

**Forbrugerens
retsbeskyttelse i
grænseoverskridende
digitale net**

Erhvervsministeriet, juni 1997

**Forbrugerens retsbeskyttelse i
grænseoverskridende digitale net**

Publikationen kan købes for
75,00 kroner inkl. moms.
Sælges hos boghandleren eller ved
henvendelse til:
Schultz Information
Herstedvang 10
2620 Albertslund
Tlf.: 4363 2300
Fax: 4363 5329
E-post: schultz@schultz.dk

Publikationen kan afhentes hos:
Schultz Erhvervsboghandel
Vognmagergade 7
1120 København K.

Publikationens kapitler "Konklusioner
og anbefalinger. Et oplæg til debat"
og "Executive Summary - Concluding
chapter for a report made by The
Danish Ministry of Business and
Industry on The Legal Protection
of Consumer Rights in Relation to
Transnational Digital Networks:
Conclusions and Recommendations.
An Introduction for Debate"
kan hentes på Erhvervsministeriets
hjemmeside: www.em.dk

Udgivet af:
Erhvervsministeriet
Slotsholmsgade 10 - 12
1216 K.
Tlf.: 3392 3350
Fax: 3312 3778
E-post adresser:
Internet: em@em.dk
X.400: C=DK; A=DK400; P=EM; S=EM

Design: Ole Jensen,
Grafisk Tegnesteue
Tryk: J. H. Schultz Grafisk A/S
Oplag: 2000

ISBN: 87-601-1915-2

Indholdsfortegnelse

Problemstilling og kommissorium	7
I. Konklusioner og anbefalinger. Et oplæg til debat	9
1. Indledning og overordnet vurdering	9
2. Fordele	11
3. Internationale aspekter af Internettet	12
4. Udfordringer	13
II. De grænseoverskridende digitale net	19
1. Problemstillingen	19
2. Den digitale teknik	20
3. Internet	21
4. Kommunikationsformer på Internettet	24
a. Elektronisk post og filoverførelse	24
b. Kommunikation i lukkede brugergrupper	24
c. Hjemmesider	24
5. Identifikation på Internettet	25
6. Domænenavne og Internet-adresser	26
7. Kryptering	29
8. Elektronisk handel	30
a. Begreb	30
b. Præstation af ydelser	31
9. Søgetjenester på Internettet	32
10. Internettets styring	33
11. Intranet	34
12. Betalingsformerne	34
a. Betalingsbegrebet og Internet-betaling	34
b. Mikro- og makro-betalinger	35
c. Ideelle krav til Internet-betalingssystemer	36
d. Konto-til-konto betalinger	37
Home-banking-systemer	38
PaymentLink	38
Netcheck	38
e. Kreditkort-baserede betalinger	38
f. Den elektroniske pung	39
Digicash	40
CyberCoin	41
Mondex	41
Danmønt-kort	42
Secure Electronic Commerce	42
III. Forbrugerrisici	43
1. Nye afgrænsningsspørgsmål	43

a. Produkt- og løsningsbegreberne	43
b. Fuldblydelseshandlinger	44
c. Forbrugerbegrebet	45
d. Markedsbegrebet	46
2. Beskyttelse af forbrugerens person	48
a. Kompromittering	48
b. Almindelig databehandlingsbeskyttelse	49
c. Elektroniske spor	50
d. Direkte markedsføring	53
3. Sikkerhedsspørgsmål	54
a. Fysisk sikkerhed	54
b. Pengeværdier	55
4. Betaling og finansiering via Internettet	56
a. Økonomisk sikkerhed	56
b. Betalingskort	57
c. Småpengekort	57
5. Aftaleindgåelse	58
a. Den digitale viljeserklæring	58
b. Web-pacts	61
c. Inkorporering	63
6. Retssstilling og retsbeskyttelse i øvrigt	64
a. Overblik over komplekse transaktioner	64
b. Købeloven	65
c. Leveringsbegrebet	65
d. Lovvalg og værneting	66
e. Fortrydelsesret	69
f. Selvreguleringens implikationer	72
g. Formkrav	72
h. Immaterialretlige begrænsninger	74
i. Bevisproblemer	78
7. Markedsføringsspørgsmål	79
a. Problemstillingen	79
b. Identifikation af den forretningsdrivende	81
c. Påtrængende markedsføring m.v	82
d. Sponsorering	84
e. Overblik, oplysning og gennemsigtighed	84
f. Lighed, konkurrence og rimelighed	85
g. EU-tiltag	85
8. Konkurrencespørgsmål i øvrigt	86
a. Standardisering	86
b. EU-ret, herunder konkurrenceret	88
IV. Principielle reguleringsovervejelser	89
1. Ressortafgrænsning	89
a. Nationalt	89
b. EU	89

2. Retspolitisk udgangspunkt	91
a. "Læren om digital fartbegrænsning"	91
b. Regulering eller selvregulering	91
3. Jurisdiktionsspørgsmålet	94
4. Styringsproblemerne	96
5. Ansvarsproblemerne	96
6. Specifikke reguleringstiltag	101
a. Beskyttelse af forbrugerens person	101
b. Sikkerhedsspørgsmål	102
c. Forbrugerens retsstilling og retsbeskyttelse	102
V. Executive Summary	105
1. Introduction and Superior Valuation	105
2. Advantages	107
3. International Aspects of the Internet	108
4. Challenges	109
Ordforklaringer	115
Forkortelser	121
Litteraturliste	123

Problemstilling og kommissorium

I begyndelsen af 1996 igangsatte Erhvervsministeriet et projekt, der skulle søge at belyse de særlige problemer, som den stigende anvendelse af grænseoverskridende informationsteknologi (anvendelse af internet-forbindelser m.v.) rejser for forbrugerbeskyttelsen.

Professor dr.jur. Mads Bryde Andersen, Københavns Universitet, blev udpeget som projektsagkyndig. Der er herefter afholdt en række møder mellem ministeriet, Forbrugerstyrelsen og den projektsagkyndige, hvor der blev enighed om at indkredse projektet således, at det omfatter følgende elementer, svarende til inddelingen af nærværende udredning:

- * Hvilke retlige problemer kan på nuværende tidspunkt identificeres indenfor ovennævnte kategorier; hvordan kan de tænkes bedømt efter gældende ret og vil en sådan bedømmelse harmonere med den gældende retspolitiske opfattelse?
- * Hvor kan det tænkes, at disse problemer vil blive genstand for politisk behandling?
- * Hvilken stillingtagen bør Danmark formulere, når en sådan politisk behandling aktualiseres?

Redegørelsens Kapitel I indeholder en beskrivelse i oversigtsform af de centrale og principielle problemstillinger, handel på Internettet rejser for forbrugerne, samt en skitsering af en række forslag og anbefalinger til mulige foranstaltninger og reguleringsinitiativer til at imødekomme den nye teknologis udfordringer. Dette tænkes brugt som et oplæg til debat.

Selve redegørelsen er bygget op således, at der i kapitel II redegøres for emnets tekniske forudsætninger: Først skitseres den digitale teknik, programmeringsteknologierne og de nye digitale kommunikationsnet (herunder navnlig Internet). Dernæst omtales de særlige teknikker til betaling m.v. på Internet.

I kapitel III, der udgør rapportens hovedafsnit, skitseres de risici, der tegner sig i dag inden for de ovenfor anførte risikoområder. Dernæst redegøres der i kapitel IV for, hvor i nationale og internationale fora disse problemer allerede er blevet og fremover kan tænkes at blive behandlet, ligesom der drøftes nogle muligheder for, hvorledes Danmark kunne formulere sine synspunkter i disse sammenhænge, eventuelt ved at gå forud med forslag.

Redegørelsen afsluttes med en engelsk udgave af redegørelsens Kapitel I.

Projektgruppens medlemmer:

Professor, dr. jur. Mads Bryde Andersen, Københavns Universitet
Kontorchef Kim Sparlund, Forbrugerstyrelsen
Kontorchef Charlotte Münter, Erhvervsministeriet
Fuldmægtig Eytan Mizrahi, Erhvervsministeriet

København, den 16. juni 1997

I. Konklusioner og anbefalinger.

Et oplæg til debat

1. Indledning og overordnet vurdering

Internettets væsentligste formål er i dag informationsudveksling. Den teknologiske udvikling har indebåret, at Internettet er blevet stadig mere sofistikeret og nemmere at bruge. Dette har medført, at virksomhederne og forbrugerne har taget Internettet til sig.

Internettet er således i stadig større omfang blevet et markedsføringsinstrument, som virksomheder, offentlige myndigheder og interesseorganisationer benytter for at få kontakt med borgerne. Samtidig benytter stadig flere borgere Internettet som kommunikationsmiddel. Nettet er kendetegnet ved, at det anvendes til envejs-kommunikation, f.eks. når to personer sender e-post til hinanden, eller når en person læser en hjemmeside og til flervejs-kommunikation, f.eks. i form af "opslagstavler"/"kontaktfora" m.v., hvor en bredere og måske ligefrem ubegrænset personkreds har adgang til at hente/indlægge information. Internettet kan også anvendes til interaktiv kommunikation.

Internettet er kendetegnet ved, at det er "grænseløst" forstået således, at når information først er tilgængelig ét sted på nettet, er informationer som udgangspunkt frit tilgængelige for alle på samme tid - uanset hvorfra i verden, man søger information. Og det vel at mærke uden væsentlige omkostninger for den, der indlægger oplysningerne. Endvidere kan der ske en hurtig og dermed løbende ændring og opdatering af de informationer, der er tilgængelige på f.eks. en hjemmeside.

