsdirektiverne men følger af de formaliserede pligter, der kan udledes af direktiverne. Forbuddet blev nedfældet i forbindelse med vedtagelsen af de tidligere udbudsdirektiver, hvor Rådet og Kommissionen afgav en fælles erklæring, trykt i EFT 1994 L 111/114. Det hedder heri, at "fremgangsmåden ved offentligt eller begrænset udbud udelukker enhver forhandling med ansøgere eller bydende om grundlæggende elementer i kontrakterne, som ikke vil kunne ændres uden fare for konkurrencefordrejning", og at der "navnlig ikke [må] forhandles om priser". Der må således kun finde drøftelser sted med ansøgere eller bydende, når det sker med henblik på at præcisere eller supplere indholdet af deres bud eller de ordregivende myndigheders krav, og i det omfang, dette ikke giver anledning til forskelsbehandling. Se om rækkevidden af dette forhandlingsforbud, *Peter Wengler-Jørgensen & Katja Høegh* i U1994B.313 ff. og *Steen Treumer:* Ligebehandlingsprincippet i EU's udbudsregler (2000), s. 139 ff. Ifølge praksis fra Klagenævnet for Udbud er forhandlings-

forbudet dog ikke til hinder for, at der senere sker ændringer eller indskrænkninger i den udbudte kontrakt, hvis sådanne ændringer efter deres tekniske beskaffenhed og omfang i forhold til det samlede projekt ikke kan anses for så væsentlige, at udbuddet burde have været annulleret af ordregiver, se hertil *Lise Groesmeyer & Henriette R. Søltoft* i U1997B.199 ff. og *Anne Rubach-Larsen & Birthe Rasmussen* i J1997.315 ff.

3. Konkurrencepræget dialog

Med de nye direktiver er indført en ny udbudsform, den "konkurrenceprægede dialog". Herved forstås en procedure, som er åben for enhver, men hvor den ordregivende myndighed fører en dialog med de ansøgere, der har fået adgang til at deltage i proceduren med henblik på at udvikle en eller flere løsninger, der kan opfylde dens behov, og som skal være grundlag for de tilbud, de valgte ansøgere dernæst opfordres til at afgive, se art. 1, stk. 2, nr. 11, litra c. Reglerne herom findes i direktivets artikel 29, der åbner mulighed for denne udbudsform i udbud vedrørende "særligt komplekse kontrakter". Dialogen går da ud på, at myndigheden offentliggør en udbudsbekendtgørelse, der angiver de efterspurgte behov og krav. På grundlag af en prækvalifikation gennemført efter reglerne i direktivets artikel 44-52 indgår myndigheden herefter i en dialog med de udvalgte (prækvalificerede ansøgere). Dialogen har til formål at indkredse og fastslå, hvorledes myndighedens behov bedst kan opfyldes. Under dialogen kan myndigheden drøfte alle aspekter ved kontrakten med de udvalgte ansøgere. Det betones dog, at alle tilbudsgivere skal behandles ens, og at der navnlig ikke må udøves forskelsbehandling ved at der meddeles oplysninger, som kan stille nogle tilbudsgivere bedre end andre. En sådan forskelsbehandling vil f.eks. foreligge, hvis myndigheden for at opnå en bestemt leverandør knytter udbuddet til en grænseflade, som kun denne leverandør reelt kan byde på.

4. Forhandlingsudbud

Udbud med forhandling indebærer, at den ordregivende myndighed henvender sig til økonomiske aktører, som den selv udvælger, og forhandler kontraktens vilkår med en eller flere af disse, jf. art. 1, stk. 2, nr. 11, litra d. En sådan fremgangsmåde kan gennemføres på to principielt forskellige måder – henholdsvis med eller uden en forudgående udbudsrunde (prækvalifikation).

I udbudsdirektivets art. 30 er angivet, under hvilke nøjagtige betingelser denne udbudsform kan anvendes *efter* forudgående udbudsbekendtgørelse. Dette er således tilfældet, når der i forbindelse med et offentligt eller et begrænset udbud eller en konkurrencepræget dialog er afgivet tilbud, som ikke er forskriftsmæssi-

ge, eller er afgivet tilbud, som er uantagelige efter nationale bestemmelser.

Udbud efter forhandling *uden* forudgående udbudsbekendtgørelse indebærer ret beset, at der slet ikke sker noget udbud. Ifølge udbudsdirektivet kan denne fremgangsmåde da også kun anvendes under helt specielle omstændigheder, jf. nærmere artikel 30, litra b-d, hvoraf navnlig litra c kan have betydning på IT-området. Ifølge denne bestemmelse kan udbudsformen anvendes i det omfang, hvor den tjenesteydelse, der skal præsteres, ikke kan specificeres tilstrækkelig nøjagtigt til, at den kan indgås ved at vælge det bedste tilbud i henhold til reglerne for offentligt eller begrænset udbud. Dette kan især tænkes, hvis det drejer sig om "intellektuelle tjenesteydelser, som for eksempel tjenesteydelser vedrørende projektering af arbejder".

6. Dynamiske indkøbssystemer

Ved et "dynamisk indkøbssystem" forstås en fuldt elektronisk indkøbsproces for almindelige indkøb, der er *generelt tilgængelige* på markedet og opfylder den ordregivende myndigheds krav; processen er endvidere tidsbegrænset og under hele sin varighed åben for enhver økonomisk aktør, der opfylder udvælgelseskriterierne og har afgivet et vejledende tilbud, der er i overensstemmelse med udbudsbetingelserne, se art. 1, stk. 2, nr. 6. Et sådant indkøb kan bl.a. tænkes i relation til standardvarer og ingredienser til IT-systemer.

7. Projektkonkurrencer

En projektkonkurrence er en procedure, hvorved den ordregivende myndighed, navnlig inden for fysisk planlægning, byplanlægning, arkitekt- og ingeniørarbejde eller *databehandling*, kan anskaffe et planlægnings- eller projekteringsarbejde, der udvælges af en bedømmelseskomité efter udskrivning af en konkurrence med eller uden præmieuddeling, se art. 1, stk. 2, nr. 11, litra e. Denne udbudsform er gennem de seneste år blevet særligt benyttet på IT-området, hvor den ordregivende myndighed ikke på forhånd har gjort sig klar, hvad der ønskes anskaffet.

Valget af udbudsform

Når en udbudspligtig ordregivende myndighed skal indgå en offentlig kontrakt, skal den ifølge artikel 28 i udbudsdirektivet anvende de myndigheder de nationale procedurer, der er tilpasset til brug i forbindelse med dette direktiv. Disse procedurer fremgår af bekendtgørelse nr. 937 af 16. september 2004 om fremgangsmåderne ved indgåelse af offentlige vareindkøbskontrakter, offentlige tjenesteydelseskontrakter og offentlige bygge- og anlægskontrakter. Som almindelig regel skal udbud gennemføres som *offentlige eller begrænsede udbud.* På de særlige betingelser, der udtrykkeligt er nævnt i artikel 29, kan de ordregivende myndigheder indgå offentlige kontrakter ved hjælp af konkurrence-

præget dialog. I de tilfælde og under de omstændigheder, der udtrykkeligt er nævnt i artikel 30 og 31, kan der anvendes udbud med forhandling, med eller uden offentliggørelse af en udbudsbekendtgørelse.

Interoperabilitet

Udbudsreglerne giver anledning til særlige vanskeligheder i relation til leverancer, der skal være interoperable med eksisterende systemer. Det giver ingen mening at invitere en leverandør til at give bud på en systemtilbygning, når det tilbyggede kun kan kobles sammen med det eksisterende, hvis man kender grænsefladerne. På den anden side vil disse grænseflader ikke altid være kendte for systemets indehaver. Denne vil vel efter omstændighederne have en ret til at dekompilere systemet, jf. nærmere ophl. § 37; men ofte vil en sådan dekompileringshandling ligge helt uden for hans forudsætninger.

Esbjerg-sagen

Dette problem er belyst i en afgørelse af 25. oktober 1995 fra Klagenævnet for Udbud: Under forberedelsen af et tilbud om levering af et trafikovervågningssystem til Esbjerg Kommune rettede elektronikvirksomheden Siemens A/S henvendelse til Esbjerg Kommune for at modtage de kommunikationsprotokoller, som det leverede udstyr skulle overholde for at passe til kommunens eksisterende trafikstyresystem. Kommunen henviste Siemens til leverandøren af det eksisterende system, som også forventedes at afgive bud under udbudsforretningen. Siemens indbragte denne afgørelse for Klagenævnet for Udbud med påstand om, at kommunen i udbudsvilkårene skulle *give oplysning* om de funktionsbeskrivelser for det eksisterende system, som var nødvendige for at kunne afgive fyldestgørende bud. Alternativt krævede Siemens det eksisterende anlæg stillet til rådighed med henblik på reverse engineering.

Klagenævnet gav Siemens medhold, idet det var et krav ifølge udbudsmaterialet, at der skulle tilvejebringes interoperabilitet mellem kommunens eksisterende anlæg og det nye anlæg. Nævnet fandt, at kommunens pligt til at sikre tilbudsgiverne lige vilkår enten måtte opfyldes ved, at kommunen i udbudsvilkårene meddelte de nødvendige tekniske data eller ved, at de stillede det eksisterende anlæg til rådighed for tilbudsgiverne med henblik på reverse engineering, jf. ophl. § 37, jf. nærmere afsnit 7.4.g. Det fremgår ikke af afgørelsen, om der i kommunens aftaleforhold med den hidtidige leverandør fandtes en hemmeligholdelsesforpligtelse. Havde dette været tilfældet, kunne nævnet formentlig ikke været nået til dette resultat, og kommunens udbudsforretning måtte i så fald være gennemført efter de særlige regler om udbud efter forhandling.

21.2.e. Eksportkontrolregler

Problemet

Det er velkendt, at hensynet til nationens og almenhedens sikkerhed undertiden må medføre modifikationer af retsregler, der i øvrigt må anses for gældende. Et eksempel herpå er reglerne om udførsel (eksport) af udstyr og teknologi, der kan anvendes til krigsførelse, overvågning eller anden sikkerhedstruende virksomhed.

Våbeneksport

Våbenloven (lovbekendtgørelse nr. 918 af 10. september 2004 med senere ændringer), forbyder bl.a. udførsel (uden justitsministerens tilladelse) af "maskiner, instrumenter, apparater og andre produktionsmidler, der overvejende anvendes til fremstilling eller vedligeholdelse af våben, ammunition eller krigsmateriel, samt dele og tilbehør til sådanne produktionsmidler", se § 6, stk. 1, nr. 4. Bestemmelsen har bl.a. praktisk betydning i virksomheder, der leverer software til højteknologiske våbensystemer.

International regulering

At håndhæve sådanne restriktioner på internationalt plan indebærer en handelshindring, der principielt er omfattet af TEF. Efter reglerne i Traktatens kapitel 4 har medlemsstaterne således overført deres kompetence til at føre individuel handelspolitik til EU. Den internationale samordning af reglerne om national sikkerhedskontrol har, bl.a. som følge af NATO-samarbejdet, været henskudt til behandling i internationale fora. Frem til 1994 blev disse spørgsmål behandlet i den koordinerende komite for multilateral eksportkontrol, COCOM, der bestod af 16 lande, herunder alle EU-medlemslande på nær Irland. COCOM blev opløst i marts 1994; men året efter besluttede 28 lande at etablere en efterfølger, kaldet the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ved en aftale tiltrådt af 31, og senere 33, lande, herunder de vestlige lande, Rusland, Ungarn, Slovakiet og Polen.

Wassenaar-ordningen

Wassenaar-ordningen kontrollerer eksport af produkter med *dobbelt anvendelse*. Hermed menes, at de pågældende produkter såvel kan anvendes til civile som til militære formål. Krypteringsudstyr er et eksempel på sidstnævnte, jf. omtalen i afsnit 8.2.e. om tillægget til Wassenaar-aftalen af 3. december 1998. For varer med udelukkende militær anvendelse findes der andre ordninger, herunder vedrørende nukleart udstyr (NSG-samarbejdet), kemiske og biologiske stoffer (den såkaldte Australiensgruppe) og missilteknologi (MTCR-aftalen, for Missile Technology Control Regime).

Dansk regulering

Det juridiske grundlag for den danske regulering af disse spørgsmål foreligger i lov om anvendelsen af visse af Det Euro-

pæiske Fællesskabs retsakter om økonomiske forbindelser til tredjelande mv., jf. lovbekendtgørelse nr. 474 af 14. juni 2005. På grundlag af denne lov har Erhvervs- og Byggestyrelsen udstedt bekendtgørelse nr. 475 af 14. juni 2005 om kontrol med udførslen af produkter og teknologi med dobbelt anvendelse ("*dual-use*") og kontrol med ydelse af teknisk bistand.

Bestemmelserne i denne bekendtgørelse supplerer to EU-retsakter: *Rådets forordning af 22. juni 2000* nr. 1334/2000 (EFT 2000 L 159/1) om en fællesskabsordning for kontrol med udførsel af varer med dobbelt anvendelse, og *Rådets afgørelse af 19. december 1994* om en fælles aktion, 94/942/FUSP (EFT 1994 L 367/8) som ændret ved afgørelse 96/613/FUSP, ved afgørelse 97/100/FUSP og ved 98/232/FUSP (EFT 1998 L92/1). Afgørelserne er vedtaget af Rådet på grundlag af TEU artikel J.3. vedrørende kontrol med udførslen af varer med dobbelt anvendelse fra Fællesskabet. Retsakterne er ændret ved Rådets afgørelse af 22. oktober 1996, EFT 1996 L 278/1. Ved denne ændring erstattes den tidligere liste med en ny i konsekvens af de aftaler, der bl.a. er gennemført ved Wassenaar-arrangementet.

Bekendtgørelsen hjemler straf af fængsel i op til 2 år (medmindre anden straf er forskyldt efter anden lovgivning) for den, der udfører produkter med dobbelt anvendelse uden at være i besiddelse af en tilladelse, jf. § 10, stk. 1. Hvilke teknologier, der kræver tilladelse, fremgår af de underliggende EU-retsaktiver. Det siges udtrykkeligt i § 2, stk. 4, at begrebet "produkter med dobbelt anvendelse" også omfatter software. Den nævnte tilladelse indhentes hos Erhvervsministeriet (Erhvervs- og Byggestyrelsen), jf. § 3.

Sagsbehandling

Bekendtgørelsens § 5 overlader det til Erhvervs- og Byggestyrelsen at fastsætte nærmere forskrifter om formkrav til ansøgninger og om benyttelse, form og indhold af udførselstilladelser.

Det EU-retlige – og heraf følgende danske – regelgrundlag, for eksportkontrol af varer med dobbelt anvendelse, udgør minimumsregler. De lister, der er sat i kraft af rådsbeslutningerne, omfatter altså ikke nationale kontrolforanstaltninger, som medlemsstaterne måtte søge at opretholde. Navnlig USA er kendt for at opretholde sådanne foranstaltninger. Dette mærkes bl.a. på krypteringsområdet, hvor der efter amerikanske regler alene kan meddeles eksporttilladelse for krypteringsprodukter, der anvender en nøglelængde på mindre end et vist antal bits. Sådanne nationale eksportkontrolregler kan få følelig virkning også uden for USA's grænser, eftersom de amerikanske regler ikke alene foreskriver sanktioner for selve den virksomhed, der overtræder reglerne, men også for virksomhedens samhandelspartnere (nemlig i form af nægtet adgang til det amerikanske marked).

USA's regulering af krypteringssamhandelen har bevæget sig i skiftende retninger. I efteråret 1996 skete der en principiel omlægning af reglerne, der bl.a. betød, at kontrollen med deres overholdelse blev flyttet fra *State Department* til *Department of Commerce*, der fører en mere "eksportvenlig" linje. Tilladelse til eksport af krypteringsprodukter vil være betinget af, at eksportøren inden en fastsat frist vil søge at opbygge et "key recovery" system, der sikrer myndighederne adgang til de nøgler, der kan dekryptere krypteret information. En yderligere liberalisering skete i efteråret 2000, jf. *Thomsen & Paytas* i 17 CLSR 11 ff. (2001). Liberaliseringen skyldes dels et internationalt pres (reglerne hæmmer amerikanske eksportvirksomheders muligheder i den internationale konkurrence), dels en opfattelse af, at reglerne i det omfang de forbyder eksport af ren viden om kryptering rummer et grundlovsproblem. Grundlovsmæssigheden af de amerikanske regler er i øvrigt blevet anfægtet under flere verserende retssager i USA. I sagerne *Bernstein v. United States* (9th Cir. 6 May 1999) og *Bernstein v. U.S. Department of State*, 922 F.Supp. 1426 (1996) fandtes de amerikanske eksportkontrolregler, der bl.a. forbyder eksport af krypteringssoftware, at stride mod den amerikanske forfatnings regler om ytringsfrihed. Se ligeledes *Junger v. Daley*, 209 F.3d 481 (6th. Cir., 2000). Begge afgørelser forkaster det synspunkt, at hensynet til den nationale sikkerhed kan begrunde sådanne indskrænkninger. Ytringsfrihedssynspunktet forudsætter, at eksporthandlingen knytter sig til kildetekstversionen, idet kildeteksten til et program betragtes som den måde, hvorpå programmører udveksler idéer vedrørende programudvikling til hinanden.

21.3. Aftaleindgåelse

21.3.a. Aftaleforhandlingen

Problemstillingen

Når parterne i en aftale, herunder i forbindelse med en IT-overdragelse, nedfælder deres vedtagelser på skrift som en forpligtende aftale, skaber de dermed et *retsgrundlag* for gennemførelsen af denne transaktion, der forpligter på samme måde som lovgivning, retssædvaner og andre retsregler. Som det gælder for den egentlige lovgivning, er også aftalen resultatet af strategier, hvoraf nogle må afgøres efter en grundig beslutningsproces, medens andre kan håndteres rutinemæssigt. Sådanne forhandlingsteknikker studeres i den egentlige forhandlingslære, jf. nærmere *PA* s. 82 ff. med henvisninger. På dette sted skitseres visse hovedlinjer af dette problemfelt med særligt sigte på forhandling af IT-aftaler.

Om forhandling af IT-aftaler se bl.a. *Nicolai Dragsted*: IT-kontrakter I og II (2000), *Christophersen & Føyen* (1981), s. 173 ff., EDBR.19 (1978): Anskaffelse af databehandlingsudstyr, og Dansk Dataforenings pjece "IT-kontrakten – hvordan og hvornår?" (1999).

Forhandlingsgrundlaget

Som grundlag for enhver aftaleindgåelse vil parterne have et ønske om at opnå en tilstand, der er *bedre* end den, de kom fra, f.eks. kunne tjene mere end de har tjent før, eller gennemføre en arbejdsrutine lettere end før. I visse tilfælde kræver afklaringen af, hvad der er "bedre" – og ikke mindst om *midlet* til at opnå denne tilstand – ekstern bistand ved konsulent el.lign. Det gælder navnlig for talrige systemoverdragelser. Et væsentligt formål med denne analyse af forhandlingsgrundlaget er desuden at opnå klarhed om, hvad kunden ønsker at betale for sin ydelse.

Kompromismuligheder

Forhandlingerne om en IT-transaktion vil ofte udmønte sig i uenighed om leverandørens garantier for systemets ydeevne og funktion. Undertiden kan man løse den slags uenigheder ved at *kalkulere en økonomisk værdi* af den pågældende risiko, som man lader den part, der ønsker den pågældende garanti, erlægge som "præmie" oveni købesummen. En sådan fastlæggelse af den økonomiske værdi af en garanti kan ligefrem være påbudt, f.eks. for at kunne sammenligne to tilbud, der er indhentet under et offentligt udbud. En anden måde at løse uenighed om leverandørens indestående for produktet på består i at identificere leverandørens *tekniske forudsætninger* for at kunne opfylde en given garanti (f.eks. uventede vanskeligheder ved implementering af del-moduler, problemer med at opnå lovede svartider, fornøden kompatibilitet med tilsluttet udstyr el.lign.) og knytte reguleringen til disse forudsætninger. Dette kan f.eks. ske ved, at man fastsætter regler for, hvorledes leverandøren skal imødegå de pågældende risici (f.eks. ved at indhente ekspertise udefra, at foreslå systemet omstruktureret, at opgradere kritiske maskinkomponenter el.lign.).

21.3.b. Aftalens form

Talrige IT-retlige aftaleforhold udspringer af mundtlige aftaler, hvor der ikke nedfældes egentlige vilkår. Dette gælder f.eks. ved køb over disken, pr. postordre eller gennem mundtlige forhandlinger med en repræsentant, jf. til illustration *ERA 3.48* (KB 10.6.1986), der forpligtede leverandøren på grundlag af udtalelser fra dennes repræsentant.

Skriftlighed?

Om en aftale bør nedfældes, beror på en række forskelligartede faktorer, jf. nærmere *PA*, s. 195 ff.: Retsforholdets latente

konflikter (parternes grundlæggende fælles eller modstående interesse), de implicerede værdier, muligheden for at foretage dækningskøb hos en anden leverandør, aftalens varighed, ydelsens enkeltstående eller løbende karakter og aftalens retsvirkninger (om parterne begrænses i deres efterfølgende handlefrihed el.lign.). Er aftalen i disse mangfoldige henseender enkel og overskuelig, er det som regel tilstrækkeligt at indgå den mundtligt, således at efterfølgende spørgsmål om misligholdelse mv. blot reguleres af de almindelige regler.

- mundtlighed

Mundtlighed er den almindelige aftaleform ved køb af mindre programmeringsopgaver mv. og ved installation af standardudstyr. Netop denne praksis har skabt problematikken om *shrink wrap*-licenser, jf. nærmere afsnit 21.3.c. Ved at nedfælde aftalen på skrift vil parterne minimere risikoen for uklarhed: De fleste tænker sig bedre om, før de forpligter sig på skrift. Ganske som aftaler om opførelse og overdragelse af fast ejendom kræver indgående studier af tekniske og juridiske spørgsmål, rummer navnlig aftaler om udvikling af større skræddersyede applikationer mv., eller om atypiske anvendelser af standardkomponenter, talrige risici for misforståelser mv. Aftaler indgået med digitale medier, f.eks. Internet, behandles i denne sammenhæng som skriftlige aftaler.

- flere versioner

Et skriftligt aftaledokument vil ofte foreligge i flere udformninger i den proces, der fører til dets færdiggørelse, f.eks. som en kravsspecifikation (behovsopgørelse), en systembeskrivelse, et tilbud, en accept eller et bilagsmateriale. Ofte vil aftalens parter anse den *seneste* – underskrevne – manifestation for gældende. Undertiden er der i den underskrevne aftale ved en fejltagelse foretaget ændringer, som ikke reflekterer parternes enighed, uanset de kommer til udtryk i dokumentet. Sådanne tilfælde må vurderes med udgangspunkt i parternes formodede vilje, sml. herved den retspraksis, der findes om uoverensstemmelse mellem slutseddel og skøde/pantebrev ved overdragelse af fast ejendom, *U 1924.764 H*, *U 1956.622 H* og *U 1989.273 V*.

Bilag

I teknisk komplekse transaktioner er det almindeligt at samle aftaledokumentet i selve aftalen og et hertil hørende antal bilag. Et sådant bilagsmateriale reserveres da til forhold af teknisk karakter, som primært må formodes læst af teknikerne. Bilaget kan f.eks. indeholde specifikationer af grænseflader, fabrikat, kapacitet og tidsplaner. Hertil føjer sig ofte bilag af delvis historisk karakter, f.eks. udbudsmateriale, kravsspecifikationer (uanset om de siden er indarbejdet i aftaleteksten eller i en systembeskrivelse), tilbud og brochurer. Da hovedkontrakten og bilagsmaterialet

kan være ligeværdige grundlag for rettigheder og forpligtelser, må der udvises samme omhu ved konciperingen af begge typer af dokumenter. Standardaftalerne på IT-området (K18, K33, EDB-rådets og ESF's kontrakter) forudsætter da også en betydelig indsats ved konciperingen af bilagene.

21.3.c. Shrink wrap-aftaler

Problemet

Et særligt problem om eksemplar-køb angår gyldigheden af de "licensvilkår", der ofte placeres under den cellofan, der omgiver programpakken, og som angiver, at man ved at bryde cellofanen tiltræder disse vilkår, såkaldte *shrink wrap*-vilkår eller -licenser. Det vil ofte være angivet i sådanne vilkår, at den potentielt forpligtede har muligheden for at levere varen tilbage mod fuld godtgørelse af erlagt betaling, hvis han ikke er parat til at acceptere vilkårene.

Udgangspunkt

I almindelighed må det antages, at vilkår, der ikke har været genstand for drøftelse, ikke er tiltrådt og derfor heller ikke udgør en del af aftalegrundlaget. Almindelige aftaleretlige regler fører til, at efterfølgende vilkår, der knyttes til en allerede indgået aftale, ikke er bindende. En aftale, der f.eks. indgås telefonisk, udgør i kombination med de udfyldende retsregler (købelov mv.) det fulde retsgrundlag mellem parterne. Skal dette retsgrundlag modificeres, kræves som udgangspunkt tiltrædelse fra begge parter. En ensidig fremsendelse af vilkår er som udgangspunkt ikke i sig selv bindende for modtageren, jf. *U 1996.1125 SH*.

Modifikationer

Dette udgangspunkt må dog underkastes visse modifikationer. Hvis brugeren for det første ved – eller bør vide – at den erhvervede vare sælges på grundlag af de velkendte klausuler, der findes i *shrink wrap*-dokumentet, fører almindelige fortolkningsregler (herunder ikke mindst forudsætningsbetragtninger) til, at brugeren er bundet af dem i denne forventede skikkelse. Men er vilkårene atypiske må de kunne afvises. Den, der vil gøre sådanne vilkår gældende, og som har grund til at tro, at brugeren ikke ville have anerkendt dem under en sædvanlig aftaleforhandling, kan ikke opnå en bedre retsstilling ved således at sælge katten i sækken.

Det kritiske spørgsmål er, om den bruger, der *ikke* kender vilkårenes typiske indhold, men dog ved, at ydelsen typisk vil være klausuleret i et eller andet omfang fra producentens side, alligevel er bundet. Er der tale om en erhvervsdrivende, og er der tale om vilkår, der er sædvanlige inden for branchen, må man formentlig nå til, at de binder: Kunden ved jo, at der følger et sæt

detailprægede aftalevilkår med, og ved ikke at sikre sig en afklaring inden aftalens indgåelse må det være rigtigt at lade ham være bundet på lige fod med den mere velinformerede kunde, jf. *GA* s. 369 f. Man kan her drage analogier til de klausuler, der ledsager en billet eller et pakkerejsearrangement bestilt telefonisk. Retsstillingen er her, at aftalen først anses for endeligt indgået på det tidspunkt, hvor kunden får vilkårene i besiddelse, smh. *Günther Petersen:* Ansvarsfraskrivelse (1957), s. 118. For så vidt er der harmoni mellem sådanne vilkår, der tildeler kunden en særlig ret til at komme ud af aftalen, og baggrundsretten. Også i denne henseende er der dog behov for modifikationer i tilfælde, hvor vilkårene har et usædvanligt eller – for kunden – særligt byrdefuldt indhold.

Konklusion

Om et shrink wrap-vilkår er aftaleforpligtende beror derfor sammenfattende på, om adressaten med rimelighed måtte kunne påregne det. Gengiver vilkårene en almindelig fulgt praksis, der nærmest har sædvanekarakter, kan man i almindelighed ikke stille store krav til vedtagelsen, jf. nærmere *Kaltoft og Søborg Hansen* i Justitia 1998 nr. 5, s. 47 ff. med analyse af bl.a. amerikansk retspraksis. Når det gælder de vilkår, der indeholder særlige og uforudsete reguleringsområder (f.eks. voldgift og lovvalg i fjerne fora og jurisdiktioner, ekstreme ansvarsbegrænsninger el.lign.), må man dog være mere tilbageholdende med at antage gyldighed. Det forhold, at leverandørerne ikke viser evne og vilje til at håndhæve disse bestemmelser, er i øvrigt ikke med til at højne den juridiske respekt for disse instrumenter.

At forbrugeren bryder forseglingen omkring en leveret programpakke medfører, at han fortaber sin ret til at gøre en fortrydelsesret gældende efter reglerne om fjernsalg. Dette fremgår udtrykkeligt af forbrugeraftalelovens § 20, stk. 3, nr. 2, men har i princippet intet at gøre med den aftaleretlige gyldighed af de vilkår, der eventuelt måtte ledsage den pågældende forsegling.

Reversklausuler

Tilsvarende problemer som dem, der angår gyldigheden af *shrink wrap*-dokumenter, har i dansk retspraksis foreligget i forbindelse med de såkaldte reverssystemer, man har anvendt ved ugebladsdistribution. Ved dommen i *U 1943.1119 H* blev en sådan klausul opretholdt overfor en kioskkøber, der i strid med klausulen tilsigtede at effektuere videreudlejning, under hensyntagen til køberens kendskab til ordningen samt til den saglige interesse heri. Et andet resultat nåede Højesteret til i *U 1935.1066 H*, der lagde til grund, at forbuddet ikke i sig selv var forpligtende. Se ligeledes *U 1930.416 H*, *U 1942.963 V*, *NJA 1939.592*, *Rt. 1940.450*, *NJA*

1949.645, *Rt. 1955.536* og i det hele *Blomqvist*: Overdragelse af ophavsrettigheder (1987), s. 114 f. I Rådsdirektivet om retlig beskyttelse af programmer har man forsøgt at aflive shrink-wrap licensen ved at stille krav om, at aftaler, der indskrænker brugerens ret til at foretage sædvanlig reproduktion af programmet under brug, skal være "udtrykkeligt fastsat". Dernæst sikrer direktivet, at brugeren altid har ret til at tage en sikkerhedskopi, for så vidt det er nødvendigt for benyttelsen. Se herved art. 5, stk. 1 og 2. Se i øvrigt *E&A* s. 319 f. og *Magnus Stray Vyrje* i Lov og Rett 1986.47., *Michael Pawlo* i NIR 1999.141 ff.

Flere amerikanske domstole har taget stilling til gyldigheden af shrink wrap-vilkår. I *Step-Saver Data Systems v. Wyse Technology and Software Link, Inc.*, 939 F2d 91 (3rd Cir. 1991), var en programpakke solgt efter telefonisk bestilling. Da pakken blev fremsendt, lå der en shrink wrap-licens i den. Vilkårene heri ansås ikke forpligtende. En tilsvarende retstilstand blev resultatet i *Arizona Retail Systems v. Software Linc., Inc.*, 831 F.Supp. 759 (D.Ariz, 1993), hvor retten dog fandt, at købers kendskab til vilkårene inden købet gav grundlag for at knytte retsvirkning til vilkårene. En skotsk Court of Session dom fra december 1995 er gået videre, se *Beta Computers (Europe) Limited v. Adobe Systems (Europe) Limited*, omtalt i 12 CLSR 1996 310 ff. (Sep-Okt). Retten fandt her, at en aftale om køb af edb-programmel, der tog udspring i en telefonbestilling, først kunne anses for indgået på det tidspunkt, hvor køberen modtog programpakken og her fik lejlighed til at studere de vedhæftede licensvilkår. Se endelig appelretsafgørelsen fra New Jersey i sagen *Steven J. Caspi et al. v. Microsoft Network*, 323 N.J. Super. 118 (2 july, 1999), der opretholdt en "click wrap"-aftale, og nærmere herom afsnit 19.2.b. Se i øvrigt *Henrik S. Spang-Hanssen* i Complex 5/01, s. 80 ff.

Pro-CD-sagen

En toneangivende amerikansk afgørelse om gyldigheden af en *shrink wrap*-licens er *Pro-CD v. Zeidenberg*, 86 F.3d 1447 (7th Cir., 1996): Martin Zeidenberg havde købt et CD-ROM-produkt, som indeholdt en database med data fra et stort antal telefonbøger. Basens oplysninger kunne ikke beskyttes efter amerikansk ophavsret, men ifølge et sæt shrink-wrap vilkår, som kom til syne på skærmen under brug, men ikke på pakken, måtte oplysningerne kun anvendes til private, ikke-erhvervsmæssige formål. Desuagtet stillede Zeidenberg basens oplysninger til rådighed fra en web-server mod betaling, hvorpå rettighedshaveren, Pro-CD, anlagde sag med påstand om, at vilkårene for licensaftalen var brudt. Retten gav Pro-CD medhold i, at aftalen var indgået på en sådan måde, at dens endelige – og ikke usædvanlige – vilkår først blev fastlagt efter brugerens formelle accept af købet. I så henseende fandt retten lighedspunkter mellem den foreliggende form

for aftaleindgåelse og køb af flybilletter o.lign., hvor kunden også blot ringer op for at bestille ydelsen, men først senere (ved billettens fremsendelse) får kendskab til de nærmere vilkår. Førsteinstansen (se 908 F.Supp. 640, W.D. Wis, 1996) havde antaget, at købet var indgået på de vilkår, kunden kunne læse på programpakkens yderside, hvorimod kunden ikke var bundet af de klausuler, som yderteksten henviste til, men ikke gengav.

Diskussion

Dommens resultat er formentlig påvirket af, at der var tale om en helt usædvanlig handling fra Zeidenbergs side, sammenholdt med, at Pro-CD kunne siges at stå i en særligt vanskelig situation, eftersom amerikansk ret ikke yder beskyttelse for databaser, der ikke har den fornødne originalitet. Det er i hvert fald langt fra givet, at en dansk domstol ville nå til samme resultat vedrørende den aftaleretlige forpligtelse, såfremt det omtvistede vilkår tilsigtede at yde rettighedshaveren en særlig fordel, f.eks. pålægger brugeren en usædvanlig ansvarsfraskrivelse eller et byrdefuldt forum for påkendelse af tvister.

I sagen *Hill v. Gateway*, 105 F.3d 1147 (7th Cir. 1997) vidste den forpligtede, at der ville være et sæt aftalevilkår, hvis nærmere indhold ikke var kendt på aftaletidspunktet, knyttet til den aftaleforpligtelse, han påtog sig. Se senest *Ma. Mortensen Co. v. Timberline Software Corp.*, 970 P.2nd 803 (Wash. App., 1999) opretholdt et aftalevilkår, der fraskrev erstatningsforpligtelser for indirekte tab. Se tilsvarende *Westendorf v. Gateway 2000 Inc.* (Del. Ch. Mar. 16, 2000).

Click wrap-vilkår

Ved elektronisk handel på Internet er der opstået en ny form for aftaleindgåelse, de såkaldte point and click-aftaler, jf. herom afsnit 19.2.b. Disse aftaleformer adskiller sig imidlertid fra shrink wrap-aftalen ved, at vilkårene lægges klart frem for brugeren *inden* aftaleindgåelsen. Her afgives den relevante viljeserklæring nemlig med fuld viden om de vilkår, der er gældende for transaktionen. Er der tale om salg fra en hjemmeside af information, der ikke er omfattet af købelovens regler, må det tilsvarende antages, at en forbruger er bundet af de ansvarsbegrænsninger, der står anført på hjemmesiden. Vilkår, der ikke på tydelig vis træder frem for brugeren, men som gøres gældende mod denne i kraft af et museklik (såkaldte click wrap-vilkår) kan dog som udgangspunkt ikke tillægges aftalegyldighed.

21.3.d. Koncipering

Generelt

Det vil altid være en smagssag, hvordan koncipisten vil koncipere og systematisere en IT-aftale, se nærmere hertil *PA* s. 132 ff. En hensigtsmæssig inddeling vil først omtale leverandørens forplig-

telser og derefter brugerens. Herefter kan aftalen regulere ydelsens levering eller aflevering. Derpå afklares de ejendoms- og immaterialretlige rettighedsspørgsmål. Senere i aftalen omtales de regler, der handler om aftalens misligholdelse og opsigelse. Til sidst følger de mere teknisk prægede regler om f.eks. voldgift, lovvalg og underskrift.

Omfang

Omfanget af en IT-aftale bør altid afpasses efter *målsætningen* med den underliggende transaktion, og herunder under fornøden hensyntagen til karakteren af de værdier og risici, der indgår i transaktionen. Jo større risikoen er for, at parterne misforstår hinanden eller ikke har noget fælles incitament til at løse opståede problemer, desto større stiger behovet for detailregulering.

Præambel

I amerikanske aftaledokumenter – der i forvejen er meget ordrige – er det almindeligt at formulere målsætningen for transaktionen i en særlig præambel. Heri fortælles det, hvem parterne er, hvilken lovgivning deres selskaber er stiftet under, hvilken type forretning de driver, og hvilken interesse de har i den foreliggende aftale. Efter danske forhold vil en sådan opremsning ofte forekomme fremmedartet – navnlig hvis aftalen angår en ukompliceret ydelse. En præambel kan dog være hensigtsmæssig, når aftalen er atypisk, f.eks. hvis parternes kontakt har en særlig baggrund. En kort og klar introduktion af, hvem parterne er, det specielle behov for databehandling og formålet med leverandørens ydelse letter læsearbejdet for den, der efterfølgende skal bruge aftalen.

Definitioner

Mange IT-aftaler indledes med en minutiøs opregning af de gældende definitioner. Denne stil, der ikke kendes på mange andre områder af dansk kontraktsret, har vistnok rod i ingeniørmæssig tænkning. Selv om man ved at definere almindeligvis kan undgå uklarheder, gælder begrænsningens kunst også på dette punkt. Definitioner bør placeres i tilknytning til de aftalepunkter, der angiver de relevante retsvirkninger. At anføre dem *en bloc* som en indledning rummer en risiko for uventede retsvirkninger, der i så fald skal underkastes korrigerende fortolkninger.

21.3.e. Beskrivelsen af ydelsen

Kompleksiteten

Som nævnt foran kompliceres IT-aftalekoncipering generelt af vanskelighederne ved at *beskrive* de tekniske og til dels immaterielle ydelser, der indgår i transaktionen. Mange af de vanskeligheder, der følger af ydelsens kompleksitet, kan imødegås gennem brug af systemterminologi, jf. nærmere afsnit 2.3.: Ved f.eks. at betragte et leveret produkt som en *komponent*, der skal indgå i et

allerede eksisterende *system*, eller det leverede system som en komponent i det system, brugerens virksomhed i forvejen udgør, har koncipisten et solidt terminologisk grundlag for at fokusere på de relevante fysiske og organisatoriske rammer og *lovmæssigheder* for systemanvendelsen. En sådan beskrivelse giver også en nærliggende fokus på de *funktioner*, der tilstræbes i de forskellige sammenhænge og grænseflader.

Aftalt betegnelse

Den måde, hvorpå ydelsen er beskrevet i aftalen, er afgørende for, hvilke forpligtelser leverandøren er underkastet. Er ydelsen beskrevet efter sin *betegnelse* – f.eks. som et varemærke – er ydelsen præsteret, så snart det leverede svarer til betegnelsen. Der er i så fald tale om en *resultatforpligtelse*, der først er præsteret, når et produkt svarende til betegnelsen foreligger. Se til illustration dommen i *ERA 1.101* (Odense byret, 2.2.1984), hvor det kom køberen til skade, at han havde anmodet om en komponent beregnet til en given interface. Skal kunden opnå sikkerhed for, at ydelsen opfylder den forventede funktion, må han selv sørge for at indføje dette i aftalens beskrivelse af ydelsen.

Opfyldelsesvalg

Dansk ret overlader opfyldelsesvalget til leverandøren. En aftale om levering af "en laserprinter" eller "en PC" – som f.eks. ofte ses i forbindelse med nøglefærdige brancheløsninger mv. – er derfor som udgangspunkt korrekt opfyldt, uanset hvilken laserprinter eller PC der leveres. I visse tilfælde kan det give anledning til tvivl, hvilket fabrikat leverandøren er pligtig at levere, sml. *U 1963.364 H*, hvor køberen af en traktor af mærket "Massey-Harris" ikke kunne forlange at få leveret en "Massey-Ferguson", selv om denne betegnelse – ved en fejltagelse – var blevet indføjet i aftaledokumentet.

Indsatsforpligtelser

Er der derimod tale om en *indsatsforpligtelse* har kunden ingen sikkerhed for, at den tilsigtede funktionalitet opnås. I sådanne aftaler skal leverandørens ydelse honoreres, hvis blot det ligger fast, at han har gjort en god og forsvarlig indsats, selv om indsatsen ikke resulterer i nogen funktionalitet for brugeren. Et eksempel herpå er aftaler om systemudvikling uden angivelse af, om det færdige resultat kan opnå praktisk brugbarhed for kunden.

Ved dommen i *U 1964.125 H* fandt Højesteret således, at en produktionsvirksomhed havde pligt til at betale udviklingsomkostningerne til frembringelse af et sprøjtestøbeværktøj, selv om dette viste sig uegnet til formålet. Afgørelsen betoner, at sælger ikke havde påtaget sig nogen garanti herfor.

Koncipering

Hvor baggrundsretten overlader leverandøren en frihed i opfyldelsesvalget, er det kundens opgave at få denne frihed begrænset

på relevant vis i kontrakten. Dette kan f.eks. ske ved at præcisere betegnelser ved henvisninger til fabrikat og specifikationer (f.eks. varemærke, processor-hastighed, disk-bestykning mv.). Som hovedregel er det op til den, der vælger at købe efter betegnelse, at udspørge leverandøren om leverancens omfang og om behovet for supplerende udstyr mv. Denne regel gælder i særdeleshed, når køberen har særlige forudsætninger for anvendelsen af systemet. *ERA 1.104* (VLD 23.5.1984) pålagde således køberen risikoen for, at hans specielle forudsætninger vedrørende anvendelsen af et faktureringsprogram (udskrivning af samme faktura på flere sprog) ikke var lagt frem for sælgeren.

Aftalt funktion

Er ydelsen beskrevet som en funktion, er aftalen opfyldt, når denne er opnået. Der er ingen grænser for, hvilke slags funktioner en kontraktspart kan påtage sig at præstere. Visse IT-funktioner knytter sig til tekniske egenskaber som f.eks. processor- og lagerkapacitet; andre angår systemets behovsopfyldelse overfor brugeren, tilladte datatyper og -mængder, svartider eller brugergrænseflader. Almindeligvis vil forskellige funktionsbeskrivelser gælde side om side. Det forhold, at koncipisten gør sig umage for at beskrive ét funktionelt aspekt i aftalen, er ikke ensbetydende med, at erhververen hermed får det, han efterspurgte. En aftale, hvorefter brugeren skal kunne udføre en bestemt type posteringer i sit lagerprogram, er alt andet lige opfyldt, selv om systemet har svartider på halve eller hele minutter.

- svartider

Aftalens beskrivelse af svartider rummer et særskilt problem. Den egenskab, der udmønter sig i en svartid, beror nemlig på, hvordan systemet anvendes. Ved integrerede systemer, der tillader samtidig afvikling af forskelligartede databehandlingsopgaver, vil muligheden for at opnå korte svartider bero på, hvilke af disse opgaver der afvikles samtidig. Hvis aftalen uden forbehold angiver, at de "gennemsnitlige" svartider vil ligge på under x sekunder, må der formentlig skulle udregnes en median over en gennemsnitlig systembelastning. Er garantien for svartider ikke betinget af gennemsnittet, må systemet som udgangspunkt til enhver tid kunne opfylde disse krav. Et andet problem knytter sig til det målepunkt, der skal danne grundlag. Er svartidsberegningen f.eks. knyttet til en skærmterminal, kan beregningen enten tage udgangspunkt i det tidspunkt, hvor et skærmbillede er fuldstændigt etableret, til det tidspunkt, hvor skærmterminalen modtager de data, der er nødvendige til at skabe skærmbilleder, eller til det tidspunkt, hvor brugeren kan tilegne sig de informationer, der typisk er nødvendige for hans brug af skærmbilledet.

Funktionsbeskrivelser

I almindelighed kan man sondre mellem funktionsbeskrivelser i kendte henholdsvis endnu ikke udviklede systemer.

- eksisterende systemer

For eksisterende systemer vil funktionsbeskrivelsen sjældent blive formuleret med sigte på den konkrete aftale. Typisk foreligger der allerede et papir, som koncipisten kan knytte sig til, f.eks. manualen, dokumentationen eller salgsmaterialet. I valget herimellem vil det som regel være mest hensigtsmæssigt at knytte funktionsbeskrivelsen til salgsmaterialet. Det er typisk holdt i brugerens sprog og med fokus på de centrale kvaliteter. Mindre hensigtsmæssigt er det at anvende manualen. Manualer hører ikke til den del af verdenslitteraturen, der læses mest intenst, og dette er ikke uden grund. Ikke sjældent er de uforståelige og usystematiske. Der kan derfor ligge væsentlige informationer om systemets begrænsninger skjult, hvor den uindviede læser mindst venter det. Da idéen med at beskrive efter funktion netop er at indfri brugerens forventninger til systemet, vil en henvisning til manualen reelt kunne rumme en ansvarsfraskrivelse. Dertil kommer, at manualer ofte ikke beskriver det leveredes funktion; der fokuseres naturligt på brugerens kommandoer mv. Endelig spiller det ind, at manualer ikke altid dækker systemets funktioner fuldt ud. Megen standardsoftware sendes på markedet i sidste øjeblik. Da trykning af manualer tager længere tid end kopiering af disketter, halter manualen ofte bagefter. Kun få leverandører tager konsekvensen heraf og indsætter rettelsesblade.

I kontrakter om større systemer beskrives den aftalte funktion ofte som en driftseffektivitet. Både EDB-rådets standardkontrakt om køb, K33, K18 og ESF's totalkontrakt forudsætter, at dette spørgsmål defineres i bilagsmaterialet. Udgangspunktet er en "sædvanlig driftseffektivitet". I K33 måles denne som en procentdel, der beregnes som forholdet mellem tilgængelig driftstid og aftalt driftstid. Hvor tærsklen ligger for uhensigtsmæssigheder, der må tolereres, afgør en sådan beskrivelse ikke. Det er derfor vigtigt at tage stilling til, hvornår der foreligger "tilgængelighed", dvs. hvilke tekniske eller betjeningsmæssige forhold der kræves overholdt. En nedsat tilgængelighed, der kan tilskrives en fejlbetjening, som brugeren selv bærer ansvaret for, bør f.eks. ikke medtages i regnestykket.

- systemer under udvikling

I K01 har man søgt at løse de vanskeligheder, der er forbundet med at beskrive funktionaliteten i systemer under udvikling, ved at indføre et særligt regelsæt om afklaringsfase, se herved aftalens pkt. 3. Dette forløb igangsættes umiddelbart efter aftaleindgåelsen og har til formål at undersøge, om det er hensigtsmæssigt at præcisere eller supplere kravspecifikationen, samt om kundens

IT-miljø lever op til kravene i aftalens (for så vidt foreløbige) specifikationsangivelse i bilag 4. Afklaringsfasen gennemføres som et samarbejde, hvor leverandøren iværksætter de aktiviteter, der anses nødvendige for at leverandøren kan opnå en yderligere detaljeret indsigt i kundens forretningsgange, behov og IT-miljø. Samtidig bibringes kunden en detaljeret indsigt i programmellets funktioner og muligheder. På grundlag heraf skal hver part fremkomme med eventuelle forslag til præciseringer og suppleringer af kravspecifikationen.

Reglerne om afklaringsfasen beskrives nærmere som følger, jf. pkt. 3, stk. 3-6:

"Afklaringsfasen er et kort og intensivt forløb, hvor hver af parterne skal yde en betydelig indsats, herunder deltage i analyser, workshops og demonstrationer. Aktiviteterne i afklaringsfasen er nærmere beskrevet i bilag 1.

I det omfang parterne foreløbig opnår enighed om præciseringer og suppleringer, skal der udarbejdes udkast herom, og der skal i den forbindelse tages stilling til, i hvilket omfang disse præciseringer og suppleringer vil få konsekvens for tidsplan, vederlag til leverandøren og eventuelle andre vilkår.

Efter eventuelle nødvendige iterationer og korrektioner forelægges det samlede udkast til tilrettet kravspecifikation med beskrivelse af konsekvenser for kunden til godkendelse. Kunden skal herefter inden 10 arbejdsdage skriftligt meddele, om det modtagne kan godkendes.

Såfremt der ikke opnås enighed om at præcisere eller supplere kravspecifikationen, jf. definitionen heraf, gælder denne uændret."

Kan der ikke opnås enighed om disse ændringer, har kunden udtrædelsesadgang, jf. pkt. 4. I perioden efter afklaringsfasen kan begge parter dernæst afgive ændringsanmodninger, jf. K01 pkt. 5. Se i det hele om disse bestemmelser *Dragsted m.fl.* (2004), s. 47 ff. Opstår der uoverensstemmelser mellem parterne om konsekvenserne af en ændringsanmodning, har kunden ret til fornøden indsigt i grundlaget for leverandørens løsningsforslag. Ved prisberegningsmodeller og lignende erhvervshemmeligheder kan leverandøren forlange, at gennemgangen foretages af en uvildig tredjemand, som er underlagt tavshedspligt, se hertil pkt. 5.1.

Andre konciperingsspørgsmål

Foruden de nævnte – mere principielle – vanskeligheder ved at beskrive IT-ydelsen tilbagestår beskrivelsen af de yderligere pligter, leverandøren er underlagt. Aftaler om installation af hardware må præcisere, hvor der skal leveres, da leveringsstedet påvirker leverandørens omkostninger (forsendelse og installation). For softwareydelser er opfyldelsesstedet af mindre betydning, da mediet typisk kan sendes eller informationen transmitteres uden større omkostninger. Dernæst må det klargøres, hvilket miljø det leverede system eller den leverede systemkomponent skal funge-

re i. Reglerne herom vil have betydning for leverandørens muligheder for at få systemet til at fungere. Deres overtrædelse vil implicere fordringshavermora, jf. herom afsnit 22.7.e.

21.3.f. Særlige klausuler

Sideløberforbud

Undertiden opstår der tvivl om, hvorvidt et papir udgør en del af aftalen, f.eks. når ydelsen er anprist i leverandørernes salgsmateriale, men ikke ledsaget af garantier i selve kontrakten. Inspireret af amerikansk aftalepraksis indeholder mange IT-kontrakter såkaldte *sideløberforbud*, dvs. klausuler om, at den skrevne aftale skal udgøre det fuldstændige retsgrundlag mellem parterne, hvorfor tidligere tilkendegivelser, mundtlige som skriftlige, ikke kan påberåbes. Hvis det kan bevises, at parterne rent faktisk har indgået en senere aftale, har sådanne forbud ingen selvstændig retsvirkning. Er køberen forbruger, gælder købelovens § 76, stk. 1, nr. 2, hvorefter der uanset modstående aftale foreligger en mangel, hvis sælgeren eller tidligere salgsled har givet urigtige og vildledende oplysninger om varen i annoncer eller i andre meddelelser, der er beregnet til at komme til almenhedens eller køberens kundskab. I erhvervsmæssige transaktioner, hvor der er en større trang til at anerkende aftaler, der fordeler en risiko mellem parterne, må man ofte fortolke sideløberforbud som udtryk for, at parterne har vedtaget en *bevisretlig* formodningsregel, der lægger en særlig bevisbyrde på den part, der vil påberåbe sig forhold, der umiddelbart strider imod aftalens ordlyd.

Bedste kundeklausuler

Kundens forventninger om rabatter mv. fører ofte til krav om indføjelse af såkaldte "bedste kunde"-klausuler (*most favoured customer*), der sikrer kunden, at andre ikke får bedre rabatter og andre prisvilkår end han. Ifølge K33, pkt. 8.1, sidste stk., har kunden i en nærmere fastsat periode krav på prisnedsættelse svarende til den, leverandøren effektuerer på et eller flere af de produkter, som leverandøren skal levere. Efter den tilsvarende regel i K18, pkt. 8.2, stk. 2, består retten til prisnedsættelser kun indtil overtagelsesdagen. En sådan klausul kan blive bekostelig for den leverandør, der af konkurrencemæssige grunde senere tvinges til at nedsætte sine listepriser. Den bør derfor altid gøres tidsbegrænset, og hvis ikke en sådan begrænsning er udtrykkeligt anført, må den indfortolkes ud fra en vurdering af de konkrete omstændigheder, der omgiver transaktionen, sml. *JÅF 2000.114*, hvor en erhvervsdrivendes løfte om "fuld returret" måtte forstås som indeholdende en 9 måneders tidsbegrænsning. I ESF's totalkontrakt vedrørende levering, installation og vedligeholdelse af

et IT-system, pkt. 2.1.3 er klausulen begrænset til det tidspunkt, hvor leverandøren er rede til at gennemføre behørig afleveringsprøve.

21.4. Produktoverdragelser

21.4.a. Kendetegn

Som nævnt i afsnit 20.1.a. er det kendetegnende for produktoverdragelser, at ydelsen *findes* på aftaletidspunktet. Har produktet *materiel* karakter, kan det derfor præsteres under en leveringshandling af velkendt indhold. Består det af information ("bits"), er flere leveringsmuligheder åbne. Levering kan f.eks. ske ved overdragelse af et medium (f.eks. en CD-ROM), ved overførelse "bit for bit" via net, eller ved at erhververen udstyres med et password, som udløser en proces, hvorefter allerede leverede data konverteres til forståelig information.

Leasing mv.

Brugsrettigheder til genstande (f.eks. maskinel eller databærende medier), der kan overdrages og tilbagetages (modsat f.eks. telelinjer), adskiller sig som udgangspunkt kun fra købet i ejendomsretlig henseende: Opfyldelseshandlinger og kvalitetsforventninger vil være de samme.

Denne lighed var en af grundene til, at EDB-rådet i sin tid kunne udsende stort set ligelydende standardformularer om henholdsvis køb og leje af databehandlingsudstyr. Se i øvrigt om leasing af IT-systemer, *Poul Gade* i U1993B.330 ff. Om en transaktion er tilrettelagt som køb eller leasing har derimod i sagens natur betydning for retsgrundlaget (herunder navnlig spørgsmålet om købelovens anvendelighed) og i ejendomsretlig henseende.

21.4.b. Retsgrundlaget

Materielle produkter

Når man skal identificere retsgrundlaget for en produktoverdragelse, er det nødvendigt at sondre mellem de forskellige aspekter af produktet og anvende regler, der er relevante for det pågældende retlige problem. For så vidt angår rent *materielle* IT-produkter (f.eks. disketter, der sælges med fysiske fejl), gælder købeloven uden videre, for så vidt disse regler ikke (gyldigt) er fraveget ved parternes aftale. Selve den praktiske gennemførelse af transaktionen volder sjældent heller tvivl: Ydelsen er veldefineret, eftersom produktet jo findes på aftaletidspunktet og i en form, hvor det kan besigtiges, overgives og tilbagetages mv.

Immaterielle produkter

Er der derimod tale om *immaterielle* produkter, hvis overdragelse ikke understøttes af en kommerciel licens, gælder kbl. ikke direkte, jf. nærmere afsnit 20.2. For disse elementer af transaktionen må der drages passende analogier til det køberetlige regelsæt, idet lovens præceptive regler samt 1-årsfristen (§ 54) ikke finder anvendelse.

Som nævnt i afsnit 21.2.c. påvirkes kbl. ikke af, at der indgår licenselementer i transaktionen. Afgørende for denne vurdering må formentlig være, om en sådan aftale overfører væsentligt andre ophavsretlige retspositioner end dem, der går over i medfør af ophl. §§ 36-37. Giver aftalen mellem rettighedshaveren og brugeren f.eks. brugeren adgang til at kopiere og videresælge programeksemplarer, må aftalen for så vidt betragtes som en licensaftale. En "immaterialret" som sådan er ikke en "vare", sml. *U 1997.707 H* og min afhandling i U1995B.169 ff. om det tilsvarende problem i relation til handelsagentloven.

21.4.c. Aftalepraksis

Der er kun gjort ganske enkelte forsøg på at aftaleregulere komponentoverdragelsen gennem standardformularer.

IT-brancheforeningen

I 1994 udsendte *IT-brancheforeningen* to sæt standardvilkår, henholdsvis for køb af et mindre IT-system og for enkeltstående køb af IT-udstyr og IT-programmel. Der er tale om meget kortfattede aftaledokumenter. De består hver af 5 bestemmelser (henholdsvis om aftalens omfang, levering, afhjælpning/ophævelse, priser/betaling og ansvar) og 2 bilag, der beskriver de overdragne produkter. Begge fremtræder i en samlet brochure med kommentarer. Brochuren indeholder herudover forslag til klausuler om bl.a. ejendomsforbehold, betaling, forsikring, misligholdelse og transport af kontrakten. Den samlede tekstmængde for de to kontrakter, deres kommentarer, indledning samt forslag om vilkår udgør i alt 10 sider.

PLS-aftalen

Konsulentfirmaet PLS Consult har i maj 1999 offentliggjort en IT-kontrakt med tilhørende vejledning, henholdsvis for standardsystemer og tilhørende tjenesteydelser og leverancer, der indeholder specielt udviklet programmel. De to kontrakter er senere sammenskrevet til én samlet kontrakt, der er tilgængelig fra <www.pls.dk>. Kontrakten tilstræber at opdatere statens standardkontrakter for henholdsvis standardiserede edb-systemer (K18) og edb-totalleverancer (K33), således at disse bringes ajour med den teknologiske udvikling og heraf følgende aftalepraksis.

Leverandørvilkår

Bortset fra disse mere officielt prægede initiativer består den typiske aftale vedrørende produktoverdragelser af leverandørvilkår, som ikke forhandles. At man uden videre lægger leverings- og licensvilkår om *standardprogrammel* til grund hænger bl.a. sammen med, at *leverandøren* som regel ikke selv råder over ophavsretten. Han optræder som distributør for en (ofte udenlandsk) softwarevirksomhed, der vil have fastlagt faste – og på det nærmeste ufravigelige – vilkår. For de kontraherende parter er programleverancen derfor *tredjepartsprogrammel*, se hertil afsnit 7.4.h. En tilsvarende forhandlingssituation foreligger, når leverancen angår *hardware*. Principielt burde en slutbruger være varsom med at indgå sådanne aftaler, som ved ikke at knytte pligter til den part, der har kontrol over ydelsen, ikke har faktisk mulighed for at præstere *naturalopfyldelse*. I praksis søger brugerne at minimere denne risiko ved alene at indgå aftaler med markedsførende virksomheder, der af hensyn til deres omdømme må formodes at være inciteret til at holde deres produkter ved lige.

21.4.d. Installation

Problemet

Implementering af større IT-produkter (mainframe-enheder og visse større computere) kræver en vis aktiv medvirken fra brugerens side i forbindelse med den praktiske installation. Almindeligvis vil leverandøren af en mere kompleks maskinkomponent også påtage sig pligt til at foretage opsætning, tilslutning og afprøvning. Bygningsmæssige foranstaltninger, el-installationer og indretning af specielle klimaanlæg falder som udgangspunkt uden for ydelsen, jf. K18 og K33, pkt. 3, stk. 2, og ESF's totalkontrakt vedrørende levering, installation og vedligeholdelse af et IT-system, pkt. 1.8. Da disse foranstaltninger vil være en forudsætning for at kunne installere maskinkomponenten, forudsættes en medvirken fra brugerens side, jf. *Lærebog i Obligationsret I* (2005), s. 50 og 149 f.

Kabelføring

Et problem, der ofte giver anledning til vanskeligheder, er kabelføringen, der selv for relativt små installationer kan være uventet bekostelig. Disse omkostninger er som hovedregel leverandøren uvedkommende. De regler, der er udviklet i retspraksis om leverandørens vejledningspligt, kan næppe anvendes på dette område, allerede fordi ydelsen ikke hører under leverandørens område og ekspertise. Omkostningerne ved en kabelføring beror ikke alene på kablets karakter, men også på brugerens ønsker om den rent lokalemæssige ledningsførelse, der – hvis blot specifika-

tionerne er overholdt – ikke har funktionel indflydelse på systemet.

En forsinkelse med bygningsmæssige forhold, der afskærer leverandøren fra at installere systemet, vil indebære fordringshavermora, der efter almindelige regler som udgangspunkt ikke fritager leverandøren for pligten til at opfylde aftalen, men blot suspenderer den, jf. nærmere *Nørager-Nielsen* (1987), s. 282 ff. Der kan være store tab forbundet med sådanne problemer, der derfor bør aftalereguleres nøje. Konsekvensen af kundens fordringshavermora vil i mange tilfælde være, at leverandørens virksomhed må ligge stille i den periode, han havde afsat til installation af systemet, og at han omvendt ikke har kapacitet ledig, når køberen herefter melder sig klar på banen. Derfor er det ikke nødvendigvis rimeligt at foretage en ækvivalent udskydelse af opfyldelsesforløbet. Kommer man 1 minut for sent til sin bus, kommer man ikke nødvendigvis (kun) 1 minut senere frem! Ikke desto mindre synes der at være praksis for, at der sker en ækvivalent udskydelse af leverandørens opfyldelsesterminer, hvis køberen er i fordringshavermora. Dette er såvel fastslået i K33, pkt. 18, som i ESF's Totalkontrakt om levering, installation og vedligeholdelse af et IT-system, pkt. 4.5.1.

21.4.e. Tillægsydelser

For at bibeholde de funktioner, kunden efterspørger i det leverede system, er det ofte nødvendigt at kunne erhverve visse ydelser fra leverandøren, der efter deres karakter først kan præsteres efter afleveringstidspunktet.

Vedligeholdelse

For det første vil brugeren ofte have behov for at indgå i en vedligeholdelsesordning, jf. herom afsnit 4.4.b. Da aftaler om vedligeholdelse indebærer en løbende betalingspligt, der går udover købesummen, opstår der et afgrænsningsproblem mellem overdragelses- og vedligeholdelsesaftalen. Ved produktoverdragelser, der involverer aktiv implementering fra leverandørens side, aftales det ofte, at leverandørens forpligtelse til at sikre produktets funktionalitet på et bestemt tidspunkt overgår til en vedligeholder, eller at produktleverandøren selv påtager sig en selvstændig vedligeholdelsespligt. Praksis herom varierer fra produkt til produkt og beror bl.a. på, om det pågældende produkt er genstand for løbende opdatering.

I *JÅF 1989.65* har Forbrugerklagenævnet på grundlag af en udtalelse fra Det danske Handelskammer (gengivet sst. s. 66) lagt til grund, at der er kutyme i IT-branchen for, at der skal tegnes service-aftaler gældende fra leveringsdagen, idet reparationer sker som regningsarbejde. Udtalelsens rækkevidde kan diskuteres. Den dækker næppe det brede marked for produktoverdragelser i dag. Den model-licenskon-

trakt, som er udarbejdet af Dansk Dataforening, forudsætter, at vedligeholdelsesafgiften i en nærmere bestemt indeståelsesperiode reduceres med et beløb svarende til leverandørens indeståelsesforpligtelse. Et tilsvarende resultat forudsættes i K33, pkt. 8.7, sidste stykke.

ERA 3.9 (Odense byret 2.2.1984) antager, at en aftalt garantiperiode for et IT-system, der skulle starte ved "mangelfri levering", måtte forstås således, at den først startede ved udløbet af en 3 måneders kontrolperiode.

For standardprogrammel, der sælges på det almindelige marked, tegner man sjældent vedligeholdelsesaftaler. I det omfang sådanne programmer ikke er konstrueret til at kunne tilpasses skiftende driftsforhold, afgiftssatser mv., løses tilpasningsproblemet almindeligvis ved den praksis, hvorefter leverandørerne med passende mellemrum tilbyder *opdateringer* af leverede programprodukter.

Tilkøb

Dernæst kan det være nødvendigt at indgå aftale om, at kunden efterfølgende kan bestille reservedele, som brugeren selv kan have behov for at udskifte, eller forbrugsvarer (f.eks. printerpatroner), som forbruges i forbindelse med driften. Ved at foreskrive, under hvilke betingelser leverandøren har pligt til at levere sådanne ydelser, hvor længe, og til hvilken pris, undgår brugeren at komme i et senere afhængighedsforhold til leverandøren, som ellers kunne risikere at medføre andre priskrav ved efterbestillinger.

Ifølge *K18* pkt. 29, stk. 2, garanterer leverandøren, at bestillinger, der afgives inden for 3 år efter kontraktens underskrift, vil blive accepteret på samme vilkår med hensyn til rabatter som de, der gælder ifølge den indgåede aftale. Det forudsættes dog, at det pågældende udstyr eller programmel markedsføres af leverandøren på ordretidspunktet.

Optioner

I *K01* er spørgsmålet om efterfølgende bestillinger og tilkøb reguleret ved reglerne om option i pkt. 8. Frem til overtagelsesdagen kan kunden bestille de i bilag 13 angivne optioner til levering samtidig med og som en del af systemet. Kundens bestillinger skal ske indenfor de aftalte frister herfor. Effektueres en sådan option, bliver det af optionerne omfattede en del af systemet og skal i øvrigt i enhver henseende behandles, som om det oprindeligt var indgået i kontrakten, se nærmere pkt. 8.1. Efter overtagelsesdagen er leverandøren forpligtet til at levere de pågældende optioner gennem levering af yderligere ydelser, herunder udstyr, programmel og/eller dokumentation, i overensstemmelse med hvad parterne nærmere har aftalt i det til kontrakten hørende bilag 13 ("Beskrivelse af optioner med priser").

21.5. Systemudvikling

21.5.a. Kendetegn

En aftale om IT-systemudvikling kendetegnes ved at bringe noget nyt til verden. Ydelsen rummer et innovativt/kreativt element, og ved vurderingen af leverandørens opfyldelsesforpligtelse og realkreditors hæveret mv. er det nærliggende at slutte analogt fra de regler, der har udviklet sig om aftaler om frembringelse af litterære eller kunstneriske værker, eller forsknings- og udviklingsaftaler, se herved *ET*, s. 463 ff. Det innovative/kreative element i udviklingsydelsen træder frem i kraft af det spektrum af valgmuligheder, hvormed udvikleren kan præge ydelsen. Jo flere frihedsgrader, man har (og jo flere programinstruktioner, der indgår i det program, han skal udvikle), desto større er sandsynligheden for, at noget uforudset sker; enten på brugerens side (efterfølgende ønsker om nye funktioner mv.) eller hos leverandøren (uforudsete vanskeligheder under implementeringen af forskellige løsninger): Udvikles en applikation under et styresystem, må man følge dets tekniske specifikationer mv., der ofte først bliver frigivet på et senere tidspunkt. Mister leverandøren den medarbejder, der skulle stå for kodningen, vil der ofte påløbe ekstraordinære omkostninger til indlæring af nye medarbejdere.

Risikoen for, at sådanne problemer opstår, bør reguleres klart i aftalen. I IT-aftaleretten støder man på to forskellige måder at afdække denne risiko på – hver med rod i sin juridiske disciplin:

Fasemodellen

Den ene støttes af leverandørinteresserne. I Danmark kommer den f.eks. til udtryk i de standardkontrakter, der er udsendt af ESF (nu IT-brancheforeningen), se f.eks. ESF's standardkontrakt vedrørende system- og programudvikling, § 5, og mere detaljeret ESF's Totalkontrakt vedrørende levering, installation og vedligeholdelse af et IT-system, pkt. 3.1.1. Opfattelsen har rod i den klassiske entrepriseret og forudsætter, at risikoen for uventede problemer mv. skal løses ved genforhandling. Under hele anskaffelsesforløbet gennemløbes et antal delforløb (faser), der i økonomisk og kontraktsretlig henseende er afsluttede. Efter afslutningen af hver fase kan kontrakten derfor genforhandles. Det samlede leveringsforløb er først tilendebragt, når de enkelte faser er det. Begge parter kan træde ud af projektet efter hver fase, f.eks. hvis projektet viser sig at koste mere eller bliver mere besværligt end forventet, eller hvis den ene part mister tilliden til den anden. I praksis fører dette til, at der må indledes nye forhandlinger, hvis de kommercielle forudsætninger for den oprin-

delige aftale brister. Dette betyder omvendt, at kunden først ved, hvad systemanskaffelsen koster ham, når systemet er leveret.

Totalleverance-modellen

Den anden løsningsmetode (der omvendt støttes af brugerinteresser) forudsætter, at omfanget af leverandørens ydelse ligger fast på aftaletidspunktet. Det er brugerens kravsspecifikation (i K18: Behovsopgørelsen), der fastslår leverandørens ydelse. Han skal levere alt det udstyr, programmel, rådgivning mv., der er nødvendigt for, at brugeren kan opnå den funktion, der er angivet heri. Viser det sig, at dette indebærer, at der må leveres mere end oprindeligt forudsat, påhviler de heraf følgende ekstraomkostninger leverandøren. Såvel i K18 som i K33 (se pkt. 2.1 i begge aftaler) hedder det således, at leverandøren skal "tilvejebringe og levere alt det maskinel og programmel, som er nødvendigt til etablering af et fuldstændigt IT-system, der er i stand til at opfylde alle de krav, der beskrives i kundens kravsspecifikation". K18, pkt. 2.1, sidste pkt., præciserer endvidere, at leverandørens egen systembeskrivelse (jf. herom nedenfor) ikke begrænser hans pligt til at opfylde behovsopgørelsen.

K01-modellen

Med vedtagelsen af K01 er der skabt en mellemløsning mellem de forannævnte to modpoler. Denne nye kontrakt, der har karakter af et *agreed document*, indeholder en række mekanismer, der på den ene side tilgodeser myndighedernes behov for at kunne føre budgetkontrol med IT-projekterne, samtidig med at den minimerer leverandørernes risici ved at give disse mulighed for at træde ud, hvis opfyldelsen undervejs i forløbet viser sig uventet kompliceret og omkostningskrævende. Dette er først og fremmest sket gennem de regler om *afklaringsfase*, der er omtalt s. 914 f. Dernæst er reglerne om den tekniske beskrivelse, der danner grundlaget for leverandørens opfyldelse, formuleret mindre skarpt end i K18 og K33. Ifølge pkt. 2.1. skal leverandøren "levere det udstyr og programmel samt den dokumentation, der er specificeret i bilag 4", idet systemet og dets enkelte dele skal besidde de egenskaber og opfylde de krav, "der fremgår af nærværende kontrakt, navnlig af bilag 2".

Der er ikke noget juridisk svar på, hvilken af disse løsninger der er den "rigtige". Valget bør bero på, hvor mange risici for ikke at kunne opfylde korrekt leverandøren er udsat for. I en relativt overskuelig og ukompliceret leverance er risikoen herfor minimal og behovet for en faseopdeling derfor mindre. Den nærmest religiøse debat om de to modeller er i højere grad økonomisk end politisk. Den leverandør, der påtager sig den risiko, han kan ifalde efter Statens standardkontrakter (K18 og K33), vil i sagens natur søge at dække sig ind ved at tage højere betaling.

21.5.b. Retsgrundlag

Udvikling

Om udviklingsydelser omfattes af købeloven, beror på lovens § 2, stk. 1. Ifølge denne bestemmelse anses bestilling af *genstande*, som først skal fremstilles, for køb. Uden for forbrugerkøb gælder dette dog kun, såfremt den overvejende del af de for fremstillingen nødvendige *materialer* skal ydes af den, der har påtaget sig fremstillingen. Brugen af ordene "genstande" og "materialer" mere end antyder, at en *immateriel* ydelse som specialfremstillet eller -tilpasset software ikke er omfattet. Problemet diskuteres – på grundlag af lovens tidligere, men i så henseende nogenlunde ensartede – formulering af *Christophersen & Føyen* (1981), s. 75, af *Nørager-Nielsen & Theilgaard* i Købelovskommentaren (1993), s. 49, med henvisninger til SOU 1976:76, s. 205, og NOU 1976:34, s. 34, og generelt (omend med henblik på den klassiske entreprise) af *Hørlyck* i Tilvirkningskøbet (1996).

Bestillingskøb?

Som tidligere nævnt er købeloven kun direkte anvendelig på udviklingstransaktioner, hvorefter systemet skal opbygges ved hjælp af materielle komponenter. Dette kan f.eks. tænkes, hvis leverandøren på grundlag af brugerens ønsker sammensætter et system bestående af standard-komponenter, hvad enten der er tale om standardiseret *software* (såkaldt "tredjepartsprogrammel") eller standard *hardware*komponenter (f.eks. processorer, lagerenheder, perifere enheder eller andet). Det færdige system "tilvirkes" ved den tekniske sammensætning og tilretning af disse komponenter. Her vil leverandøren *yde det stof* (dvs. de komponenter), der indgår i den færdige ydelse, hvorved transaktionen må karakteriseres som bestillingskøb. Stiller kunden derimod selv disse komponenter til rådighed, vil leverandøren alene *sammensætte* disse. Denne bistandsydelse vil allerede af denne grund ikke være omfattet af købeloven.

Tjenesteydelse?

Selv om man retter blikket mod "specialprogrammel", hører det i dag til sjældenhederne, at programmel udvikles fra grunden. En programmør, der får til opgave at "udvikle" et edb-system, der skal løse en opgave, som intet standardsystem kan klare, vil i praksis altid betjene sig af en række avancerede værktøjer til programudvikling. Ved hjælp af sådanne værktøjer kan han for det første opbygge det "individuelt udviklede" edb-program på grundlag af præ-eksisterende moduler. For det andet kan han i vid udstrækning overlade en del af programmeringen til særlige programgenereringsfunktioner i det pågældende programmel (såkaldt CASE-programmering – Computer Assisted Software Engineering). Derfor spiller den isolerede "tjenesteydelse" en anden

rolle i udviklingstransaktionen end tidligere. De specialudviklede programmer er så at sige blevet mere standardiserede, og de standardiserede programmer rejser som følge af deres kompleksitet et stadigt større behov for, at aflevering, igangsætning og drift understøttes ved bistand fra leverandøren – en bistand, der ofte præsteres i skikkelse af selvstændige aftaler om konsulent- og uddannelsesbistand samt om vedligeholdelse.

Standardrammesystemer

Talrige programløsninger fremstår overfor kunden som specialudviklede til trods for, at der er tale om tilpasninger til bestående standardsystemer. Disse såkaldte *standardrammesystemer* indebærer på den ene side en standardisering af den specielle programudvikling, men på den anden side også et behov for, at standardsystemet afleveres og igangsættes under bistand fra leverandøren eller ved selvstændige aftaler fra tredjeparter om konsulent- og uddannelsesbistand og vedligeholdelse mv. Ved vurderingen af, om en sådan transaktion udgør et køb eller en tjenesteydelse, må indholdet af leverandørens præstation være afgørende, jf. herom straks nedenfor. Det forhold, at en systemkomponent, f.eks. en pc, konfigureres efter køberens specifikationer, forvandler ikke købet til et bestillingskøb, jf. *JÅF 1998.114*, hvor dette spørgsmål blev afgjort i relation til forbrugeraftalelovens § 10, stk. 3, nr. 1.

Kriterier

Blandt de kriterier, der må være afgørende for, om der foreligger en tjenesteydelse, kan man sammenfattende pege på, om programmet *eksisterer* på tidspunktet for aftaleindgåelsen, og om dets udvikling er forbundet med et vist *risikomoment*, som parterne dermed må tage højde for i deres aftale, se herved betænkning 738/1975, s. 78. Derimod kan det ikke være afgørende, hvilken *betegnelse* leverandøren vælger at markedsføre et programprodukt under, jf. mine bemærkninger i U1995B.172 f. om handelsagentloven. Hvis leverandøren inden aftaleindgåelsen præsterer en *konsulentydelse* i forberedelse af leverancen og f.eks. analyserer kundens databehandlingsbehov, må dette arbejde isoleret set betragtes som en tjenesteydelse af konsulentkarakter, ligesom andre rådgivningsydelser, der præsteres på grundlag af timebetaling. Det samme gælder den *specialudvikling*, der sker i medfør af en særskilt udviklingsaftale, samt den efterfølgende vedligeholdelse i form af løbende efterfølgende teknisk fejlretning, -foregribelse og optimering. I det omfang sådanne elementer indgår i transaktionen, får den karakter af tjenesteydelse eller værksleje. I tvivlstilfælde må man skele til hvilken økonomisk værdi de enkelte elementer af transaktionen har, jf. nærmere hertil min førnævnte afhandling, s. 173 f.