Samtidig er Internettet kendetegnet ved, at det ikke er muligt at udpege en central kontrolinstans, som kan påse, at det, der lægges på nettet, opfylder visse regler. Internettet adskiller sig således markant fra andre medier - f.eks. TV og bøger - hvor udgiveren har "kontrol over", hvilken information mediet videregiver.

Disse forhold indebærer, at Internettet populært sagt er uafhængig af tid og sted, og at den enkelte har fået væsentlig nemmere - ikke blot ved at indsamle information, men også ved at sprede information; herunder påtrængende, urigtig, uetisk eller ligefrem ulovlig information.

Den stadige udvikling af Internettet må forventes at indebære, at det i stigende grad får karakter af en markedsplads, hvor virksomheder og forbrugere kan handle direkte med hinanden, og hvor betalingen kommer til at ske direkte over nettet. Internettet vil således i stadig større omfang blive brugt i kommercielt øjemed. Denne udvikling stiller en række krav til såvel forbrugerne som virksomhederne og myndighederne. Internettet vil ændre væsentligt ved eksisterende samhandelsmønstre og konkurrenceforhold.

De åbne digitale net skaber ikke kun nye markedspladser, men også nye produkter - såkaldte digitale produkter - som ikke eksisterer i fysisk form, men som alene leveres i digital form, og som hentes ind på brugerens computer via Internettet. Som eksempler på digitale produkter kan nævnes edb-programmer samt andre informationsprodukter, herunder nyhedsstof, bøger og musik.

Fremkomsten af såvel nye og grænseløse markedspladser som af rene digitale produkter rejser en række forbrugerpolitiske udfordringer. Rapporten peger på en række forbrugerrelevante risikoområder, og den indeholder en række overvejelser om en tidssvarende forbrugerpolitik i forhold til grænseoverskridende markedsføring og handel, som sker via åbne digitale net. En sådan politik må være afbalanceret mellem forbruger- og erhvervsinteresser, og den må samtidig tage hensyn til de åbne nets klare samfundsmæssige fordele og perspektivrige dimensioner. Endelig må politiken tage hensyn til, at informationsteknologien er inde i en hastig udvikling, som løbende vil kunne ændre de risikoområder, som ud fra en forbrugerpolitisk synsvinkel har størst prioritet.

Hvis Internettet skal have en fremtid som et succesfuldt middel til effektiv, hurtig og billig omsætning af varer og tjenesteydelser, er det vigtigt, at der løbende tages initiativer, som minimerer de væsentligste risici, således at erhvervslivet og forbrugerne har tillid til Internettet. Det er samtidig vigtigt, at disse initiativer tages så hurtigt som muligt, idet det hverken for virksomhederne eller forbrugerne er hensigtsmæssigt, at der på centrale punkter er tvivl om, hvilke spilleregler der gælder. Det er således ikke hensigtsmæssigt, at man mere generelt fører en "laissez faire"-politik, hvor man anfører, at de påpegede tvivlsspørgsmål/problemer først må finde deres løsning ved, at myndigheder og domstole (forsøger at) anvende den gældende lovgivning.

OVERORDNET VURDERING:

Internettet kan medføre flere fordele for forbrugerne:

- Forbedring af forbrugernes muligheder for at træffe rationelle forbrugervalg,
- Styrkelse af den politiske forbrugers indflydelse,
- Øgede muligheder for at overgå fra masseproduktion til kundetilpasset produktion, samt
- En stigning i antallet af leverandører samt fremkomsten af nye produkter - herunder digitale produkter - hvilket alt andet lige vil føre til skærpet konkurrence og dermed lavere priser.

På den anden side rejser Internettets brug af digital informationsudveksling en række forbrugerpolitiske betænkeligheder, hvor navnlig følgende må fremhæves:

- Virksomhederne får helt nye muligheder for at indsamle, bearbejde, videregive og bruge informationer om den enkelte forbruger.
- Det bliver væsentlig nemmere og billigere for virksomhederne at komme i kontakt med forbrugerne, hvilket øger mulighederne for at anvende påtrængende og uetiske markedsføringsmetoder.
- Internettets grænseløshed indebærer, at visse personer/virksomheder kan udnytte, at nogle lande ikke har en lovgivning, som giver borgerne en acceptabel beskyttelse.

Derfor er de væsentligste forbrugerpolitiske udfordringer ved Internettet:

- At sikre forbrugerens integritet, såvel med hensyn til virksomhedernes indsamling og brug af personhenførbare informationer, som virksomhedernes brug af påtrængende og uetiske markedsføringsformer,
- At sætte forbrugerne i stand til at bruge Internettet, så Internettets positive sider kan blive en realitet,
- At sikre, at dansk lovgivning løbende - og så tidligt som muligt - tilpasses den igangværende IT-udvikling,
- At øge det internationale samarbejde, således at der på centrale områder etableres international lovgivning, og således at myndighedernes muligheder for at samarbejde forbedres.

2. Fordele

Fordelene ved handel på det globale net er mangfoldige. Forbrugeren kan i et hidtil ukendt omfang - få uhindret og fleksibel adgang til de informationer, tilbud, nyheder m.v., der lige netop interesserer ham. Han kan modtage reklamer og tilbud fra udbydere på den anden side af jorden lige så enkelt som det materiale, der kommer fra den lokale forretning. Informationerne er tilgængelige i alle døgnets timer, alle ugens dage - og principielt uanset hvor forbrugeren måtte befinde sig. Forretningernes traditionelle åbningstider vil spille en mindre rolle. Reklamerne kan sammenlignes hurtigt og effektivt, f.eks. ved hjælp af særlige søgeprogrammer, så det bliver nemmere at sortere i mængden af reklamemateriale og finde frem til det billigste og mest fordelagtige tilbud. Annoncerne kan uden større udgift for annoncørerne indeholde meget udførlige informationer om produkternes egenskaber og indhold. Endvidere kan informationerne løbende ajourføres, således at informationsniveauet forbedres.

Teknologien åbner mulighed for, at reklamerne på nettet udover tekst kan indeholde billeder, lyd og tredimensional grafik. Mediets interaktivitet betyder, at forbrugeren ved et klik på musen kan aktivere det udstillede produkt. Forbrugeren kan således f.eks. vende frakken om og se dens bagside/foer eller opleve et produkts bevægelsesmuligheder. Forbrugeren vil også kunne designe produkter, der opfylder netop forbrugers ønsker. Dette kan ske ved at kombinere materialer, moduler, farver m.v. Der åbnes mulighed for hurtig og enkel bestilling af varer, og internettet vil understøtte den igangværende udvikling, som indebærer, at stadig flere varer bliver produceret efter forbrugers individuelle ønske og behov.

Da forbrugerne ikke behøver at møde op i forretningen, er de sikret lige behandling og information uanset etnisk oprindelse, hudfarve, køn eller religion.

Internettet vil skabe øget konkurrence. Samtidig vil en række virksomheder kunne mindske deres omkostninger (til lokaler, lager, annoncering m.v.) ved brug af Internettet. Det forventes således, at Internettet - hvis det bruges på den rigtige måde - vil kunne forbedre forbrugernes muligheder for at træffe rationelle forbrugsvalg. Dette forhold vil antageligt medføre billigere priser på en række produkter.

3. Internationale aspekter af Internettet

Elektronisk handel giver ikke alene forbrugerne fordele men rummer også væsentlige risici. Sikring af forbrugernes interesse imod misbrug af de nye teknologiske muligheder må naturligvis foretages på en måde, som ikke undergraver Internettets fordele som åben og lettilgængelig informationsudveksling. Opgaven er herefter at formulere og gennemføre en politik, som tager højde for Internettets særlige "natur" med den unikke, decentraliserede og internationale struktur, således at forbrugerne vil få gavn af teknologiens bekvemmelighed med størst mulig retssikkerhed.

Internettets grænseløshed indebærer, at et enkelt land ikke vil kunne lovgive og håndhæve egne regler over for alle udenlandske borgere og virksomheder. Det er derfor givet, at internettet kræver en opprioritering af internationalt samarbejde, såvel om udarbejdelsen af nye/harmoniserede regler som om håndhævelsen af reglerne.

Da Internettet er globalt vil det være ønskeligt med samarbejde i et fora, der er så internationalt som muligt. Dette vil kunne være i nordisk regi, EU eller OECD. Det nordiske forum er - på grund af det kulturelle fællesskab, den retslige enhed og de tætte kommunikationskanaler - velegnet til først at afprøve muligheder for fælles forslag og initiativer. De initiativer, der i nordisk regi er enighed om, vil man herefter kunne søge fremmet enten i EU-regi, OECD-regi eller eventuelt i FN-regi.

Selvom internationalt samarbejde er ønskeligt, kan nationale og regionale instanser (f.eks. danske myndigheder og EU) ikke afvente "globale løsninger", idet disse ikke er realistiske inden for en acceptabel tidshorisont. Virksom-

hederne må derfor være indstillet på, at nationale myndigheder og regionale instanser tager initiativer, som vil regulere deres adfærd på internettet - også selvom der findes lande, som ikke vil finde anledning til at påtale eller regulere den pågældende adfærd.

Virksomhederne må således være opmærksomme på, at Internettet i den grad giver udtrykket "den globale landsby" mening. Når virksomhederne går på Internettet, kommer de i kontakt med forbrugere og myndigheder i en lang række lande (landsbyer), som interesserer sig for, hvad der findes på Internettet, og som er parate til - ud fra netop deres etiske, religiøse og politiske opfattelser - at reagere på det materiale, som støder dem.