21.5.c. Aftaleindgåelsen

Behovsopgørelse

Aftaler om udvikling af IT vil typisk blive sluttet på grundlag af et forhandlingsforløb, i hvilket parterne har udvekslet information om, hvilke behov systemet forventes at løse, henholdsvis mulighederne for at tilfredsstille disse behov til forskellige priser. Det første dokument af denne art vil typisk være kundens kravsspecifikation (på engelsk ofte kaldet *request for proposal*, eller RFP – i K18 kaldet *behovsopgørelsen*), som fremsendes til leverandøren – eventuelt i forbindelse med en offentlig udbudsforretning – med en opfordring til denne om at fremsætte tilbud om løsningen. Ved offentlige udbud skal behovsopgørelsen være ledsaget af et udkast til aftalegrundlag, eftersom den lighedsforpligtelse, der foreskrives ved EU-udbudsreglerne, forhindrer vedtagelse af efterfølgende individuelle aftaler.

Beskrivelsesprincip

Kravsspecifikationer kan udformes efter forskellige principper. Hvis den specificerer nogle egenskaber ved den løsning, der ønskes, taler man om, at ydelsen er beskrevet efter *funktion*, se hertil *PA*, s. 282 ff. Dette sker ved angivelse af tekniske egenskaber som f.eks. hastighed, kompatibilitet og udbygningsmuligheder. For at kunne gøre dette kræves en betydelig teknisk indsigt, og kunden vil derfor ofte lade sig bistå af en konsulent i dette arbejde. En anden metode består i at beskrive produktet efter *betegnelse*, f.eks. "en processor mrk. XYZ". Herved tager køberen risikoen for, at det leverede overhovedet kan opfylde hans behov. Også her kan konsulentassistance derfor være nødvendig. I offentlige udbudsforretninger kan sådanne beskrivelser ikke anvendes, eftersom de på forhånd afgrænser kredsen af mulige budgivere.

Når køberen selv – uden særlig ekspertise – formulerer en kravsspecifikation, vil denne ofte blot specificere en række mere generelt definerede funktionelle krav til det leverede. Aftalen er i så fald først rigtigt opfyldt, når systemet kan præstere disse krav. Til gengæld vil den samlede anskaffelsessum for et sådant nøglefærdigt system ofte være langt højere end for det modulært opbyggede system, som sammensættes efter konsulentens anvisninger.

Systembeskrivelse

Ønsker leverandøren at afgive tilbud, vil han herefter fremsende et sådant i forbindelse med sit forslag til en beskrivelse af det tilbudte system og dets enkelte komponenter med respektive funktioner. Denne *beskrivelse* optræder i K18 som bilag 4 og omtales forudsætningsvis i pkt. 2.1. I K33 er der givet særlige regler for den såkaldte *systembeskrivelse* i pkt. 2.2. Systembe-

skrivelsen er her en del af leverandørens ydelse; en mellemting mellem en præcision af det oprindelige tilbud og en kvalitetssikring af selve leverancen. Formålet med den er at give kunden indblik i, hvordan leverancen vil blive opfyldt og – hvis beskrivelsen giver anledning til alvorlig bekymring – frigøre sig fra aftalen efter de særlige regler herom. Ved afvigelser mellem kravsspecifikationen og systembeskrivelsen vil kravsspecifikationen efter K33 være gældende, medmindre andet er aftalt. Uden sådan særlig aftale vil man formentlig anse kravsspecifikationen for erstattet af systembeskrivelsen. Dette er i øvrigt reglen i medfør af pkt. 1.0.9 i ESF's totalkontrakt vedrørende levering, installation og vedligeholdelse af et IT-system.

Samarbejdsorganisation

Uanset hvor megen energi, parterne lægger i arbejdet med at koncipere deres aftaleforhold, er det umuligt at tage højde for ethvert forhold, der kan opstå under udviklingsarbejdet. Under en kompliceret udviklingsproces vil der uvilkårligt dukke problemer op, som ikke kunne forudses. Bl.a. for at fange disse problemer, men også for at sikre en effektiv løbende kommunikation mellem parterne, etableres ofte en samarbejdsorganisation mellem leverandør og bruger i perioden fra aftalens indgåelse og frem til afleveringsprøven. Både K33 (pkt. 20) og ESF's standardkontrakter (henholdsvis pkt. 2.4.1 og § 3) opererer med styregrupper, som foruden at skulle sikre den fornødne koordination mellem parterne samt at tilvejebringe det testmateriale, der skal indgå i afleveringsprøven, fungerer som forum for genforhandling og præcisering af kontrakten. Styregruppen vil almindeligvis bestå af mindst to repræsentanter fra hver af parterne – et bemyndiget medlem, der har kompetence til at foretage de nævnte kontraktsmodifikationer, og et teknisk medlem (evt. en konsulent), der har overblik over de teknisk-funktionelle konsekvenser heraf.

21.5.d. Opfyldelseshindringer og ændrede forhold

Ændringsret

Som nævnt gennemføres enhver systemudvikling med risiko for, at der indtræder uventede opfyldelseshindringer eller andre ændrede forhold, som gør udviklingsprocessen mere vanskelig end oprindeligt antaget. Sådanne forhold kan enten komme *udefra* (f.eks. ved underleverandørers forsinkelse eller misligholdelse), de kan udspringe af en for ringe *indsigt* i opgavens omfang og kompleksitet, eller de kan skyldes, at kunden undervejs *skifter mening* mht. sine ønsker til systemet. Spørgsmålet om, hvem der bør bære risikoen for de ekstraomkostninger, der kan tænkes at følge heraf – eller for, at kunden i konsekvens heraf vælger at

bringe udviklingsprojektet til ophør uafsluttet – beror, i mangel af særlig aftale, på karakteren af den pågældende opfyldelseshindring mv.

Aftaletilfælde

Da ingen af parterne har interesse i, at aftalegrundlaget på forhånd låses fast, giver de fleste IT-aftaler parterne mulighed for inden for de givne pris- og funktionsmæssige rammer at foretage ændringer i den ydelse, der skal præsteres. En sådan ordning er indført i K18 pkt. 2.3 (i relation til senere markedsført udstyr) og pkt. 2.4 (om mindre konfigurationsændringer i øvrigt) og tilsvarende K33 pkt. 2.6. *Torvund* (1997), s. 123 ff., argumenterer – under inddragelse af erfaringsmateriale fra andre, teknisk prægede kontraktstyper – for, at begge parter vil have en gennemsnitlig interesse i en sådan ændringsret. En tilsvarende ændringsret kendes fra entrepriseområdet, se AB92 § 14, jf. i det hele *Christian Johansen*: Bygherrens ændringsret (1999). Udgangspunktet er dog, at en sådan ret kræver særskilt aftale.

Prisændringer

Ved længerevarende opfyldelsesforløb, der involverer underleverancer fra tredjeparter, kan leverandøren have en velbegrundet interesse i at lade købesummens størrelse bero på, hvilke priser (evt. hvilken kurs) der i sidste ende skal betales til den eller de pågældende underleverandører. K18 bygger også på dette punkt på et princip om fast pris, jf. udtrykkeligt pkt. 8.1; men det er ikke ualmindeligt, at leverandøren gennem særlige klausuler flytter risikoen for prisændringer hos underleverandører af standardudstyr over på køberen.

Deadlock

Det kan i ekstreme tilfælde forekomme, at parterne undervejs i et udviklingsprojekt vælger at afslutte projektet, inden dette har fået en skikkelse, der kan være til nytte for brugeren. Den almindelige regel er her, at leverandørens arbejde bør honoreres, når der er ydet en god og forsvarlig indsats, se herved *Stig Jørgensen & Torben Wanscher* i J1967.425, betænkning 1133/1988, s. 53, og *Bryde Andersen & Lookofsky* (2005), s. 42 f.

Således pålagde *U 1964.125 H* bestilleren at betale udviklingsomkostningerne til frembringelse af et værktøj, selv om dette viste sig uegnet til formålet. Retten betoner, at sælger ikke havde påtaget sig nogen garanti herfor. *U 1895.803 GKS* drejede sig om en aftale vedrørende udvikling af et udskænkningsapparat med særlige egenskaber. Under hensyn til, at bestilleren tilså udviklingsarbejdet "og lod gjøre Forandringer ved samme", fandtes han at skulle betale herfor, selv om resultatet ikke blev som ventet. Retten bemærker, at det drejede sig om "en Opgave, hvis heldige Løsning ikke kunde anses forud sikker".

21.5.e. Aflevering og risikoovergang

Begreb

Levering af IT-systemer er på mange måder anderledes end levering af andet kontorudstyr mv., fordi systemet ikke leveres, men "afleveres". Hvor en levering indeholder de handlinger, der giver køberen ydelsen i hånden (forsendelse og evt. opstilling), indeholder en aflevering tillige en foranstaltning, der skal godtgøre, at det leverede fungerer som lovet, jf. nærmere *ET*, s. 274 ff. Aflevering benyttes navnlig vedrørende ydelser, om hvis aftalemæssighed der kan være begrundet tvivl. Jo større denne risiko er, desto mere intenst bør parterne aftaleregulere afleveringsprøven. Man behøver sjældent foranstalte aflevering af en standardprogrampakke eller en skærm, medmindre dette skal indgå i samspil med noget andet med risiko for uforudsete komplikationer.

Risikoovergang

Da afleveringen er det tidspunkt, hvor leverandøren slipper sit tag i ydelsen, og hvor brugeren tilsvarende tager fat, er tidspunktet for denne handling et hensigtsmæssigt skæringspunkt for risikoens overgang, jf. *Nørager-Nielsen* (1987), s. 97 og *Christophersen & Føyen* (1981), s. 272 ff. I visse tilfælde når parterne ikke at foranstalte aflevering. I så fald må man ud fra en vurdering af sagens konkrete omstændigheder tage stilling til, hvornår ydelsen i hovedsagen er overgivet.

F.eks. blev det i *U 1985.411 H* ikke tillagt vægt ved afgørelsen af, om der var sket "overgivelse" efter reglerne i den dagældende afbetalingslov, at nogle programmer til en større IT-installation først skulle leveres efterfølgende. Systemet var rent faktisk sat i drift forinden. Det danske Handelskammer har den 23. maj 1998 udtalt, at det ikke mener at kunne konstatere nogen sædvane eller kutyme for, at sælger foretager "prøvekørsler" og indhenter "leverancegodkendelse" fra køber, før levering anses for fyldestgjort og købers pligt til betaling dermed udløses, se Advokaten 2/1999, s. 35. Der er principielt intet til hinder for, at den faktiske ibrugtagning af systemet betragtes som aflevering, jf. *U 1975.733 H* hvor dette – gyldigt – var bestemt i aftalegrundlaget for en entreprise.

Andre retsvirkninger

Typisk markerer den gennemførte afleveringsprøve det tidspunkt, hvor køberen får glæde af ydelsen. Dette tidspunkt anvendes derfor som begyndelsestidspunkt for beregning af *frister* for reklamationer og garantier. Når ydelsen afprøves, har parterne deres fulde opmærksomhed rettet mod dets kvaliteter og svagheder. Det giver en naturlig tilskyndelse til at gøre opmærksom på, at det leverede er – eller ikke er – som aftalt, sml. princippet i kbl. § 51. Godkendelsen af en afleveringsprøve afskærer dog ikke kunden fra at gøre krav gældende for forhold, som ikke blev

afsløret som mangler, medmindre denne kunne og burde have været opmærksom på dem.

De argumenter, *Christophersen & Føyen* (1981), s. 236, anfører til støtte for det modsatte resultat (bevisproblemer henholdsvis manglende interesse i en efterfølgende ophævelse), synes ikke afgørende. Om en fejl *kunne* være opdaget, kan efterfølgende klargøres, hvis parterne – hvad man må tilråde – opbevarer det anvendte testmateriale eller fører logbog. Om den *burde* være det, jf. princippet i kbl. § 47 (undladt efterkommelse af sælgers opfordring) og § 51 (den undersøgelse, som "ordentlig forretningsbrug" kræver), beror på konkrete forhold.

Besidder brugeren ikke nogen særlig IT-ekspertise, og har han ikke søgt at skaffe sig en sådan, f.eks. ved konsulentbistand, vil hans påpasselighedspligt almindeligvis være begrænset, sml. afgørelsen i *U 1960.41 H*, hvor en huskøber, der ved købet havde været ledsaget af en arkitekt, ikke kunne påberåbe sig mangler ved det solgte. For at afskære tvivl desangående aftales det ofte, at kundens godkendelse af afleveringsprøven eller andre hændelser i forbindelse med aftalens opfyldelse ikke indebærer noget afkald på hans rettigheder, se f.eks. K33 pkt. 9.1, sidste pkt. og K18 pkt. 11, stk. 1, sidste pkt.

Undladt prøve

Som allerede antydet hænder det ikke sjældent, at selv kostbare og mere komplicerede IT-systemer overdrages og igangsættes uden afleveringsprøve. I sådanne tilfælde må det tidspunkt, hvor kunden udstyres med komponenter og medier, lægges til grund som udgangspunkt for *risikoens overgang*. I systemleverancer må det derimod være afgørende, om kunden rent faktisk har taget systemet i brug, sml. *TBB 2000.450 VBA*, hvor komponenter til et byggeri var leveret, men ikke taget i brug af bygherren. Der foreligger ingen praksis om spørgsmålet i relation til IT-kontrakter. Pkt. 3.1.8 i ESF's totalkontrakt vedrørende levering, installation og vedligeholdelse af et IT-system fastslår, at kunden anses for at have godkendt en leverance, som tages i brug, selv om behørig afleveringsprøve ikke er gennemført. Dette gælder dog ikke, hvis årsagen til den manglende aflevering er, at leverandøren har overskredet tidsfristen for den pågældende leverance, og kunden skriftligt har tilkendegivet sit behov for ibrugtagning. I så fald anses ydelsen ikke for afleveret og risikoen derfor heller ikke for overgået. Det er nærliggende at læse bestemmelsen som udtryk for en deklaratorisk regel.

Disse betragtninger er ikke nødvendigvis afgørende for, hvordan fristen for *mangelsreklamation* skal beregnes. Tager man den tid, der almindeligvis vil medgå ved en formel aflevering, i betragtning,

vil det være nærliggende at udfinde et tænkt tidspunkt, inden for hvilket aflevering sædvanligvis måtte forventes tilendebragt, og lægge dette til grund.

Nægtet godkendelse

Hvis kunden nægter at godkende afleveringsprøven, men leverandøren fastholder, at grundlaget for en sådan godkendelse er tilstede, må det bero på en efterfølgende bevisvurdering, om nægtelsen var berettiget. Kunden tager hermed en *standpunktsrisiko*, jf. herom *Bryde Andersen & Lookofsky* (2005), s. 184 ff. Er dette ikke tilfældet, må systemet anses for leveret på det tidspunkt, hvor kunden burde have afgivet sin godkendelse, jf. *TBB 2000.518 VBA*, hvor det dog skyldtes indsigelser vedrørende den formelle udfærdigelse af afleveringsprotokollen i en entreprise, at bygherren ikke ville underskrive.

Prøvens gennemførelse

En afleveringsprøve kan ikke gennemføres uden klare rammer af formel karakter (hvad skal parterne gøre, hvordan og hvornår?) og af materiel karakter (hvilken funktion skal systemet præstere?). Jo mere præcist disse rammer er defineret, desto lettere er det at tage stilling til, om der er sket rigtig opfyldelse af kontrakten. Der findes forskellige metoder til at godtgøre funktionerne i et IT-system.

Benchmark-tests

Ved en såkaldt *benchmark-test* udsættes systemet for en kendt belastning, som dets ydeevne ("performance") herefter sættes i forhold til. Vanskeligheden ved at gennemføre benchmark-tests består i at definere grundlaget for den pågældende ydeevne. Objektive sammenligninger er ofte umulige at udføre i et levende system.

Testprocedure

En mere hyppigt anvendt afleveringsform anvender testprocedurer, der så at sige eksaminerer systemet. De prøver, der anvendes, formuleres mere præcist af den koordinations- eller styregruppe, der skal stå for den løbende kontrol med og tilrettelæggelse af projektet, jf. K33, pkt. 22, og § 3 i ESF's standardkontrakt vedrørende system- og programmeludvikling. Udarbejdelsen af sådanne tests er ikke uproblematisk. Leverandøren af et dårligt edb-program vil kunne gennemløbe en succesfuld "test", blot han selv er herre over, hvilke funktioner der kaldes, og hvilke data systemet udsættes for. Omvendt kan enhver bruger formentlig fremvise funktioner eller funktionssituationer, der belaster selv det bedste program så hårdt, at det ikke lever fuldt op til forventningerne. I K33 etableres der tre prøver: en installationsprøve, en overtagelsesprøve og en driftsprøve, jf. nærmere pkt. 10. K18 og K01 opererer kun med to prøver: en overtagelsesprøve og en driftsprøve, jf. nærmere pkt. 10, henholdsvis pkt. 12.

Installationsprøve

Formålet med installationsprøven er at sikre, at maskinel og systemprogrammel er parat til påbegyndelse af overtagelsesprøve. Her afklarer man alle de tekniske detaljer, der sædvanligvis træder frem som små-problemer, når systemets komponenter skal forbindes i det samlede system. Meningen med installationsprøven er at udskille disse – typisk overkommelige – problemer, inden man går i gang med at teste systemet på det udvalgte datamateriale.

Overtagelsesprøve

Den anden prøve, overtagelsesprøven, er i K18 og K33 tilrettelagt som en funktionsprøve, hvor maskin- og programprodukter kontrolleres enkeltvis og integreret og sammenholdes med kravsspecifikationen, systembeskrivelsen og dokumentationen. Det er ved denne prøve, at testmaterialet får betydning. Når testresultaterne viser sig, sondrer man som regel mellem grove og mindre grove fejl. Det er sædvanligt foreløbigt at se bort fra funktionsfejl, som ikke hindrer en meningsfuld udnyttelse af systemet til de tiltænkte funktioner, således at systemet anses som leveret til trods for sådanne fejl. Som eksempler herpå anføres mindre overskridelser af svartider, fejl på enkelte udskrivningsenheder eller fejl, som efter leverandørens anvisning kan omgås på en simpel måde. Forudsætningen for at anse systemet som afleveret i sådanne tilfælde må dog være, at leverandøren retter den slags fejl uden vederlag inden for en kortere periode, f.eks. 2 eller 4 uger. Efter et sådant tidsrum vil leverandøren efter omstændighederne komme i misligholdelse, men ikke nødvendigvis i væsentlig misligholdelse. Afsluttes afleveringen med et godt resultat, forfalder sidste rate af betalingen. Når køberen har konstateret, at det leverede svarer til det aftalte, har han ingen gyldig grund til at holde sin betaling tilbage. Dette vil sædvanligvis også gælde i de tilfælde, hvor der er aftalt en driftsprøve, jf. herved reglen herom i K33, pkt. 9, stk. 2.

Driftsprøve

Formålet med driftsprøven er at konstatere, hvorvidt leverancen overholder de opstillede servicemål, jf. K01 pkt. 12.2. Driftsprøven afvikles, mens det leverede system anvendes i brugerens virksomhed i en nærmere fastlagt periode. I K33 er denne periode på 60 dage. I K01 er de nærmere regler om prøvens procedure, indhold og godkendelseskriterier samt afslutningsfrist henskudt til afgørelse i bilag (bilag 8). I løbet af den periode, prøven varer, kan brugeren konstatere, om systemet rummer fejl, der i praksis kun kan opdages under sædvanlig anvendelse af systemet. For at sikre sig beviset for forløbet af afleveringsprøven må der føres nøje rapport om dens udfald. Når der aftales driftsprøve, bør brugeren føre logbog under hele driftsprøvens forløb.

I ESF's standardkontrakt vedrørende system- og programudvikling foretages der kun én egentlig prøve. Kontrakten sondrer mellem programmelafprøvning (§ 7) og aflevering (§ 8). Programmelafprøvningen er den prøve, der afvikles på grundlag af et repræsentativt datamateriale, som kunden har ansvaret for at fremskaffe. Kan kunden på dette grundlag godkende programmet, iværksættes den egentlige aflevering, hvor de fornødne godkendelser mv. udveksles. Afleveringen er altså her afslutningen på programmelafprøvningen. Vil kunden ikke godkende programmet, må han fremlægge en mangelsliste, som – hvis den er berettiget – vil indebære, at systemet ikke er færdigudviklet. ESF's totalkontrakt vedrørende levering, installation og vedligeholdelse af et IT-system giver i pkt. 3.1. regler om "Afleveringsprøve". Kontrakten forudsætter som nævnt, at leverancen er opdelt i delleverancer, og at hver delleverance afsluttes med en afleveringsprøve, som dokumenterer, at de funktioner, der er beskrevet i systembeskrivelsen – enkeltvis og i sammenhæng – kan udføres, og at den afleverede delleverance kan fungere sammen med tidligere godkendte delleverancer, pkt. 3.1.1.

Standardprogrammel

Ved levering af standardprogrammel ved hjælp af fast medium (f.eks. ved overdragelse af disketter eller CD-ROM, hvorpå programmet er indlagt) kan kunden risikere, at programmediet går tabt eller ødelægges, inden programmet er installeret og sikkerhedskopiering er udført, jf. ophl. § 36, stk. 1, nr. 2. Det spørgsmål opstår da, om ydelsesrisikoen i en sådan situation er gået over på kunden, eller om leverandøren kan blive pålagt pligt til at efterlevere et program-eksemplar, evt. mod betaling af de direkte produktionsomkostninger. Er særlig aftale ikke indgået herom, er udgangspunktet for besvarelsen af dette spørgsmål klart: Når levering er sket, jf. de almindelige regler herom, er risikoen som udgangspunkt gået over til køberen, jf. princippet i kbl. § 17, og denne bærer da også risikoen for, at grundlaget for at udøve en ophavsretlig licens bortfalder. Det forhold, at værdien af den pågældende transaktion knytter sig til det immaterielle indhold af programmediet, gør i princippet ingen forandring heri. Situationen er principiel den samme ved køb af musik-cd'er, hvor materialeomkostningen (udgiften til frembringelse af cd'en og dens indpakning) ofte udgør under 10% af salgsværdien. Selv om man, som anført af *Torvund* (1997), s. 109, kan argumentere for det rimelige i en sådan situation at lade køberen erhverve en ny licens mod betaling af produktionsomkostningerne hertil, er der ikke belæg for at nå til et sådant resultat gennem retssystemets almindelige regler. Forholdet bør derfor give anledning til aftaleregulering.

21.6. Facility management, outsourcing og ASP

21.6.a. Kendetegn

Gennem de seneste 40 års IT-udvikling har der været forskellige traditioner for, hvordan og under hvilke rammer en IT-drift afvikles. I de første år, hvor systemerne var store, kostbare og vanskelige at håndtere, var der et betydeligt marked for såkaldte *servicebureauydelser*, hvor kunden erhvervede en bestemt type funktionalitet, som samme leverandør herefter præsterede til en flerhed af brugere (f.eks. bogholderi og lønregnskab), hvis brugeren da ikke havde økonomisk mulighed for at erhverve det kostbare maskinel selv. Med fremkomsten af 1980'ernes IT-løsninger, der også kunne erhverves af små og mellemstore virksomheder, blev det almindeligt for mange brugere at overtage den samlede funktionalitet i egne rammer. Man købte de nødvendige systemer og stod herefter selv for driften.

Men gennem de seneste år har man set en stigende tendens til påny at lade leverandøren afvikle brugerens databehandlingsbehov, f.eks. i form af såkaldt facility management eller ASP, jf. om disse begreber straks nedenfor. Baggrunden herfor ligger i flere forhold: Den øgede konkurrence inden for talrige samfundssektorer har skabt et pres på brugerne for at koncentrere sig om "*core business*" og populært sagt "blive bedre til det, man er god til". Denne udvikling er sket i takt med, at systemerne er blevet stadigt vanskeligere at drive (hyppige opdateringer og stadigt flere problemer med at integrere forskellige løsninger med hinanden). Dernæst har den stadigt lavere pris på telekommunikationstjenester (som følge af den teknologiske udvikling og liberaliseringen af denne sektor) gjort det enkelt at afvikle IT-løsninger i én virksomhed fra et IT-system, der befinder sig i en anden virksomhed. Med den udvikling, der er fulgt med de seneste års globalisering, har denne form for outsourcing navnlig vist sig rationel i relation til IT-funktioner, som med stor effektivitet og mod – i vestlig sammenhæng – beskeden betaling kan udføres i en række af de nye økonomier i den tredje verden, herunder Indien. Den stigende trang til specialisering har også gjort det almindeligt at outsource andre typer af virksomhedsopgaver, f.eks. rengøring, kantinedrift, bogholderi mv. Se i øvrigt om outsourcing, *ET* s. 287 ff.

Denne udvikling har navnlig frembragt to typer af transaktioner: Facility Management og Outsourcing.

FM

En aftale om *facility* (eller facilities) *management* – i det følgende betegnet som FM – kendetegnes ved, at leverandøren (FM-leverandøren) overtager ansvaret for at indkøbe, vedligeholde og betjene det udstyr og det programmel, der understøtter kundens virksomhed. Aftalens kendetegn er, at FM-leverandøren herefter kontrollerer disse dele af brugerens virksomhed, idet kunden fortsat bruger dem på samme måde, som han ville have gjort, hvis opgaven var løst af kunden selv. Men meget mere fælles kan næppe heller siges om disse typer af transaktioner. Der er tale om en kombinationsaftale, der i endnu højere grad end de øvrige IT-aftaler kombinerer vidt forskellige typer af ydelser.

Driften kan enten afvikles hos kunden eller – hvilket med de faldende priser for teleydelser bliver stadigt mere almindeligt – via en teleopkobling til leverandøren. Fordelen ved den sidstnævnte variant ligger i muligheden for stordriftsfordele: Leverandøren kan bruge det samme udstyr og – i visse tilfælde – samme programmel overfor en flerhed af brugere. I begge tilfælde opleves den daglige drift som en del af kundens egen virksomhed.

Facility management adskiller sig fra servicebureaudrift ved, at det system, der løser kundens behov (men ikke nødvendigvis de maskiner, hvorpå systemet afvikles), udelukkende anvendes af kunden. I en aftale om servicebureaudrift anvendes servicebureauets IT-system af en flerhed af kunder. Dernæst opfylder FM-aftalen som regel et langt bredere spektrum af IT-funktioner end typisk i servicebureau-aftaler, omend ikke alle. Som eksempel på et område, der kan tænkes fortsat at befinde sig i kundens egen IT-organisation efter en FM/O-omlægning, er visse udviklingsopgaver.

Outsourcing

FM gennemføres ofte gennem *outsourcing*, hvorved brugeren flytter en arbejdsopgave, han hidtil selv har udført, til leverandøren – undertiden også med et antal medarbejdere, der da ansættes hos leverandøren. Aftalen resulterer for så vidt i en slags *virksomhedsoverdragelse*. Herved opstår spørgsmålet, om også rettighederne til det anvendte edb-programmel uden videre kan følge med over. Problemerne vedrørende overtagelse af medarbejdere ved outsourcing er omtalt i Konkurrencestyrelsens vejledning: Kontrakter om komplekse IT-ydelser (1999) s. 35 ff. og de hertil knyttede forslag til aftalevilkår samme sted s. 42 ff. Se hertil afsnit 21.6.e.

Servicebureau-ydelser

Servicebureauvirksomhed består i at udføre databehandling for en kunde på bureauets anlæg. Sådanne aftaler har naturligvis kun mening, hvis kunden ikke selv kan foretage denne databehandling lige så effektivt som bureauet. Den særlige værdi i ydelsen skyldes, at denne indgår sammen med en særlig ekspertise fra

bureauets side, hvorved den samlede ydelse får en vis specialiseret eller teknisk karakter (f.eks. bogholderi- og skatteindberetningsfunktioner eller betalingstransaktioner). Af samme grund er disse ydelser fokuseret på sådanne særlige opgaver, hvor der er stordriftsfordele ved at samle ekspertisen ét sted.

Servicebureau-markedet er som nævnt blevet mindre i takt med, at prisen for general purpose-systemer er faldet, jf. nærmere *Nørager-Nielsen* (1987), s. 33 ff. EDB-serviceforeningen (senere Edb-systemleverandørernes forening og nu: IT-brancheforeningen) udsendte i januar 1980 en "Kontrakt for EDB-servicebureaukørsel", der ikke siden er fulgt op. Aftalen er forholdsvis kortfattet og indeholder foruden en præcisering af kundens pligt til at aflevere korrekt og rettidigt *grundmateriale*, henholdsvis bureauets pligt til at aflevere korrekt *resultatmateriale*, samt overholde sikkerhedskrav mv.

En servicebureauydelse tager almindeligvis sigte på databehandling, der sker lokalemæssigt adskilt fra virksomheden. Derimod sker såkaldt *facility management* ofte fra klientvirksomhedens egne lokaler.

ASP

Gennem de seneste år er et marked for såkaldte ASP-ydelser vokset frem. ASP-konceptet (ASP = Application Service Provision) indebærer, at leverandøren så at sige via *"et stik i væggen"* leverer al den funktionalitet, brugeren efterspørger: Drift, udvikling, vedligeholdelse osv. På nær arbejdspladsterminalerne befinder alt programmel og udstyr sig hos leverandøren. Forbindelsen skabes via en telekommunikationsforbindelse med den fornødne kapacitet og driftseffektivitet. Foruden finansieringsmæssige fordele på kort sigt kan brugeren herved opnå fordel af ikke selv at skulle stå for drift, vedligeholdelse og opdatering af programmer. Den væsentligste fordel for ASP-leverandøren (der pga. telekommunikationsdelen optræder i samspil med en teleleverandør) ligger i muligheden for at knytte kunderne tættere til sig ved de løbende betalinger. ASP-konceptets fordel for leverandøren ligger dernæst i hans mulighed for at (gen-)bruge standardiserede opsætninger af sine produkter.

For kunden beror værdien af en ASP-løsning selvsagt på, hvad det koster at oppebære de nævnte ydelser, sammenholdt med, hvad totalomkostningen ved at drive systemet i eget regi ville beløbe sig til (*"total cost of ownership"*). I brancheprаksis anvendes forskellige prismodeller. Nogle leverandører udbyder deres tjenester til et fast beløb pr. måned pr. bruger. Andre beregner vederlaget efter den faktisk gjorte anvendelse af de enkelte funktioner, evt. med degressiv betaling, jo mere der således "forbruges". Også kombinationer af disse modeller kan forekomme.

21.6.b. Retsgrundlag

Inter partes

Som udgangspunkt må den aftale, der giver en bruger ret til at bruge et IT-system, som enten ejes eller drives af andre, behandles på samme måde som andre brugsretsaftaler, herunder lejeaftaler. Heraf følger, at købeloven ikke gælder, hvorimod det kan komme på tale at anvende lovens principper analogt. Særlige retsgrundlag kan dog være gældende for særlige typer af brug, se således nedenfor om database- og samtrafikaftaler. Der henvises herom i det hele til fremstillingen i afsnit 21.5.b.

21.6.c. Aftalepraksis

Aftaleindgåelsen

Aftaleindgåelse vedrørende facility management-ydelser minder på mange måder om aftaleindgåelse vedrørende de systemer, der understøtter de pågældende systemer. Et kendetegn er det dog, at FM-aftaler almindeligvis indplaceres i en faseopdeling, der indbefatter mindst to faser: En *planlægningsfase*, hvor der sker en teknisk afklaring af opgavens karakter, og en *driftsfase*, hvor FM/O-leverandøren forestår den pågældende drift (hvis ellers parterne bliver enige om de tekniske, retlige og økonomiske rammer herfor). Anvendelsen af denne form for faseopdeling (jf. om dette begreb afsnit 21.5.a.) er i disse tilfælde noget nær uomgængelig, da det ikke er muligt for FM/O-leverandøren at kende karakteren af sin ydelse, før han har foretaget en grundlæggende undersøgelse af kundens systemer og virksomhed. Hvis der under denne afklaring bringes forhold frem, som forrykker det økonomiske grundlag, hvorpå leverandøren allerede har afgivet et tilbud – sammenholdt med de rent udbudsretlige aspekter ovenfor i afsnit 21.2.d. – vil det ofte være aftalt, at leverandøren kan foretage en korrektion af de vederlag, der korresponderer med disse ændringer.

Planlægningsfasen har visse lighedspunkter med den *due diligence*, der ofte gennemføres i forbindelse med en virksomhedsoverdragelse, se hertil *ET*, s. 98 ff.: Der er tale om en undersøgelseshandling, der nødvendigvis må gennemføres inden selve transaktionen igangsættes, men som af forskellige grunde (herunder primært hensynet til at beskytte virksomhedens erhvervshemmeligheder) ikke kan foretages forudgående. I den nedenfor angivne vejledning fra Konkurrencestyrelsen vedrørende kontrakter om komplekse IT-ydelser foreslås regler indført, der giver leverandøren adgang til at stille spørgsmål til enhver kundes medarbejdere i det omfang, det er nødvendigt for at sikre den fornødne viden om de af kontrakten omfattede opgaver (s. 29 f.). Ved afslutningen af planlægningsfasen fremlæg-

ger leverandøren en rapport, hvis indhold skal tiltrædes af kunden, som herefter indgår i kontraktsgrundlaget. Aftaleudkastet giver dernæst parterne mulighed for at frigøre sig fra aftalen, såfremt der kommer nye oplysninger frem under planlægningsfasen, og parterne ikke kan blive enige om i givet fald at justere aftalegrundlaget.

Formularret?

Der findes ingen statslige standardaftaler om FM/O, men flere vejledninger. Emnet er derimod genstand for en grundig behandling i *Nicolai Dragsted:* IT-kontrakter II (2000). *Forskningsministeriet* har i 1995 udsendt en vejledning herom med titlen: Facility Management – Vejledning om udbud og licitation af statens IT-opgaver (januar 1995). En arbejdsgruppe nedsat af *Konkurrencestyrelsen* har i 1999 udsendt en vejledning med titlen "Kontrakter om komplekse IT-ydelser", hvorved bl.a. sigtes til facility management/outsourcing, IT-konsulentydelser og netværksbaserede tjenester. Vejledningen indeholder en række specifikke forslag til kontraktsklausuler, med hovedvægten lagt på aftaler om outsourcing, hvor navnlig spørgsmålet om overtagelse af medarbejdere og videreførelse af licensbetingelser er i fokus.

OIO-aftalen om web-services

I forbindelse med OIO-projektet (Offentlig Information Online), der har til formål at samle formidlingen af de initiativer og aktiviteter vedrørende de tekniske og kommunikative aspekter af digital forvaltning og elektronisk betjening af borgere og virksomheder, er der udsendt en "Standardaftale for Web services" (version 1.0 af 31. maj 2005). Aftalen er beregnet på offentlige myndigheders aftaler om udveksling af data og/eller funktionalitet via XML-baserede tjenester, hvor en offentlig myndighed optræder som serviceudbyder og en anden offentlig myndighed (eller en anden *gren* inden for samme myndighed) som serviceaftager. Standardaftalen fungerer som en skabelon, der udfyldes med to sæt generelle betingelser, henholdsvis for intern (dvs. inden for samme myndighed) og ekstern brug (dvs. mellem myndigheder). Der er ligeledes udarbejdet en vejledning til standardaftalen. Alle dokumenter er tilgængelige fra <www.oio.dk>.

21.6.d. Rettighedsspørgsmål

Facility management vil typisk indebære, at FM-leverandøren under en eller anden form *bruger* programmer, som kunden har erhvervet fra en programleverandør. Ved en sådan brug frembringes et antal *eksemplarer* af det pågældende programmel, kopier som i givet fald må dækkes af en legal eller aftalt licens. Gennemføres transaktionen i forbindelse med en *outsourcing*, vil der dernæst kunne være tale om, at selve programeksemplaret –

eventuelt som dette er indføjet i det anvendte udstyr – *overdrages* fra kunden til leverandøren, jf. ophl. § 19. Dermed opstår spørgsmålet, om licensvilkårene for det pågældende program er til hinder for disse elementer af en sådan transaktion.

Aftaletilfælde

For mere omfattende programprodukter vil der ofte være taget stilling til dette spørgsmål i licensaftalen. Når en programlicens er afgrænset til *bestemte personer*, ligger der heri, at andre (herunder en FM-leverandør) ikke har ret til at benytte programmet. Er der som led i licensen aftalt *forbud mod videreoverdragelse*, må det bero på en vurdering af, om FM-transaktionen indebærer en sådan overdragelse, jf. herom nedenfor. En hemmeligholdelsesklausul (forudsat denne ikke blot er indsat ensidigt, f.eks. i en *shrink wrap*-aftale) vil som udgangspunkt afskære en FM-leverandørs brug af programmet.

Ophl. § 36

I relation til ophl. § 36 er problemet, om FM-transaktionen indebærer to brugssituationer (og dermed nødvendiggør erhvervelse af flere licenser), fordi systemet befinder sig hos brugeren, samtidigt med at det stilles til rådighed for tjenesteyderen (eller omvendt). Svaret på dette spørgsmål beror på det *typeforudsætningssynspunkt*, der er udviklet i afsnit 7.4.b. I den forbindelse må det tillægges særlig vægt, om den pågældende udnyttelsesform udsætter rettighedshaveren for en ødelæggende konkurrence. Hvis brugeren gennem et FM/O-arrangement underminerer det marked, rettighedshaveren sigtede mod, da han udviklede sit program, taler stærke argumenter for, at arrangementet falder uden for formålet med licensen. Er der derimod tale om, at FM/O-aftalen blot gennemfører en driftssituation, som gyldigt kunne realiseres gennem overdragelse af programmet (jf. herom i det følgende), taler meget for at antage, at brugssituationen er gyldigt etableret ifølge den legale programlicens i ophl. § 36.

Overdragelser

Det vil ofte kunne give anledning til tvivl, om en FM-transaktion udvirker en overdragelse, der kan ske i overensstemmelse med konsumptionsprincippet i ophl. § 19, eller blot en teknisk tilrådighedsstillelse. Hvis "erhververen" opnår rådighed over programmet via telekommunikation på en måde, der afskærer kunden fra at bruge (kopiere) programmet så længe denne brugssituation (FM-samarbejdsforholdet) varer, vil det være nærliggende at betragte forholdet som ligestillet med en overdragelse. En sådan betragtning er dog næppe bæredygtig. Når § 19 taler om overdragelse af eksemplarer, tænkes utvivlsomt på overdragelse af det medium, hvorpå disse eksemplarer ("atomer") er manifesteret, jf. bemærkningerne herom ovenfor i afsnit 6.4.d. Er der tale om et programeksemplar, må dette fysisk overdrages. Er

"eksemplaret" overdraget på grundlag af en kode eller anden teknisk begrænsning, må der gennemføres foranstaltninger, der sikrer, at overdrageren definitivt er berøvet sin adgang til at bruge (og dermed kopiere) programmet.

21.6.e. Forholdet til medabejdere

Et særligt problem i forbindelse med gennemførelsen af FM/O-transaktioner, er forholdet til de medarbejdere, der efter en gennemført outsourcing skal indtræde i leverandørens virksomhed. Problemerne herom er omtalt i *Konkurrencestyrelsens* vejledning: Kontrakter om komplekse IT-ydelser (1999) s. 35 ff. Ofte – ja nærmest, typisk – vil lov om lønmodtageres retsstilling ved virksomhedsoverdragelse (jf. lovbekendtgørelse nr. 710 af 20. august 2003) finde anvendelse. Loven indebærer, at leverandøren indtræder i de rettigheder og forpligtelser, der på overdragelsestidspunktet bestod i henhold til indgåede, individuelle eller kollektive arbejdsaftaler, jf. § 2, stk. 1. Er dette tilfældet, må erhververen (FM/O-leverandøren) sikre sig detaljeret viden om, hvilke økonomiske forpligtelser dette indebærer. Gælder loven ikke, men forudsættes medarbejderstaben desuagtet at indtræde i FM/O-leverandørens virksomhed, må det på forhånd fastlægges, hvilke vilkår leverandøren påtænker at ansætte de pågældende medarbejdere efter.

Problemerne vedrørende lovens anvendelse ved offentlig og privat outsourcing er behandlet af *Werlauff* i Udlicitering af medarbejdere, 2. udg. (2001), se navnlig om afgrænsningen af virksomhedsbegrebet ifølge EF-domstolens praksis, s. 13 ff.

21.7. Konsulentydelser

21.7.a. Kendetegn

Begreb

Begrebet konsulentydelse dækker et vidt spektrum af forskellige former for rådgivning og praktiske bistandsydelser. I en *tilbudsfase* er det ofte en særligt antaget konsulent, der formulerer kravsspecifikationen eller forhandler tilbuddet. Under opfyldelsen kan han stå for *projektledelse* og senere *afleveringsprøve*. Men det kan også være konsulenten, der står for de praktiske implementeringshandlinger, når et system (f.eks. et lokalnet baseret på standardkomponenter) leveres, ligesom konsulenten kan

foreståa egentlige udviklingsopgaver ved at færdiggøre programdele mv.

Variationer

Af disse grunde spænder markedet for IT-konsulenter lige fra revisorer og ingeniører over "self-made" IT-kyndige, der virker personligt eller i enkeltmandsfirmaer, og til de internationale konsulentfirmaer, der tilbyder deres ydelser på verdensplan. Der er ingen brancheorganisation for IT-konsulenter i Danmark. En række større konsulentvirksomheder, der (også) yder rådgivning på IT-området, er samlet i foreningen Dansk Management Råd (DMR), der fungerer som branche- og interesseorganisation for "virksomheder, som leverer viden og rådgivning om eller gennemfører ledelse og forretningsudvikling til beslutningstagere og ledere i private virksomheder, organisationer og offentlige institutioner", jf. § 3 i rådets vedtægter. DMR er en medlemsforening under Dansk Industri. Det er en betingelse for en virksomheds optagelse i foreningen, at den forpligter sig til at følge DMR's Branchekodeks. En virksomhed, der er i betalingsstandsning eller under konkursbehandling eller som ikke har fuld rådighed over deres bo, kan ikke optages. I den nævnte Branchekodeks fastslås en række almindelige principper om konsulentens pligt til at løse opgaverne på effektiv, kvalificeret og loyal vis på grundlag af afbalancerede, skriftlige aftalevilkår. I tillæg til pligten til at præstere loyalt arbejde forbyder kodeks konsulenten samtidig at have opgaver for indbyrdes konkurrerende kunder på strategiske og/eller potentielt konfliktende områder "uden forlods at orientere begge kunder herom og opnå deres accept". Overtrædelse af kodeks kan indbringes for rådets erhvervsetiske nævn, hvis afgørelser offentliggøres på rådets hjemmeside. Se nærmere <www.danskmanagementraad.dk>.

Konsulentydelsen har store økonomiske implikationer. Er konsulenten årsag til, at kunden køber for meget IT, har kunden spildt sine penge; køber kunden for lidt, risikerer han uforudsete udgifter. Accepterer konsulenten en afleveringsprøve, kan kunden være afskåret fra at fremsætte yderligere krav. At kunden er repræsenteret ved en konsulent, kan ligefrem få betydning for den retlige vurdering af kundens egen skyld el.lign., sml. dommen i *U 1985.334 H*. Derfor kan såvel valget af konsulent som aftaleindgåelsen siges at være mindst ligeså vigtigt som valget af leverandør og system. Disse erstatningsspørgsmål behandles i kapitel 18, afsnit 18.4.

Arbejdsopgaver

I relation til beskrivelsen af konsulentens faktiske arbejdsopgaver bør aftalen afklare, om der alene skal præsteres en *arbejdsydelse*, eller om der kontraheres om en *resultatforpligtelse*. Væl-

ger man at kontrahere om en arbejdsydelse, bør konsulenthvervet struktureres i faser. Selv om de færreste konsulenthverv vil være uopsigelige, kan en sådan fasestruktur gøre det mere ubesværet for klienten at skifte til en anden konsulent. Første fase kan f.eks. forpligte konsulenten til at udarbejde et udbudsmateriale – ofte kaldet "leverancekoncept" – der viser, hvorledes han har tænkt sig at gribe sin opgave an. Næste fase kan føre til en konkret udvælgelse af leverandører etc.

21.7.b. Retsgrundlaget

Inter partes

Da købeloven ikke gælder for tjenesteydelser og salg af information (rådgivning), må retsforholdet med konsulenten baseres på den indgåede aftale, således som denne kan suppleres med almindelige forudsætningssynspunkter mv. I *ERA 1.161* (Skive byret 17.2.1984) fandtes et oplæg, der var udarbejdet af en konsulent, så uanvendeligt, at der ikke var pligt til at betale for det. I *U 1987.676 H* blev en opdragsgiver friholdt for at skulle betale det resterende honorar til en arkitekt, hvis mangelfulde arbejde havde medført en række lovliggørelsesudgifter, der ville overstige det resterende honorar. I mangel af modstående aftale vil konsulenten som udgangspunkt kunne uddebitere sin bistand som *regningsarbejde*, eventuelt efter overslag, sml. om risikoen for fejlskøn herved *U 1957.987 SH*.

Som nærmere redegjort for i min bog *Advokatretten* (2005), s. 68 ff. og 94 ff., har man inden for en række liberale erhverv forsøgt at gennemføre en form for selvregulering. Gennem fagligt-etiske vedtagelser i de organisationer, der hører til hvert liberalt erhverv, søger man at fastslå de faglige og etiske krav, som udøveren af den enkelte profession forventes at efterleve. Professionen defineres dermed gennem disse krav, som – når de tilsidesættes – kan give grundlag for retlige sanktioner enten i forholdet til organisationen (f.eks. ved bøder eller eksklusion) eller overfor kunden (f.eks. i form af erstatningsansvar eller nedsættelse eller bort fald af honorar). Bortset fra det forsøg, der er gjort herpå regi af Dansk Management Råd, er der ikke gjort bestræbelser på at samle IT-konsulenter i en samlet organiation, og man kan derfor heller ikke sige, at der gælder et egentligt *professionsansvar* for denne gruppe af konsulenter (selv om selve tilstedeværelsen af et *aftaleforhold* selvsagt almindeligvis vil skærpe ansvaret). Den kunde, der kontraherer med en IT-konsulent, må derfor sørge for at have et klart aftalegrundlag med denne. Se tilsvarende om

denne problemstilling Bonnerup-udvalgets rapport (2001), s. 22 (pkt. 4.5).

Interesse-konflikter

Når konsulenter yder rådgivning om valg af system og leverandør kan der opstå risiko for interessekonflikter. Det kan for det første tænkes, at konsulenten vænner sig så meget til at arbejde med særlige løsninger, at han overser, at der er andre og måske mere adækvate løsninger (f.eks. et bestemt styresystem eller applikation) på det givne problem. Dernæst kan konsulentens løbende kontakt med leverandører af sådanne systemer afføde en sådan nærhed, at konsulenten måske i højere grad kan føle sig knyttet til leverandøren (med hvem han også skal arbejde i senere opdrag) end med kunden.

Der findes ingen tilsvarende regulering af de interessekonflikter, en konsulent kan befinde sig i mellem sin loyalitet overfor henholdsvis kunden og en fast indarbejdet leverandør. Som nærmere redegjort for i min bog *Advokatretten* (2005), kapitel 9, frembyder læren om interessekonflikter særdeles vanskelige teoretiske afgrænsninger på grund af de forskelligartede hensyn, der spiller ind. Læren har betydning for hovedparten af de tjenesteydelser, der fordrer et element af loyalitet og/eller fortrolighed mellem parterne. De fleste regulerede liberale erhverv har derfor særlige regler herom i deres branchevedtagelser, når det gælder de interessekonflikter, der kan opstå mellem forskellige kunder. En tilsvarende regulering er sjældnere forekommende, når interessekonflikten har mere indirekte karakter, fordi den udspringer af det – måske ubevidste – ønske om at vælge det kendte og sikre. En absolut ydergrænse findes dog med strfl. § 299, der hjemler straf for den egentlige returkommission.

21.7.c. Aftalepraksis

Hvert konsulentfirma opererer typisk med egne standardaftaler. Aftalerne er sjældent meget omfattende. De indeholder typisk regler om arbejdets omfang, betaling (typisk beregnet efter timesats), ansvarsforhold (ganske ofte i form af en diskutabel ansvarsfraskrivelse for fejlrådgivning) samt opsigelse. For så vidt angår det statslige område udsendte det daværende Administrations- og Personaledepartement i 1987 et forslag til en kontrakt om konsulentopgaver. Ligeledes har APD i 1989 udsendt en vejledning for statsinstitutioner om konsulentanvendelse (hvori kontrakten er optrykt). Vejledningen dækker alle typer konsulentopdrag inden for ledelsesrådgivning mv. og giver bl.a. anvisninger på, hvorle-

des sådanne aftaler indgås, og hvordan konsulentopgaverne afgrænses.

Udbudsforretning

I mange tilfælde udvælges en konsulent efter en forudgående udbudsforretning. Vil opdraget være forbundet med en betaling, der overstiger gældende tærskelværdier, vil denne procedure være pålagt de offentlige myndigheder efter EU's indkøbsregler. APD's vejledning til statsinstitutioner om konsulentanvendelse (1989), s. 22 ff. giver anvisninger for gennemførelsen af en sådan udbudsforretning. Se ligeledes *Christophersen & Føyen* (1981), s. 170 ff.

Forundersøgelser

Inden aftalens indgåelse kan det være hensigtsmæssigt at undersøge den virksomhed, konsulenten optræder i; hvor velkonsolideret den er, hvilke personer der skal stå for opgaven, og hvilke personlige og uddannelsesmæssige forudsætninger disse personer har. Det kan også være formålstjenligt at undersøge konsulentfirmaets kapital- og forsikringsgrundlag samt dets alder. Navnlig kan det være hensigtsmæssigt, at klienten udbeder sig en referenceliste fra konsulenten, der redegør for, hvilke større opgaver af lignende karakter han har været involveret i. Ofte fremlægger konsulentfirmaerne selv sådanne lister som en del af markedsføringen. For at imødegå konsulentens mulige præference for visse systemer/leverandører kan man evt. anmode om en redegørelse over, hvilket system/leverandørvalg han har peget på i sine sidste f.eks. 10 opdrag. Viser det sig herigennem, at en konsulent løbende udpeger en bestemt IT-løsning, kan dette efter omstændighederne indicere en særlig tilknytning, som bør afklares, før aftalen indgås.

Kundens rolle

Som det gælder for andre IT-aftaler, er det vigtigt, at kunden ikke blot overlader ansvaret for selve opfyldelsesforløbet til konsulenten. Lige så lidt som man ved antagelse af en arkitekt kan undlade at have en mening om, hvilken slags hus man vil bygge, lige så vigtigt er det, at opdragsgiveren bevarer kontrollen med de beslutninger, konsulenten rådgiver om. Konsulenten er netop rådgiver – ikke beslutningstager, og hans ekspertise skal kun anvendes til det, der er kerneområdet i hans virke: til at konsultere om et emneområde, klienten ikke selv behersker.

Supplerende litteratur

Nordisk retslitteratur er begavet med en række monografier inden for det IT-kontraktsretlige område. Fra det danske område fremhæves *Jacob Nørager-Nielsen:* Edb-kontrakter (1987) og *Nicolai Dragsted:* IT-kontrakter I og II (2000). I Norge foreligger *Jørgen Bull*: Edb-kontrak-

ter. Oslo (1981), *Odd-Einar Christophersen & Arve Føyen*: EDB-anskaffelser – fremgangsmåde og avtalutformning. Oslo (1981) og *Olav Torvund*: Kontraktsregulering – IT-kontrakter. Tano Aschehoug, Oslo (1997).

En god gennemgang af den nye standardaftale K01 er udarbejdet af *Nicolai Dragsted, Ole Horsfeldt, Jesper Langemark & Claus Sørensen*: K01 med kommentarer (2004). I Thomsons Paradigma-serie har *Anders Kildsgaard, Ole Horsfeldt & Jesper Langemark* udsendt bogen Internetkontrakter (2002). *Ole Horsfeldt* har ligeledes udsendt den praktiske håndbog IT-outsourcing – forhandling og styring af outsourcing kontrakter (2005).

Nærmere oplysninger om *Wassenaar-arrangementet* findes på <www.wassenaar.org>. For en oversigt over de danske regler henvises til Erhvervs- og Byggestyrelsens Eksportkontrolguide, der findes på <www.ebst.dk/eksportkontrol>. En god oversigt over retsstillingen på området verden over findes hos *Stewart A. Baker & Paul R. Hurst*: The Limits of Trust – Cryptography, Governments, and Electronic Commerce (Kluwer Law International, The Hague, 1998).

Litteraturen om *IT-konsulenter* findes sporadisk i enkelte monografier. Se herved *Christophersen & Føyen* (1981), s. 350 ff. og *Nørager-Nielsen* (1987), s. 390 f. Herudover findes den primært i form af tidsskriftsartikler. Fra den udenlandske tidsskriftslitteratur henvises til de kritiske indlæg hos *James O'Connor* i 18 Jurimetrics Journal 256 (1978), og *Kevin S. MacKinnon* i 23 Santa Clara Law Review 1065 (1983), der advokerer for en nærmere regulering af konsulenthvervet, henholdsvis ved offentligretlig kontrol og gennem ansvarsfiksering.

Som flere gange nævnt i teksten har en arbejdsgruppe nedsat af *Erhvervsministeriet* i 1999 udsendt vejledningen Kontrakter om komplekse IT-ydelser, hvorved bl.a. sigtes til aftaler om facility management/outsourcing, IT-konsulentydelser og netværksbaserede tjenester. Vejledningen indeholder en række specifikke forslag til kontraktsklausuler, med hovedvægten lagt på aftaler om outsourcing, hvor navnlig spørgsmålet om overtagelse af medarbejdere og videreførelse af licensbetingelser er i fokus.

I USA er der udgivet en række praktisk orienterede fremstillinger af IT-kontraktens koncipering og fortolkning. Litteraturen florerer, og det er vanskeligt at at fremhæve et værk frem for et andet.

Kapitel 22. MISLIGHOLDELSE AF IT-KONTRAKTER

22.1. Begreb og retsgrundlag

22.1.a. Generel karakteristik

Problemstillingen

Reglerne om misligholdelse af IT-kontrakter giver anledning til to hovedspørgsmål: Hvornår foreligger en misligholdelse (se hertil afsnittene 22.2 og 22.3), og hvilke sanktioner kan en sådan misligholdelse udløse (afsnittene 22.4-22.6)? Dernæst opstår spørgsmålet om, hvornår en misligholdelsesbeføjelse fortabes, f.eks. ved aftale eller passivitet (afsnit 22.7). Uden særskilt aftale vil svaret på begge spørgsmål bero på almindelige obligationsretlige regler, jf. *Bryde Andersen & Lookofsky* (2005), s. 52 ff. Det generelle kriterium er, om det leverede er som aftalt eller med rette forudsat: En funktionalitet er f.eks. ikke tilgængelig, eller er det kun ad besværlige "omveje"; en svartid overstiger aftalte minimumskrav, eller manualen er ulæselig eller vildledende.

Mangelsvurderingen

I mangelsvurderingen indgår en række momenter: *Leverandørens beskrivelser* af det leverede i manualer, tilbuds- eller salgsmateriale, en vurdering af, hvilke *almindelige krav* der inden for branchen stilles til systemer af den pågældende art samt de *særlige forudsætninger*, som brugeren med rette kunne anlægge. I overensstemmelse med gængs obligationsretlig sprogbrug kan man således sondre mellem *generelle mangler*, der vil opstå for enhver kunde til den pågældende ydelse, og *individuelle mangler*, der alene har betydning for den enkelte kunde (ud fra dennes specifikke aftale eller forudsætninger), sml. herom afsnit 22.1.c. om leverandørens vejledningspligt. Også praksis og sædvaner indgår selvsagt med en betydelig vægt. Men da der ofte ikke vil være nogen praksis at støtte sig til, føres man over i en juridisk afvejning, der må udfoldes i lyset af ydelsens teknisk komplekse og til dels immaterielle beskaffenhed. Afvejningen vanskeliggøres ved, at forventningerne til "fejlfri" ydelse ændrer sig over tid i takt med, at teknologien er blevet mere driftssikker.

Hoved- og biforpligtelser

Fordi IT-ydelsen ofte ikke kan udledes præcist af aftalegrundlaget, og fordi leverandøren ofte vil ønske at lade ydelser af anden art (vedligeholdelse, ændring etc.) træde i stedet for de almindelige misligholdelsesbeføjelser, vil der ofte indgå en flerhed af forskelligartede ydelser i kontraktsforholdet, som det kan være vanskeligt at udsondre i en misligholdelsesvurdering. Dette beskrivelsesproblem er dog ikke stort. Som nærmere udviklet i *Bryde Andersen & Lookofsky* (2005), afsnit 2.1.b., er sondringen mellem hoved- og biydelse – trods dens pædagogiske fordele – for det første uden større *praktisk* værdi i mere komplekse transaktioner, hvor det kan være vanskeligt at udskille den ene delydelse fra den anden. For det andet – og vigtigere – er sondringen uden afgørende *retlig* betydning: Også misligholdelse af "biforpligtelser" kan efter omstændighederne udløse helt samme misligholdelsesbeføjelser af samme art som ved misligholdelse af "hovedforpligtelser".

I overensstemmelse med dette udgangspunkt sondrer ingen af de statslige IT-kontraktsformularer mellem de ydelser, som kan siges at være "accessoriske" i forhold til den tilsagte funktionalitet, og "hovedydelsen" (forstået som det, der måles på under afleveringsprøven). Den almindelige misligholdelsesregel i K18 pkt. 15.2 henviser således i det hele til "dansk rets almindelige regler om beføjelser i anledning af forsinket eller udeblevet levering", dog med forbehold for erstatningsreguleringen i pkt. 16 og force majeure-reglen i pkt. 18.

Selv om der altså ikke kan udpeges klare sondringsgrundlag kan det på dette sted være hensigtsmæssigt at pege på nogle af de underforståede forpligtelser, som IT-leverandøren også *uden udtrykkelig aftale* ofte antages at påtage sig, og som kan give anledning til misligholdelseslignende sanktioner. Blandt disse kan i hvert fald fremhæves to: Sikkerhedspligten (afsnit 22.1.b.) og vejledningspligten (afsnit 22.1.c.).

22.1.b. Leverandørens IT-sikkerhedspligt

Det er idag almindeligt antaget, at IT-leverancer må opfylde visse krav om *sikkerhed* for at være kontraktsmæssige. Dette princip følger dels af lovgivningen (et forbud mod salg af farlige og underlødige produkter antages at kunne udledes af mfl. § 1 og kan efter omstændighederne give anledning til indgriben efter produktsikkerhedsloven), dels følger det af almindelige typeforudsætninger.

Er der tale om mere komplekse ydelser vil leverandøren ofte forpligte sig til også at stille et IT-sikkerhedskoncept til brugerens rådighed, f.eks. med adgangskontrol, logning, kryptering etc. Sådanne forpligtelser indgår da som en primær ydelse, der afleveres og mangelsvurderes som sådan.

En tilsidesættelse af denne forpligtelse kan føre til en *mangelsvurdering* af helt sædvanlig karakter. At der består en fare for at miste data el.lign. er således egnet til at nedsætte anvendeligheden af det leverede og dermed fratage brugeren dets forudsatte funktionalitet. Dernæst kan tilsidesættelsen føre til en *erstatningspligt* efter almindelige erstatningsregler.

Der findes ingen trykte afgørelser, der direkte tager stilling til dette. Forbrugerklagenævnsafgørelsen i *JÅF 1999.150* nærmer sig dog problemet ved at lægge til grund, at der forelå en mangel ved en bærbar pc, da remmen til den medfølgende taske knækkede. Den usikre rem fandtes at udgøre en defekt ved det samlede køb (taske + rem) og gav køberen ret til vederlagsfri afhjælpning.

22.1.c. Leverandørens vejledningspligt

I nær forbindelse med den underforståede sikkerhedspligt er de leverandørforpligtelser, der kan udledes af den almindelige kontraktsretlige omsorgspligt. Det antages bl.a., at denne indebærer, at en part med en særlig sagkundskab ikke alene må advare sin medkontrahent om farer, der udspringer af kontrakten eller dens genstand, men også i et vist omfang har en aktiv pligt til at *fraråde* brugeren at foretage en anskaffelse, som med en vis sandsynlighed må formodes at blive uden værdi.

Erstatning

Forpligtelsen har for det første *erstatningsretlig* karakter: I en aftale om løbende IT-funktionalitet vil parterne være forpligtet til at holde hinanden underrettet om uregelmæssigheder eller trusler vedrørende sikkerheden af det pågældende system, herunder forsøg på misbrug af passwords, se hertil afsnit 18.2.b. En tilsvarende oplysningspligt gælder formentlig i almindelighed for oplysninger, der påfører den anden part tab, men som først bliver kendt efter opfyldelseshandlingerne.

Denne forpligtelse er i tidlig erstatningsretlig praksis fastslået i aftaler om salg af inficerede husdyr. I dag er den udtrykkeligt fastslået i produktsikkerhedsloven § 12, stk. 1, der giver kontrolmyndigheden hjemmel til at påbyde en part, der har bragt et farligt produkt i omsætning, at give efterfølgende oplysning om faren og dens forebyggelse, eller at afhjælpe, tilbagetrække eller at destruere produktet. Se hertil afsnit 15.6.

Vederlagsfortabelse

Dernæst kan forpligtelsen indebære, at leverandøren fortaber sit vederlagskrav. En leverandør, der fører sin kunde ud i en udgift, som kunden åbenbart ikke vil få glæde af at præstere, vil således ikke kunne oppebære det i øvrigt aftalte eller forudsatte vederlag. I *JÅF 1995.170* havde en kunde således indleveret sin 5 år gamle printer til reparation, fordi der var slør i skrivehovedet, idet han – printerens alder taget i betragtning – anmodede om et overslag (en anmodning, som leverandøren dog bestred at have fået). Overslaget udeblev, men leverandøren præsenterede i stedet kunden for en færdigrepareret printer samt en regning på 2.150 kr. Forbrugerklagenævnet fandt, at den erhvervsdrivende burde have vejledt forbrugeren om, at det var tvivlsomt, om en reparation ville være rentabel, og nedsatte vederlaget til 1.000 kr.

Mfl. § 3

For det tredje kan leverandørens pligt til at vejlede brugeren udledes af den offentligretlige lovgivning. Efter mfl. § 3 skal der ved afgivelsen af et tilbud eller indgåelsen af en aftale gives "en efter formuegodets eller ydelsens art forsvarlig vejledning, når denne er af betydning for bedømmelsen af ... [bl.a.] brugsegenskaber, holdbarhed, farlighed og vedligeholdelsesmulighed".

Aftalevirkning

Endelig kan vejledningspligten have *aftaleretlig* betydning: Leverandørens manglende vejledning om ydelsens egenskaber (og begrænsninger) kan således efter omstændighederne føre til, at den mindre sagkyndige kunde kan frigøre sig fra aftaleforholdet, når kritiske forhold, som for kunden var uforudsete, og hvis tilstedeværelse gør ydelsen langt vanskeligere at opfylde, indtræder, jf. herom straks nedenfor.

Omfang

Uanset retsgrundlaget beror omfanget af leverandørens vejledningspligt på en række konkrete faktorer. Navnlig den fortrolighed og afhængighed, aftaleforholdet etablerer, spiller en rolle. En langvarig aftale skaber flere biforpligtelser end en kortvarig. Det samme gælder aftaler, der involverer udveksling af følsom information sammenlignet med en aftale, der angår salg af standardvarer på det almindelige marked. Ved dommen i *U 1974.557 SH* blev det antaget, at leverandørens pligt til at give køberen anvisning i brugen af det leverede ikke var udtømt ved udlevering af systemets installationsforskrifter (manualer). Se ligeledes den i afsnit 22.3.e. omtalte *U 1985.334 H*, hvis resultat ligeledes kan forklares med, at leverandøren havde tilsidesat sin vejledningsforpligtelse. I *JÅF 2000.130* fandt Forbrugerklagenævnet, at det var en væsentlig mangel ved en motorcykel, at denne kun var forsynet med en spansk instruktionsbog, idet forbrugeren ikke var blevet oplyst herom inden købet.

Jo mere kompliceret og kostbart udstyret er, desto større pligt har man i praksis pålagt leverandøren til at sikre sig, at brugeren har brug for det. På dette punkt synes danske domstole at stille noget videre krav til IT-leverandører end til leverandører af andre ydelser. *ERA 2.131* (VLD 17.3.1986) lægger til grund, at sælgeren havde misligholdt en IT-kontrakt ved ikke i tilstrækkeligt omfang at have sat sig ind i, hvilke behov og ønsker køberen havde med hensyn til systemet. Selv om denne misligholdelse ikke ansås som grov, gav den køber ret til yderligere afhjælpning. *ERA 2.56* (Vejle civilret, 24.7.1985) antog, at der var svigtet en væsentlig forudsætning for køberen ved, at det leverede system havde en ringere kapacitet end det hidtil anvendte. Er der omvendt tale om et system, hvis egenskaber er almindeligt kendte, har leverandøren ingen pligt til at give køberen nogen nærmere instruktion i de begrænsninger, systemet på enkelte punkter rummer i forhold til andre. Se herved Forbrugerklagenævnets afgørelse i *JÅF 1996.109*, hvor forbrugeren ikke kunne påberåbe sig forudsætningssvigt ved køb af en OS/2-baseret computer, trods det mere begrænsede programudbud, markedet stiller til rådighed for OS/2-platformen sammenlignet med f.eks. Windows-platformen.

22.2. Misligholdelsesformer

22.2.a. Faktiske mangler

Standard-produkter

Den form for misligholdelse, der består i, at den præsterede ydelse lider af faktiske mangler, har størst praktisk betydning ved overdragelse af *standardprodukter*. Er der tale om *udviklingsydelser* vil manglende funktionalitet ofte indebære forsinkelse af ydelsen, jf. herom afsnit 22.2.b. De fleste IT-produkter indeholder – som andre komplekse informationsprodukter – et vist antal fejl. Derfor vil der ofte opstå tvivl om, hvorvidt en sådan fejl kan rubriceres som en *mangel* – dvs. at den for det første bibringer ydelsen en ringere anvendelighed og funktionalitet end aftalt eller forudsat – eller om den befinder sig under den tålegrænse, IT-brugeren må acceptere.

Dette spørgsmål kan i sagens natur ikke besvares generelt, men må løses med udgangspunkt i det konkrete system og ud fra en afvejning af de hensyn, der gør sig gældende, jf. nærmere herom i afsnit 22.3. Navnlig to centrale forhold, gør sig gældende:

For det første vil en mangel i et standardprodukt almindeligvis ramme alle kunder til det pågældende system. Med en sprogbrug lånt fra produktansvarsrettens terminologi vil manglen dermed have karakter af "systemmangel". En antagelse af, at leverandøren kan mødes med retlige sanktioner i anledning af en sådan mangel, vil ofte få ganske indgribende konsekvenser for denne – og undertiden (hvis der er tale om en "lille" leverandør) – være ensbetydende med økonomisk ruin.

Dette forhold fik prægnant udtryk i de mangelssager, der kom op til overfladen ved overgangen til det nye årtusinde. At årtusindskiftet ikke medførte nogen banebrydende "leading case" på dette område skyldes næppe, at der ikke har været problemer. Derimod kan det nok antages, at de *alvorlige* problemer, der har været, har været så store, at alle parter har set en interesse i at løse dem på et strategisk plan ved gennemgribende genforhandlinger af indgåede aftaler, fusioner eller virksomhedsoverdragelser eller andet, snarere end gennem principielle sagsførelser, hvis endemål på forhånd kunne forudses at være ensbetydende med et fuldstændigt virksomhedsophør og dermed også med manglende fejlretning og vedligeholdelse.

At antagelsen af, at et forhold ved en IT-komponent udgør en mangel, i disse tilfælde vil ramme alle produkter inden for den pågældende serie kan – alene ud fra at proportionalitetssynspunkt – tale for at lade visse defekter falde under en bagatelgrænse. Ved afgørelsen i *Forbrugerjura 2003.55* (afsnit 6.3.1) udtalte Forbrugerklagenævnet således, at en computer, som indeholdt to *pixelfejl* (bestående af en permanent lysende rød subpixel og en permanent lysende grøn subpixel placeret hhv. 3 og 30 mm fra øverste skærmkant) ikke udgjorde en mangel i købelovens forstand. Forbrugerklagenævnet fandt det i den forbindelse ikke afgørende, at sælgeren i forbindelse med købets indgåelse havde undladt at give oplysning om risikoen for pixelfejl. Under sagen forelå der en sagkyndig udtalelse, hvoraf det fremgik, at de nævnte pixels faldt inden for rammerne af en ISO-standard, og at fejlene var så små, at de normalt næppe ville kunne ses.

For det andet vil en nedsat teknisk anvendelighed mv. ofte have årsag i den specifikke systemopsætning, brugeren har valgt. At IT-systemer kan bygges sammen af forskellige komponenter skyldes, at de overholder givne grænsefladespecifikationer. At en systemkomponent overholder sådanne krav er dog ikke nogen garanti for, at der ikke indtræder utilsigtede funktionsnedsættelser mv.

Når den slags problemer opstår ved brugen af de hyppigst anvendte programfunktioner i produktet volder det sjældent vanskeligheder at anlægge traditionelle mangelsvurderinger ud fra sædvane- og forudsætningsbetragtninger. Sådanne vurderinger kan imidlertid være vanskeligere – og leverandørens ønske om ikke at hæfte for mangler tilsvarende mere forståeligt – i det omfang den manglende funktionalitet alene indtræder ved brug af funktioner i programmet, som alene vil blive aktiveret i helt særlige situationer og under helt særegne konfigurationer.

Udviklede systemer

I aftaler om IT-systemer, der skal udvikles eller implementeres som led i aftaleopfyldelsen (herunder udviklingsydelser og standardrammesystemer), antager mangelsproblematikken en anden karakter, fordi ydelsen konstrueres efter kundens behov. Kunden kan i princippet få, hvad han ønsker, hvis ellers han vil betale den præsumptivt kvalificerede leverandør for det. I det omfang leverandøren har pligt til at hidføre den ønskede funktion, vil problemet i praksis være, *hvornår* en sådan ydelse kan præsteres. Hvis kontraktens sanktioner ved mangler er stærkere end ved forsinkelse, vil leverandøren have et incitament til at levere, men således, at det system, der kunne være blevet leveret med en mangel, i stedet leveres for sent.

Afvisningsret?

Et vanskeligt spørgsmål opstår i den forbindelse om, hvorvidt kunden har ret til at afvise at modtage en mangelfuld ydelse med den virkning, at der kan påstås ophævelse efter reglerne om misligholdelse. Undertiden kan det synes tilfældigt, om man rubricerer misligholdelse af en udviklingsydelse som forsinkelse eller mangler, jf. nærmere *Nørager-Nielsen* (1987), s. 108 ff.

I aftaler om udviklingsydelser vil leverandøren i almindelighed have en adgang til at afværge en ophævelse gennem afhjælpning af de – væsentlige – mangler, der er til stede i det leverede. En pligt for kunden til at modtage systemet (hvorved kunden afskæres fra at påberåbe sig forsinkelse, hvor en sådan afhjælpningsmulighed i sagens natur ikke er aktuel) vil derfor stille leverandøren bedre. Spørgsmålet drøftes af *Jørgen Nørgaard* i U1997B.523 ff. på baggrund af dommen i *U 1995.974 H*, der i sin antagelse af, at tilvirkningskøberen af et skib ikke havde pligt til at modtage dette, lagde vægt på, at skibet led af "en række fejl af væsentlig betydning", der var afgørende for dets funktionsdygtighed.

I AB 92 § 28, stk. 1, anses aflevering at have fundet sted, når aflevering har fundet sted uden "væsentlige mangler". En tilsvarende regulering er ikke indeholdt i K18, pkt. 11, og K01, pkt. 12.1, der blot forudsætter, at kunden kan udstede godkendelse af overtagelsesprøven, uanset at der består fejl, som parterne er op-

mærksomme på. I så fald bør disse anføres i en mangelliste. Manglende optagelse i denne liste indebærer intet afkald fra kundens side på at kræve fejl afhjulpet. Det må dog antages, at kunden er berettiget til at afvise et system, der lider af væsentlige mangler, selv om leverandøren må formodes at kunne afhjælpe disse efterfølgende.

Inddelingsgrundlag

Mangelstyper i IT-aftaleforhold kan enten inddeles efter *årsagen* til den pågældende fejl (f.eks. fejl i mediet, formateringen, programmeringen, implementeringen el.lign.), eller til den konkrete *virkning* af fejlen. Begge inddelingsgrundlag er relevante, men tjener forskellige formål. Er spørgsmålet, om kunden kan hæve en IT-aftale, får det betydning, hvilke *virkninger* manglen har haft. Er spørgsmålet, om nogen kan gøres erstatningsansvarlig herfor uden for tilfælde af garanti (hvor garantiens ordlyd i alle tilfælde er afgørende), er *årsagen* det centrale. I det følgende knyttes nogle bemærkninger til nogle ofte forekommende fejltyper:

Enkelte forfattere har forsøgt at opstille kataloger over forskellige mangelstyper, dog uden dybere overvejelser om disse sondringsgrundlags funktion. Se f.eks. *Christophersen & Føyen* (1981), s. 79 ff., *Bender & Bruun Nielsen* (1989), s. 27 ff. samt i det hele *Nørager-Nielsen* (1987), der i vid udstrækning bygger på de retsgrundsætninger, der er udviklet i entrepriseretten. *Ellen-Kathrine Thrap-Meyer* har i sin afhandling om Forbrugerkjøp og edb (Complex 5/89, s. 68 ff.) foretaget en opdeling i forskellige typer af edb-mangler, herunder fejl i mediet, formaterings- og kopieringsfejl, programmeringsfejl og systemfejl. Opdelingen tjener primært til at illustrere købelovgivningens anvendelighed på IT-området og markerer ingen udtømmende opdeling af mulige mangelstilfælde endsige generelle typeforudsætninger.

Periodiske fejl

Som antydet ovenfor kan kunden ikke forvente, at IT-systemer er fejlfri. En fejl, der alene dukker op under atypiske omstændigheder, vil næppe uden videre konstituere væsentlighed, hvis brugeren relativt enkelt kan komme uden om den, uanset dette er forbundet med betjeningsmæssige omveje, der ikke var forudsat i dokumentationsmateriale mv., sml. *U 1988.535 H* som omtalt nedenfor. Fejl, der derimod berøver systemet en forventet funktionalitet, eller som i et langsigtet perspektiv har essentiel betydning for brugen af det, vil derimod nok blive anset som væsentlige.

Kompatibilitetsfejl

Et problem, der undertiden opstår ved køb af standardkomponenter inden for PC-miljøet, har at gøre med manglende kompatibilitet. I takt med, at der udvikles standarder for printer-kommunikation, dokumentkonvertering og indbygning af hardware-en-

heder af forskellig art, opstår risikoen for, at en komponent ikke lever op til disse standarder og derfor ikke præsterer den interoperabilitet, som var forudsat. Dette kan medføre, at systemet antages at lide af en faktisk mangel, som kan give kunden en misligholdelsesbeføjelse.