For virksomheder indebærer dette i praksis, at de - når de går på Internettet med en hjemmeside - må være opmærksom på, at de politiske forbrugere i ethvert land kan reagere, fordi de finder, at virksomhedens adfærd (på internettet) er uetisk/uacceptabel.

4. Udfordringer

Størstedelen af de problemer, en forbruger kan støde på, når forbrugeren anvender Internettet, kan genfindes i den "almindelige kommercielle verden", men nogle af problemerne ændrer karakter på grund af Internettets særlige egenskaber. Der er således ikke tale om, at man står over for en lang række ukendte forbrugerpolitiske udfordringer, men derimod at man står over for nogle få nye og en række kendte forbrugerpolitiske udfordringer, som dog på flere punkter væsentligt har ændret karakter.

Det grundlæggende udgangspunkt bør være, at man så vidt muligt bør undgå særregler, som alene regulerer Internettet. Er der behov for ny eller revideret lovgivning, bør reglerne i størst muligt omfang gælde uafhængigt af, om handlingen sker over et åbent digitalt net eller via andre medier. Gældende lovgivning, som findes utidssvarende, må i nødvendigt omfang revideres og tilpasses den teknologiske udvikling. En (ny) regulering skal i videst muligt omfang udformes under hensyntagen til den dynamiske udvikling, der sker inden for informationsteknologien, og man bør så vidt muligt undgå, at reglerne virker hæmmende for en fornuftig teknologisk udvikling.

Virksomhedernes brug af Internettet vil i en årrække have karakter af "learning by doing", forstået på den måde, at virksomhederne i en årrække vil stå over for et nyt medie, som de ikke helt ved, hvordan de skal "udnytte". Dette vil indebære, at virksomhederne vil forsøge sig frem, og at en række virksomheder i denne proces vil begå en række fejl. Samtidig vil virksomhederne føle sig fristet til at bruge en række tekniske muligheder på en måde som set ud fra en samfundsmæssig synsvinkel ikke er acceptabel - f.eks. mere direkte markedsføring og øget registrering af forbrugernes adfærd.

Også forbrugerne står over for et nyt medium - og nye markedsføringstiltag. Dette stiller øgede krav til forbrugernes "kritiske sans", ligesom det øger behovet for forbrugerinformation. Det er vigtigt, at forbrugerne udnytter de

muligheder, som internettet giver for at udveksle information om virksomheder/produkter og for at påvirke virksomhederne til at handle korrekt. Det må antages, at en række af de problemer, den øgede grænseoverskridende handel medfører, på sigt vil blive reduceret som følge af forbrugernes egne rationelle adfærdsmønstre. En højnelse af den almindelige "forbrugerbevidsthed" gennem uddannelse, forbrugerinformation og lignende bør indtage en central rolle.

På baggrund af de problemstillinger, der er skitseret i rapporten, må man forvente, at bl.a. følgende problemstillinger vil få central betydning i de kommende år:

- Øget registrering af oplysninger om forbrugernes adfærd, når de surfer og handler på nettet (elektronisk spor) samt øget brug/videregivelse af disse oplysninger i den fremtidige markedsføring. Det vil ikke umiddelbart være muligt for forbrugerne eller myndighederne at vide/kontrollere, hvad der registreres, og hvordan registreringerne bruges.
- Påtrængende og/eller skjult markedsføring via Internettet, herunder brug af incitamentsordninger (rabatter m.v.), som ydes på betingelse af, at forbrugerne accepterer, at de afgiver visse oplysninger eller "modtager" visse reklamespots m.v., når de benytter nettet eller særlige ydelser, som udbydes via nettet.
- En vækst i mængden af markedsføringsmateriale. Samtidig vil markedsføringsmateriale undergå hyppigere ændringer. Disse forhold vil give flere sager, hvor myndighederne må vurdere, om markedsføringsmateriale er i overensstemmelse med lovgivningen.
- Øget brug af standardvilkår (herunder i kraft af henvisninger), samt hyppigere ændringer af standardvilkårene, kan tvinge forbrugerne til at anvende væsentlig mere tid på at tage stilling til, om de ønsker at indgå aftale på netop disse vilkår, ligesom risikoen for urimelige standardvilkår øges.
- Sager, hvor forbrugeren ved en betjeningsfejl kommer til at bestille produkter, som det ikke var forbrugerens hensigt at bestille.
- Øget antal sager, hvor produkter, der er bestilt over Internettet, enten ikke leveres (rettidigt) eller ikke svarer til de forventninger, forbrugeren havde til produktet som følge af markedsføringsmateriale.
- Bevisproblemer med hensyn til, hvilke informationer den erhvervsdrivende har givet via internettet. Hyppige ændringer af markedsføringsmateriale - og det forhold at forbrugerne ofte ikke vil være i besiddelse af det markedsføringsmateriale, som de har set på nettet - vil øge antallet af sager, hvor der er uenighed om, hvad virksomheden har stillet forbrugeren i udsigt.

FORSLAG TIL INITIATIVER:

På baggrund af de problemstillinger, der er skitseret i denne rapport, bør man navnlig overveje følgende initiativer:

- 1) At forbrugerne og virksomhederne får nem og billig adgang til Internettet, som skal fungere driftsikkert og med hurtige svartider.
- 2) At kommunikationen på Internettet kan ske i krypteret form og med anvendelse af digital signatur.
- 3) At Internettet fungerer uzensureret.
- 4) At virksomheder, der anvender Internettet kommercielt, altid skal opgive deres identitet, herunder deres fysiske adresse. Dette gælder såvel, når virksomheden anvender Internettet til markedsføring, som når den indgår aftaler med forbrugere/virksomheder via Internettet.
- 5) At ændre købeloven, produktansvarsloven og produktsikkerhedsloven. Disse love synes at være "blinde" over for eksistensen af rent digitale produkter.

På grund af retsenheden i Norden vil det være naturligt, at man søger at igangsætte et nordisk arbejde om denne problemstilling - navnlig i relation til købeloven.

- 6) At ændre dørsalgsloven, så den tager højde for de nye kommunikationsteknikker og markedsføringsformer, som informations-teknologien giver mulighed for.

Her tænkes bl.a. på risikoen for "informationsforurening", hvor en virksomhed udsender markedsføringsmateriale til en bredere personkreds på Internettet (i modsætning til markedsføring rettet mod bestemte og relevante forbrugere), uden at modtagerne har bedt om at modtage materialet. For at imødegå "informationsforurening" bør der endvidere være mulighed for, at forbrugerne over for virksomheder - der udsender "måltrettet" markedsføringsmateriale - kan frabede sig at modtage fremtidigt markedsføringsmateriale fra den pågældende virksomhed.

Ændringerne bør samtidig have til formål dels at forenkle dørsalgsloven, dels at gennemføre direktiv 97/7 om forbrugerbeskyttelse i forbindelse med aftaler vedrørende fjernsalg.

- 7) At ændre registerlovgivningen for at sikre forbrugerne mod urimelige registreringer - herunder brug af eventuelle registreringer - når de surfer eller handler på Internettet. Samtidig bør det overvejes, om EU-reglerne på området giver mulighed for tilstrækkelig beskyttelse af forbrugerne.

Da Justitsministeriet har nedsat et registerudvalg vil det være naturligt, at man i første omgang beder udvalget om at undersøge, om den gældende lovgivning/direktivet giver den fornødne beskyttelse, herunder dels om lovgivningen giver forbrugerne den fornødne viden om, hvilke registreringer, den enkelte virksomhed foretager, dels om de gældende tilsynsmuligheder er tilstrækkelige. Også IT-sikkerhedsrådet bør inddrages i disse undersøgelser.

- 8) At ændre prismærkningsloven, så virksomheder skal oplyse om priser m.v., når de giver mulighed for fjernsalg af varer og tjenesteydelser via Internettet. Ligeledes bør det overvejes, om en virksomhed, der har en hjemmeside på Internettet, mere generelt bør give samme prisoplysninger m.v. på Internettet, som de skal give ved opslag i forretningslokalet.
- 9) At ændre retsplejeloven. Straffeloven og visse særlove, f.eks. varemærkeloven, der giver mulighed for at konfiskere (eller tilintetgøre) fysisk materiale. Som supplement til disse regler bør man overveje at indføre et retsmiddel, der gør det muligt at gribe ind over for digital information og digitale produkter, som findes på åbne digitale net, og som kontinuerligt vil kunne reproducere og på ny placeres på nettet. Det bør overvejes, om retsplejeloven bør ændres, så det bliver muligt for myndighederne at pålægge Internetudbydere at lukke for en persons/virksomheds adgang til Internettet, når myndigheder og/eller domstole flere gange har grebet ind over for ulovligt materiale, som den pågældende har lagt ud på nettet. Da der er tale om et vidtgående indgreb, bør dette kun bruges i situationer, hvor andre retsmidler viser sig ikke at slå til.
- 10) At indføre en generel bestemmelse i EU om god markedsførings-skik. Reglen kan svare til markedsføringslovens § 1, således at der i alle EU-landene gælder et vist minimumskrav til virksomhedernes adfærd, blandt andet når de anvender Internettet til markedsføring.
- 11) At der arbejdes for indførelse af internationale regler, så en virksomhed kan sagsøges af myndigheder og forbrugerorganisationer - der varetager forbrugernes kollektive interesser - ved domstolene i det land, hvor virksomheden ved sin markedsføring overtræder præceptive forbrugerbeskyttelsesregler. En dom - som nedlægger et forbud/påbud, som giver forbrugeren krav på erstatning, eller som indebærer, at virksomheden ifalder bødestraf - bør være umiddelbart eksegibel i det land, hvor virksomheden har sit hjemsted.
- 12) At der arbejdes for indførelse af en international forbrugerkøbelov - f.eks. i form af en EU-forbrugerkøbelov - som gælder, når en forbruger fra et land og en virksomhed fra et andet land handler sammen i form af fjernsalg. Da der allerede er udarbejdet en international købelov (CISG), som gælder for handler mellem erhvervsdrivende, kan man hente en vis inspiration fra disse regler.

Indtil sådanne regler er gennemført, bør man fra dansk side arbejde på at ændre lovvalgskonventionens artikel 5, således at det præciseres, at det er forbrugers lovgivning, der skal anvendes, når forbrugeren foretager internationale køb via Internettet.

- 13) At der udarbejdes særlige regler, som regulerer interaktiv markedsføring rettet mod børn og unge. Disse regler bør gælde globalt, men nordiske regler eller EU-regler vil i første omgang være et væsentligt skridt i den rigtige retning.
- 14) At myndigheder og forbrugerorganisationer tager initiativer, der sikrer, at forbrugerne har viden omkring internettets muligheder og risici, samt at de får mulighed for at anvende Internettet til indhentning/udveksling af information omkring forbrugerrelevante emner.

Sammenfattende kan det konkluderes, at i dette spæde stadium af Internettets rolle som en reel global markedsplads til gavn for forbrugere og omsættere af varer og tjenesteydelser, er det næppe muligt at løse alle tænkelige forbrugerrisici ad lovgivningsvejen. Et yderligere frugtbart middel i kampen for mere loyal markedsføring, sikre produkter, troværdige betalingssystemer, bevarelse af personlig integritet og ansvarlighed ved handel på Internettet kan være en dialog og et samarbejde mellem erhvervsdrivende, industrien og forbrugere, suppleret med en række enkle nødvendige spilleregler fra lovgivernes side.

Med den hastige udvikling er det ikke urealistisk at forvente, at teknologien, gennem indførelse af sorteringsprogrammer og udvælgelsesmekanismer, vil kunne tilbyde forbrugerne en mere effektiv kontrol over hvilke informationer, der strømmer ind til den personlige computer via Internettet.

Samtidig kan forbrugerne, der går sammen, udgøre en økonomisk og kommerciel magt, der kan tvinge vareproducenter og Internet-udbydere til at forbedre kontrol og kvalitet af de udbudte produkter og at overholde bestemte spilleregler, som mærkning af de udsendte materialer, og at forsyne bestemte informationsprodukter med advarselsmærke eller internationalt vedtagne logoer og symboler. Endelig kan myndighedernes opgave være at lovgive på områder, hvor praksis vil vise behov herfor, og at uddanne forbrugerne til at bruge og nyde mediets fordele, men samtidig at være opmærksomme på dets risici.

II. De grænseoverskridende digitale net

1. Problemstillingen

Moderne informationsteknologi anvender digital teknik. Informationen repræsenteres altså ved tal - populært sagt som "nuller og ettaller". Denne talbehandling har gjort det muligt at skabe, ændre, lagre, sprede og fremvise enhver form for information, uanset om der er tale om tal, tekst, billeder, film, lyd, eller om informationen fremtræder på anden vis. Udviklingen i forholdet mellem pris og ydelse har gjort dette muligt hurtigere og mere effektivt end nogensinde før. Intet tyder på, at denne udvikling på kortere sigt vil standse.

At den effektive digitalisering har samfundsmæssige følger er forlængst erkendt og har allerede været genstand for en række udredninger herhjemme og i udlandet. Herhjemme indtager Dybkjær/Christensen-rapporten om Informationsfundet år 2000 en fremtrædende stilling, bl.a. fordi denne rapport blev grundlaget for den nuværende regerings prioritering af de IT-politiske spørgsmål. 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 det private. Rapporten er fulgt op af - indtil videre - to handlingsplaner fra Forskningsministeriet, nemlig 1) og 2). Også på EU-plan har man blikket rettet mod det særlige behov, der kan være for at regulere de livsforhold og transaktioner, der vil basere sig på digital teknik. En række af de udkomne rapporter omtales i det følgende.

Det er velkendt, at der ved forbrugerens køb af ydelser, der præsteres som digital information, kan opstå retlige problemer eller særlige beskyttelsesbehov, som kan give anledning til vanskelige fortolkningsspørgsmål og eventuelt retspolitiske behov om lovændringer. Disse problemer har allerede givet anledning til en betydelig praksis fra Forbrugerklagenævnet, jf. for sidste beretningsår, Juridisk Årbog 1995, s. 159 ff. Selvom sådanne sager kan være præget af, at ydelsen angår digital teknik (problemer vedrørende komplekse mangelstyper m.v.), er det muligt at håndtere disse spørgsmål inden for rammerne af den gældende køberetlige lovgivning, jf. Mads Bryde Andersen: Lærebog i edb-ret (1991), s. 452 ff. Det er altså ikke her, de store retspolitiske udfordringer ligger. Problemerne herom drøftes nedenfor i kapitel III.6.a.

Derimod opstår der en række nye - og til dels hidtil ukendte - spørgsmål, når forbrugeren optræder som frivillig eller ufrivillig *bruger* af de nye digitale kommunikationssystemer - f.eks. ved at forbrugeren med enkelte tastetryk/museklik fremkalder retsvirkninger, afgiver information, erhverver eller overdrager varer og tjenester og i det hele taget forpligter sig. Den digitale teknologi bruges her som *medium* for at forpligte sig og opnå rettigheder i forhold til andre brugere. Selvom brug af tekniske midler til aftaleindgåelse ikke er ukendt (automatsalg m.v.), må det erkendes, at vi her står overfor en

række tilfælde, hvor der kun er et beskedent erfaringsmateriale at bygge videre på.

Denne brug af digital teknik skyldes, at der i løbet af de seneste 5 år er etableret en række åbne digitale kommunikationssystemer, som man kan træde i kontakt med og anvende til de nævnte formål ligeså enkelt, som det er at tænde for et TV-apparat eller løfte røret på en telefon. I øjeblikket investeres der gigantiske beløb i udviklingen af disse "digitale superhighways", og dette arbejde støttes meget stærkt af offentlige myndigheder, såvel i Danmark, i EU som i USA. Det er primært disse teknologier, der giver anledning til ukendte problemstillinger. For at få overblik over problemstillingerne er det nødvendigt at se nærmere på, hvilke teknikker, der er tale om, og hvorledes de adskiller sig fra anden moderne teknologi.

2. Den digitale teknik

Når den digitale teknik har opnået så stor udbredelse til behandling og spredning af information, er det på grund af dens nye muligheder for at behandle information. Teknologien gør det muligt at frembringe 100% perfekte kopier af en informationsmængde (f.eks. en tekst, et billede eller en lydsekvens), og disse kopier kan herefter spredes med lysets hastighed til alle klodens afkroge.

Det tekniske grundlag for denne effektivitet ligger i computerens anvendelse af formalsprog. Når enhver information defineres med en numerisk værdi, bliver det muligt maskinelt løbende at kontrollere, om informationen har denne værdi, når den anvendes, lagres, overføres m.v. Samtidigt er det muligt at håndtere informationsmængden som andre numeriske værdier, der kan gøres til genstand for beregninger og dermed for *programmering* m.v. For brugeren betyder dette for det første, at den digitale information - alt efter sit indhold og efter den ramme, hvori den indgår - fremstår i "perfekt" form. Muligheden for at programmere informationssystemerne til at varetage særlige funktioner betyder for det andet, at forbrugeren ofte vil opleve, at systemet optræder "menneskeligt" (f.eks. ved at tale til forbrugeren og reagere "intelligent" på hans henvendelser). Tilmed kan forbrugeren ofte selv programmere systemet til at udføre bestemte funktioner m.v. med risikoen for, at der i overensstemmelse med en sådan forprogrammering "automatisk" påføres forbrugeren en forpligtelse.

Sammenfattende fører den nye teknologi altså til nye måder at markedsføre ydelser på, samt nye måder at forpligte sig på. Til dette kommer, at teknologien har sat forbrugeren i en ny, immaterialretlig rolle i forhold til sin leverandør og dennes leverandør. For at kunne bruge digital information - et program, en datamængde - er brugeren nødt til at *kopiere* den. Er informationen (f.eks. et edb-program eller en elektronisk bog) beskyttet af en ophavsret, vil brugeren hermed gøre noget, der kræver tilladelse (licens) efter de ophavsretlige regler. Denne placering af forbrugeren i rollen som licenshaver, rejser særlige problemer, se nedenfor i kapitel III.6.h.

Den ubesværede mulighed for at kopiere store mængder digital information i perfekte kopier til billige medier eller via teleforbindelser indebærer dernæst, at den *materielle* side af det produkt, forbrugeren erhverver, får en mindre fremtrædende placering. Store og komplicerede programmer til en værdi af tusindvis af kroner kan ubesværet overdrages på CD-ROM eller hentes ned fra Internet. De tilfælde, hvor forbrugeren køber edb-programmer m.v. ved fysisk at tage et *programprodukt* ned fra hylden, bliver stadigt færre. Fremtrædende er derimod den formidling af bitstrømme, der kan ske hurtigt og effektivt via åbne netforbindelser fra leverandør til (for)bruger. I sådanne rene informations-transaktioner bliver oplevelsen af, hvad der er "levering", "tilbagegivelse" og virkningerne af "ophævelse" af en ydelse dermed fundamentalt anderledes end i den "materielle" transaktion. Ligeledes vil spørgsmålet om afhjælpning af mangler ved det leverede blive relevant, idet afhjælpning ofte kan ske omkostningsfrit ved at formidle en ny og korrekt bitstrøm.