Når man skal vurdere dette spørgsmål er det væsentligt at påpege, at interoperabilitet og kompatibilitet ikke er et spørgsmål om enten/eller, men om mere eller mindre. Ofte vil to komponenter kunne kommunikere med hinanden uden fuld overholdelse af en standard. Dette forhold er velkendt, når dokumenter med dansk tegnsæt søges inkorporeret i tekstbehandlingssammenhænge, der alene anerkender engelsk tegnsæt. I vurderingen må derfor i hvert fald indgå to komponenter: For det første: Hvor indarbejdet er den pågældende standard? Og for det andet: Hvor kritisk er det for den pågældende funktionalitet (målt kvantitativt i fejlhyppighed, såvel som kvalitativt, i hvor indgribende den pågældende fejl er)?

Hvis interoperabiliteten er baseret på en offentliggjort *de jure-standard* (f.eks. en mobiltelefon baseret på GSM-standarden), vil enhver afvigelse fra denne standard, der reducerer systemets funktion, som udgangspunkt udgøre en mangel. I disse tilfælde har producenten samtlige de oplysninger til sin rådighed, som er nødvendige for at hidføre fuld kompatibilitet. Søger produkter derimod at leve op til den *de facto-standard*, som der ikke foreligger offentliggjorte specifikationer til, vil man formentlig i højere grad kunne acceptere afvigelser. Det samme gælder, hvis afvigelsen ikke har en særlig funktionel betydning for brugeren.

I *JÅF 1995.161* klagede en forbruger over, at en printer, som var købt sammen med andre komponenter i et samlet system, ikke kunne håndtere alle de tegnsæt, som hørte til det tekstbehandlingssystem, der indgik i dette system. Ved købet havde forbrugeren angivet et maksimum for, hvad den samlede systemanskaffelse måtte koste. Forhandleren havde derfor valgt en printer, der svarede til dette prisleje og ikke en dyrere laserprinter, der understøttede alle de tegn, det pågældende tekstbehandlingssystem arbejdede med. Forbrugerklagenævnet fandt, at forhandleren i denne situation ikke var underkastet nogen forpligtelse til at foreslå mere avancerede – og dyrere – laserprintere for at opfylde køberens behov. Se også *JÅF 1995.165*, hvor det forhold, at en printer ikke benyttede dansk sprog i displayet, fandtes at udgøre en hævebegrundende mangel, idet kunden havde tillagt forholdet væsentlig betydning ved aftaleindgåelsen. I *JÅF 1996.110* fandt nævnet – utvivlsomt med rette – at det var en væsentlig mangel

ved en computer, at den ikke, som annonceret, var forsynet med en Pentium 586 processor, men alene med en "Nx586-P90"-processor, der ifølge nævnets sagkyndige havde "væsentlig ringere anvendelsesmuligheder". Købet kunne derfor hæves.

Samme leverandør

Som udgangspunkt har IT-leverandøren ikke pligt til at sikre, at en leverance kan fungere i samspil med *tidligere leverancer*. Hertil kræves en særlig aftale. Problemet er her, at sammenbygning med et system, der er udviklet specielt til kunden, enten vil kræve en faktisk adgang – og et indgående kendskab – til den bagvedliggende kildetekst, eller sikker viden om, hvilken almindeligt kendt standard de to systemer knytter sig til. Ved leverancer fra *samme leverandør* som den, der tidligere har leveret IT til kunden, vil der dog være en formodning om, at en efterfølgende leverance til et allerede leveret system er kompatibel med den tidligere leverance, jf. tilsvarende *Lindberg & Westman*: Praktisk IT-rätt (1999) s. 305.

Omvendt kan køberen som udgangspunkt ikke stille krav om, at et indkøbt program er kompatibelt med eksisterende udstyr, jf. *JÅF 1993-94.96*. I denne sag udtalte Forbrugerklagenævnet, at forbrugere, der anskaffer komplekse komponenter som f.eks. bundkort, grafikkort, lydkort, cd-rom drev mv. med henblik på selv at foretage installation af disse i en computer, har pligt til selv at søge oplysning om hvorvidt de pågældende komponenter er kompatible til den købte computer, og at en sådan pligt særligt gælder inden for områder, hvor der ikke eksisterer vedtagne (de jure) standarder. I den pågældende sag var den omtvistede standard IBM's pc-standard.

"Kloner"

Under det tidligere marked for "PC-kloner" opstod der ofte tvivl om, i hvilket omfang ikke-IBM-udstyr var kompatible med IBM's PC. I sådanne tilfælde må man formentlig kræve, at den kan afvikle de mest udbredte standardpakker inden for tekstbehandling, administrative systemer og kommunikation. Heri lå netop salgsargumentet for disse maskiner. I relation til mere særegne applikationer må den, der køber klon-udstyr, til en vis grad bære risikoen for kompatibilitetsfejl, jf. den førnævnte afgørelse i *JÅF 1993-94.96*. I dag opstår sådanne kompatibilitetsproblemer hyppigt i relation til de processorer, som dominerende chip-fabrikanter udbyder under angivelse af præcise instruktionssæt, og som herefter "klones" af konkurrerende chip-fabrikanter. Et eksempel herpå er Forbrugerklagenævnets afgørelse i *JÅF 1995.162*, hvor en bærbar pc var betegnet som "486 SLC 25 MHz med 4 MB RAM standard og mulighed for udvidelse op til 20 MB". Da det ikke var præciseret, at der ikke var tale om en Intel 486-PC (idet den solgte

processor kun kunne anvendes på et systemkort, der var udviklet til en anden processor) fandtes computeren ikke at svare til den solgte betegnelse. Da denne mangel fandtes væsentlig, kunne kunden hæve.

Instruktionsfejl

Talrige IT-mangelstilfælde kan tilskrives brugerens manglende kendskab til, hvordan systemet skal håndteres. Et af IT-leverandørernes standardforsvar i sager om påståede mangler ved IT-systemer er da også, at brugeren ikke betjener produktet korrekt, se f.eks. *ERA 1.34* (VLD 4.3.1980) og *ERA 1.101* (Odense byret, 2.2.1984). I relation til IT-systemer og andre komplekse ydelser, der stiller særlige krav til betjeningen, er det vigtigt at præcisere, at der kun foreligger en mangel, såfremt "kunden anvender det leverede korrekt i overensstemmelse med den udarbejdede dokumentation og nærværende kontrakts bestemmelser", jf. K18 pkt. 14.1.

Dermed opstår spørgsmålet om, hvem der har ansvar for brugerens fejlbetjening. Dette problem må systematisk betragtes som et spørgsmål om kravene til leverandørens vejledningspligt, jf. herom afsnit 22.1.c. Som antaget her, har leverandøren undertiden en eksplicit pligt til at vejlede ved overdragelser af større og mere komplekse systemer. I relation til mindre, standardiserede systemer må brugeren almindeligvis kunne forvente at blive forsynet med en anvendelig brugervejledning. Fejl ved brugervejledninger må betragtes som en integreret del af den køberetlige mangelsvurdering, jf. f.eks. *U 1952.932 Ø* og *ERA 2.155* (VLD 7.4.1986) og *JÅF 1999.134*, hvor mangelfuld vejledning gav adgang til ophævelse. Se tilsvarende *Torvund* (1997), s. 203 f. med righoldige henvisninger til norsk praksis.

Udbygningsmuligheder

I det omfang kunden har ret til at forudsætte, at det leverede system kan udbygges, vil en manglende adgang hertil skulle rubriceres som en mangel, jf. *JÅF 1995.159*, der fandt, at en sådan mangel på en PC var hævebegrundende. At man må se med særlig alvor på dette forhold skyldes, at den manglende udbygningsmulighed på længere sigt vil fratage systemet dets funktionalitet under de ændrede brugssituationer, kunden ofte må forventes at befinde sig i senere.

22.2.b. Leverandørforsinkelse

Den misligholdelse, der består i, at et IT-system ikke leveres til tiden, opstår erfaringsmæssigt ofte i udviklingsprojekter. Her kan der tilstøde uforudsete opfyldelsesvanskeligheder, når man be-

væger sig fra det strategiske tegnebords-stadium og ned til den egentlige systemkonstruktion.

I vurderingen af, hvornår der foreligger forsinkelse, vil der ofte være tale om, at parterne efterfølgende har fraveget den oprindelige aftale. Dette vil ofte ske stiltiende, når brugeren undlader at fastholde leverandøren på de tidsterminer, der er lagt til grund for systemarbejdet, og måske tilmed indlader sig på efterfølgende drøftelser med henblik på at opnå en anden funktionalitet end den oprindeligt aftalte. Sådanne ændrede forhold er velkendte inden for entrepriseretten, men forekommer i tilsvarende omfang på IT-området.

Standard-komponenter

Også for standardydelser (og her typisk de nyeste modeller) kan efterspørgslen være så stærk, at produkterne ikke kommer frem som ventet. Problemet har dog her en anden karakter: Hvor det kan være vanskeligt på forhånd at overskue omfanget af en udviklingsopgave, vil det i almindelighed være enkelt for leverandøren af en standardkomponent, der skal erhverves fra en underleverandør, at overskue, om underleverandøren kan levere ydelsen til det aftalte tidspunkt. Kan underleverandøren ikke det, vil leverandøren ofte kunne gøre et forsinkelsesansvar gældende mod denne. Sådanne spørgsmål kan uden videre behandles efter de køberetlige regler, jf. *Nørager-Nielsen* (1987), s. 110, uanset om der er tale om hardware eller om software. Et eksempel herpå er *JÅF 1999.140*, hvor Forbrugerklagenævnet undlod at tage leverandørens påstand om ansvarsfrihed til følge, jf. kbl. § 24, i en situation, hvor levering af RAM-kort til en computer var blevet vanskeliggjort som følge af et jordskælv i Taiwan.

Udviklings-opgaver

De køberetlige regler om ophævelse ved forsinkelse er imidlertid ikke velegnede som grundlag for en regulering af forsinkede udviklingsopgaver. Som nærmere udviklet hos *Bryde Andersen & Lookofsky* (2005), s. 213 ff., er bestemmelsen om køberens ret til ophævelse ved "enhver" forsinkelse i handelskøb ganske streng og i hvert fald – som det udtrykkes i den norske højesteretsdom i *U1923B.292* – lidet skikket til anvendelse på langsigtede bestillingskontrakter om specialmaskiner af meget betydelig værdi og mindre kurant omsættelighed. I sådanne kontrakter, hvortil IT-udviklingskontrakter hører, vil det typisk ligge helt uden for parternes mening, at en sådan hævebeføjelse kunne komme på tale. For brugeren vil en ophævelse føre til, at man må gentage proceduren omkring kontraktens indgåelse og specifikation, dvs. foranstalte ny kontraktsforhandling, ny implementering og ny afleveringsprøve. For leverandøren vil en ophævelse ofte betyde, at det arbejde, der er lagt i aftalen, er spildt. Derfor må

man med stor sikkerhed antage, at købelovens regler om ophævelse ved handelskøbsforsinkelse ikke gælder i aftaler om systemudvikling, se herved *Nørager-Nielsen* (1987), s. 122.

Konventionalbod

I aftaler om større installationer er det sædvanligt at bestemme, at der betales bod i tilfælde af forsinkelse, se f.eks. K01, pkt. 16.1.1, K33 pkt. 14.5 (mangler) og 15.2 (forsinket eller udebleven levering) samt de tilsvarende regler i K18 henholdsvis pkt. 14.3 og 15.1. Bodens størrelse må i sagens natur variere efter, hvor essentielt det er for kunden at få leveret til tiden. Fører forsinkelse til, at erhververen vil komme i misligholdelse overfor sine kunder, bør beløbet sættes højt. Fører den blot til irritation (men ikke til egentlige udgifter), er der sjældent realt belæg for krav om store konventionalbøder.

Det er ikke ualmindeligt at fastsætte boden til 1 o/oo pr. arbejdsdag af den samlede kontraktssum suppleret med en regel om, at forsinkelse udover f.eks. 60 arbejdsdage giver kunden ret til at ophæve kontrakten. Ligeledes ser man ofte bestemmelser om, at det samlede bodsbeløb i tilfælde af ophævelse ikke kan overstige 10 % af den samlede kontraktssum. Se således K33, pkt. 15.2. I K18, pkt. 15.1, er boden gradueret, således at den udgør 0,2% til og med den 10. arbejdsdag, 0,3% pr. følgende arbejdsdag til og med den 20. arbejdsdag og derefter 0,5%. Også her er boden maksimeret til 10% af den samlede kontraktssum. I K01 pkt. 16.1.1. er der aftalt en dagbod på 0,25% pr. arbejdsdag, såfremt den aftalte overtagelsesdag overskrides som følge af forhold, som leverandøren hæfter for. Boden beregnes pr. arbejdsdag af systemvederlaget, jf. aftalens pkt. 10.2, og er maksimeret til 10% af dette vederlag.

22.2.c. Betalingsforsinkelse

Kundens misligholdelse med betalingsforpligtelsen giver ikke anledning til særlige problemer på IT-området. I større leverancer vil der typisk være udarbejdet en betalingsplan, hvorefter kundens betaling skal falde i rater. Misligholdelse med ratebetaling vil her udløse pligt til at betale morarente i overensstemmelse med rentelovens almindelige regler, medmindre andet er aftalt. I vurderingen af, om en betalingsmisligholdelse herudover kan udløse ret for leverandøren til at hæve aftalen, finder de almindelige synspunkter vedrørende ophævelse af IT-kontrakter tilsvarende anvendelse. Også her stilles der kvalificerede krav for at en ophævelse kan komme på tale.

I transaktioner, hvor leverandørens ydelse i hovedsagen er en *indsatsforpligtelse*, se hertil *Bryde Andersen & Lookofsky* (2005), s. 42 ff., kan der opstå tvivl om, hvorvidt kunden er forpligtet til at betale, hvis ikke leverandørens indsats bibringer køberen den forventede behovsopfyldelse. Det er her det almindelige princip i dansk ret, at "den gode, men mislykkede indsats" også må honoreres, jf. a.st. og *Stig Jørgensen & Torben Wanscher* i J1967.426. Se også dommen i ERA I.161, der dog frifandt for en helt værdiløs indsats. *U 1964.125 H* fastslog tilsvarende, at kunden havde pligt til at betale udviklingsomkostningerne til frembringelse af et værktøj, selvom dette viste sig uegnet til formålet, idet det betones, at sælger ikke havde påtaget sig nogen garanti herfor.

22.2.d. Retsmangler

Den omstændighed, at IT-systemer og -komponenter typisk er dækket af immaterialrettigheder, indebærer en latent risiko for, at tredjemand har rettigheder over det leverede, der kolliderer med brugerens anvendelse. I det omfang, en sådan ret kan gøres gældende, vil den blokere anvendelsen af det pågældende system på ganske samme måde, som hvis der forelå mangel eller forsinkelse.

Derfor må IT-køberen sikres mod retskrav fra tredjemands side. Erfaringsmæssigt fremsættes sådanne krav sjældent, men den uklarhed, der består om talrige immaterialrettigheders rækkevidde, indebærer – sammen med den mangel på respekt, der ofte består omkring håndhævelsen af disse rettigheder – at der i dag er tale om et latent problem af potentielt store dimensioner.

Som udgangspunkt gælder de almindelige kontraktsretlige regler. Heraf følger, at leverandøren i hvert fald ifalder erstatningsansvar for *garanti* og *culpa*. Ligeledes må det efter en analogi af købelovens mangelsregler antages, at køberen har ret til at hæve, hvis den pågældende retsmangel er væsentlig. Det interessante spørgsmål knytter sig til, om leverandøren kan gøres erstatningsansvarlig for sådanne retsmangler på objektivt grundlag.

Et sådant resultat kan have gode grunde for sig, jf. i det hele min afhandling i U1987B.121 ff. De synspunkter, der normalt fremføres til støtte for et objektivt ansvar for farlige egenskaber (se f.eks. *Børge Dahl*: Produktansvar, s. 339 og 363 ff.), må således tillægges vægt: Leverandøren har langt bedre muligheder end brugeren for at gennemføre en regres mod den part, som er skyld i, at retskravet opstår. Dernæst har den immaterialretlige vanhjemmel betydelige lighedspunkter med den ejendomsretlige vanhjemmel, der udtrykkelig er reguleret i kbl. § 59. Et objektivt ansvar er endelig i harmoni med en udbredt IT-kontraktspraksis.

Se f.eks. K33, pkt. 23, K18 pkt. 22, og EDB-rådets standardkontrakt om køb, § 16.

Som udviklingen på IT-immaterialrettens område er forløbet er der imidlertid også væsentlige argumenter mod at opstille et sådant objektivt ansvar. I takt med, at der opstår stadigt flere typer af immaterialrettigheder, og stadigt flere produkter, der kan tænkes at krænke sådanne rettigheder, bliver det stadigt vanskeligere for den enkelte leverandør at undgå, at hans produkt kommer til at krænke sådanne rettigheder. I sådanne tilfælde kan der være grundlag for at modificere udgangspunktet om, at ansvaret er objektivt. På det generelle plan giver spørgsmålet således anledning til en betydelig tvivl, som endnu ikke er afklaret ved domstolene.

22.3. Misligholdelsesvurderingen

22.3.a. Udgangspunktet

Når det kan konstateres, at der foreligger en misligholdelse fra leverandørens side, råder kunden som udgangspunkt over de misligholdelsesbeføjelser, der kan udledes af det almindelige obligationsretlige system, dvs. *naturalopfyldelse* (i form af krav om udbedring), *forholdsmæssigt afslag*, *ophævelse* samt *erstatning*. Hver af disse retskrav kræver, at visse yderligere forhold gør sig gældende ved den enkelte misligholdelse: Et krav om *naturalopfyldelse* kan således ikke gennemføres, hvis en gennemtvingelse vil være ensbetydende med et uforholdsmæssigt værdispild mv., jf. *Bryde Andersen & Lookofsky* (2005), s. 202 ff. Forholdsmæssigt *afslag* kommer alene på tale i relation til indtrådte mangler, såfremt – og alene i det omfang – det kan konstateres, at disse har været værdiforringende, jf. f.eks. *JÅF 1995.168* om et tekstbehandlingsprogram, der ikke kunne udskrive danske karakterer korrekt. Krav om *ophævelse* forudsætter, at der foreligger en væsentlig misligholdelse (mangel, forsinkelse eller vanhjemmel). Og krav om *erstatning* forudsætter, at der foreligger et ansvarsgrundlag, der udløser en erstatningspligt (f.eks. culpa).

I stort set alle disse tilfælde vil det imidlertid bero på en afvejning, om der foreligger en misligholdelse og – i bekræftende fald – om der er grundlag for at gøre misligholdelsesbeføjelsen gældende. I det følgende skitseres en række af de synspunkter, der indgår i denne juridiske afvejning.

22.3.b. Udviklingssynspunktet

Det er velkendt, at ingen IT-systemer er fuldstændigt fejlfri. Småfejl er uundgåelige selv i de produkter, der markedsføres af branchens største aktører, der afholder astronomiske omkostninger til udvikling og aftestning af nye systemer. Samtidig forløber udviklingen så hastigt, at forbrugerne stiller stigende krav til fejlfri ydelse. Ud fra denne betragtning har man tidligere anlagt et såkaldt *udviklingssynspunkt* svarende til det, der er omtalt ovenfor under det almindelige erstatningsansvar: Vil man understøtte et marked for systemer, der beror på kompleks og koncis information, må man til en vis grad respektere de vilkår, hvorunder sådanne systemer bliver til.

Synspunktet er bl.a. fremført af *Nørager-Nielsen* (1987), s. 44, med ordene *absolutum obsoletum*: Når det virker, er det forældet! Se ligeledes *Christophersen & Føyen* (1981), s. 112 ff.

Når synspunktet rejses, kan der være grund til at drøfte de omstændigheder, der indebærer, at et system kan være mangelfuldt. Det ligger vel klart, at mange brugere typisk kan leve med småfejl, der alene fremtræder som irritationsmomenter, enten pga. deres lave frekvens, eller fordi de ikke opleves som hæmmende for brugerens primære anvendelse af systemet. Men det er en kendsgerning, at selv markedsdominerende systemer ganske ofte er behæftet med fejl, der ikke alene frembringer småirritation, men som hyppigt medfører længerevarende driftsbrud i vitale administrative systemer (f.eks. e-post servere el.lign.). I sådanne tilfælde kan der næppe være plads for et udviklingssynspunkt, og heraf følgende nedbrud må derfor i mangel af anden aftale mangelsvurderes efter de almindelige køberetlige principper. Den ikke-opfyldelse, der er konsekvensen af, at leverandøren hellere har villet være "først" med et nyt produkt end slet ikke at være med med et produkt, der fungerer, skal ikke bæres af brugeren.

Versioner

Standardprogrammel markedsføres typisk med angivelse af henholdsvis "version" og "release". At der er tale om en given *version* markerer systemets placering i et udviklingsforløb; for hver version indlægges nye funktioner. En *release* udsendes, efterhånden som fejl og uhensigtsmæssigheder rettes hos programudvikleren. At man køber en programpakke i en sådan produktudvikling indebærer ikke i sig selv en fraskrivelse af retten til at gøre mangelsansvar gældende for fejl, der efterfølgende rettes i senere versioner.

22.3.c. Vederlagets størrelse

Man kan spørge, om prisen for en IT-ydelse giver en part ret til at forudsætte en vis kvalitet. Svaret på dette spørgsmål må formentlig besvares benægtende, når der tales om standardvarer (f.eks. standard-programmel), se herved diskussionen i *E&A*, s. 359 f. Da de variable omkostninger her er forsvindende, sættes prisen primært af markedets omfang samt konkurrencesituationen.

At *U 1988.535 H* kom til, at det ikke var en hævebegrundende mangel, at en PC-skærm ikke kunne stå oven på PC'en, kan formentlig ses i lyset af, at køberen havde betalt over 20.000 kr. for den pågældende PC, der – ifølge sagens oplysninger – dengang var markedets billigste. Da sagen blev afgjort, kunne tilsvarende kloner erhverves for beløb i nærheden af 5.000 kr. Den køber, der ser en sådan markedsudvikling som tilskyndelse til en sagsførelse, mødes næppe med venlige øjne. Spørgsmålet om prisens betydning for mangelsvurderingen drøftes bl.a. af *Torvund* (1997), s. 194 f, der heller ikke vil lægge vægt på pris- og rabatforhold.

22.3.d. Sælgers oplysninger

Ifølge kbl. § 76, stk. 1, nr. 2, jf. nr. 1, spiller det bl.a. en rolle for mangelsvurderingen i forbrugerkøb, om hvilke oplysninger sælgeren eller tidligere salgsled har givet om varens betegnelse eller andre forhold, der kan have betydning for køberens bedømmelse af salgsgenstanden. Bestemmelsen bygger på en forudsætning om, at sælgeren som den part, der har det bedste kendskab til det solgte, gør de informationskilder, som han må indse, at køberen skaffer sig via offentliggjort materiale fra sælger og tidligere salgsled, til sine egne. Princippet antages at have generel anvendelse og fører på IT-området til den regel, at oplysninger i manualer, systembeskrivelser, salgsmateriale og anden formel dokumentation vedrørende det solgte, kan gøres gældende mod leverandøren.

Navnlig på forbrugerområdet spiller dette mangelskriterium en stor praktisk rolle, idet kunden ofte vil vælge det leverede ud fra en vurdering af offentliggjorte oplysninger. I mange tilfælde vil det salgspersonale, der står for selve salget i forretningen (f.eks. et supermarked), således have begrænset teknisk indsigt.

I *JÅF 1999.148* havde en forretning reklameret med en laserprinter med angivelse af, at der var tale om "en stærk, personlig printer til den professionelle bruger, som ønsker høj ydeevne til en fornuftig pris", som kunne skrive "6 sider i minuttet i ægte 600 DPI", idet det

bl.a. fremgik, at printeren havde "2MB RAM (max. 35 MB)". Det viste sig imidlertid, at ydeevnen 6 sider i minuttet alene kunne opnås ved udprint af almindelige tekstsider, og at der skulle en RAM-udvidelse til for ca. 1.000 kr., hvis systemet også skulle håndtere udprint af grafiske sider. Forbrugerklagenævnet fandt manglen væsentlig og gav køberen ret til at hæve.

Den omvendte regel gælder derimod ikke. Som udgangspunkt kan leverandøren således ikke påberåbe sig, at et forhold, der er anført i et sådant dokument, skal fratage leverandøren en forpligtelse til at stille en funktion til rådighed, som kunden på andet grundlag kunne gøre gældende. I K18 er dette princip fastslået i pkt. 2.1, stk. 5, der fastslår, at leverandøren ikke kan påberåbe sig, at det, der fremgår af bilag 4 (leverandørens beskrivelser af udstyr og programmel, herunder allerede eksisterende dokumentation), medfører, at krav eller beskrivelser i bilag 2 (kundens behovsopgørelse med eventuelle aftalte ændringer og forbehold) ikke kan opfyldes.

Certifikater

Er den leverede ydelse *certificeret*, vil certifikatet typisk indgå som en del af aftalegrundlaget mellem parterne. Udbydes en programpakke med oplysning om, at den er certificeret af X myndighed, hæfter udbyderen for, at denne faktiske omstændighed er korrekt. Er der tale om forbrugerkøb, fremgår dette udtrykkeligt af købelovens § 76, stk. 1, 2. pkt., hvorefter der foreligger en mangel ved det solgte, hvis sælgeren eller et tidligere salgsled i annoncer eller i andre meddelelser, der er beregnet til at komme til almenhedens eller køberens kundskab, har givet oplysninger, der kan antages at have haft betydning for køberens bedømmelse af genstanden. Bestemmelsen, der ofte vil kunne anvendes analogt, indebærer, at en køber kan påberåbe sig certifikatet som grundlag for en påstand om, at det solgte er mangelfuldt. Dette kan efter omstændighederne give ret til afhjælpning, forholdsmæssigt afslag eller ophævelse.

Problemstillingen belyses ved *U 1992.43 SH*, hvor køberen af en vindmølle, der var erhvervet som led i et skatteteknisk leasingprojekt, fik medhold i et krav om ophævelse af aftalen under henvisning til, at vindmøllen ikke – som fremhævet i udbudsmaterialet – var "kvalitetssikret ved certificering af Det norske Veritas". En certificering forelå ikke på tegningstidspunktet og kom heller ikke til at foreligge. SH fastslog, at certificering fra Det norske Veritas ville have givet øget kvalitetssikkerhed og medført en forbedring af den retlige og faktiske stilling for det kommanditselskab, investeringen angik. Se ligeledes *U 1979.504 H*, der frifandt Statens Skibstilsyn for hæftelse for fejl, forvoldt ved påstået forsømmelighed begået af Det norske Veritas, som tilsynet havde udpeget som klassifikationsselskab. At et manglende certifikat kan implicere, at der ikke er leve-

ret rigtig ydelse, er ikke ensbetydende med, at leverandøren bliver erstatningspligtig overfor erhververen ud fra et *garantisynspunkt,* se herved dommen i *U 1989.862 V*. Her havde sælgeren af et hus i slutsedlen henvist til en varmesynsrapport. Retten fandt imidlertid ikke, at udleveringen af varmesynsrapporten kunne anses for at rumme en tilsikring af, at den solgte ejendom i energimæssig henseende var som angivet i rapporten. Et modsat resultat nåede Østre Landsret til i *U 1991.363 Ø* og Vestre Landsret til i *U 1995.238 V*. Se i øvrigt *JÅF 2000.103*, hvor Forbrugerklagenævnet anså det for en hævebegrundende mangel, at en computer ikke var forsynet med CE-mærkning.

22.3.e. Subjektive forhold

Det har været diskuteret, om kundens subjektive forhold (kendskab eller mangel herpå til IT) skal influere på mangelsvurderingen, eller ligefrem på kundens muligheder for at blive løst fra et aftaleforhold. Kan leverandøren f.eks. regne med, at kunden selv sætter sig ind i de tekniske forhold, der er afgørende for en succesfuld implementering af det solgte? Spørgsmålet kan ikke besvares generelt, men må bero på, hvilke parter der er tale om samt forløbet vedrørende aftaleindgåelsen. Hvis aftalen indgås med leverandøren som den drivende kraft og således, at kunden i kraft af leverandørens oplysninger overtales til at erhverve et system, hvis begrænsninger kunden kunne have indset med lidt teknisk assistance, tyder retspraksis på, at kunden har ret til at påberåbe sig en sådan uvidenhed.

Dette resultat blev således antaget i *U 1985.334 H*. Her var spørgsmålet, hvem af parterne der skulle bære risikoen for, at en systemleverance blev ca. 400.000 kr. dyrere end forventet på grund af meromkostninger ved tredjemands udvikling af nødvendigt specialprogrammel. Brugeren var ikke klar over, at hardware og software blev leveret af to forskellige virksomheder, og regnede for så vidt med, at sælgeren – der havde skønnet, at omkostningerne ville udgøre ca. 80.000 kr. – havde fuldt overblik over de økonomiske konsekvenser af udviklingsopgaven. Højesteret fandt, at leverandøren, "der måtte være bekendt med det tilbudte programmels muligheder og begrænsninger, og som ikke fandt det fornødent at foretage nærmere undersøgelser til oplysning om [brugerens] behov", måtte bære risikoen for, at brugerens "afgørende drifts- og prismæssige forudsætninger for kontrakten svigtede". U 1985.334 H

Se om dommen bl.a. *Nørager-Nielsen* (1987), s. 257 med kritik, og generelt om edb-leverandørens "uskrevne" rådgivnings- og specialforpligtelser *Ole Bruun Nielsen* i NÅR 1987.188.

Efterfølgende forhold

I den almindelige mangelsvurdering spiller det ind, hvordan brugeren har optrådt under afhjælpningsforløbet. Har han gentagne gange markeret sin interesse i snarest muligt at få mangelfri ydelse, vil dette skærpe leverandørens pligt hertil. En modsat effekt har brugerens løbende tiltrædelse af, at der sker udskydelser af den endelige aflevering. Brugeren kan formentlig modsætte sig en afhjælpning på et standardsystem, som reelt har karakter af *udviklingsarbejde*. Afhjælpningsretten er noget videre i forbrugerkøb, sml. kbl. § 79. Ved Forbrugerklagenævnets afgørelse af 5. september 1984 (*ERA 1.113*) fandtes sælger i et forbrugerkøb ikke at have yderligere afhjælpningsret efter 4 omleveringer.

22.4. Naturalopfyldelse og afslag

22.4.a. Naturalopfyldelse

Efter dansk ret hører realkreditors ret til naturalopfyldelse hjemme i det almindelige katalog af misligholdelsesbeføjelser. At netop denne beføjelse er et særligt velegnet instrument til at håndtere leverandørmisligholdelse i IT-forhold vidner kontraktspraksis om, hvor leverandørens afhjælpningspligt ofte indgår som den eneste retsvirkning, kunden kan gøre gældende, når der foreligger faktiske mangler.

Kildetekst

Naturalopfyldelse er imidlertid ikke noget uproblematisk retsmiddel i tilfælde, hvor leverandøren ikke er indstillet på at medvirke til f.eks. en mangelsafhjælpning eller forsinket programudvikling. Uden for tilfælde, hvor der er tale om standardkomponenter, vil en naturalopfyldelse vedrørende en programudvikling forudsætte, at brugeren har adgang til den anvendte kildetekst. Dermed opstår det spørgsmål, der drøftes i afsnit 4.4.b., om brugeren kan forlange kildeteksten udleveret. Da kildeteksten almindeligvis anses som leverandørens eksklusive erhvervshemmelighed, vil han – eller hans konkursbo – sjældent ønske at give den fra sig. Som nævnt det anførte sted er det her nærliggende at anlægge en kvalificeret væsentlighedsvurdering, der afvejer brugerens skadevirkninger ved ikke at kunne få adgang til den tilsagte funktionalitet med leverandørens risiko for kompromittering af erhvervshemmeligheder mv.

Dette kan begrunde et krav om, at leverandøren skal have udvist væsentlig misligholdelse, før et udleveringskrav kan tages til følge. Brugerens ret til at anvende kildeteksten bør i alle tilfælde være begrænset til de dele af den, der er nødvendige for at

kunne rette opståede fejl og kunne foretage nødvendige opdateringer. Dernæst bør adgangen kun bestå, så længe det er nødvendigt af hensyn til fejlretningen.

Som nærmere udviklet hos *Bryde Andersen & Lookofsky* (2005), s. 202 f. antages det almindeligvis, at kravet om naturalopfyldelse må modificeres, hvis de omkostninger, der er forbundet herved, vil repræsentere et urimeligt værdispild. Denne betragtning kan næppe begrunde, at kunden fratages adgang til selv at foretage en omprogrammering, der vil afhjælpe en konstateret mangel. Ej heller kan betragtningen føre til, at en leverandør, der har påtaget sig en uopsigelig vedligeholdelse af et system, der i teknologisk henseende er blevet forældet inden periodens ophør, friholdes for pligten hertil.

22.4.b. Forholdsmæssigt afslag

Det følger af almindelige obligationsretlige principper, at leverandøren af en mangelfuld ydelse, der ikke afhjælpes, må tåle et forholdsmæssigt afslag i ydelsen svarende til den værdiforringelse, manglen repræsenterer. Dette princip, der er fastsat i kbl. §§ 42, stk. 1, og 43, stk. 1, gælder tilsvarende i IT-leverancer, sml. K18 pkt. 13.2, stk. 3, der giver leverandøren en noget luftig adgang (denne forudsætter nemlig, at kunden erklærer sig indforstået hermed) til at frigøre sig fra fremtidige vedligeholdelsesforpligtelser ved (bl.a.) at yde et afslag i vedligeholdelsesafgiften.

De trykte afgørelser, der findes om mangelfulde IT-system-leverancer, har dog ikke drejet sig om afslagsbeføjelsen. Hvis et system trods alt er så funktionsdueligt, at kunden vælger at køre videre med det, frem for at skride til ophævelse og erstatning, vil der ofte være gode muligheder for – som også forudsat i den citerede K18-bestemmelse – at opnå en forligsmæssig løsning vedrørende et afslag. Tankevækkende er det da også, at køberen i *U 1988.535 H* end ikke havde påstået sig tilkendt et forholdsmæssigt afslag for manglerne ved den leverede PC.

Fra forbrugerklagenævnspraksis kan dog nævnes afgørelsen i *JÅF 1995.168*, hvor et tekstbehandlingssystem var mangelfuldt, idet der brug af visse skriftstyper ikke kunne skrives Ø og ø (et generelt problematisk bogstav i tegnsætsverdenen, fordi tallet 0 også kan angives således). Tekstbehandlingsprogrammet havde kostet 999 kr., og nævnet ydede forbrugeren et skønsmæssigt afslag på 350 kr.

22.5. Hævebeføjelsen

22.5.a. Udgangspunktet

Efter kbl. § 21 kan en part hæve købet, hvis den anden part har gjort sig skyldig i væsentlig forsinkelse. I handelskøb er enhver forsinkelse "væsentlig". Som tidligere nævnt kan denne bestemmelse dog ikke finde anvendelse i aftaler om systemleverancer, der har karakter af entreprise eller bestillingskøb. Det forhold, at den skyldes leverandørers forsinkelse, har ingen betydning, jf. kbl. § 24.

Kundens ret til at ophæve en aftale om køb af IT beror her – som andetsteds i obligationsretten – på, hvilken karakter den leverede ydelse har, og herunder hvilke omkostninger en ophævelse vil påføre leverandøren. Er der tale om *standardprodukter*, der købes "fra hylden", er der ingen grund til at fravige de almindelige regler: Ydelsen kan her leveres tilbage igen i samme omfang som ved overdragelse af fysiske produkter, ved at brugeren fratages den licens, der ligger til grund for hans brugskopiering. Sådanne krav må derimod stilles, hvis der er tale om et *specialudviklet system,* der er skabt specielt til kunden og som repræsenterer en væsentlig indsats, navnlig når denne indsats – som det typisk vil være tilfældet – ikke kan nyttiggøres gennem (gen-)salg til andre kunder. I sådanne tilfælde vil en ophævelse betyde, at leverandørens investering er forspildt.

For køberen af standardudstyr vil en ophævelse ofte indebære, at han kan gå ud på markedet og købe tilsvarende – eller bedre – udstyr til lavere pris. Udsigten til på denne måde at opnå glæde af en deflatorisk prisudvikling for fremtiden, kan gøre det inciterende for en kunde at påberåbe sig, at det leverede lider af en hævebegrundende mangel. Højesterets dom i *U 1988.535 H* antyder dog, at man i sådanne tilfælde ikke kan vente nogen særligt lempelig vurdering af ophævelseskravene.

22.5.b. Væsentlighedsbetingelsen

Det kritiske spørgsmål i læren om ophævelse af IT-kontrakter er spørgsmålet om, hvornår der foreligger en *væsentlig* mangel. For en nærmere indføring i de almindelige krav hertil henvises til *Bryde Andersen & Lookofsky* (2005), s. 207 ff. Kravene hertil beror på, om der er tale om standardvarer eller om systemudvikling.

Standardvarer

U 1988.535 H omhandlede en IBM PC-klon, der var købt i marts 1985 for 20.850 kr. excl. moms og skulle anvendes til en

konsulentopgave, køberen skulle forestå. Manglen bestod i, at PC'en ofte ikke startede, som den skulle. Fejlen identificeredes omsider som forårsaget af elektromagnetiske forstyrrelser forvoldt ved, at køberen havde anbragt skærmen ovenpå centralenheden. Det ville nu koste et mindre beløb (et par hundrede kr.) at foretage den fornødne afskærmning; men køberen – der på tidspunktet for ophævelsen var i stand til at købe tilsvarende udstyr for langt mindre beløb – ønskede at hæve. Der var ingen særlig aftale om kvalitetskrav eller tekniske specifikationer til PC'en. I Sø- og Handelsrettens dom, som stadfæstedes af Højesteret, lagdes det til grund, at det er sædvanligt, at skærme kan anbringes oven på computere, og at køberen uden at dette har været udtalt overfor sælgeren har antaget, at dette også lod sig gøre med hensyn til den købte PC. Imidlertid fandt retten ikke, at dette udgjorde nogen væsentlig mangel ved anlægget. Retten fandt heller ikke grundlag for køberens krav om betaling for fejlfinding.

Dommen tager ikke stilling til, om en køber kan rejse andre krav i sådanne tilfælde. Påstanden gjaldt kun retten til ophævelse, og dommen angår derfor kun dette spørgsmål. Når dommen slår fast, at det er "sædvanligt" at placere en skærm ovenpå computeren, er det nok underforstået, at man har anset systemet for mangelfuldt. Derfor kunne køberen – hvis der var nedlagt påstand herom – nok have rejst krav om forholdsmæssigt afslag, eventuelt udmålt til afskærmningsomkostningerne.

Kompatibilitetsfejl

Om kompatibilitetsmangler er hævebegrundende beror på, hvilken funktion de udfører. At manglende kompatibilitet ikke gør det muligt at opnå maksimal kapacitet fra systemet er som udgangspunkt ikke i sig selv en hævebegrundende mangel, jf. *JÅF 1999.148*. Hvis manglen derimod bevirker, at systemets primære funktioner udebliver eller væsentligt reduceres, nærmer man sig en hævebegrundende situation.

Fejl i brugerinterface

Man har tidligere været afvisende overfor at lade fejl i systemets brugergrænseflade – herunder ringe brugervenlighed – udgøre hævebegrundende mangler. Systembetingede svagheder i programmer vil sjældent være mangler i køberetlig forstand, allerede fordi de alene træder frem i dialogen med brugeren. Et vidtgående – og i dag utvivlsomt *for* vidtgående – eksempel er *ERA 1.104* (VLD 23.5.1984), som fandt, at brugeren ikke kunne anstille forudsætninger om at kunne arbejde med et IT-system med mindre svartider end de konstaterede (op til 26 minutter).

Udbygningsmuligheder

Også en manglende adgang til at kunne udbygge det erhvervede system, kan begrunde en ophævelsesadgang. I *JÅF 1995.159*

havde en forbruger købt en pc, som ifølge aftalen var forsynet med 8 MB RAM. Køberen havde fået det indtryk, at systemet kunne udbygges til 16 MB RAM, hvilket viste sig at være fejlagtigt, og hvilket sælger i øvrigt bestred at have oplyst. Forbrugerklagenævnet fandt imidlertid, at køberen som typeforudsætning havde kunnet forvente, at pc'en kunne udvides med op til 16 MB RAM intern hukommelse som angivet i manualens tekniske specifikationer. Den således konstaterede mangel fandtes væsentlig og hævebegrundende.

Just-in-time

Når der er aftalt levering efter just-in-time-konceptet, taler såvel præventive hensyn som interessen i at sikre den krænkede part oprejsning for at kunne redressere forsinkelser strengt, herunder ved ophævelse. Aftalereguleringen af sådanne transaktioner bør tage højde for tilfælde af *force majeure*, hvor forsinkelsen skyldes udefrakommende forhold eller forhold i virksomheden (herunder overenskomststridige arbejdsnedlæggelser), som denne ikke har indflydelse på. Netop indførelsen af just-in-time-konceptet giver medarbejderkredsen et meget stærkt kort i hænde.

Ved sin dom af 11. januar 1991 (BS 1406/89) fandt Tårnby ret, at leverandørens overskridelse af den sidste frist, kunden havde sat for at få bragt systemet funktionsdygtigt, med 45 minutter, var hævebegrundende. På dette punkt er afgørelsen dog begrundet med, at leverandøren ikke havde bragt systemet i funktionsdygtig stand blot ved sin (45 minutter forsinkede) aflevering af båndet med de nødvendige data. Sagen blev efter tilkendegivelse om stadfæstelse forligt for Østre Landsret.

22.5.c. Hel eller delvis ophævelse?

Når en hævebeføjelse skal gøres gældende, må der tages stilling til, hvilke dele af aftaleforholdet den skal ramme. Reglerne om ophævelse bygger på en forudsætning om, at aftalen er en enhed, som i sig selv fastlægger virkningerne af en ophævelse. Det er imidlertid problematisk at betragte "aftalen" som et systembegreb, hvis afgrænsning skal være afgørende for, hvordan ophævelsens rækkevidde afgrænses. Når virkningen af en ophævelse skal fastlægges, må man frigøre sig fra sådanne begrebsforestillinger og i stedet tage stilling til ophævelsens rækkevidde ud fra en vurdering af aftalens indhold og de beføjede forudsætninger, der ligger bag dens indgåelse, jf. nærmere *Bryde Andersen & Lookofsky* (2005), s. 183 f. *Forudsætningsbetragtninger* fører således i almindelighed til, at en ophævelse i hvert fald bør ramme sådanne ydelser, hvis betydning for realkreditor (kunden) i det væsentlige beror på deres samspil med andre ydelser, som realde-

bitor (leverandøren) præsterer. Eller sagt med et eksempel fra dagligdagen: Fordi den mælk, man køber hos købmanden, er sur, giver det ikke køberen ret til også at hæve købet vedrørende det mangelfrie smør, der blev købt ved samme lejlighed.

Flere afgørelser støtter denne antagelse på IT-kontraktsrettens område. Ved Tårnby Rets utrykte dom af 11. januar 1991 (BS 1406/89) – som efter tilkendegivelse om stadfæstelse blev forligt for Østre Landsret – fik køberen af en computer med tilhørende standardprogrammel ret til at hæve hele købet, da softwareleverancen blev forsinket. I præmisserne lægger retten til grund, at køberen havde været interesseret i programmet, og at dette derfor ikke kunne betragtes som en biydelse til maskinen. Se tilsvarende *JÅF 1993-94.221*, hvor mangler ved et objektiv ikke gav køberen ret til at hæve det samlede køb af kamerahus + objektiv. Afgørelsen er begrundet med, at den pågældende mangel kunne udbedres.

22.5.d. Flere aftalegrundlag

Som grundlag for en IT-overdragelse vil der ofte foreligge flere aftaledokumenter, f.eks. en købsaftale om overdragelse af hardware, en licensaftale om retten til at anvende hertil hørende software, en særskilt vedligeholdelsesaftale, aftaler om genkøb etc. etc. Ganske ofte vil sådanne aftaler være indgået med forskellige parter, f.eks. – som i *U 1985.334 H* – mellem en hovedleverandør og kunden og mellem kunden og en underleverandør af specialprogrammel. Når der indtræder misligholdelse opstår da spørgsmålet om, hvorvidt misligholdelse af ét af disse aftalegrundlag skal få afsmittende betydning for andre.

Mellem parterne

Som nærmere udviklet i *GA* 337 f., kan man i almindelighed ikke finde svaret på sådanne spørgsmål ved blot at fokusere på, om der foreligger en eller flere "aftaler". Retsvirkningerne af en misligholdelse må i stedet fastlægges ud fra en fortolkning af de løfter, som aftalen består af. Når det gælder muligheden for efter omstændighederne at give grundlag for "delvis ophævelse" mv. har domstolene ikke følt sig begrænset af noget generelt princip om "aftalens enhed", se hertil *E&A* s. 340 ff. Også andre dele af kontraktsretten må leve med, at aftaleforhold reguleres af forskellige retsgrundlag (f.eks. entrepriseretten) og nedfældes på forskellige aftaledokumenter (f.eks. ansættelsesretten).

Tilsvarende gælder, når der er tale om at skulle knytte misligholdelsesvirkninger til andre aftaleforhold, sml. bemærkningerne hos *Poul Gade* i U1993B.330, s. 333. Bedømmelsen af dette misligholdelsesspørgsmål kan være vanskeligt at løsrive fra spørgsmålet om aftalefortolkning samt vurderingen af, om afta-

len er gyldig. Dette afgrænsningsproblem har dog generel karakter. Flere afgørelser har således ladet en leverandør bære risikoen for misligholdelse begået af en anden leverandør ved på dette grundlag at lade aftalen bortfalde ud fra synspunkter om bristede forudsætninger, se f.eks. *U 1984.1032 Ø* og *U 1985.334 H*.

22.5.e. Ydelsens tilbagegivelse mv.

Utilbagegivelighed

Muligheden for at ophæve en aftale kan være afskåret, fordi ydelsen er utilbagegivelig. Dette er f.eks. tilfældet, hvis ydelsen består af rådgivning eller der er tale om en brugsrettighed mv., som kunden (realkreditor) har haft glæde af i den forløbne periode. I sådanne tilfælde fører almindelige obligationsretlige regler til, at der alene kan ophæves *for fremtiden*. Hvis kunden ikke har haft glæde af ydelsen i den forløbne periode, f.eks. fordi denne har været behæftet med fatale mangler, må vederlaget for denne periode justeres i nedadgående retning eller efter omstændighederne helt bortfalde.

Det har været drøftet, om det giver mening at tilbagegive information, der ikke har en så fast tilknytning til et medium, at det ikke er praktisk muligt eller meningsfuldt at sikre, at informationen efter tilbagegivelsen effektivt er berøvet den kunde, som fremsætter kravet om ophævelse. Er der tale om *fleksibel information* – f.eks. et råd – ligger det klart, at tilbagegivelse ikke er mulig. Omvendt er det klart, at tilbagegivelse af *integreret information* ingen vanskeligheder volder. Vanskelighederne opstår derimod – som altid – i relation til den *mediekompatible information*, jf. nærmere afsnit 20.2.b. Som her anført må det antages, at leverandøren i kraft af en ophavsret til at råde over eksemplaret af et værk kan gennemtvinge en tilbagetagelse, f.eks. i forbindelse med en ophævelse af aftaleforholdet. Anderledes, hvis der er tale om programmel mv. i *public domain*. Sådanne softwareprodukter må rubriceres på samme måde som fleksibel information: Der kan følgelig ikke ske ophævelse og tilbagegivelse vedrørende denne del af aftalen.

22.6. Erstatningsbeføjelsen

22.6.a. Problemstillingen

I de tilfælde, hvor et krav på naturalopfyldelse ikke kan gennemføres, vil kunden være henvist til at gøre et erstatningsansvar

gældende. Det følger af almindelige regler, at krav på erstatning i kontraktsforhold skal have hjemmel. Denne hjemmel kan enten findes i et *garantisynspunkt*, altså en betragtning om, at den ansvarlige har lovet at yde erstatning (se herom afsnit 22.6.b.), ud fra den tanke, at den ansvarlige har handlet *culpøst* (se herom afsnit 22.6.c.) eller på grundlag af særlig *lovhjemmel* (se herom afsnit 22.6.d.).

22.6.b. Garantisynspunktet

Når leverandørens erstatningsansvar efter garantisynspunktet drøftes er det væsentligt at pege på, at IT-branchen udfolder sig under en massiv og mangeårig tradition for leverandør-ansvarsfraskrivelser. De situationer, hvor garantisynspunktet har betydning, er derfor afgrænset til tilfælde, hvor der ingen udtrykkelig aftale foreligger (det kan f.eks. være tilfældet i relation til IT-konsulenter og i forbrugerkøb), eller hvor aftale foreligger, men hvor ansvaret for det pågældende tab ikke er fraskrevet (hvilket er tilfældet i K18, pkt. 16, der gør leverandøren erstatningsansvarlig over for kunden efter dansk rets almindelige regler).

Denne massive tradition for ansvarsfraskrivelser må spille ind, når der rejses spørgsmål ved, om leverandøren stiltiende kan siges at have indestået på en sådan måde for systemets funktionalitet, at et erstatningsansvar kommer på tale, sml. herved kbl. § 42, stk. 2, der åbner op for et ansvar, når en egenskab "må anses for tilsikret". Betragtningen fører dog til, at leverandøren af en komponent, der ved indbygning i et system beskadiger andre komponenter, er objektivt ansvarlig for de således opståede tab, jf. hertil *JÅF 1999.150*, der ved at give kunden ret til refusion af leverandørens reparationsregning, da en bærbar pc blev beskadiget, efter at remmen til den medfølgende taske var knækket. Se også afgørelsen *Forbrugerjura 2003.102 ff.* hvor forbrugeren havde forsøgt at opdatere den firmware, der hørte til et digitalkamera, ved at hente et opdateringsprogram via producentens hjemmeside. Opdateringen mislykkedes, idet kun en del af opgraderingsfilen blev kopieret ind til kameraets CF-kort, hvorefter kameraet blev funktionsudygtigt. Forbrugerklagenævnet lagde til grund, at kameraet var blevet beskadiget under opdateringen "som følge af manglende driftssikkerhed ved producentens opdateringsprogram, som således må antages at have været fejlbehæftet". Producentens forbehold om, at opdateringen skete "for kundens egen regning og risiko" indebar ikke en accept af risikoen for

sådanne tab. Producenten blev derfor pålagt pligt til at betale erstatning for en anslået reparationspris på 3061 kr.

Se tilsvarende *U 1988.803 V* om et stålrør, der skulle monteres i en lastvognskran, hvor det påførte kranens cylinder skader. Da leverandøren fandtes at have givet tilsikring om rørets pasform, fandtes han erstatningspligtig herfor.

Problemet har dog næppe den store praktiske betydning i relation til de praktisk nok så væsentlige tilfælde af datatab, eftersom skader af den nævnte karakter almindeligvis vil kunne afbødes gennem sædvanlig sikkerhedskopiering af programmer og data.

22.6.c. Culpabetragtninger

For det andet kan et erstatningsansvar komme på tale, hvis det kan siges at være culpøst, at leverandøren ikke præsterer aftalt ydelse, og denne misligholdelse påfører brugeren et tab. Når den tabsudløsende faktor er selve misligholdelsen (der f.eks. kan påføre kunden et tab svarende til en genanskaffelsesværdi el.lign.) antages det, at der må anlægges en skærpet culpavurdering (såkaldt kontraktsculpa). Dette ansvar vil bl.a. få betydning ved forsinkelse af standardkomponenter.

22.6.d. Lovhjemmel

Der er ikke hjemmel til at gøre IT-leverandører erstatningsansvarlige på andet grundlag end culpa og tilsikring for ikke-opfyldelse af en leverance. I det omfang købeloven gælder, og ydelsen har karakter af genus, kan et strikt ansvar baseres på kbl. § 24, sml. herved *JÅF 1999.140*, hvor Forbrugerklagenævnet gjorde leverandøren ansvarlig efter denne bestemmelse i en situation, hvor levering af RAM-kort til en computer var blevet vanskeliggjort som følge af jordskælvet i Taiwan den 21. september 1999. Det bemærkes i den forbindelse, at programmel, som leverandøren skal udvikle, ikke har karakter af genus, se modsat *Nørager-Nielsen* (1987), bl.a. s. 104 f. og 135 ff.

Et genusansvar for forsinkelse af den slags ydelser er heller ikke antaget, hverken i domspraksis eller i litteraturen, jf. i samme retning *Christophersen & Føyen* (1981), s. 318. At retsstillingen muligvis er en anden i entrepriseretten, kan ikke tillægges afgørende vægt.

22.7. Bortfald af misligholdelsesbeføjelser

22.7.a. For sen reklamation mv.

I almindelighed gælder det, at undladt reklamation vil afskære køberen fra at gøre en misligholdelsesbeføjelse gældende. Som udgangspunkt skal meddelelse om reklamation fremsættes overfor den part, der er aftaleretligt forpligtet til at levere rigtig ydelse. Er det derimod aftalt eller forudsat, at mangler ved ydelsen skal afhjælpes af en tredjepart – typisk producenten – kan reklamation dog fremsættes overfor denne, hvis dette sker som led i en aftalt eller forudsat afhjælpningsforanstaltning. Denne regel er udtrykkeligt fastsat i forbrugerkøb, jf. kbl. § 84 og *JÅF 1999.147*.

Frist

Retspraksis kan ikke siges at have etableret klare regler for, hvornår der bør reklameres i IT-køb. *ERA 3.57* (Rudkøbing ret, 13.6.86) anerkender en reklamation som rettidig, selv om den fremkom ca. 7 måneder efter, at manglen havde vist sig. *ERA 3.71* (Holsted byret 26.9.1986) afskar derimod ophævelse, fordi køberen havde været passiv i 1½ måned.

Nachfrist

Fordi der ofte vil være usikkerhed om kravene til ydelsen, kan det være rimeligt at betinge misligholdelsesbeføjelserne af, at kunden giver meddelelse til leverandøren om, at han vil gøre hævebeføjelsen gældende, hvis ikke leverandøren har rettet op på det pågældende forhold inden en bestemt frist, såkaldt *Nachfrist*. En sådan forpligtelse kræver som udgangspunkt hjemmel i aftalen; men enkelte forfattere har argumenteret for, at kravet kan opstilles på almindeligt grundlag, se *Bender & Bruun Nielsen* (1989), der til støtte herfor henviser til *ERA 2.131* (VLD 17.3.1986), hvor ophævelse blev nægtet i en situation, hvor nachfrist ikke var afgivet. Præmisserne sammenkæder ikke udtrykkeligt disse to forhold, men det er nærliggende at antage, at en meddelt Nachfrist kunne have ændret vurderingen. En udtrykkelig regel af dette indhold findes i ESF's totalkontrakt vedrørende levering, installation og vedligeholdelse af et IT-system, pkt. 5.4.6. Regler om nachfrist kan undertiden opstilles på alment grundlag, se nærmere *Bryde Andersen & Lookofsky* (2005), s. 221 ff. Særskilte regler herom findes i CISG art. 47 og 49.

22.7.b. Leverandørens afhjælpningsret

Efter dansk ret kan leverandøren som hovedregel ikke smyge virkningerne af en misligholdelse af sig ved at afhjælpe mangler, der viser sig efter leveringstidspunktet. Efter kbl. § 49 skal køberen kun finde sig i en afhjælpning, der kan gennemføres inden den tid, hvor levering skulle være sket. Dermed er afhjælpningsmulighederne begrænset til de situationer, hvor der leveres før det aftalte tidspunkt, eller hvor leveringsfristen anses for udskudt.

Denne hovedregel medfører ofte urimelige konsekvenser på IT-området. Navnlig når det leverede skal fungere i sammenhæng med andre systemkomponenter, kan det være vanskeligt – om overhovedet muligt – for leverandøren at overskue, om bestemte egenskaber vil udmønte sig i fejl under brugen. Dernæst vil der ofte være misforhold mellem årsagen til fejlen og følgerne af en ophævelse, ligesom mulige erstatningskrav mod leverandøren i talrige tilfælde er ude af proportion med den omkostning, der vil være forbundet med yderligere afhjælpningsforsøg fra leverandørens side.

IT-området

Af disse grunde synes der at være enighed om, at leverandøren af et IT-system, der skal udvikles som led i aftalen, har en i forhold til andre leverandører udvidet *afhjælpningsret*, altså at leverandøren kan afværge de misligholdelsesbeføjelser (herunder navnlig krav om ophævelse og erstatning), der ellers ville tilkomme brugeren, ved inden for rimelig tid at afhjælpe mangler. En sådan udvidet afhjælpningsret antages således af *Nørager-Nielsen* (1987), s. 213 f., *Bruun Nielsen* i Bryde Andersen (1987), s. 69, *Bender & Bruun Nielsen* (1989), s. 32 f. og *Christophersen & Føyen* (1981), s. 306 f. Det springende punkt er herefter, hvad der skal betragtes som "rimelig tid" til denne afhjælpning. Fra domspraksis kan nævnes dommen i *U 1952.534 H*, der gav ret til ophævelse ved væsentlige mangler, der ikke var afhjulpet inden for en periode på ca. 1 1/4 år, og *U 1974.557 SH*, der antog, at leverandøren af et integreret bogholderisystem til en vekselervirksomhed måtte tåle en ophævelse, da det efter adskillige servicebesøg over en periode af 3 måneder ikke var lykkedes for ham at bringe anlægget i funktionsdygtig stand.

Varighed

Udover at afhjælpningen skal kunne ske inden rimelig tid, skal den kunne ske uden væsentlig ulempe for kunden. Når dette kriterium afgrænses er man nødt til at forholde sig til den enkelte udviklingsydelse og de omstændigheder, der ledsager den. Ofte vil parterne i løbet af et udviklingsforløb lægge den underskrevne

kontrakt i skuffen i mere end én forstand og indgå efterfølgende – udtrykkelige eller stiltiende – aftaler, der reelt indebærer, at en aftalt produktleverance forvandler sig til en aftale om systemudvikling. Foreligger sådanne efterfølgende dispositioner kan kunden ikke uden videre vende tilbage til den oprindelige aftale og fastholde dens terminer mv.

Herudover har det betydning, hvilken type mangel der er tale om, og hvilken udsigt der er til at opnå udbedring. Er der f.eks. tale om et nyt og uprøvet system, som brugeren ved, at leverandøren helt eller delvis skal udvikle som led i sin opfyldelse af aftalen, må man utvivlsomt efterlade et større spillerum for leverandøren til at rette mangler, jf. *Torvund* (1997), s. 202, med henvisning til bl.a. dommen i *Rt. 1935.497*.

Komponenter mv.

Det er tvivlsomt, om en tilsvarende afhjælpningsret også gælder for leverandøren af en fysisk IT-komponent. Som anført i afsnit 22.3.b er det hyppigt forekommende, at selv markedsdominerende standardsystemer er behæftet med fejl, hvoraf nogle måske vil blive afhjulpet i senere *versioner*. Om leverandøren af et sådant produkt kan vise et mangelsansvar fra sig under henvisning til, at fejlen vil være rettet i en efterfølgende version, beror selvsagt på indholdet af den indgåede aftale. Udenfor tilfælde, hvor der foreligger en sådan aftale, eller en i øvrigt forpligtende sædvane, er retsstillingen forholdsvis klar: Er produktet mangelfuldt på det tidspunkt, hvor leverandøren skulle præstere rigtig opfyldelse, kan kunden gøre mangelsindsigelse gældende uanset udsigten til, at en fejl mv. vil blive rettet ved en efterfølgende opdatering. Det vanskelige spørgsmål er, om udsigten til, at en fejl rettes i næste opdatering, kan få betydning for selve mangelsvurderingen, f.eks. således at der stilles strengere krav for at anse produktet for mangelfuldt. Det er vanskeligt at nå til et sådant resultat på alment grundlag.

Torvund (1997), s. 88, diskuterer, om kunden bør betale for nye versioner af et program, som alene indeholder fejlrettelser. Under henvisning til, at et program i praksis altid indeholder fejl, når han til, at det i sådanne tilfælde ikke vil være urimeligt at lade kunden afholde distributionsomkostningerne. Som ligeledes anført kan spørgsmålet være vanskeligt at håndtere i praksis, når programopdateringer både indeholder fejlrettelser og nye funktioner.

Udskiftning

I visse aftaler betinger leverandøren sig at kunne udskifte det leverede udstyr med andet udstyr af tilsvarende karakter. Den slags bestemmelser kan være rimelige, navnlig hvis udskiftningen sker i forbindelse med en almindelig opgradering af syste-

met. Det kan dog være risikabelt at give leverandøren ret til at substituere ydelser, der beskrives efter *betegnelse,* idet leverandøren dermed ikke har påtaget sig noget ansvar for den specifikke funktion, kunden efterspørger. En opgradering til en ny processor kan f.eks. medføre problemer med systemets kompatibilitet til interne eller eksterne enheder, som brugeren næppe i almindelighed har pligt til at tåle.

Erstatning

At leverandøren har ret til afhjælpning fritager ham ikke fra pligt til at betale erstatning for det tab, misligholdelsen påfører køberen, herunder tab som følge af selve afhjælpningshandlingen. Ligeledes må afhjælpningen ske på en måde, der funktionelt stiller køberen på samme måde som, hvis ydelsen ikke havde været mangelfuld. I Forbrugerklagenævnets afgørelse i *JÅF 1996.109* blev leverandøren således pålagt pligt til at geninstallere de programmer, køberen havde installeret på en harddisk, der viste sig mangelfuld.

22.7.c. Kundens egne afhjælpningsforsøg

Når kunden har krav på, at leverandøren afhjælper opståede fejl, er det almindeligt at aftale, at denne afhjælpningsret bortfalder, hvis kunden selv har foretaget rettelser eller ændringer i systemet. En sådan begrænsning er navnlig naturlig i relation til afhjælpning af fejl i programmer. Ved at (udvikle og) vedligeholde et program opbygger en leverandør et detaljeret kendskab til systemet. Hvis andre ændrer i systemet, ødelægges eller ændres måske afgørende detaljer og dermed leverandørens muligheder for at kunne vedligeholde.

Tilsvarende kan det forhold, at kunden anvender uoriginale reservedele i forbindelse med den almindelige brug, efter omstændighederne fratage kunden en misligholdelsesbeføjelse. Forudsætningen herfor er dog, at der kan påvises funktionelle vanskeligheder med at anvende den uoriginale reservedel mv., jf. hertil *JÅF 1998.116* om uoriginalt blæk til en printer.

22.7.d. Leverandørens ansvarsfraskrivelse

Som følge af de mange risici, der består for, at et IT-projekt ikke forløber som ventet – hvad enten dette går ud på udvikling eller overdragelse af IT – er der praksis for, at leverandører fraskriver sig ansvar for misligholdelse. Ansvarsfraskrivelserne forekommer dels som *maskinklausuler*, der begrænser køberens beføjel-

ser til alene at udgøre krav på afhjælpning mv. (jf. nærmere *Bryde Andersen & Lookofsky* (2005), afsnit 8.4.e.), dels som begrænsninger i *ansvarets omfang*, hvorved leverandøren i alle tilfælde alene pålægges ansvar for et maksimumbeløb (f.eks. kontraktssummen) og i alle tilfælde således, at der ikke er ansvar for driftstab og andre afledte tab.

Hvor klausuler af den sidstnævnte karakter nyder almindelig udbredelse i de fleste kommercielle aftaleforhold, kan man umiddelbart undre sig over, at den tekniske udvikling mod stadigt mere stabile systemer ikke har ført til en aftalepraksis, hvorefter leverandører i højere grad står inde for de leverede systemer. En praksis for ansvarsfraskrivelse kan være forståelig i en teknisk pionerperiode, hvor der er usikkerhed om ydelsens tekniske formåen, men hører ikke hjemme i et fuldt udviklet teknologisk miljø, hvor ydelsen markedsføres mod den almindelige forbruger. At aftalepraksis imidlertid befinder sig på niveau med den, man finder inden for maskinindustrien og på entrepriseområdet, skyldes den almindelige vanskelighed, producenterne har med at overskue systemernes funktionalitet i det praktiske brugsmiljø, sml. herom i afsnit 2.1.a. om det såkaldte *Vico*-paradoks. Informationssystemer kan opfylde vidt forskellige typer af opgaver, og deres funktionalitet beror i høj grad på, hvilken konfiguration og hvilken praktisk brugssituation de optræder i. Allerede de bevismæssige vanskeligheder ved at skulle afklare, hvem – blandt flere mulige – der har ansvar for en specifik mangel eller uregelmæssighed får naturligt leverandørerne til at vige tilbage for retligt forpligtende indeståelser. At det – fortsat – forholder sig således illustreres ved de drøftelser, man havde omkring årtusindskiftet om leverandørernes hæftelse for mangler, der kunne henføres til, at systemerne ikke kunne gå fra "99" til "00". Trods ihærdige anstrengelser fra Forskningsministeriets side om at få branchen til at acceptere et særligt "2000 Parat"-mærke, var det kun ganske få leverandører, der tilsluttede sig dette mærke og dets erklæringer (der ikke indebar nogen form for garanti) om, at det mærkede system kunne klare denne kritiske datohåndtering.

Udgangspunkt

Sådanne aftaler om ansvarsfraskrivelse er som udgangspunkt gyldige, jf. nærmere *Bryde Andersen & Lookofsky* (2005), s. 396 ff. I overensstemmelse med koncipistreglen fortolkes ansvarsfraskrivelser ofte indskrænkende.

- objektivt omfang

Denne fortolkningsstil slår for det første igennem i fortolkningen af klausulens objektive omfang. I *U 1975.339 SH* ansås en fejlagtig rådgivning således ikke at være omfattet af en ansvarsbegrænsning og tilsvarende *U 1986.938 SH*, *U 1974.557 SH* og *ERA 3.48* (KB 10.6.1986), der begge bortfortolkede ansvarsregulerende klausuler.

I samme kategori af "brugervenlige" domstolsfortolkninger er dommen i *U 1984.1032 Ø*, der antog, at et leasingselskab var

nærmere til at bære risikoen for leverandørens misligholdelse end brugeren.

- subjektivt omfang

Dernæst er domstolene tilbageholdende med at fortolke vidtgående ansvarsfraskrivelser efter deres ordlyd i tilfælde, hvor det ligger klart, at der foreligger subjektiv skyld fra realdebitors side. Dette princip er første gang slået fast i den klassiske dom om flyttefirmaet ADAM, *U 1929.707 H*. På IT-området kan *U 1974.557 SH*, der ikke lod en ansvarsfraskrivelse fritage leverandøren for erstatningsansvar i tilfælde, hvor en opstået mangel ikke blev afhjulpet inden for rimelig tid (3 måneder efter), ses som udtryk for samme tanke.

Maskinklausuler

Med sine umiddelbare lighedspunkter med maskinområdet er det ikke overraskende, at der ofte forekommer maskinklausuler i IT-kontrakter. Sådanne klausuler fortolkes normalt indskrænkende, hvis leverandøren misligholder sin afhjælpningspligt, se *Bryde Andersen & Lookofsky* (2005), 401 ff. og til illustration dommen i *U 1986.654 H*, hvor en ansvarsfraskrivelse ikke fandtes at være gældende, efter at leverandøren af et sprøjtestøbeværktøj til en *beauty box* forgæves havde forsøgt at udbedre mangler gennem mere end et halvt år.

Afleveringsprøven

Et særligt spørgsmål er det, om kundens positive tilkendegivelser i forbindelse med gennemgåelse af afleveringsprøven indebærer et frafald af mangelsbeføjelser. Udgangspunktet er her, at de meldinger kunden – eller den for kunden befuldmægtigede (f.eks. en IT-konsulent) – afgiver herom, er forpligtende, men at enhver melding må fortolkes i lyset af det grundlag, hvorpå den afgives. Godkender man en afleveringsprøve, dækker denne godkendelse som udgangspunkt kun de fejl, som burde være opdaget i forbindelse med afleveringsprøven.

Spørgsmålet gør sig modsvarende gældende for leverandøren. Hvis leverandøren forudgående har godkendt det installationssted, hvorpå systemet skal installeres, kan leverandøren som udgangspunkt ikke kræve betaling for de meromkostninger, som kunne være undgået ved en mere nøje gennemgang af installationsstedet, jf. *Torvund* (1997), s. 99 f. Men viser installationsstedet sig at byde på uventede vanskeligheder for gennemførelsen af leverancen, kan denne godkendelse ikke i sig selv indebære et afkald på retten til at gøre krav herom gældende, f.eks. dækning af ekstra omkostninger i forbindelse med istandsættelse eller krav om udskydelse af tidsplanen.

22.7.e. Andre tilfælde

Undladt opfølgning

Når en misligholdelsesbeføjelse gøres gældende, har kunden en vis pligt til at følge op på den. Undlader han det, og fortsætter leverandøren sine præstations- eller afhjælpningsbestræbelser, må man ofte nå til, at kunden har frafaldet sin ret til at gøre den konstaterede misligholdelse gældende. Tilsvarende er kunden bundet af det tilsagn, han måtte have afgivet til leverandøren om ret til yderligere afhjælpningsforsøg. I *JÅF 1998.154* kunne en forbruger f.eks. ikke hæve købet vedrørende en bil, da han efter 12 afhjælpningsforsøg havde givet leverandøren ret til at foretage endnu ét.

Undladt backup

Når leverandørens misligholdelse, f.eks. som følge af mangler eller skadegørende handlinger, forvolder tab af data hos brugeren, og brugeren ikke har dækket sig ind herimod gennem sikkerhedskopiering, opstår spørgsmålet om det faktisk lidte tab skal erstattes fuldt ud, eller om brugeren selv må tåle en afkortning i tabet, der fører til en erstatning svarende til det tab, der ville være lidt, hvis brugeren havde foretaget en sædvanlig sikkerhedskopiering. Som anført i afsnit 18.2.a. må det som udgangspunkt antages, at skadelidtes tab som følge af tab af data må reduceres til et normaltab, hvis den manglende kopiering kan bebrejdes brugeren som culpøs.

Ifølge et responsum fra interesseorganisationen HTS (tidligere Handelskammmeret), trykt i Advokaten 9/2003, s. 252, er der kutyme i IT-branchen for, at en transportør/edb-tekniker sikrer sig, at kunden har taget back-up. Der er ikke i branchen kutyme for, at transportøren/edb-teknikeren udfører et "dump" af data fra serveren til en i forvejen tilsluttet arbejdsstation. Ej heller kan der konstateres en sædvane for anden sikring forinden fysisk transport – dog bør denne foregå i henhold til producentens anvisninger.

I Forbrugerklagenævnets afgørelse i *Forbrugerredegørelsen 2002-2003.168* fandtes den erhvervsdrivende erstatningsansvarlig for i forbindelse med reparation af forbrugerens PC (der var ramt af virus) at have slettet et program til bevarelse af data med den virkning, at forbrugerens data gik tabt. Forbrugeren fik følgelig tilkendt tilbagebetaling af vederlaget for reparationen samt erstatning på 900 kr. til geninstallering af et nyt program som det slettede.

Det andet spørgsmål, der falder i nær forlængelse heraf, er om den leverandør, der udfører servicearbejde på brugerens udstyr, under omstændigheder, hvor det må fremstå som muligt, at der

indtræder datatab, i almindelighed har pligt til at sikre sig, at der sker sikkerhedskopiering af data.

Nicolai Dragsted (2000), s. 36 (enslydende side i begge værkets bind), antager, at en sådan pligt består generelt. Se modsat *Ole Horsfelt* i Advokaten 2000.262, der antager, at pligten alene er gældende, hvis leverandøren må indse, at arbejdet vil rumme særlige farer for kunden. Da leverandøren som den sagkyndige utvivlsomt må bære risikoen for, at den nævnte faremulighed består, er forskellen mellem de to opfattelser dog næppe mærkbar, og for de fleste praktiske formål må det således antages, at leverandøren har pligt til at sikre sig, at der er sket fornøden sikkerhedskopiering.

Supplerende litteratur

Der henvises i det hele til litteraturoversigten i slutningen af kapitel 21.

Kapitel 23. KONFLIKTLØSNING

23.1. Domstolsprocessen

23.1.a. National domstolskompetence

Stedlig kompetence

Ifølge rpl. § 235 skal retssager som udgangspunkt anlægges ved sagsøgtes hjemting, dvs. hvor sagsøgte har bopæl, medmindre andet er bestemt ved lov. Forretningsdrivende kan sagsøges på det sted, hvorfra virksomheden udøves, jf. § 237. Man kan i den forbindelse rejse det spørgsmål, hvor "stedet" for en virksomhed, der udøves fra nettet, befinder sig, f.eks. når virksomheden udøver sine aktiviteter fra en hjemmeside.

Denne tvivl bør dog ikke være stor. Uanset den "grænseløshed", der præger Internet, må det være udgangspunktet, at det er virksomhedens *fysiske* tilstedeværelse i form af kontor, placering af medarbejdere og driftsfunktioner, der er afgørende for jurisdiktionsspørgsmålet. Lod man placeringen af serveren for den hjemmeside, hvorfra virksomheden giver sig tilkende overfor omverdenen, være afgørende, ville man reelt kunne ophæve kravet om stedlig tilknytning. Det er således både ukompliceret og ofte omkostningsfrit at flytte serviceringen af en hjemmeside fra en server til en anden, og med nutidens muligheder for effektiv og billig telekommunikation, er der sjældent nævneværdige tekniske fordele forbundet ved at have en server placeret tæt på den virksomhed, hvorfra den primære drift udøves. Et server-kriterium ville i øvrigt også volde vanskeligheder i tilfælde, hvor en virksomhed benytter forskelligt udstyr til forskellige former for servicering – f.eks. e-mail service på én maskine og www-service på en anden.

Problemet opstår også i relation til det internationale lovvalg. At en hjemmeside optræder under et ccTLD-*topleveldomænenavn*, der hører til et bestemt land, skaber ikke nødvendigvis nogen tilknytning til det pågældende land, se herom afsnit 11.4, hvor de forskellige regler for administration af domænenavne er forklaret. Tværtimod er der talrige eksempler på, at domænenavne, der formelt er tilknyttet eksotiske himmelstrøg, opnår en be-

tydelig søgning for bestemte typer af virksomheder, der intet har at gøre med den pågældende lokalitet.

Eksempler herpå er ccTLD-domænet "NU" (for det lille ørige Niue) og "TM" (for Turkmenistan), og som kan give det indtryk, at et domæne registreret herunder dermed har status som varemærke (TM = Trademark). NU-domænet er særligt benyttet af svenske virksomheder, der herigennem kan få en tilstedeværelse på nettet uanset de restriktive regler for registrering af domænenavne under .se-domænet.

Saglig kompetence

Sager mellem private parter skal som udgangspunkt anlægges ved de almindelige domstole. Retsplejeloven foreskriver ingen særregler om sager, der beror på en særlig indsigt af teknisk eller anden karakter. Sådanne særregler findes kun på ganske enkelte områder; se f.eks. rpl. § 6, stk. 5, om søsager og § 125 i lov om social service om tvangsfjernelsessager mv.

SHR

En vis, begrænset, mulighed for at inddrage IT-sagkundskab i det dømmende kollegium foreligger, når sagen anlægges ved Sø- og Handelsretten. Det er dog væsentligt at slå fast, at lægdommerelementet i Sø- og Handelsretssager ikke er begrundet med ønsket om at opnå *teknisk* indsigt. I sager om handelsforhold er lægdommerne typisk repræsentanter for forbruger- og erhvervsinteresser, og sagsførelsen indebærer derfor ingen egentlig særlig teknisk prøvelse i dommerpanelet. Erfaringsmæssigt forsøger Sø- og Handelsretten dog at udmelde lægdommere, der har forudsætninger for at forstå den involverede teknik, når sagen berører tekniske områder.