3. Internet

Det uden tvivl vigtigste af disse nye kommunikationsnet - og i alle tilfælde det største af dem - er Internet. Internet blev skabt i 1969 som et forskningsprojekt under det amerikanske forsvarsministerium (Department of Defence, DoD). Man oprettede et antal såkaldte *routers*, d.v.s. computere, der var bygget til at kunne modtage og afsende pakker af data, og *hosts*, d.v.s. computere, der kunne lagre programmer og data. Routers og hosts blev koblet sammen gennem et antal *netforbindelser*, som blev drevet af de offentlige teleselskaber.

Projektet betegnedes ARPA (Advanced Research - Projects Agency) og skulle tilvejebringe et decentralt datanet, som - i mangel af *ét* centralt knudepunkt - ville være mindre sårbart over for militære angreb eller sabotageforsøg. Dette mål blev opnået ved, at man tilvejebragte et stort antal netforbindelser mellem de mange computere. 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 rute mellem to computere.

DoD trak sig i 1991 ud af Internet-samarbejdet for i stedet at opbygge det lukkede MilNet. Internet blev herefter videreført af uddannelsesinstitutionerne under en stigende kommerciel deltagelse. Internet var - og er - ikke det eneste globale netværk. Andre eksempler er CompuServe og IBM Global Network. Da disse net imidlertid er koblet sammen med Internet i dag, taler man ofte om "Internet", selvom der er tale om flere net, og det siges da også, at Internettet er et netværk bestående af netværk.

De standarder, der ligger til grund for Internet, er ikke skabt af en enkelt aktør, men derimod af den gruppe af aktører, der deltog i udviklingen af ARPA-nettet. Nettet blev bygget op om et antal protokolstandarder, der sikrer dataudveksling. Som følge af den kontakt, der består mellem DoD og de amerikanske universitetsforskningsmiljøer, blev ARPA-nettet gradvis taget i brug i universitets-verdenen.

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. Protokollen benytter sig af såkaldt "packet-switching": Hver meddelelse ("brev") deles op i et antal mindre meddelelser ("postkort"), der herefter postes. 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 bliver optaget, kan det tænkes, at nogle postkort må komme frem via andre routere. Først når alle postkortene er fremme ved modtageren, samles de, så det oprindelige brev igen dannes.

Denne funktion kan beskrives som kommunikation *uden central styring*. Det er ikke nødvendigt, at én computer styrer kommunikationen. Det enkelte "postkort" finder selv frem til sit bestemmelsessted, hvor det stykkes sammen med de andre "postkort" og dermed danner den oprindelige meddelelse.

Internet-protokollen anvendes, uanset hvordan afsender og modtager kommunikerer. Den meget udbredte kommunikationsform på Internettet er *elektronisk post*, men en mindst ligeså udbredt er brug af *databaser* eller anden informationsudbud. I takt med udbredelsen af Internettet er stadigt flere databaser blevet tilsluttet. Oprindelig skete opkald til og indhentning af information fra disse databaser på samme måde som afsendelse og modtagelse af elektronisk post, nemlig ved målrettede søgninger mod specifikke adresser.

I 1992 udvikledes en ny teknik til at sende kommunikation via Internet-databaser, nemlig ved brug af såkaldte "hypertekst-links". *Hypertekst* er tekst, der er kodet på en sådan måde, at den ikke nødvendigvis behøver at blive behandlet, som man læser en sætning, altså som en række af tegn, der er struktureret fra venstre mod højre. I hypertekst er teksten forsynet med koder, som er indsat ud fra *redaktionelle* overvejelser. På grundlag af disse koder kan brugeren strukturere teksten, som han vil (alt efter, hvad koderne tillader), og han kan f.eks. beslutte sig til at læse den ikke-lineært, f.eks. "foldet ud" efter 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.

Hypertekst kan for det første anvendes på Internet, ved at brugeren *inden for en tekst* "klikker" på bestemte ord, for herved at bevæge sig ind i underniveauer af den. Men for det andet kan teknikken også benyttes til at sætte brugeren i forbindelse med *andre tekster* (andre databaser, hjemmesider m.v.), som der, ved den forudgående kodning, skabes en umiddelbar netforbindelse (såkaldt hypertekst-link) til. F.eks. kan en bruger "klikke" sig fra ét niveau i teksten på en skærmside (f.eks. et stikord i en database) til et andet niveau (f.eks. den side, hvor stikordet forekommer), og derfra måske til en helt anden tekst (f.eks. en anden database, der da er forbundet med denne hypertekst-link). Når man anvender hypertekst på Internettet, mærker brugeren ikke, hvorfra han henter sin information. De 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.

Kombinationen af hyptertekst-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 Internettet stiller information til rådighed over hele verden. Brugerens adgang til WWW er hans browser-program. Der findes i dag forskellige browserprogrammer. Flere centrale udbydere satser i øjeblikket på, at deres teknologi kommer til at sætte standarden for kommunikation på nettet, ganske som DOS satte standarden for 1980'ernes PC-teknologi og Windows for 90'ernes.

Det er navnlig udviklingen af WWW, der har fået Internet til at eksplodere. I 1981 var færre end 300 computere forbundet med nettet. I 1989 var tallet 90.000. I dag regner man med, at der er mere end 9.400.000 værtscomputere (hosts) knyttet til Internettet. Man regner med, at der i 1995 var 170.000 kommercielle adresser på Internettet - en seksdobling i forhold til året før. De analyser, der foreligger, når til meget forskellige tal. Open Market Inc. anslår antallet af deciderede forretningssteder til at være på 20.000; Andersen Consulting opgør tallet til 100.000 i 1996 mod 1.700 i 1994. En rapport fra McKinsey & Co. anslår værdien af den deciderede online-handel til 350. mio. US \$, og tallet ventes at eksplodere efter årtusindeskiftet.

Denne voldsomme vækst kan forklares ved at sammenligne nettet med de digitale kommunikationsformer, der tidligere stod til rådighed. Det har længe været muligt - for beskedne midler - at forbinde en PC med det offentlige telefonnet. Denne form for transmission skete forholdsvis langsomt, fordi telefonnettene oprindeligt var bygget til tale i *analog* form og ikke til talbehandling i *digital* form. En bruger, der ville transmittere data på denne måde, måtte derfor modulere dem til digitale signaler, ligesom han for at kunne læse modtagne telefon-data måtte udføre en demodulation. Redskabet hertil var - og er - et såkaldt modem (*modulation/demodulation*), men dette redskab var indtil Internettets salgssucces forbeholdt særligt interesserede brugergrupper, bl.a. fordi det krævede en vis teknisk ekspertise hos afsenderen at tilpasse modemets den kommunikationsform, modtageren anvendte - og omvendt.

Problemet er velkendt, også fra tidligere forløb af den IT-teknologiske udvikling: Først da IBM med DOS-styresystemet gik foran og satte standarden for PC'en, blev der skabt grundlag for det brede marked for PC'ere. Dermed får disse underliggende standarder en vis indirekte betydning for forståelsen af Internettet. Problemerne herom berøres nedenfor i kapitel III.8.a.

Denne massive udbredelse af et kommunikationsmedium, der kan bestorme den enkelte bruger med massive informationsmængder, og som præsenteres i en form, der giver mulighed for interaktiv dialog, har aktualiseret spørgsmålet om forbrugerbeskyttelse. En virksomhed, der ønsker at begrænse sine udgifter til annoncering på papir eller i æterbårne massemedier, kan henvise til en hjemmeside på WWW, ligesom virksomheden ved hjælp af E-post meget billigt vil kunne sende reklame direkte til den enkelte forbrugers PC'er. Sådan E-post kan ske ved hjælp af virksomhedernes registre om kundernes E-post eller ved "cold-calling", hvor virksomhedens computer automatisk sender E-post til en række bestemte adressater. Indgår virksomheden i en international koncern, vil

den ofte henviser til en international hjemmeside, hvor oplysningerne foreligger på engelsk. Dette rejser en række spørgsmål om, hvor grænserne går for vildledende reklame m.v.

4. Kommunikationsformer på Internettet

a. Elektronisk post og filoverførelse

Da internettet 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"), eller ved at der overføres elektroniske meddelelser, d.v.s. særskilte meddelelser (elektronisk post) og isolerede tekstmængder (såkaldt filoverførelse).

b. Kommunikation i lukkede brugergrupper

Undertiden finder grupper af brugere sammen for at kommunikere fra *en til mange* ("one-to-many"). Dette kan f.eks. ske på grundlag af en værtscomputer, som på initiativ af en enkelt bruger eller grupper af brugere stilles til rådighed for et bestemt antal udefra kommende brugere. Kommunikation i lukkede brugergrupper har været kendt længe før Internettet, nemlig ved de såkaldte bulletin board systems (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 en udvalgt 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 Internettet, er, at et hovedkontor kommunikerer med sine afdelingskontorer via modemforbindelser eller med teleforbindelser, der har været lejet til formålet.

c. Hjemmesider

En hjemmeside er en database, der er tilsluttet Internettet, og som præsenterer sig i grafisk form i overensstemmelse med en af de standarder, der er vedtaget for Internettet, f.eks. i form af tekst, grafik og anden information. Det kendetegnende for hjemmesiden er den grafiske brugergrænseflade, der med det rette udstyr (grafikkort og højopløselig farveskærm) får hjemmesiden til at tage sig ud som en avanceret elektronisk opslagstavle.