For at kunne anlægge en sag ved Sø- og Handelsretten kræves for det første, at sagen har værneting i hovedstadsområdet i kraft af de almindelige regler, jf. nærmere rpl. § 9, stk. 2, eller i kraft af aftale, jf. § 9, stk. 5. Dernæst skal kravet være på mere end 100.000 kr. (§ 9, stk. 4). Hertil knytter sig det grundlæggende krav, at fagkundskab til handelsforhold skønnes at være af betydning. Ved afgørelsen af, om en sag er en sø- eller handelssag, skal der efter bestemmelsen tages særligt hensyn til, om parterne ønsker, at retten skal tiltrædes af sagkyndige medlemmer. Selv i disse tilfælde vil det dog være hovedreglen, at også sø- og handelssager skal oplyses som andre sager, f.eks. ved syn og skøn.

23.1.b. Internationalt værneting

Udgangspunktet

Reglerne om domstolenes internationale kompetence frembyder en kompliceret struktur, der gennemgås nærmere i faget IP-ret. Valget af forum for en retssag afføder nogle virkninger, som kan få uventet stor betydning for sagens forløb. For det første indebærer forumvalget en stillingtagen til, hvilke regler om *internatio-*

nal privatret der skal være gældende, dvs. hermed en foregribelse af, hvilket regelsæt der skal lægges til grund for afgørelsen. For det andet tillader retsplejeordningen i visse stater (herunder USA) brug af *oplysningsmidler*, som kan forekomme fremmedartede for en dansk tankegang. Et eksempel herpå er de regler om *discovery*, der er hjemmel til efter Federal Rules of Civil Procedure, jf. nærmere neden for under 23.4.d.

For så vidt angår de danske domstoles kompetence i internationale sager gælder reglerne i rpl. §§ 246-247. Af § 246 fremgår det, at sager mod personer, selskaber, foreninger, private institutioner og andre sammenslutninger, der ikke har hjemting i Danmark, kan anlægges her i landet, for så vidt der er kompetence hertil efter reglerne i §§ 237, 238, stk. 2, 241, 242, 243 og 245. Således følger det af rpl. § 247, at sager, der er omfattet af en konvention, som er gennemført i dansk ret ved lov om EF-domskonventionen mv. (herunder ved bekendtgørelse i medfør af den nævnte lovs § 15), reguleres af værnetingsreglerne for den pågældende konvention.

Forbrugersager

I sager om forbrugeraftaler gælder den særlige regel, at forbrugeren kan anlægge sagen mod den udenlandske virksomhed ved sit eget hjemting, "såfremt fremsættelsen af *særligt tilbud eller reklamering* i Danmark er gået forud for aftalens indgåelse og forbrugeren her i landet har foretaget de dispositioner, der er nødvendige til indgåelse af aftalen", jf. rpl. § 246, stk. 1, 2. pkt. Bestemmelsen giver anledning til en del tvivl, navnlig i relation til markedsføring på Internet, der ofte sker til et globalt publikum ved brug af et sprog, der nyder vid international udbredelse (typisk engelsk).

Begrebet "reklame" tager almindeligvis sigte på handlinger, der har karakter af opsøgende informationsvirksomhed, der tager sigte på salg mv., sml. definitionen i rådsdirektivet om reklame for humanmedicinske lægemidler (92/28), art. 1, stk. 3. Det kan imidlertid være vanskeligt at opretholde en forestilling om, at der udøves en sådan form for opsøgende virksomhed i relation til enhver bruger, der er forbundet med Internet. For at antage, at en reklamering i et fremmed land tager sigte på danske forbrugere, må der formentlig kræves en yderligere aktiv indsats end blot dette, at information fra det fremmede land kan nås via Internet fra forbrugere i Danmark. En sådan yderligere indsats kan f.eks. bestå i, at den fremmede erhvervsdrivende ved annoncering i Danmark henviser til den hjemmeside, hvorpå yderligere information kan nås, eller ved at man aktivt etablerer hypertekst-for-

bindelser til den fremmede hjemmeside. Se hertil *Wallberg* i U2000B.132 f.

Når en hjemmeside befinder sig under .dk-topdomænet vil der i almindelighed bestå en formodning for, at det retter sig mod danske brugere. Denne formodning gælder også, selv om webannoncen dækker over en link, der bringer brugeren i kontakt med en server, der befinder sig i en anden jurisdiktion. En tilsvarende formodning for anvendelsen af dansk ret gælder, når den pågældende hjemmeside befinder sig under et *g*TLD (i praksis .com, .net eller .org) eller et *cc*TLD, der rummer associationer til ord, der optræder i det danske sprog (f.eks. .nu eller .tv), såfremt hjemmesiden indeholder information *på dansk*. Valget af dette sprog, der netop kendetegnes ved kun at være udbredt i (Syd)Danmark, rummer en nærmest uafviselig markering af, at der sigtes mod danske forbrugere.

Flere amerikanske afgørelser har i relation til valget mellem delstatslovgivninger forudsat en modsat regel. Ved dommen i *CompuServe Inc. v. Patterson* (89 F.3rd 1257, 6th. cir. 1996) fandt appelretten for 6th circuit, at en Mr. Patterson, der som forfatter af et edb-program havde indgået aftale med CompuServe om dette firmas distribution af programmet, var undergivet jurisdiktion i Ohio, selvom Patterson ikke fysisk havde været tilstede her. Aftalen var indgået som en såkaldt *point-and-click*-aftale via en server, der stod i Ohio. Retten baserede sin afgørelse på en integreret vurdering, der tog en række forhold i betragtning, herunder det forhold, at sagsøgte havde placeret sin software på serveren i Ohio, hvorpå han ligeledes havde indgået aftale med CompuServe. Ligeledes spillede det en rolle, at Mr. Patterson var professionel bruger af Internet. Man kan formentlig betragte dette ræsonnement således, at Mr. Patterson dermed måtte antages at have accepteret den særlige form for "tilstedeværelse", dette medium giver mulighed for. Retten fandt derimod ikke, at Mr. Patterson var undergivet jurisdiktion i alle de stater, hvor hans programpakke blev solgt. Se ligeledes *McDonough v. Fallon McElligott* (S.D. Calif, 1996) og *Inset Systems v. Instruction Set Inc.* (Dist.C. Conn.).

De førnævnte regler gælder generelt, uanset hvilken nationalitet den udenlandske part har. De viger imidlertid for de særlige regler, der følger af konventionsregulering, bl.a. inden for EU, jf. nærmere *Lookofsky*: International privatret, 3. udg. (2004), kapitel 2.

Med rådsforordning nr. 44/2001 af 22. december 2000 (EFT 2000 L 12/1) om retternes kompetence og om anerkendelse og fuldbyrdelse af retsafgørelser på det civil- og handelsretlige område er *Bruxelles-konventionen* om retternes kompetence og om fuldbyrdelse af retsafgørelser i borgerlige sager erstattet med en forordning med

umiddelbar anvendelighed (dog ikke for Danmarks vedkommende, se præamblens pkt. 22, der opretholder Bruxelles-konventionen i forholdet mellem Danmark og de EU-medlemsstater, der er bundet af forordningen). Forordningen svarer i hovedsagen til konventionen; men på enkelte punkter er der væsentlige forskelle. Således fremgår det af art. 15, stk. 1, litra c), jf. art. 16, at en forbruger har ret til at anlægge sag mod den erhvervsdrivende ved sit eget hjemting under visse nærmere betingelser. Denne bestemmelse har været kraftigt kritiseret fra erhvervsside. Forslaget til forordningen, der træder i kraft den 1. marts 2002, er fremsat i KOM(1999) 348 endelig udg.

23.1.c. Internationalt lovvalg

Spørgsmålet om, hvilket lands ret der skal lægges til grund for prøvelsen af en retlig uoverensstemmelse, beror på, hvilket regelsæt den pågældende sag skal bedømmes efter. De problemer herom, der har størst praktisk betydning i relation til den elektroniske handel, falder inden for to hovedgrupper. Den ene hovedgruppe angår lovvalget i kontraktsforhold, hvor den internationale privatrets almindelige regler indgår i et tæt samspil med de konventionsløsninger, der er nået inden for særlige sagsområder. Den anden gruppe drejer sig om de tilfælde, hvor der i lovgivningen er indført særlige regler, som beskytter en part mod en uønsket form for markedsføring, registrering eller anden brug af digital teknologi.

Rom-konventionen

I sager mellem parter domicileret inden for EU/EØS gælder Rom-konventionen om hvilken lov der skal anvendes på kontraktlige forpligtelser mv. (80/934/EØF), jf. lov nr. 188 af 9. maj 1984. Konventionen gælder kun for kontraktsforpligtelser. Uden for EU-området gælder stedets IP-retlige regler.

- aftale

Ifølge hovedreglen i konventionens art. 3 er en aftale underkastet den lov, parterne har vedtaget. Lovvalget skal være udtrykkeligt eller fremgå med rimelig sikkerhed af kontraktens bestemmelser eller omstændighederne i øvrigt.

- nærmeste tilknytning

I det omfang, der ikke er truffet gyldig aftale om lovvalget, gælder art. 4, stk. 1, hvorefter aftalen skal være underkastet loven i det land, som den har sin nærmeste tilknytning til. Der opstilles her en formodning for, at aftalen har den nærmeste tilknytning til det land, hvor den part, som skal præstere "den for aftalen karakteristiske ydelse", havde domicil på tidspunktet for aftalens indgåelse. Således fandt *U 2002.1370 ØLK*, at en sag om betaling for udvikling af en web-site angik en realydelse, som måtte betragtes som en tjenesteydelse. Romkonventionen fandt derfor anvendelse ved fastlæggelsen af opfyldelsesstedet. Den for aftalen karakteristiske ydelse var softwaren til web-siten, som var udvik-

let af sagsøgte, der havde hovedsæde i Danmark. Aftalen havde derfor sin nærmeste tilknytning til Danmark, jf. Romkonventionens artikel 4, stk. 2.

- forbrugerforhold

Hovedreglen fraviges ved art. 5 om forbrugeraftaler om levering af løsøregenstande eller tjenesteydelser eller om ydelse til kredit til forbrugerformål. Af denne artikel følger, at parternes lovvalg i visse tilfælde ikke kan medføre, at forbrugeren berøves den beskyttelse, der tilkommer ham i medfør af ufravigelige regler i loven i det land, hvor han har sin bopæl, såfremt der i dette land forud for aftalens indgåelse er fremsat særligt tilbud over for ham eller er foretaget reklamering, og han dér har foretaget de handlinger, der fra hans side er nødvendige for aftalens indgåelse. Den tvivl, som denne bestemmelse rejser ved Internet-baserede transaktioner, må håndteres efter de principper, der er udviklet ovenfor i afsnit 23.1.b vedrørende rpl. § 246, stk. 1, 2. pkt.

Andre lovvalgsspørgsmål

De lovvalgsspørgsmål, der kan opstå i relation til de forskellige særregler, der indebærer brug af digital kommunikation over landegrænser, er i sagens natur mangfoldige. Det er ikke muligt at opstille generelle principper for, hvordan sådanne særlige lovvalgsproblemer skal løses. Spørgsmålene må derfor løses ud fra en konkret fortolkning af de enkelte retsområder. Problemstillingen berøres ikke yderligere her. Se generelt om disse spørgsmål *Henrik Spang-Hanssen* i Complex 5/01 og samme forfatters store afhandling Cyberspace & international law on jurisdiction: possibilities of dividing cyberspace into jurisdictions with help of filters and firewall software (2004).

Ifølge e-handelslovens § 3 skal en informationssamfundstjeneste, der leveres af en tjenesteyder, som er etableret i Danmark, inden for det koordinerede område, jf. § 2, nr. 8, udøves i overensstemmelse med *dansk ret*. Dette gælder, uanset om tjenesten alene retter sig mod et andet land inden for Den Europæiske Union/Det Europæiske Økonomiske Samarbejdsområde. Bestemmelsen indfører e-handelsdirektivets art. 3, stk. 2. Ifølge betragtning 57 til dette direktiv (der henviser til "Domstolens faste retspraksis") bevarer en medlemsstat retten til at træffe foranstaltninger over for en tjenesteyder, der er etableret i en anden medlemsstat, men hvis aktivitet udelukkende eller hovedsagelig er rettet mod førstnævnte medlemsstats territorium, såfremt etableringen har fundet sted med det formål at omgå den lovgivning, som tjenesteyderen ville være underlagt, hvis han var etableret på førstnævnte medlemsstats territorium. Det må antages, at § 3 må læses med et tilsvarende forbehold.

23.1.d. Sagsoplysning

Syn og skøn

Retsplejeloven angiver en række måder til at oplyse retssager om tekniske forhold. Den hyppigst anvendte metode består i at afholde syn og skøn, hvorved en af retten udmeldt sagkyndig person (eller flere) besigtiger ("syn") det tekniske fænomen, som beviset angår, og udtaler sin sagkyndige vurdering herom ("skøn").

Parternes beslutning om, hvorvidt der skal udmeldes syn og skøn, må på den ene side bero på ønsket om at oplyse sagen så godt som muligt og dermed give den dømmende instans det bedste grundlag for at træffe afgørelse, og på den anden side tage højde for de involverede omkostninger. En syns- og skønserklæring er almindeligvis kostbar. Skønsmandens honorar fastsættes af retten, men i praksis betales det beløb, skønsmanden forlanger for sin bistand, typisk udmålt på samme måde som betaling for konsulenttid. Derfor beror prisen på omfanget og kompleksiteten af de spørgsmål, parterne stiller skønsmanden.

Syns- og skønserklæringen rummer svaret på de spørgsmål, parterne har stillet syns- og skønsmanden efter forudgående at have konfereret herom. Skønsmandens udtalelse er som udgangspunkt begrænset til sagens faktiske omstændigheder. Dette følger forudsætningsvis af rpl. § 201, hvorefter det i udmeldelsesdekretet tydeligt må angives, hvad der er forretningens genstand og øjemed, jf. ligeledes rpl. § 301 om skønsmandens adgang til at "bese og gøre sig bekendt med forretningens genstand". Undertiden er det vanskeligt at udskille denne tekniske beskrivelse fra den juridiske beskrivelse, der ligger til grund for retsreglen. Dette problem opstår f.eks., når parterne anmoder skønsmanden om at udtale sig om, hvorvidt en mangel er "væsentlig", om et edb-program besidder den fornødne "originalitet", eller om en patenteret opfindelse har den fornødne "opfindelseshøjde".

Spørgsmålene

Som udgangspunkt er vurderingen af sådanne spørgsmål af juridisk karakter, og skønsmanden bør derfor ikke tage stilling til dem. Gør han nemlig det, forskydes domsmyndigheden reelt til en person uden de fornødne juridiske forudsætninger og uden den fornødne kompetence. Dette udgangspunkt modificeres imidlertid i relation til regler, der efter almindelig forståelse knytter sig til et objektiviserbart skøn udøvet af en fagmand. Det krav om opfindelseshøjde, der stilles i PL § 2, stk. 1, vil ofte forudsætte en vurdering af, om opfindelsen repræsenterer en løsning på det pågældende tekniske problem, der er nærliggende for en gennemsnitsfagmand på området. En sådan vurdering kan næppe

anses for rent subjektiv, og den må derfor kunne falde inden for en syns- og skønsmands hverv. På tilsvarende vis har man i sager om, hvorvidt der forelå den for brugskunst nødvendige værkshøjde, henholdsvis om det ene værk indebar en krænkelse af det andet, i vidt omfang lagt syns- og skønsudtalelser til grund.

Se nærmere *Koktvedgaard* (1965), s. 119 ff. og samme forfatter og *Lise Østerborg*: Patentloven med kommentarer, 2. udg. (1979), s. 95. I en skrivelse af 16. juni 1989 til De danske patentagenters Forening som svar på en konkret forespørgsel fra denne forening har præsidenten for Højesteret udtalt, at den omstændighed, at afgørelsen af et spørgsmål er overladt til domstolene, ikke i sig selv udelukker, at skønsmændene giver udtryk for deres mening derom, hvis de bliver spurgt.

Institutionel udpegning

Da skønsmandens funktion i mange henseender minder om den funktion, en IT-konsulent har ved en IT-anskaffelse, og da hans erklæring ofte vil have afgørende betydning for sagens udfald, bør parterne være mindst lige så kritiske i valget af syns- og skønsmand, som de er (eller bør være) ved valget af konsulent, jf. i det hele fremstillingen herom i afsnit 21.7. Der findes ingen egentlig uddannelse for syns- og skønsmænd. Som regel udpeges de af en instans, som parterne og retten anser for kvalificeret hertil. Hvem skønsmanden er, og hvilke nærmere kvaliteter han har som skønsmand, ved parterne sjældent. Kender den ene part til skønsmanden, uden at den anden gør det, vil den anden part typisk protestere mod valget af ham af frygt for uvedkommende påvirkning.

Aftalt udpegning

Det optimale vil være, at parterne i fællesskab foreslår retten, at der udpeges en skønsmand, der på forhånd er identificeret. Opnås en sådan enighed ikke, bør der i den anmodning, hvori en fagkyndig instans anmodes om at *pege på* skønsmanden, tegnes en klar *profil* over, hvilke kvalifikationer parterne efterspørger. Selv om sagens bilag almindeligvis medsendes anmodningen, har den udpegende instans i praksis ingen mulighed for at få overblik over mere detaljerede krav, da indholdet af disse krav bl.a. vil bero på sagens juridiske problemstilling. En skønsmandsprofil kan foruden det specielle emneområde angive uddannelsesmæssige kriterier samt kriterier, der knytter sig til skønsmandens praktiske erfaringsgrundlag.

Sagkyndige vidner

I visse tilfælde kan det være hensigtsmæssigt at afhøre sagkyndige vidner. Dette kan f.eks. tænkes, hvis der skal føres et teknisk/logisk sandsynlighedsbevis. Det sagkyndige vidne kombinerer vidnebevisets fordele i henseende til fleksibilitet og bevisumiddelbarhed med skønserklæringens fordele i henseende

til ekspertise. Denne oplysningsform er almindeligt brugt i USA. Danske dommere føler sig imidlertid i almindelighed bedre tilpas med skriftlige redegørelser fra sagkyndige, som begge parter har peget på, og dette system har da også sine åbenbare fordele. Bl.a. sparer det tid og ressourcer. Sine ligeså klare ulemper har det dog også. Når en sag bygges op omkring udsagn fra en ekspert, får vedkommende ofte – psykologisk eller faktisk – rollen som teknisk opmand. Dette kan føre til, at dommeren i stedet for at gå ind i det tekniske problem forlader sig på ekspertens konklusion om de faktiske forhold, som herefter omskrives til dommens juridiske resultat.

Isoleret bevisoptagelse

De almindelige regler om syn og skøn tager som udgangspunkt sigte på det bevis, der føres for den dømmende instans. Proceduren iværksættes derfor som udgangspunkt, når sagen er i gang. Den tid, det tager, fra en sag er anlagt (berammelse, forberedende retsmøder mv.), og til der foreligger en syns- og skønserklæring, vil ofte være så lang, at beviset i mellemtiden er gået tabt. Et leveret system er f.eks. blevet demonteret for at give plads for erstatningssystemet, eller de omstændigheder, hvorom der skal føres bevis, udspiller sig kun i kort tid endnu. I disse tilfælde kan det være nødvendigt at føre beviset, uden at sag samtidig er anlagt. Efter rpl. § 343 kan retten tillade, at der optages bevis, selv om dette ikke sker til brug for en verserende retssag. Gør man brug af en sådan isoleret bevisoptagelse, kan man føre ganske samme beviser som dem, man ville have ført under en sædvanlig retssag. Hvorvidt dette retsmiddel kan anvendes, beror på et judicielt skøn, se f.eks. *U 1989.631 SH*, der nægtede syn og skøn udenfor retssag under hensyntagen til den interesse, indstævnte kunne have i en egentlig sagsforberedelse.

Anmodning om isoleret bevisoptagelse indgives til retten på det sted, hvor det pågældende vidne bor eller opholder sig. Ønsker man under en isoleret bevisoptagelse at afholde syn og skøn, indgives anmodningen til byretten for den retskreds, hvor genstanden – f.eks. et leveret IT-system – befinder sig. Udgifterne ved bevisoptagelse afholdes af den part, der ønsker beviset optaget. Retten kan kræve, at der stilles sikkerhed for de udgifter, bevisoptagelsen vil medføre. § 343 giver ikke hjemmel for at pålægge tredjemand omkostninger, se *U 1989.943 V*. Afgiften ved selve bevisoptagelsen er forholdsvis beskeden. Hvor retsafgiften for at skulle anlægge en almindelig retssag er på ca. 2 % af værdien af det fremsatte krav, koster det kun 400 kr. at begære isoleret bevisoptagelse, jf. retsafgiftslovens § 14.

23.1.e. Editionspligt mv.

Discovery

Som nævnt ovenfor indeholder visse andre retssystemer hjemmel for, at en procespart af bevismæssige grunde kan forlange dokumentationsmateriale udleveret af sin modpart i en civil retssag, der verserer eller – hyppigere – forventes anlagt. En manglende efterkommelse af en sådan begæring kan resultere i processuel skadevirkning, sml. herom oversigtsmæssigt *PA* s. 431 ff. Reglerne kan derfor også få betydning for en dansk virksomhed, der bliver modpart i en sag anlagt i USA.

Af særlig betydning er det, at den part, der anmoder om *discovery*, også kan forventes at få ret til at få adgang til modpartens optegnelser i digital form, f.eks. ved at skanne dennes e-postopregnelser ved hjælp af dertil byggede værktøjer. Således antages retsstillingen at være i USA. Praksis har dog antaget, at discovery-proceedings ikke kan forpligte modparten til at stille kildetekst til rådighed, jf. sagen *Rare Coin-It, Inc. v. I.J.E. Inc.*, Fla. App., 12. oktober 1992, her citeret fra 9 CLAB 1 (1994), s. 32.

Konkurrence-regler

En lignende ret til at forlange oplysninger udleveret fra en virksomheds IT-systemer kan følge af offentligretlige regler. Efter kkl. § 17 kan konkurrencerådet således kræve alle oplysninger, herunder regnskaber, regnskabsmateriale, udskrift af bøger, andre forretningspapirer og "elektronisk lagrede data", som skønnes nødvendige for dets virksomhed eller til afgørelse af, om et forhold er omfattet af lovens bestemmelser, udleveret. I henhold til lovens § 18 kan der efter retskendelse foretages ransagninger og tages kopier af sådant materiale med bistand af politiet. Oplysningspligten kan sanktioneres med bøder og tvangsbøder. Konkurrencemyndighederne skal tillige yde bistand til kontrolundersøgelser efter EU-konkurrencereglerne, se lovens §§ 18a og 23a.

23.2. Administrativ konfliktløsning

23.2.a. Forbrugerklagenævn

Lovgrundlaget

Ifølge § 1 i lov om forbrugerklager, nr. 456 af 10. juni 2003, kan klager fra forbrugere vedrørende varer, arbejds- og tjenesteydelser indbringes for et godkendt, privat klage- eller ankenævn eller for Forbrugerklagenævnet. En klage kan angå samtlige omstændigheder i retsforholdet mellem parterne, jf. § 2. Klage kan rejses mod den, der efter retsplejelovens regler kan sagsøges ved en

dansk domstol om de spørgsmål, klagen omfatter. Aftaler om, at retstvister skal behandles ved voldgift eller andet særligt forum, udelukker ikke, at klage kan indgives til et klagenævn, jf. § 2, stk. 2.

Forbruger-begrebet

Klager, der rejses i medfør af loven om forbrugerklager, kan kun rejses af "forbrugere", hvilket ifølge § 3 i bekendtgørelse nr. 1118 af 12. december 2003 om forbrugerklager defineres som "en person, der hovedsageligt handler uden for sit erhverv". Samme bekendtgørelse afgrænser i øvrigt forbrugerklagenævnets kompetence i relation til en række specifikke varer og tjenester, se nærmere § 3, stk. 3. IT-leverancer falder inden for, og det samme gør rådgivning, der præsteres af IT-konsulenter, medmindre virksomheden udøves i medfør af en videregående, offentlig anerkendt uddannelse eller en offentlig autorisation eller beskikkelse, se § 3, stk. 3, nr. 9.

Gennem årene har Forbrugerklagenævnet truffet afgørelse i en lang række sager af betydning for IT-området, jf. de årlige Juridiske årbøger fra Forbrugerstyrelsen. For parterne består den største fordel i en nævnsbehandling i den grundighed, smidighed og hurtighed, hvormed nævnet behandler sine sager. Gebyr for sagens behandling er 150 kr. Hvis forbrugeren får medhold i en klage, eller sagen må afvises som uegnet, tilbagebetales klagegebyret. For dette beløb får man dels en juridisk afgørelse, men dertil undertiden også en sagkyndig sagsoplysning. Hvor parterne i en retssag ofte vil være tilbageholdende med at indhente sagkyndige erklæringer mv., jf. bemærkningerne herom ovenfor, vil Forbrugerklagenævnet skulle afholde disse omkostninger i en nævnssag. I klagesager om små hjemmecomputere har nævnet indhentet kostbare syns- og skønserklæringer med detaljerede oplysninger om karakteren af påståede mangler mv.

De mange klager vedrørende køb af IT-udstyr har gennem de seneste år udsat Forbrugerklagenævnet for et betydeligt pres. I juli 2003 har Forbrugerklagenævnet godkendt et nyt privat ankenævn på teleområdet, nemlig Teleankenævnet. Nævnet, som er oprettet af telebranchen og Forbrugerrådet, har kompetence til at behandle klager fra slutbrugere over telefonabonnementer, registrering og debitering af indholdstjenester og internet-abonnementer. Erhvervsdrivende kan som udgangspunkt ikke klage til Telenævnet (denne mulighed står dog åben, hvis klagen angår størrelsen af et registreret forbrug). Teleankenævnet berører ikke Teleklagenævnets og Telebrugernævnets kompetence som rekursinstanser i relation til afgørelser truffet af IT- og Telestyrelsen.

Forbrugerklagenævnets afgørelser har isoleret set kun karakter af uforbindende udtalelser, som ikke kan gennemtvinges. Parterne kan imidlertid vedtage at lægge nævnets afgørelse til grund, som om det var en voldgiftsafgørelse. Har begge parter forudgående erklæret, at de vil følge nævnets afgørelse, virker dettes afgørelse i realiteten som en voldgiftskendelse.

Tilsyn og klage

De fleste konkurrenceretlige regler håndhæves af myndigheder, som ofte træder i funktion på grundlag af indgivne klager. *Forbrugerombudsmanden* fører tilsyn med, at markedsføringsloven overholdes, jf. nærmere mfl. § 15, stk. 1, der indebærer en prioritering af "hensynet til forbrugerne". Man kan således ikke forvente, at Forbrugerombudsmanden vil tage sager op, der alene berører erhvervsmæssige interesser (f.eks. om plagiering af teknologi mv.). Ligeledes modtager *Konkurrencerådet* og *Kommissionen* klager indgivet af personer, der mener sig udsat for en konkurrencemæssig adfærd, der strider mod henholdsvis nationale og EU-retlige konkurrenceregler.

23.2.b. Immaterialrettigheder

Sager om fortolkning og håndhævelse af immaterialrettigheder prøves som udgangspunkt ved de almindelige domstole. I dette udgangspunkt gælder der dog visse modifikationer. Den ene gælder i tilfælde, hvor immaterialretten erhverves gennem registrering, og hvor der kan blive tale om at påklage registreringsmyndighedens beslutning. Den anden gælder i de særlige tilfælde, hvor der er hjemmel til at forvalte ophavsrettigheder gennem reglerne om tvangs- eller aftalelicens. Da disse sidstnævnte regler – endnu? – ikke spiller den store rolle på IT-området, knyttes i det følgende blot nogle enkelte bemærkninger til den mulighed, der består for at påkende klager over registrering af immaterialrettigheder og domænenavne.

Industriel ejendomsret

Afgørelser, der træffes i henhold til patent- og halvlederloven, kan indbringes for Patentankenævnet (Ankenævnet for Patenter og Varemærker), se herved PL § 25 og HLL § 17. Nævnets afgørelser er tilgængelige fra <www.pvanke.dk>. For prøvelsen af patenters gyldighed er det væsentligt, at der ved lov nr. 1057 af 23. december 1992 er indført regler i patentloven om administrativ omprøvning, se nærmere lovens §§ 53b – 53f. Hermed kan indsigeren undgå det langt bekosteligere alternativ til en sådan prøvelse, nemlig domstolsprøvelsen.

Domæneklager

Som nærmere udviklet i afsnit 11.4.f. har proceduren vedrørende klager om registrerede domænenavne udviklet sig til et

fintmasket regelværk, der tager udgangspunkt i det berørte topdomænenavn. Generelt gælder efterhånden det princip, at navnekrænkelser i praksis løses ved en instans, der alene træffer afgørelse i relation til den stedfundne registrering. Selv om prøvelsen sker på grundlag af de materielle navne- og kendetegnsretlige regler, er den således i hovedsagen *formel*: Klagesagens udfald er alene afgørende for, hvorledes det pågældende domæne registreres. Den endelige afgørelse af dette spørgsmål henhører under domstolene, medmindre andet er aftalt mellem parterne.

23.2.c. Offentlige indkøb

En særlig klageprocedure i sager vedrørende offentlige indkøb er institueret ved lov nr. 415 af 31. maj 2000 om Klagenævnet for Udbud med senere ændringer. Loven er – ligesom sin forgænger – indført på baggrund af det såkaldte kontroldirektiv (89/665/EØF, EFT 1989 L 395). Nævnet skal tage sig af klager over offentlige virksomheder, som ikke overholder de EF-retlige udbudsregler. Både danske og udenlandske leverandører kan klage til nævnet. Nævnet har kompetence til at standse ulovligheder samt til – i særlige tilfælde – at annullere en ulovlig beslutning. Under trussel om bødestraf kan nævnet kræve alle nødvendige *oplysninger* forelagt. Lovens § 6, stk. 3, giver dernæst nævnet kompetence til at yde klageren *erstatning* for tab, der er lidt som følge af overtrædelse af udbudsreglerne.

23.3. Alternativ konfliktløsning

23.3.a. Problemstillingen

Beslutningen om at føre sag er ikke et enten-eller. Inden man formelt anlægger en sag, må det være afklaret, om der findes alternative muligheder for konfliktløsning ved pådømmelse, forlig eller gennem forskelligartede mellemformer. I lyset af de omkostninger, der er forbundet med at føre sager om IT-forhold, har der udviklet sig en tradition for netop her at gøre brug af alternativ konfliktløsning (i engelsk terminologi: ADR – Alternative Dispute Resolution), se nærmere *PA* afsnit 9.5 og om forhandling, sst. s. 92 ff.

Der er flere grunde til at beskæftige sig med netop den IT-retlige konfliktløsning. Sager, der vanskeliggøres af faktiske beskrivelsesproblemer, kræver teknisk indsigt hos såvel advokat som

domsmyndighed. En sådan indsigt forventes danske dommere sædvanligvis ikke at være udrustet med. Derfor vil retssagen rumme et betydeligt og fordyrende indlæringsforløb. IT-sagernes faktiske og juridiske kompleksitet er ofte større end i de mere traditionelle sager inden for "the lawyers law". De juridiske beskrivelsesproblemer, der træder frem indenfor kontrakts- og erstatningsretten samt i læren om ophavsret, opdrag og finansiering, rummer talrige, men grundlæggende tvivlselementer. Beror sagens udfald på en retlig standard, kommer hertil den usikkerhed, der følger af, at der typisk savnes klare forestillinger om det ideelle IT-handlemønster.

Overfor disse vanskeligheder står det behov for en hurtig og effektiv løsning på sagen, som synes særligt påtrængende på IT-området. Uklarhed om, hvorvidt en teknologi er beskyttet, gør det vanskeligere at finansiere eller markedsføre produkter, hvori denne teknologi indgår. Opstår der tvivl om, hvorvidt der er mangler ved afleverede og igangsatte IT-systemer, vil denne tvivl kunne lamme systemet og tvinge brugeren til at tage en ubehagelig standpunktsrisiko, f.eks. ved at iværksætte erstatningskøb. Dette behov for en hurtig afslutning på IT-sagen kolliderer med den kendsgerning, at IT-sager – bl.a. af de førnævnte grunde – erfaringsmæssigt er langvarige.

Objektivisering

Uanset man altså aldrig kan sikre sig mod konflikter, er det muligt for de involverede parter at foretage et vist konflikt-forebyggende arbejde. Konfliktrisikoen mindskes for det første, jo mere præcist man har angivet indholdet af retsfaktum og retsfølge i aftalegrundlaget, se nærmere herom *PA* s. 139 ff. (Gyldige) aftaler, der lader de almindelige regler om tabets opgørelse erstatte af bestemmelser om konventionalbod, kan fjerne senere diskussion om tabets størrelse mv., ligesom håndfaste regler om afleveringsprøvens indhold og gennemførelse samt om fremgangsmåder ved fejlrettelse mv. kan skabe klarhed om, hvorvidt ydelsen er korrekt præsteret.

Procedure-regulering

For det andet kan man gennem aftaler af proceduremæssig karakter reducere konfliktrisikoen. Ofte vil parterne vælge at henskyde de problemer, der ikke er aktualiseret ved kontraktens underskrivelse, til afgørelse i særlige styregrupper, der herefter reelt genforhandler de uafklarede dele af kontrakten. Ligesom regler om *Nachfrist* kan afklare tvivl om, hvorvidt der foreligger en væsentlig misligholdelse, kan proceduremæssige regler pålægge den part, der vil kunne gøre indsigelser gældende om faktiske mangler mv., at sikre beviset herfor, f.eks. ved at føre log.

Ved et sådant påbud vil aftalen reelt sætte en ramme for, hvordan den efterfølgende bevisvurdering anlægges.

23.3.b. Voldgift

Den ældste alternative konfliktløsningsmodel består i at aftale voldgift. Man kan dog diskutere, hvor "alternativ" voldgift er. I sin kontradiktoriske form med to parter, der konfronterer hinanden for en dømmende myndighed, er voldgiftsformen meget lig den almindelige domstolsform. I så henseende består den væsentligste forskel i, at voldgiftsretten har grundlag i en aftale, indgået mellem parterne, forudgående eller efterfølgende.

Efter lov om voldgift, lov nr. 553 af 24. juni 2005, § 8 skal retssag om tvister, som efter aftale mellem parterne skal afgøres ved voldgift, afvises fra domstolene efter påstand. Parterne kan altså godt anlægge sag, selv om de har aftalt voldgift, blot de er enige herom. Omvendt kan en sag, der er – eller overvejes – anlagt ved de almindelige domstole, i stedet afgøres ved voldgift, hvis parterne på dette tidspunkt enes herom. Voldgiftsafgørelser er kun bindende mellem de parter, der har indgået voldgiftsaftalen. Hvis afgørelsen i sagen skal kunne gøres gældende overfor tredjemand (f.eks. sager om, hvorvidt et ophavsretligt værk har værkshøjde eller om et patents gyldighed), bør parterne i almindelighed ikke gøre brug af voldgift.

Fordele

Der er både fordele og ulemper ved voldgiftsbehandling. Fordelen er først og fremmest muligheden for herigennem at få sagen pådømt hos et dommerpanel med den fornødne tekniske sagkundskab. En anden iøjnefaldende fordel ved voldgiftsbehandlingen ligger i, at den er unddraget offentligheden. Dernæst kan en voldgiftsprocedure – bl.a. fordi, der i almindelighed ikke er mulighed for appel – typisk afsluttes hurtigere end en almindelig retssag. Hurtighed er imidlertid ikke noget nødvendigt kendetegn ved førsteinstans-behandling af en voldgiftssag.

Ulemper

Set fra et retssikkerhedssynspunkt er ulempen ved voldgift for det første, at voldgiftskendelsen ikke kan appelleres. Dernæst er voldgiftssager kostbare. Hvor dommeren i en almindelig retssag betales af det offentlige, skal parterne i en voldgiftssag selv honorere voldgiftsdommerne. Efter voldgiftslovens § 34 fastsætter voldgiftsretten selv sit vederlag, men vederlagets størrelse kan efter anmodning af en part prøves særskilt ved domstolene inden for en 30 dages frist. Ofte fastsættes vederlaget til et beløb svarende til det proceduresalær, advokaterne vil oppebære, men som

regel foretager voldgiftsretten et skøn over tidsforbruget samt over sagens størrelse og kompleksitet. I de fleste større sager – som trods alt udgør hovedparten af de sager, som parterne ønsker underkastet voldgiftsbehandling – vil vederlagets størrelse være betydeligt større end den retsafgift, der ville være udløst ved de almindelige domstole.

Fordele

En fordel ved at aftale voldgift ligger i, at parterne selv kan bestemme, hvilken nærmere procedure voldgiftsretten skal følge ved sin behandling af sagen. En hensigtsmæssig voldgiftsaftale vil f.eks. lade spørgsmålet om antallet af voldgiftspersoner afhænge af sagens størrelse. Giver voldgiftsaftalen regler herfor, gælder disse regler på lige fod med de regler i retsplejeloven, der almindeligvis vil tjene som udfyldende grundlag for voldgiftsrettens arbejde.

Som udgangspunkt har en voldgiftsret samme kompetence til at afgøre sagen, som en almindelig domstol ville have i et retsforhold, der alene berører parterne. Særlig undtagelse er gjort for visse sagstyper ved voldgiftslovens § 1, stk. 5 (faglig voldgift mv.), men disse undtagelser har ingen praktisk betydning på IT-området. Danske voldgiftskendelser kan ligeledes fuldbyrdes efter de almindelige regler i retsplejeloven, jf. voldgiftslovens § 38.

23.3.c. Særlige fremgangsmåder

Mægling og mediation

En af de først anvendte teknikker til alternativ konfliktløsning er den formaliserede eksterne forligsmægling. På engelsk betegnes denne løsningsform enten som *mediation* eller som *conciliation*.

Som antydet ved min debat med *Claus Kaare Pedersen*, jf. indlæggende i Advokaten 1/2005, s. 27 ff. og 31 ff., og i Advokaten 3/2005, s. 125 ff. og 128, hersker der endnu ikke fuld enighed herhjemme om, hvor grænsen går mellem mediation og anden mæglingsbistand.

Mediation

Det synes at være det overvejende synspunkt herhjemme, navnlig blandt medlemmer af foreningen Danske Mediatoradvokater, at mediationsbetegnelsen anvendes om tilfælde, hvor den upartiske mægler holder sig helt på afstand af konflikten uden på noget tidspunkt at udtale sin vurdering af gældende ret mv. Se i øvrigt om alternativ konfliktløsning *PA* afsnit 9.5 (s. 453 ff.) og om mediation, *Tina Monberg:* To vindere (2002), samme: Konfliktens redskaber (2005) og *Vibeke Vindeløv*: Konfliktmægling, mediation – retsmægling (2004).

Forligsmægling

En formaliseret forligsmægling indledes ved, at parterne udpeger en uafhængig person, der påtager sig at finde en hensigts-

mæssig løsning på den opståede tvist. I særlige tilfælde vil det være nødvendigt at udpege to forligsmænd, hvoraf parterne hver peger på en. Hermed åbnes mulighed for at opnå en frivillig, helt privat, ikke-bindende og frem for alt uformel måde at løse de opståede problemer på. Fra sin upartiske position kan mæglingsmanden således i højere grad end parterne fremlægge nye kompromisforslag, ligesom han kan filtrere og ikke mindst artikulere de urealistiske krav, som parterne ellers kan føle sig tilskyndet til at fremsætte under en forhandling.

Det ligger i begrebets natur, at man ikke kan tvinge den anden part i sagen til at gøre brug af forligsmægling ved mellemmand. Derfor har det strengt taget ingen reel mening at indgå udtrykkelig aftale herom. Ikke desto mindre kan det være hensigtsmæssigt, om parterne i aftalen tilkendegiver en intention om at søge konflikter afbødet gennem mindelige forhandlinger mv. Den nærmere fremgangsmåde kan da senere aftales. En fremgangsmåde kan her være, at virksomheden på forhånd erklærer sin villighed til at deltage i sådanne bestræbelser, hvis der skulle opstå en konflikt.

En sådan *Corporate Policy Statement on ADR* kan f.eks. lyde: "In the event of a business dispute between our company and another company which has made or will then make a similar statement, we are prepared to explore with that other party resolution of the dispute through negotiation or ADR techniques before pursuing full-scale litigation. If either party believes that the dispute is not suitable for ADR techniques, or if such techniques do not produce results satisfactory to the disputants, either party may proceed with litigation." Se ligeledes standardbestemmelse nr. 7, stk. 1, litra a, i de standardkontraktbestemmelser, Kommissionen godkendte den 15. juni 2001 som et tilstrækkeligt beskyttelsesniveau ved dataeksport, jf. afsnit 19.3.d. Ifølge bestemmelsen er parterne enige om at acceptere den registreredes beslutning om at henvise tvisten til mægling foretaget af en uafhængig person, eller i givet fald af tilsynsmyndigheden. En lignende mediationsløsning findes i den artikel V, som Kommissionen godkendte den 27. december 2004. En generel mediationsløsning er indeholdt i K01 pkt. 28, stk. 1. Inden en uenighed i givet fald løses ved voldgift, skal parterne "med en positiv, samarbejdende og ansvarlig holdning søge at indlede forhandlinger med henblik på at løse tvisten. Om nødvendigt skal forhandlingerne søges løftet op på højt plan i parternes organisationer. Såfremt der ej heller herved opnås nogen løsning, skal parterne søge at opnå enighed om i fællesskab at udpege en uafhængig og sagkyndig mægler, der kan mægle og komme med ikke-bindende forslag til tvistens løsning."

I valget af forligsmand er det væsentligt at tage højde for menneskelige kvalifikationer, herunder ikke mindst forligsmandens forventede tålmodighed. En del af idéen med at gøre brug af forligsmænd er at give parterne mulighed for at tilkendegive deres synspunkter i en mere uformel form og efter behov få afløb for personlige antipatier over for den anden part el.lign. Forligsmanden skal således besidde en betydelig tolerance, herunder også for de angreb på hans personlige integritet, han uvilkårligt vil blive udsat for i kampens hede.

Når forligsmanden er udpeget, er det som hovedregel op til ham at styre forhandlingen. Ofte må der gøres brug af en slags "shuttle diplomacy". Først besøges den ene part, dernæst den anden. Under besøgene lodder forligsmanden mulighederne for, at parterne vil indgå forskellige former for kompromiser. Er det aftalt, kan forligsmanden undervejs – og eventuelt under bistand af en hertil knyttet uafhængig teknisk ekspert – udtale sin opfattelse af de stridspunkter, uenighed rummer. En god forligsmand kan gennem denne metode give parterne mulighed for at indrømme, på hvilke punkter de strengt taget godt kan mene at have et medansvar for den opståede tvist.

Modsat forholdene i udlandet har vi ingen veletableret procedure for at udpege forligsmænd herhjemme. Navnlig i USA er der fremkommet en række private firmaer, der tilbyder bistand til mægling af forskellige typer af sager, se f.eks. *Mazero & Forseth's* oversigt i Franchising Law Journal, spring 1992, s. 118 ff. Til denne rådgivning hører ikke alene bistand ved udpegning af forligsmænd m.fl., men tillige tilvejebringelse af de ydre rammer for forligsforhandlingen. Center for Public Resources i New York har i 1987 udgivet et sæt retningslinjer med titlen Model ADR Procedures, der bl.a. indeholder regler for Mediation of Business Disputes. Retningslinjerne giver bl.a. anvisning om, hvorledes forligsmanden udvælges; hvilke møder han bør holde og hvornår, samt parternes forpligtelser under det forløb, hvor forligsmanden fungerer.

Regulering

Udover de særlige – og for IT-retten uinteressante – lovregler, der understøtter mægling på forskellige områder (arbejdskonflikter, ægteskabssager mv.) findes der ingen almindelige regler om mægling i dansk ret. UNCITRAL har i 1980 udsendt et sæt Model Conciliation Rules, se hertil *PA* s. 458. Herudover har forskellige institutioner på privatretligt grundlag markedsført mæglingsydelser, undertiden under betegnelsen "mediation". Se ligeledes *Henry & Lieberman* (1985), s. 57 ff. Der findes imidlertid intet generelt institut til håndtering af mægling i IT-sager.

Mini-voldgift

Den frihed til at bestemme voldgiftsrettens sammensætning og sagsbehandling, der følger af voldgiftslovens regler, giver par-

terne en stor frihed til at finde en ramme for deres konfliktløsning, der ikke lever helt op til sædvanlige retsplejeidealer. Undertiden betegnes en sådan modificeret voldgiftsinstans som "minivoldgift".

Konstatering

En variant af denne fremgangsmåde findes i K18 og K33. Pkt. 12, stk. 3, i begge disse kontrakter fastslår, at en part kan anmode om en uvildig afgørelse af en uenighed om, hvorvidt kravene til driftseffektivitet og/eller svartider er opfyldte i en bestemt periode. Afgørelsen træffes af en sagkyndig, der efter anmodning udmeldes af Dansk IT. Den sagkyndige afgør herefter spørgsmålet – herunder om størrelsen af afvigelsen – endeligt og bindende for begge parter. Som bestemmelsen er formuleret, vil skønsmanden dermed få den endelige afgørelse af det pågældende problem. Da han i de færreste tilfælde vil have nogen juridisk uddannelse, kan dette vel synes betænkeligt. Bestemmelsen har så vidt vides aldrig givet anledning til sager. I betragtning af den komplicerede og uforholdsmæssigt kostbare bevisførelse, spørgsmål om svartid efterfølgende kan give anledning til, synes der ikke at være grundlæggende betænkeligheder mod at gøre brug af en sådan fremgangsmåde, hvis blot der udmeldes en person med de rette kvalifikationer.

Summarisk procedure

En kombination af mægling ved forligsmand og mini-voldgift findes i den såkaldte summariske procedure (på engelsk: mini-trial). En *mini-trial* er en forligs-proces. Den resulterer ikke i nogen voldgiftskendelse eller andet dokument, der som sådant kan eksekveres. Tvisten henlægges til et forum bestående af tre personer: en kompetent repræsentant for hver af de stridende parter (f.eks. bestyrelsesformanden i et aktieselskab) med den person, der tidligere har fungeret som forligsmand som formand. Fordelen ved dette system består i, at hver part får klarhed over sine egne, henholdsvis modpartens, stærke og svage punkter i sagen. Dette giver i sig selv et stærkt incitament for at forlige den.

Flere forudsætninger må være opfyldte for at kunne gøre brug af summarisk procedure. For det første må de "voldgiftsmænd", parterne udpeger, have kompetence inden for deres respektive organisationer, så de kan udvirke en bindende juridisk afgørelse i sagen. Hertil stiller man normalt krav om, at de personer, der medvirker i den summariske procedure, iagttager fuldstændig tavshed om dens forløb. Systemet minder for så vidt om den ordning, man gør brug af i styregrupper. De pågældende må derfor være relativt højt placeret i virksomheden. Dernæst må de ikke tidligere have haft med sagen at gøre. Gennem et sådant

krav undgår man dels forudindtagethed, dels den faktor, der ligger i at dække over det mulige medansvar for sagens opståen.

For at kunne opfylde disse tre krav må de involverede parter være virksomheder af en vis størrelse. Da det som regel også er sådanne virksomheder, der løber ind i de største udgifter til konfliktløsning, passer problem og løsning godt sammen. Et af formålene med at gennemføre en mini trial er at forkorte den tid, der medgår til processen. I almindelighed bør sagen ikke vare længere end 1 – 2 dage, bl.a. fordi den forudsættes at lægge beslag på højt placeret personale hos begge de stridende parter.

Supplerende litteratur

De særlige problemer, der er forbundet med sagsførelser indenfor den *civile retspleje* om teknisk komplicerede forhold, er ligeledes kun sparsomt behandlet i litteraturen. Se som et enkeltstående eksempel *Holm-Nielsen & Plesner*: Sager inden for immaterialretten, trykt i W. E. von Eyben (red.): Proceduren (1980), s. 337 ff.

De international-privatretlige regler anledning til store praktiske vanskeligheder i forbindelse med den elektroniske handel. For en redegørelse over disse spørgsmål henvises til *Kim Østergaards* ph.d.-afhandling: Elektronisk handel og international proces- og privatret (2003), der analyserer den betydning e-handel har for anvendelsen af de IP-retlige regler i henholdsvis USA og EU.

Dansk rets regler om *voldgift* er grundlæggende ændret efter indførelsen af voldgiftsloven af 2005. Den tidligere voldgiftslov er bl.a. behandlet af *Jakob Juul og Peter Fauerholdt Thommesen*: Voldgiftsret (2003) og af *Bernt Hjejle*: Voldgift, 3. udg. (1987).

Litteraturen om mediation og anden alternativ konfliktmægling er gennem de seneste år vokset med eksplosiv hast. Blandt den seneste tilkommende kan henvises til *Tina Monberg*: To vindere (2002) og samme: Konfliktens redskaber (2005) og *Vibeke Vindeløv*: Konfliktmægling, mediation – retsmægling (2004). Se ligeledes *Hans Boserup & Susse Humle:* Mediationsprocessen (2001) og *Vibeke Vindeløvs* doktorafhandling Konflikt, tvist og mægling – konfliktløsning ved forhandling (1997).

LOV- OG LITTERATURFORKORTELSER

ABCNY	Association of the Bar of the City of New York (anvendes om skriftserie herfra).
ACM	The Association of Computing Machinery (anvendes om skriftserie herfra).
aftl.	Aftaleloven.
BGH	Bundesgerichtshof. Den tyske forbundshøjesteret.
BKL	Lov om betalingskort (ophævet). Se nu LVB.
CISG	United Nations Convention on Contracts for the International Sale of Goods. Optrykt på dansk som bilag til International købelov, nr. 733 af 7. december 1988: De Forenede Nationers konvention om aftaler om internationale køb.
CLAB	Computer Law Association Bulletin.
C/LJ	Computer/Law Journal, international journal of computer, communication & information law. Udgivet af Center for Computer/Law, University of Southern California Law Center.
CL&P	Computer Law and Practice. Engelsk IT-retligt tidsskrift.
CLR	Computer Law Reporter – a monthly journal of computer law and practice.
CLSR	Computer Law & Security Report. Udgivet af Eclipse Publications Ltd., London.
CL&TR	Computer Law & Tax Report. Udgivet af Roditti Reports Corp., New York.
Complex	Skriftserien Complex. Udgivet af Institutt for Rettsinformatikk, Universitetet i Oslo.
CPR-lov	Lov om det centrale personregister, jf. lovbekendtgørelse nr. 140 af 3. marts 2004 med senere ændringer.
CuR	Computer und Recht. Forum für die Praxis des Rechts der Datenverarbeitung, Information und Automation. Tidsskrift udgivet af Otto Schmidt Verlag, Köln.
DEK	Dansk Elektroteknisk Komité.

DG	Directorate Générale – Generaldirektorat under kommissionen for de Europæiske Fællesskaber.
DL	Danske Lov.
DS	Dansk Standard.
DuD	Datenschutz und Datensicherheit, Recht und Sicherheit der Informations- und Kommunikationssysteme. Tysk tidsskrift.
DVA	Dansk Varekode Administration.
EAL	Erstatningsansvarsloven, jf. lovbekendtgørelse nr. 750 af 4. september 2002 med senere ændringer.
ECMA	European Computer Manufacturers' Association.
EDBR	Edb-rådets rapport.
e-handels-direktivet	Direktiv 2000/31/EF om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked, EFT 2000 L 178/1.
e-handels-loven	Lov nr. 227 af 22. april 2002 om tjenester i informationssamfundet og visse aspekter af elektronisk handel.
EMRK	Den Europæiske Menneskerettighedskonvention.
EOTC	European Organization for Testing and Certification.
EPK	Europapatentkonventionen.
EPO	European Patent Office – Det europæiske Patentkontor.
ERA	Edb-retlige afgørelser (bd. I - III), se litteraturliste.
ET	Mads Bryde Andersen: Enkelte transaktioner (2004)
EØFT	Traktaten om det europæiske økonomiske fællesskab.
E&A	Mads Bryde Andersen: Edb og ansvar – studier i edb-erstatningsrettens beskrivelsesproblematik (1988).
F.Supp.	Federal Supplement. Amerikansk domssamling.
F.2nd	Federal Reporter, second series. Amerikansk samling af appelretsdomme.
F.3rd	Federal Reporter, third series. Amerikansk samling af appelretsdomme.
FKNbrtn.	Forbrugerklagenævnets årsberetning (1975-1988; herefter afløst af JÅF).
FObrtn.	Forbrugerombudsmandens årsberetning (1975-1988; herefter afløst af JÅF).

FUL	Lov om retsforholdet mellem arbejdsgivere og funktionærer (funktionærloven), jf. lovbekendtgørelse nr. 68 af 21. januar 2005.
GA	Mads Bryde Andersen: Grundlæggende aftaleret, 2. udg. (2002).
gbl.	Gældsbrevsloven, jf. lovbekendtgørelse nr. 669 af 23. september 1986 med senere ændringer.
HLL	Halvlederloven: Lov nr. 778 af 9. december 1987 om beskyttelse af halvlederprodukters uformning (topografi).
IBL	International Business Lawyer. Journal of the Section on Business Law of the International Bar Association
IDL	Internetdomæneloven, lov nr. 598 af 24. juni 2005 om internetdomæner, der særligt tildeles Danmark.
IRI-rapport	Skriftserie udgivet af IRI, Institutet för Rettsinformatik (Stockholm).
J	Juristen, hhv. Juristen & Økonomen.
JT	Juridisk Tidskrift vid Stockholms Universitet.
Jurim.	The Jurimetrics Journal of Law, Science and Technology. Udgivet af the American Bar Association, Section of Science and Technology.
JÅF	Juridisk Årbog fra Forbrugerstyrelsen.
KAL	Kreditaftaleloven, jf. lov nr. 398 af 13. juni 1990 med senere ændringer.
KB	Københavns Byret.
kbl.	Købeloven, jf. lovbekendtgørelse nr. 28 af 21. januar 1980 med senere ændringer.
KFE	Kendelser om fast ejendom. Samling af miljø- og entrepriseretlige afgørelser.
KL	Konkursloven, jf. lovbekendtgørelse nr. 118 af 4. februar 1997 med senere ændringer.
HAL	Handelsagentloven, lov nr. 272 af 2. maj 1990 om handelsagenter og handelsrejsende.
INFOSOC-direktivet	Europa-parlamentets og Rådets direktiv 2001/29/EF om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet.
Konkurrence-loven	Senest bekendtgjort ved lovbekendtgørelse nr. 539 af 28. juni 2002.

KL	Konkursloven, jf. lovbekendtgørelse nr. 118 af 4. februar 1997.
LBP	Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger.
LL	Lejelov, jf. lovbekendtgørelse nr. 920 af 10. september 2004 med senere ændringer.
L&D	Tidsskriftet Lov og Data, udgivet af stiftelsen Lovdata, Oslo.
L.J.	Law Journal, anvendes ligesom L.R., s.d.
LMI	Lov nr. 430 af 1. juni 1994 om massemediers informationsdatabaser med senere ændringer.
LOR	Lov om offentlige myndigheders registre. Ophævet. Se nu LBP.
LPR	Lov om private registre. Ophævet. Se nu LBP.
L.R.	(i forbindelse med anden forkortelse): Law Review, f.eks. New England L.R.
LVB	Lov om visse betalingsmidler, jf. lovbekendtgørelse nr. 1501 af 20. december 2004 med senere ændringer.
mfl.	Lov om markedsføring, jf. lovbekendtgørelse nr. 699 af 17. juli 2000.
NAT	Nordisk Administrativt Tidsskrift.
NEK	Nordisk Embetsmannskomité för konsumentspørsmål. Udgiver af rapportserie.
NIR	Nordiskt Immateriellt Rättsskydd (tidsskrift).
NJA	Nytt Juridiskt Arkiv (Svensk domssamling).
NJM	Forhandlingerne på de Nordiske Juristmøder. I henviser til de trykte indlæg; II til de mundtlige.
NÅR	Nordisk årbog for retsinformatik.
ophl.	lov om ophavsret (ophavsretsloven), jf. lovbekendtgørelse nr. 725 af 6. juli 2005.
PA	Mads Bryde Andersen: Praktisk aftaleret, 2. udg. (2003).
PAL	Produktansvarsloven: Lov nr. 371 af 7. juni 1989 om produktansvar, som ændret ved lov nr. 1041 af 28. november 2000.
PIA	Pengeinstitutankenævnet (kendelse fra).

PL	Patentloven, jf. lovbekendtgørelse nr. 1136 af 16. november 2004 med senere ændringer.
rpl.	Retsplejeloven, jf. lovbekendtgørelse nr. 961 af 21. september 2004 med senere ændringer.
Rutgers	Rutgers Computer & Technology Law Journal.
RÅB	Registertilsynets Årsberetning.
R&R	Revision og Regnskabsvæsen. Tidsskrift udgivet af Foreningen af Statsautoriserede Revisorer.
SLB	The Software Law Bulletin.
strfl.	Borgerlig straffelov, jf. lovbekendtgørelse nr. 960 af 21. september 2004 med senere ændringer.
SvJT	Svensk Juristtidning.
TBB	Tidsskrift for Bygge og Boligret.
TEF	Traktaten om de Europæiske Fællesskaber (Amsterdam-traktaten).
telebekendtgørelsen	Bekendtgørelse nr. 638 af 20. juni 2005 om udbud af elektroniske kommunikationsnet og tjenester.
teleforbrugerloven	Lov nr. 428 af 31. maj 2000 om konkurrence- og forbrugerforhold på telemarkedet, jf. lovbekendtgørelse nr. 679 af 23. juni 2004.
TL	Tinglysningsloven, jf. lovbekendtgørelse nr. 622 af 15. juni 1986 med senere ændringer.

LITTERATUROVERSIGT

Denne litteraturliste omfatter et udvalg af toneangivende værker inden for de almene juridiske, IT-retlige og IT-tekniske områder, der berøres i bogen. Mere speciel litteratur anføres enten i teksten eller i den litteraturliste, der hører til de enkelte kapitler.

Lars Aggergren, Poul Bostrup & Nicolai Dragsted (red).: *Fakta IT jura og sikkerhed* (2000).

Lennart Lynge Andersen, Palle Bo Madsen & Jørgen Nørgaard: *Aftaler og mellemmænd*, 4. udg. (2001).

Mads Bryde Andersen: *Advokatretten* (2005).

Mads Bryde Andersen (red): *Edb-ret for brugere* (1987).

Mads Bryde Andersen: *Edb og ansvar–studier i edb-erstatningsrettens beskrivelsesproblematik* (1988).

Mads Bryde Andersen (red.): *Edb-retten i Europa* (1991).

Mads Bryde Andersen: *Enkelte transaktioner* (2004).

Mads Bryde Andersen: *Nogle IT-retlige problemer ved årtusindskiftet–en juridisk oversigt*. År 2000-sekretariatet (juni 1998).

Mads Bryde Andersen: *Praktisk aftaleret*, 2. udg. (2002).

Mads Bryde Andersen: *Lov om arbejdstageres opfindelser med kommentarer* (1995).

Mads Bryde Andersen: *Grundlæggende aftaleret*, 2. udg. (2002).

Poul Andreasen & Peter Græbe: *Shareware-håndbogen* (1990).

John Abrahamsen & Lars Frank: *Edb-ordbogen* (1991).

Troels Andreasen m.fl. (under faglig redaktion af Klaus Hansen): *IT-lex–det store informatik-leksikon*, 2. udg. (2001).

Stewart A. Baker & Paul R. Hurst: *The limits of trust–cryptography, governments, and electronic commerce* (Kluwer Law International, The Hague, 1998).

Michael S. Baum: *Federal Certification Authority liability and policy* (1994).

Strange Beck & Ole Bruun Nielsen: *Edb-retlige afgørelser 1* (1984).

Strange Beck & Ole Bruun Nielsen: *Edb-retlige afgørelser 2* (1986).

Hans Jørgen Beck, Ole Monrad & Inge-Lise Salomon: *Datamater, programmer og sprog* (1990).

David Bender: *Computer law–software protection and litigation, vol. I–II.* New York (1986) med senere releases.

Hanne Bender: *Edb-rettigheder* (1998).

Hanne Bender & Ole Bruun Nielsen: *Edb-ret: ansvar og rettigheder*. Juridisk bogformidling, Århus. Stencileret (1988).

Hanne Bender & Ole Bruun Nielsen: *Edb-retlige afgørelser 3* (1988).

Richard L. Bernacchi m.fl.: *Bernacchi on computer law, vol. I – II.* Boston, Toronto (1986).

Tim Berners-Lee (with Mark Fischetti): *Weaving the web. The past, present and future of the World Wide Web by its inventor* (1999). På dansk: *Webbets vej til verden* (2001).

Jon Bing & Knut S. Selmer: *A decade of computers and law*. Oslo (1980).

Jon Bing: *Rettslige kommunikasjonsprosesser*. Oslo (1982).

Bjørn Bjerke: *Reverse engineering av datamaskinprogrammer*. Complex 9/94.

Lars Jakob Blanck (red.): *Dommer og kjennelser i EDB-rett I*. Oslo (1980).
Jørgen Blomqvist: *Overdragelse af ophavsrettigheder – rettighedsoverdragelsen og dens fortolkning* (1987).
Peter Blume: *Databaseret* (1996).
Peter Blume: *Personoplysningsloven* (2001).
Peter Blume: *Retsinformationssamfundet* (1986).
Peter Blume: *Retsbeskyttelse af edb* (1989).
Peter Blume m.fl.: *IT-retlige emner* (1998).
Peter Blume & Mette Reissmann: *Beskyttelse af forbrugeroplysninger* (2003).
Bonnerup-rapporten (Teknologirådet): *Erfaringer fra Statslige IT-projekter – hvordan gør man det bedre?* (2001).
John J. Borking: *Third party protection of software and firmware – direct protection of zeros and ones*. North Holland, Amsterdam (1985).
Dick H. Brandon & Sidney Segelstein: *Data processing contracts – structure, contents, and negotiations*. Second edition. New York (1984).
Frederick P. Brooks, Jr.: *The mythical man-month – essays on software engineering*. Reasing, Massachussetts (1972, 1975, 1982).
Jørgen Bull: *EDB-kontrakter*. Oslo (1981).
Sten Bønsing: *Brancheregler og brancheproces* (2001).
Vagn Carstensen & Thomas Rørdam: *Pant,* 7. udg. (2002).
Michael Chissick & Alistair Kelman: *Electronic commerce – law and practice*. London (1999).
Odd-Einar Christophersen & Arve Føyen: *Edb-anskaffelser – fremgangsmåte og avtaleutforming*. Oslo (1981).
Anthony Lawrence Clapes: *Software, copyright and competition – the "look and feel" of the law*. New York (1989).
Dansk Standardiseringsråd: *Kryptografi og datasikkerhed*. DS/INF/43, (1988).
Nicolai Dragsted: *IT-kontrakter I og II* (2000).
Nicolai Dragsted, Ole Horsfeldt,. Jesper Langemark & Claus Sørensen: *Ko1 med kommentarer* (2004).
Fred I. Dretske: *Knowledge and the flow of information*. Oxford (1981).
Gerald Dworkin & Richard D. Taylor: *Blackstone's guide to the copyright, designs & patents act 1988*. London (1989).
Eivind Einersen: *Elektronisk aftale- og bevisret* (1992).
Erhvervs- og Selskabsstyrelsen: *Bogføringsvejledning* (1991).
Bo von Eyben: *Ansvar for graveskader – erstatningsretlige problemer i forbindelse med ledningsregistrering og ledningsbeskadigelse* (1990).
Bo von Eyben & Helle Isager: *Lærebog i erstatningsret*, 5. udg. (2003).
W. E. von Eyben: *Panterettigheder*, 8. udg. ved Henning Skovgaard (1987).
Jens Fejø m.fl.: *Legal Aspects of Electronic Commerce*. Juristforbundets Forlag, København (2001).
Charles H. Ferguson & Charles H. Morris: *Computer wars – the fall of IBM and the future of global technology.* Times Books, New York (1993, 1994).
Warwick Ford & Michael S. Baum: *Secure Electronic Commerce – building the infrastructure for Digital Signatures and Encryption.* Prentice Hall PTR (1997).
Tom Forester & Perry Morrison: *Computer ethics – cautionary tales and ethical dilemmas in computing.* Cambridge, Massachusetts (1990).
Lars Frank: *Edb-sikkerhed* (1987).
Kim Frost: *Informationsydelsen* (2002).
Andreas Galtung: *Paperless systems and EDI.* Complex 4/91.
Andreas Galtung: *Personvern og den forbrukerrettede elektroniske betalingsformidling.* NEK-arbeids-

rapport 1989, Nordisk Ministerråd, NORD 1989:84.
Bernhard Gomard: *Almindelig kontraktsret – indgåelse, gyldighed, fortolkning*, 3. udg. (1996).
Bernhard Gomard: *Forholdet mellem erstatningsregler i og udenfor kontraktsforhold* (1958).
Bernhard Gomard: *Obligationsret, 1. del*, 3. udg. (1998).
Bernhard Gomard: *Civilprocessen*, 5. udg. (2001).
Vagn Greve: *Edb-strafferet*, 2. udg. (1986).
Vagn Greve & Lars Bo Langsted: *Erhvervsstrafferetten*, 5. udgave (2000).
P.N. Grabosky & Russell G. Smith: *Crime in the Digital Age – controlling telecommunications and cyberspace illegalities*. New Brunswick, New Jersey (1998).
H. W. A. M. Hanneman: *The patentability of computer software – an international guide to the protection of computer-related inventions*. Kluwer, (1985).
Jørgen Hansen: *Licensaftalen* (1981).
Jørgen Hansen: *Teknikeraftalen – almindelig del* (1984).
Olaf Hasselager m.fl.: *Bogføring, regnskab og skat – med kommentar til Bogføringsloven og Mindstekravsbekendtgørelsen* (2000).
Kasper Heine, Martin von Haller Grønbæk & Jan Trzaskowski: *Internet.Jura*, 2. udg. (2002).
Roger Henriksen: *The legal aspects of paper-less international trade and transport.* København (1982).
Johnny Herre: *Nordisk implementering av distansavtalsdirektivet – särskilt ur konsumentskyddssynspunkt.* TemaNord 1998:532.
Paul S. Hoffman (ed.): *Internet and Web Related Forms Collection – 2000.* Computer Law Association (2000).
ICC: *GUIDEC – General Usage for International Digital Electronic Commerce*, 2nd. ed., Paris 2001.
Ole Horsfeldt: *IT-outsourcing – forhandling og styring af outsourcing kontrakter* (2005).
J. Hartvig Jacobsen: *Forlagsretten* (1951).
Søren Sandfeld Jakobsen: *Medieret i informationssamfundet – en retlig analyse af sammensmeltningen mellem telekommunikation, Internet og radio/tv* (2004).
Klaus Østergaard Jensen: *Elektronisk udveksling af informationer i juridisk belysning.* EDB-gruppen Herning, Oktober 1996.
A. Egebjerg Johansen, Jens P. Jensen, H. Fabricius Olsen, Frede Dybkjær & Peter Zangenberg: *Databehandling for edb-brugeren* (1986).
Pernille Kallehave: *Hvad må jeg? – Ophavsret i teknologistøttet uddannelse.* Center for Teknologistøttet Uddannelse (1997).
Susanne Karstoft: *Elektronisk dokumentudveksling – retlige aspekter* (1994).
H. W. K. Kaspersen & A. Oskamp (ed.): *Amongst friends in computers and law – a collection of essays in remembrance of Guy Vandenberghe* (1991).
Anders Kildsgaard, Ole Horsfeldt & Jesper Langemark: *Internetkontrakter. Thomson Paradigma* (2002).
Mogens Koktvedgaard: *Immaterialretspositioner – bidrag til læren om de lovbestemte enerettigheder og deres forhold til den almene konkurrenceret* (1965).
Mogens Koktvedgaard: *Lærebog i konkurrenceret*, 5. udg. (2003).
Mogens Koktvedgaard: *Lærebog i immaterialret*, 7. udgave ved Jens Schovsbo (2005).
Ragnar Knoph: *Åndsretten*. Oslo (1936).
A. Vinding Kruse: *Erstatningsretten*, 5. udgave under medvirken af Jens Møller (1989).
Christian Kragelund, Martin Dahl Pedersen & Thomas Munk Rasmussen: *Domænenavne – en juridisk håndbog* (2003).

A. Vinding Kruse: *Købsretten*, 2. udgave under medvirken af Jens Møller (1989).
L. J. Kutten: *Computer software – protection/liability/law/forms.* New York (1989 med senere updates).
L. J. Kutten, Bernard D. Reams & Allen E. Strehler: *Electronic contracting law – EDI and business transactions.* New York (1991).
Agne Lindberg: *Elektroniska originaldokument och elektronisk signatur.* IRI-rapport 1987:7.
Agne Lindberg & Daniel Westman: *Praktisk IT-rätt. Andra upplagan.* Stockholm (1999).
Seth E. Lipner & Stephen Kalman: *Computer law – cases and materials.* Merrill Publishing Co., Columbus m.fl. (1989).
Colin D. Long: *Telecommunications law and practice.* London, (1988).
Johan Lundberg: *Domännamn & svensk rätt – särskilt om så kallade domänstölder.* Justus förlag, Stockholm (1997).
Palle Bo Madsen: *Markedsret Del 1: Konkurrencebegrænsningsret*, 3. udg. (1997).
Palle Bo Madsen: *Markedsret Del 2: Lovbestemte enerettigheder, markedsføringsregler, erhvervshemmeligheder mv.*, 3. udg. (1997).
Palle Bo Madsen & Anne-Dorte Bruun Nielsen: *Dansk forbrugerret* (1986).
Steven L. Mandell: *Computers, data processing, and the law. Text and cases.* New York (1984).
Jacob Plesner Mathiasen, Niels Bo Jørgensen & Johan Schlüter: *E-handelsloven med kommentarer* (2004).
Rolf Molich (red.): *Brugervenlige edb-systemer* (1986).
Richard Morgan & Graham Stedman: *Computer contracts*. Third edition. London (1987).
Keld I. Nielsen, Henry Nielsen & Hans Siggaard Jensen: *Skruen uden ende. Den vestlige teknologis historie* (1990).
Kristian Korfits Nielsen & Henrik Waaben: *Lov om behandling af personoplysninger* (2001).
Kristian Korfits Nielsen & Henrik Waaben: *Lov om behandling af personoplysninger med kommentarer* (2001).
Ruth Nielsen: *E-handelsret* (2001).
Ruth Nielsen: *E-handelsret,* 2. udg. (2004)
Raymond T. Nimmer: *The law of computer technology*. Boston (1985).
Jacob Nørager-Nielsen: *Edb-kontrakter* (1987).
Jacob Nørager-Nielsen & Søren Theilgaard: *Købeloven med kommentarer*, 2. udg. (1993).
Birgitte Kofod Olsen: *Identifikationsteknologi og individbeskyttelse – en øvelse i juridisk teknologivurdering* (1998).
Mogens Kühn Pedersen: *EDI i virksomheden* (1990).
William E. Perry: *The manager's guide to computer systems.* New York (1982, 1984).
Julius C.S. Pinckaers: *From privacy toward a new intellectual property right in persona.* Kluwer Law International, The Hague (1996).
Y. Poullet & G.P.V. Vandenberghe (eds.): *Telebanking, teleshopping and the law.* Deventer, Holland, (1988).
Richard Raysman & Peter Brown: *Computer law: drafting and negotiating forms and agreements.* New York (1984) med senere updates.
Chris Reed & John Angel (ed.): *Computer law*. 4th. edition. Blackstone Press, London (2000).
Thomas Riis: *Immaterialretlig beskyttelse af IT-produkter.* Trykt i Blume m.fl.: IT-retlige emner (1998), s. 115 ff.
Thomas Riis: *Immaterialret & IT* (2002).
Rolf Riisnæs (red.): *Elektronisk betalingsformidling og forbrukerinteresser I.* Complex 5/90.

Rolf Riisnæs (red.): *Elektronisk betalingsformidling og forbrukerinteresser II. Arbeidsdokumenter til den nordiske konferanse 1990.* Complex 5/91.

Jonathan Rosenoer: *CyberLaw – the law of the Internet* (Springer Verlag, New York 1997).

Dag Wiese Schartum (red.): *IRI's Spectrum – 20 artikler i anledning av institutt for rettsinformatikk's 20 års jubileum.* Complex 1/90.

Peter Schønning: *Ophavsretsloven med kommentarer,* 3. udg. (2003).

Per Håkon Schmidt: *Retsbeskyttelse af edb-programmer* (1998).

Per Håkon Schmidt: *Teknologi og immaterialret – Et studie i patent- og ophavsretten særligt med henblik på retsbeskyttelsen af edb-programmer og micro-chips* (1989).

Bruce Schneier: *Applied cryptography*, 2nd. ed. John Wiley & Sons, New York (1996).

Bruce Schneier: *Secrets and lies – digital security in a networked world.* John Wiley & Sons, New York (2000).

Peter Seipel: *Computing law – perspectives on a new legal discipline.* Stockholm (1977).

Peter Seipel: *Juridik och IT – introduktion till rättsinformatiken.* Sjunde upplagan, Stockholm (2001).

Peter Seipel: *Juristen och datorn – introduktion till rättsinformatiken, tredje upplagan.* Stockholm (1990).

John T. Soma: *Computer technology and the law.* Colorado Springs (1983), med senere releases.

Henrik Spang-Hanssen: *Cyberspace jurisdiction in the US from an alien's point of view*. Complex 5/01.

Henrik Spang-Hanssen: *Cyberspace & international law on jurisdiction: possibilities of dividing cyberspace into jurisdictions with help of filters and firewall software* (2004).

Tarjei Stensaasen: *Opphavsrettslovens § 43 ("Katalogregelen")*. Complex 10/85 (1985).

Tarjei Stensaasen: *Rettslig vern av edb-programmer og databaser.* Oslo (1987).

Lars Stoltze: *Internet Ret* (2001).

Colin Tapper: *Computer law*, fourth edition. London (1989).

Teknologirådet: Erfaringer fra Statslige IT-projekter – hvordan gør man det bedre? (2001).

Robin Thrap-Meyer: *Pantsettelse av datamaskinprogrammer og databaser.* Complex 4/89.

Olav Torvund: *Kontraktsregulering – IT-kontrakter.* Tano Aschehoug, Oslo (1997).

Henrik Udsen: *Den digitale signatur – ansvarsspørgsmål* (2002).

Henry Ussing: *Aftaler på formuerettens område*, 3. udg. (1950).

Henry Ussing: *Køb.* 4. udgave ved A. Vinding Kruse (1967).

Perttu Virtanen: *Database Rights in Safe Europeam Home: The Path to More Rigorous Protection of Information*. Acta Universitatis Lappeenrantaensis 202 (2005).

Miko Välimäki: *The Rise of Open Source Licensing – A Challenge to the Use of Intellectual Property in the Software Industry* (Turre Publishing, 2005).

Ian Walden (ed.): *EDI and the law*. London (1989).

DOMSREGISTER

Ugeskrift for Retsvæsen

Tidsskrift for Bolig- og Byggeret

Tidsskrift for Kriminalret

Norske højesteretsdomme

Svenske højesteretsdomme

Amerikanske domme

STIKORD

En række tværgående emner i denne ordliste optræder under forskellige systematiske sammenhænge (tekniske eller juridiske, almene eller specielle). Meningen er, at man dermed kan slå sådanne emner op ud fra forskellige kriterier.

I listen optræder tillige henvisninger til de lovbestemmelser, hvortil der i bogen er knyttet særlige fortolkningsbidrag. Henvisningerne til enkelte lovbestemmelser er derfor ikke udtømmende.

*Ord, der er forsynet med *, optræder tillige i IT-ordbogen, s. 25 ff.*

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z

Æ

Å