Hjemmesider er typisk forsynet med hypertext-links, således at 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 m.v.). 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.

Der er ingen retlige begrænsninger i adgangen til at oprette hjemmesider på Internettet, 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 (WebSite). Ved hjælp af standardprogrammer kan en virksomhed sætte en hjemmeside til rådighed på Internet. En erhvervsvirksomhed, som ikke selv ønsker at stå for dette arbejde, kan henvende sig til en leverandørvirksomhed, der yder denne service - et såkaldt "web-hotel". En tredje løsning er at lade en professionel designer udarbejde hjemmesiden. Denne løsning vil navnlig være relevant for virksomheder m.v., der imødeser en intens kommunikation til og fra hjemmesiden, eller som ikke kan leve med de pladsmæssige begrænsninger, som et web-hotel typisk vil sætte for hjemmesidens udformning.

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 ske for, at virksomheden kan vurdere, 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 bevis. Medaljens bagside er, at denne registrering kan true forbrugers integritet. Dette kan dels ske, hvis lagrede oplysninger om, hvad, hvornår og hvordan forbrugeren har efterspurgt bestemte produkter, kompromitteres, dvs bliver tilgængelige for andre. En trussel mod forbrugere kan endvidere ske derved, at den virksomhed, som forbrugeren har henvendt sig til på Internettet, foretager sådanne markedsføringstiltag, der indebærer den omtalte form for registrering. Spørgsmål om de såkaldt "elektroniske spor" drøftes i kapitel III.2.

5. Identifikation på Internettet

Kommunikation på Internettet foregår altid til og fra Internet-adresser. Når man kommunikerer med andre på Internettet og måske ønsker at indgå aftale med dem, er der behov for at kunne identificere sig og modparten. Behovet for identifikation af modpartens "adresse" på nettet ("adresseidentifikation") er nødvendig for at kunne gentage kontakten. Dernæst er en identifikation af den retlige identitet, der råder over adressen ("personidentifikation"), nødvendig for at opnå sikkerhed for, at indgåede forpligtelser opfyldes. Som Internettet er organiseret, har man *kun* sikkerhed for adresseidentifikation. Elektroniske postadresser udstedes decentralt af de enkelte Internet-udbydere. Derfor er det en enkel sag for en person eller en virksomhed at gemme sig under skiftende net-identiteter. Det behov, der er for at kunne identificere den bagvedliggende identitet ("personidentifikation"), søges løst gennem *digital signatur*.

En digital signatur er et talbevis, der kan dokumentere, at afsenderen af en digital meddelelse er, hvem han giver sig ud for at være. Dermed får

modtageren sikkerhed for meddelelsens autencitet både i relation til indholdet og afsenderens identitet. Den teknik, der anvendes til digital signatur, anvender matematik og udnytter edb-teknologiens muligheder for hurtig talbehandling. Meddelelsen opfattes som en talværdi (populært sagt en række ettalere og nuller), og denne talværdi bliver nu bearbejdet i overensstemmelse med en matematisk algoritme, således at der fremkommer en ny talværdi. Når man kan betragte dette hele som en digital signatur, skyldes det muligheden for, at tredjemand kan *verificere*, at den nye talværdi er skabt på grundlag af den gamle talværdi. Hvis værdien 7 skal påføres en digital signatur ved hjælp af algoritmen "+ 1", udgør den digitale signatur tallet 8. Såfremt modtageren B ved, at kun afsenderen A vil betjene sig af denne algoritme, ved B også, at signaturen "8" på meddelelsen "7" kommer fra A, ligesom B vil vide, at signaturen "33" på meddelelsen "32" kommer fra A.

Digital signatur har betydning i relation til datas *autenticitet*, d.v.s. for at dataerne er afgivet af rette vedkommende. Behovet for sikkerhed opstår først og fremmest, når der kommunikeres i åbne net, hvor den ene bit-streng ligner den anden og tilmed kan ændres og manipuleres. I papirets verden har man tilvejebragt denne sikkerhed gennem forsegling og underskrift, men den slags tiltag fungerer ikke i relation til digitale meddelelser, hvor datamediet (f.eks. en diskette) sjældent ændres permanent ved datalagringer. Skal man etablere en digital ækvivalent til papirets originalitet forudsættes i stedet brug af troværdige tredjeparter, der autoritativt udtaler sig om meddelelsens tekniske udspring.

De teknikker, der i dag anvendes til digital signatur, er selvsagt langt mere komplekse end dette eksempel lader formode. Med edb-systemers kapacitet er det muligt at anvende komplicerede matematiske algoritmer som grundlag for udregningen af den digitale signatur. De sandsynligheder, man hermed opnår, er så høje, at det i praksis ikke lader sig gøre at "gætte" eller på anden måde bryde sikkerheden i de anvendte algoritmer.

6. Domænenavne og Internet-adresser

En Internet-adresse fungerer på samme måde som et telefonnummer og består i sin maskinlæsbare udformning også af et antal tal (f.eks. 194.72.244.100). For brugeren fremtræder disse tal imidlertid i en kombination af bogstaver og tal. En fuldstændig Internet-adresse - f.eks. navn@firma.com - består af forskellige elementer. De elementer, der følger efter @-tegnet, betegnes som domænenavnet. Afhængig af, hvor mange punktnumre ("dots"), der optræder i domænenavnet, taler man om root, sub-root eller sub-sub-root domænenavne. Feltet umiddelbart til venstre for @-tegnet angiver andet niveau af domænenavnet og bestemmes af indehaveren.

I dag findes der verden over ca. 160 nationale hostmastere, der står for root-domæne. I relation til nærværende udredning er det væsentligt at påpege, at disse hostmasters opererer på privatretligt grundlag og uden særligt retsgrundlag.

I USA optræder syv root domæner. Root-domænet ".edu", der henviser til højere uddannelsesinstitutioner, var indtil Internettets kommercialisering det mest hyppige root domænenavn. Nu indtager ".com" (for kommercielle virksomheder) denne plads. De øvrige root domænenavne er ".org", der anvendes for ikke-kommercielle organisationer; ".int", der anvendes for ikke-kommercielle internationale organisationer; ".net", der anvendes for network gateways, ".gov", der anvendes for offentlige myndigheder og ".mil", der anvendes for militære myndigheder. Udenfor USA er topdomænenavnet sammenfaldende med indehaverens nationalitets-forkortelse, d.v.s. i Danmark "dk". Det er ikke et krav, at man skal vælge et domænenavn i eget land. Således kan danske virksomheder optræde på nettet under fx. domænenavnet ".com" eller andre.

Fordeelingen af root-domænenavne indenfor top-domænerne ".com", ".org", ".gov", ".edu" og ".net" varetages af en privat organisation ved navn NSI, Network Solutions Inc., der har lagt arbejdet i hænderne på Internet Information Center, også kaldet InterNIC. InterNIC fungerer som såkaldt hostmaster for disse root-domænenavne, der i princippet er globale, men som i praksis reserveres for virksomheder i USA eller virksomheder med internationale afsætningskanaler.

Der er fra flere sider fremlagt forslag til at forbedre registreringssystemet for domænenavne.

En international ad hoc komite, bestående af en række af de betydelige interessenter på området, har således fremlagt et forslag, der indfører 7 internationale topdomæner. Registreringen af domænenavne under disse topdomæner skal foretages af en række hostmasters geografisk fordelt over hele verden. Det foreslås, at der indføres en tvungen voldgift til løsning af mulige konflikter i den forbindelse. Voldgiftsinstitutet skal være det allerede eksisterende institut under WIPO. Ad hoc-gruppen anbefaler, at et tilsvarende system, d.v.s. med underafdelinger af topdomænet og tvungen voldgift, indføres på national plan. Forslaget skal drøftes på et møde i WIPO i maj 1997.

Fra anden side er det foreslået, at der oprettes et internationalt "varemærkeregister", der så af forbrugerne m.fl. kan bruges som adgangsnøgle på nettet. Ideen er, at der til hvert varemærke knyttes links til mærkeindehaverens officielle hjemmeside. Praktisk set vil det fungere således, at når man slår op på mærket i registret og klikker på mærket, bringes man direkte til den ønskede hjemmeside. Man behøver altså her ikke at have kendskab til domænenavnet. Dette vil lette presset på domænenavnregistre, da det så ikke længere er afgørende, hvordan ens domænenavn ser ud.

Endelig kan en forbedring af de eksisterende søgemaskiner bidrage i samme retning, idet disse ikke blot søger på domænenavnene men på selve hjemmesidernes indhold. Derfor vil man også ad denne vej kunne komme frem til den rette hjemmeside uden at kende domænenavnet.

Opindeligt registrerede NSI domæneområder efter princippet om først til mølle, først malet. Dette princip indebærer risiko for, at en virksomhed fik domæne-registrering af et navn, der indeholdt et navn, forretningskendetegn eller

varemærke for en anden virksomhed. Derfor Indførte InterNIC i slutningen af 1995 nye regler for registrering af andet niveau af domænenavnet. Ansøgeren må indestå for, at han har ret til at benytte det ansøgte navn, at han agter at anvende det, og at denne anvendelse ikke kolliderer med andres rettigheder. NSI kan tilbagekalde et domænenavn på grundlag af en retskendelse eller voldgiftsavgørelse, som fastslår, at den pågældende betegnelse tilkommer tredjemand.

Tildeling af domænenavne ligger herhjemme hos Dknet, som er den danske hostmaster. Dknet er i dag et selskab i TeleDanmark-koncernen, men selskabets arbejde med tildeling af domænenavne foregår i tæt samarbejde med Foreningen af danske leverandører af Internet-adgang (FIL), der har nedsat et Hostmasterudvalg til at behandle disse spørgsmål. I de tidligere Regler for registrering under dk-domænet, der var udstedt den 13. juni 1996, krævedes det, at en ansøger kunne dokumentere retten til det navn, der ønskedes registreret som domænenavn, f.eks. et selskabsnavn, firmanavn eller en varemærkeregistrering. Man kunne ikke registrere navne, der indeholdt begreber, stednavne eller personnavne. Det fremgik ligeledes, at alle konflikter angående disse regler henvistes til DK-Hostmaster appeludvalget, der var nedsat af FIL. Disse restriktioner blev imidlertid ophævet med virkning fra den 15. januar 1997, således at alle i dag kan registrere stednavne, personnavne og begreber, ligesom det er muligt at registrere mere end et navn, uden at man behøver at dokumentere retten til det enkelte valgte navn. Dog skal ansøgeren, når han henvender sig til sin internetudbyder, udfylde en formular, hvori man erklærer, at man ikke krænker tredjemands rettigheder. Hvis ikke navnet er registreret i forvejen, får man retten til navnet. Hermed har FIL fralagt sig ansvaret for eventuelle tvister om retten til domænenavne, da parterne henvises til de almindelige domstole.

Fra England foreligger en "Britain High Court and Justice" afgørelse af den 14. januar 1997, refereret i "Wired"-homepage (www.wired.com/news/), hvorefter det britiske stormagasin "Harrods" har vundet retten til at bruge sit navn på Internet, således at navnet "harrods.com" måtte overdrages til magasinet fra den tidligere indehaver af navnet, en gruppe af navnepirater. Dommen blev begrundet med, at der var tale om "en klar krænkelse af Harrods registrerede varemærke." Fra Tyskland foreligger en byretsafgørelse afsagt 8. marts 1996 af Landgericht Mannheim. Afgørelsen fastslår, at Heidelbergs bystyre havde ret til registrering af domænenavnet "heidelberg.de" forud for en privat virksomhed, der havde fået et sådant navn registreret forinden (efter forgæves forhandlinger med bystyret om deres ret hertil). Dommen er omtalt af Christopher Kuner i IBA International Technology Newsletter, vol. 14, no. 2, August 1996, s. 5.

Reglerne for NSI konfliktløsning kan findes på <ftp://rs.internic.net/policy>. De tilsvarende regler for Danmark ligger på URL-adressen <ftp://ftp.nic.dk/regler/>. Reglerne, der bl.a. indeholder specifikke forskrifter for, hvordan domænenavne overføres m.v., er i øvrigt for nylig blevet anfægtet under en verserende retssag, se *Roadrunner Computer Systems, Inc. v. Network Solutions Inc.*, Civil Action No. 96-413-A (E.D. Va. April 25, 1996).

Både virksomheder og personer kan få registreret flere navne. Den, der ønsker en Internet-adresse, vil typisk henvende sig til en Internet-leverandør, der som sådan optræder på nettet med sin e-post adresse, f.eks. per.hansen@teledanmark.dk., eller med sin hjemmeside under domænenavnet www.perhansen.dk.

Registreringen af et domænenavn koster herhjemme ca. 1000. kr. excl. moms, og i USA 100 USD, men er ikke forbundet med pligt til løbende betaling.

FILs nuværende regler kolliderer til dels med varemærkerettens regler, hvor man som hovedregel erhverver eneretten i relation til bestemte *vareklasser*, se vml. § 17. Varemærkeretten tillader med andre ord, at der i relation til forskellige vareklasser kan være flere ejere af et varemærke. Da varemærkeretten er national eller (med EU-varemærkeretten) regional, kan det dernæst tænkes, at virksomhed A har retten til et varemærke i land X, medens virksomhed B har den i land Y. Hvor det sidste problem tildels løses ved topdomæne-registreringen (hvor domænenavnet tildeles med landetilføjelserne .dk, .de, .uk etc.), er det andet problem noget vanskeligere at løse. Det kan tænkes, at to virksomheder anvender samme navn om forskellige grupper af varer og tjenesteydelser (f.eks. "Tivoli" henholdsvis en forlystelsespark og for fotokopipapir).

I sådanne tilfælde favoriserer først-til-mølle-princippet den forudseende part, der sikrer sig registrering først. Der har endnu ikke været danske afgørelser om retten til kolliderende domænenavne.

7. Kryptering

Man taler om kryptering, når informationen kodes, så den opnår en udformning, der er uforståelig for ude fra kommende. Kryptering har været kendt i alle samfund. Den form for kryptering, der består i at forvandle et ord ved at flytte hvert enkelt bogstav et vist antal pladser i alfabetet, er måske den mest kendte. Denne krypteringsmetode betegnes som Caesar-kryptering, fordi den først blev introduceret af Julius Cæsar. I Caesar-kryptering udgør antallet af pladser i alfabetet (i eksemplet ovenfor 1) krypteringsnøglen. Når denne nøgle er kendt af begge parter, kan den benyttes til at lukke disse parters kommunikation af for omverdenen.

En sådan kryptering betegnes som *symmetrisk*, fordi man udfører samme operation ved kodning (enkryptering) som ved afkodning (dekryptering). Asymmetrisk kryptering (eller public key-kryptering) adskiller sig herfra ved, at der anvendes to forskellige nøgler til henholdsvis kodning og afkodning. De to nøgler er indbyrdes afhængige, men man kan ikke regne den ene nøgle ud, selvom man kender den anden. Forholdet mellem de to nøgler kan sammenlignes med forholdet mellem en dansk-kinesisk og en kinesisk-dansk ordbog. Det er praktisk umuligt at oversætte en kinesisk tekst med en dansk-kinesisk ordbog og omvendt. Asymmetrisk kryptering har den fordel, at parterne ikke nødvendigvis behøver at have udvekslet nøgler med hinanden før. Ved at gøre den ene nøgle hemmelig og den anden offentlig, kan man nøjes med at udveksle den offentlige nøgle via en troværdig tredjepart, der da indestår for

nøgleindehaverens identitet. Det må forventes at dette princip vil blive lagt til grund i den kommende lovgivning om digital signatur.

Interessen for at anvende krypteringsværktøjer i forbindelse med kommunikation, ydelsespræstation og aftaleindgåelse via Internettet hænger sammen med, at dette værktøj kan løse centrale problemer:

Sikkerhed for *uafviselighed* angår risikoen for, at afsenderen af en digital meddelelse, sidenhen gør gældende, at disse data ikke er afgivet eller afsendt af ham. I papirets verden har den personlige underskrift traditionelt udgjort sikkerheden for, at afgiveren var bundet af et dokument. Men fordi underskriften netop er bundet til papiret (som den for så vidt forandrer) må man tage andre løsninger i brug for at skabe en tilsvarende sikkerhed i den digitale verden. En af disse teknikker anvender såkaldt digital signatur ved brug af troværdige tredjeparter.

At data er sikret *fortrolighed* betyder, at de ikke kan læses af uvedkommende. Interessen heri er iøjnefaldende for den enkelte (Big Brother-syndromet) og grundlæggende for den tillid, der må herske til ethvert edb-system. Fortrolighed kan sikres, hvis man lukker linjerne for uvedkommende eller låser sine datamedier inde. Men det kan man netop ikke i de åbne netforbindelser, der fungerer som en slags offentlige transportmidler, hvor alle skal kunne være. I stedet må man bruge *logisk* sikring. Til gengæld for, at data er tilgængelige, gør man dem uforståelige for uvedkommende gennem kryptering. Brugen af krypteringsværktøjer, der tillader *hemmeligholdelse* af information støder imidlertid på barrierer af anden beskaffenhed. Når kommunikerende parter krypterer, efterlader dette de kontrollerende og efterforskende myndigheder overfor det problem, at man ikke længere kan foretage aflytning med retskendelse, hvilket hidtil har været betragtet som et naturligt og acceptabelt element i myndighedernes efterforskning. Dette skisma har givet anledning til omfattende drøftelser på internationalt plan, blandt andet i Europarådet og OECD.

8. Elektronisk handel

a. Begreb

Udtrykket elektronisk handel bruges almindeligvis om kommerciel aftaleindgåelse, betaling og eventuelt præstation af ydelser ved hjælp af digitale kommunikationsnet. Elektronisk handel kendetegnes ved, at aftalens indgåelse og undertiden tilmed opfyldelse kan ske hurtigt og med et minimum af transaktionsomkostninger. Dernæst er det kendetegnende, at kontakten mellem forbrugeren og den erhvervsdrivende nås uafhængigt af tid og rum. Parterne behøver hverken være til stede på samme sted eller på samme tid, hvis blot de er i stand til effektivt og med den fornødne tillid at afgive de relevante meddelelser om, hvad der købes, til hvilken pris og med hvilke leveringsvilkår.

I USA har den føderale regering understøttet elektronisk handel med særlige bevillinger. Man har afsat et beløb på i alt 6 mio. US \$, der skal løbe over tre år, til etablering af et konsortium, ved navn CommerceNet, der bl.a. har udarbejdet kataloger over relevante aktører samt særlige services (herunder

betalingssystemer) til brug for elektronisk handel. Nærmere oplysninger herom kan indhentes på <http://www.commerce.net/>.

Herhjemme har Forskningsministeriet i samarbejde med Erhvervsministeriet samt en række private aktører i november måned 1996 fremlagt en national EDI-handlingsplan med navnet "Elektronisk handel i Danmark". Planen indeholder syv initiativer, hvoraf det første går ud på, at der senest med udgangen af 1998 skal ske en udmøntning af EDIFACT-standarder i alle brancher og sektorer, f.eks. ordrer, fakturaer, betalingsmeddelelser, transportsedler og tinglysning. Målet er at sikre en væsentlig forudsætning for virksomhedernes muligheder for at deltage på den elektroniske markedsplads, indenfor handel, produktion, transport og finans m.v. Planen er vedtaget sammen med de berørte brancher. Dansk EDI-råd vil varetage den centrale igangsættende og tværgående rolle i gennemførelsen af handlingsplanen.

Lignende initiativer er igangsat på globalt og regionalt niveau. G7-landene har i februar 1996 etableret et projekt om Electronic Commerce med undertitlen "A global Marketplace for SMEs". Under dette projekt er bl.a. nedsat en arbejdsgruppe om "financial issues". Projektets formål er at stimulere små og mellemstore virksomheder til at tage nettet i brug som markedsplads. Opfølgingsarbejdet er delt mellem EU-kommission (SME Requirements - Legal, Institutional and Technical) Japan (Global Information Network) og USA (International Testbeds for Electronic Commerce). Under EU-Kommissionens TEDIS-projekt er der igangsat en række projekter, der tilsigter at bringe EDI i praktisk anvendelse.

b. Præstation af ydelser

Når information i digital form skal præsteres som ydelse i henhold til aftale, kan dette ske på to måder. Enten ved at informationsmængden kopieres til et nyt medium, eller ved at et medium, der indeholder informationen, overdrages (med henblik på efterfølgende at blive kopieret ind i brugerens edb-system). I papirets verden sker informationsoverdragelse typisk ved overdragelse af medier (bøger, aviser, grammofonplader etc.), og denne form har også været anvendt ved de første generationer af digitale informationsprodukter (edb-programmer, CD'ere etc.). Med udbredelsen af de digitale kommunikationsnet overdrages information i stigende grad som bit-strømme via disse net, d.v.s. uden at noget medium fysisk overdrages. Sådanne overdragelsesformer giver anledning til særlige vanskeligheder, når forbrugeren ønsker at *videresælge* den information, han har *købt*. Er han afskåret herfra p.g.a. ophavsrettens regler, kan forbrugeren lide skuffelser og tab. Disse spørgsmål, der angår såvel ophavsretten som den almene aftaleret behandles nedenfor i kapitel III.6.h.

I de første digitale generationer har sådanne overdragelsesformer primært drejet sig om bogstavbaserede informationsprodukter, d.v.s. nyhedstjenester, bøger og edb-programmer. Denne begrænsning har skyldtes pladshensyn. Den digitale informationsmængde i et tekstbaseret informationsprodukt er langt mindre, end når der er tale om information i form af billeder (og herunder navnlig levende billeder) og lyd. Pladsbegrænsningen gør sig gældende, såvel når information overdrages fysisk i et medium (f.eks. en diskette eller CD-ROM), som når

information overføres via en netforbindelse (f.eks. ved såkaldt downloadning fra Internet). I takt med, at der udvikles nye teknikker, vil informationernes omfang udgøre en afgørende begrænsning, idet der vil medgå en betydelig mængde telefontid, som dels vil føles som en belastende ventetid, dels vil være forbundet med en udgift. I takt med udbygningen af nettenes kapacitet vil denne begrænsning imidlertid blive mindre betydningsfuld, og man vil dermed befinde sig i en situation, hvor en række forskellige informationstjenester er umiddelbart til forbrugers rådighed.

9. Søgnetjenester på Internettet

Som nævnt ovenfor er antallet af informationsudbydere på Internettet steget eksponentielt. Det er i dag efterhånden reglen, at erhvervsvirksomheder, institutioner, offentlige myndigheder, og et stort antal enkeltpersoner viser deres ansigt med en hjemmeside på Internet.

Hermed er der opstået behov for at finde vej rundt på Internettet. Dette behov varetages gennem et antal søgnetjenester, der via hjemmesider stilles til rådighed på erhvervsmæssigt grundlag, d.v.s. finansieret gennem salg af reklamer på de relevante brugergrænseflader. Eksempler herpå er AltaVista og Yahoo. Hos disse søgnetjenester kan man søge efter emner og stikord. En søgning resulterer i et antal hjemmesider, der reflekterer på søgekriteriet.

Når spørgsmålet siden hen i denne redegørelse rejses om muligheden for at regulere markedsføringshandlinger på Internettet, er det væsentligt at være opmærksom på den rolle, disse søgnetjenester spiller. Kan der knyttes et ansvar til den handling, hvorved man leder informationsefterspørgeren hen til en hjemmeside, hvor der realiseres et retsbrud (f.eks. i form af ulovlig markedsføring eller spredning af anden form for ulovlig information), kan man ramme et væsentligst reguleringsbehov. Disse spørgsmål drøftes nedenfor i kapitel IV.5.

Sådanne søgnetjenester kan enten tænkes finansieret ved *brugerbetaling* (se herom nedenfor kapitel II.11. om betaling på Internettet) eller ved *sponsorering*, hvorved brugeren "betaler" for nytteværdien ved at finde sig i at blive udsat for en reklamering. Hvor holdningen til sådanne reklameringsforanstaltninger hidtil har fokuseret på brugerens interesse i at være i fred og i ikke at blive udsat for påtrængende eller upassende markedsføringshandlinger, er der en yderligere dimension knyttet til Internet-reklamering. Det er kostbart i transmissionstid at distribuere den grafiske information m.v., som den slags reklamer typisk fremtræder i, og denne tid betaler brugeren for med ventetid, transmissionstid og i enkelte tilfælde også med en øget risiko for teknisk nedbrud af kommunikationsforbindelsen. Problemerne vedrørende Internet-markedsføring behandles nedenfor i kapitel III.7.

10. Internettets styring

En række af de sikkerhedsmæssige problemer, der opstår, når forbrugere disponerer i de nye digitale kommunikationsnet, har at gøre med den særlige form for anarki, der har været fremherskende ved opbygningen af Internettet. Som nævnt ovenfor foregår der en central opgavevaretagelse ved administration og tildeling af domænenavne og i standardiseringsarbejdet. Selve Internettet er ikke underkastet nogen særlig kontrol, som dem vi f.eks. kender fra radio og TV. Som det vil fremgå af det følgende, stilles der ingen krav om autorisation til at etablere en udbyder-virksomhed. Der er tvivl om Internettets redaktionelle ansvar vedrørende det, der gør tilgængelige på nettet og vedrørende adgangen til at optræde anonymt på Internettet. At et sådant anarki er opstået skyldes utvivlsomt nettets udspring af forskningsmæssige miljøer med tradition for at styre sig selv på grundlag af fælles opfattelser af etik og god skik.

Det relative anarki hænger til dels sammen med, at der ikke er nogen "ejer" af Internettet. De telelinjer, der forbinder Internettet, er ejet af teleoperatørerne, men disse net har været lejet ud til de nationale Internet-operatører. I takt med at nye, luftbårne linjer etableres, vil denne centrale styring være stadigt vanskeligere. De protokoller, der anvendes ved Internet-kommunikation, er frit tilgængelige og er altså ikke søgt beskyttet af patenter el.lign. Deltagerne i dette standardiseringsarbejde har ikke været nødt til at skulle enes om, hvilke protokoller og hvilke former for software, der skulle anvendes.

Den datatrafik, der transmitteres over Internettet, finansieres ved, at hver bruger betaler for at få transporteret sine data fra sit eget edb-system og frem til næste netværksknudepunkt. En privat bruger opnår kontakt med Internettet ved at lade sin computer (med modem) kalde op til det telefonnummer, hans Internet-leverandør anvender. Internet-udbyderen sørger herefter for, at der opnås forbindelse til Internettet, idet brugeren kun betaler sædvanlig telefontakst, uanset hvilke adresser på Internet, han når.

Det manglende "ejerskab" til Internettet betyder, at der heller ingen særlige Internet-love findes, endsiige nogen central kontrolinstans ("Internet-politi") til at håndhæve de færdselsregler, der bør følges. Derimod er det klart, at lovgivningens almindelige regler også skal overholdes i relation til Internettet. Er det forbudt at udsprede injurier eller forhånende racistiske udtalelser, rammes man også, hvis dette sker ved hjælp af Internettet.

Der har været gjort enkelte private, og halvprivate initiativer for at råde bod på denne mangel på styring. For et par år siden etablerede en række erhvervs-virksomheder med særlig interesse i Internet-handel m.v. (IBM, Microsoft, Netscape, Oracle, Visa international m.fl.) the Internet Law & Policy Forum, tidligere Internet Law Task Force (ILPF). ILPF vil søge at fremskynde udviklingen af løsninger på de påtrængende retlige og politiske spørgsmål, der er blevet aktualiseret ved den stigende anvendelse af Internet-baseret elektronisk handel. Nærmere oplysninger om ILPF kan hentes på <http://www.ilpf.org>.

Et forsøg på at løse de problemer, der følger af den relative anonymitet, hvormed man optræder på Internet, er i USA gjort ved etablering af The

NetCheck Commerce Bureau, der tager sig af klager over forretningsdrivende på Internettet, hvad enten der er tale om manglende vilje til at efterleve aftaler eller om manglende betalingsevne. Ved at blive medlem af NetCheck opnår virksomheden et blåt stempel, der herefter vil understøtte markedsføringen. Brugeren kan tilmelde sig NetCheck og herefter opnå adgang til dette index over virksomheden samt i øvrigt adgang til at klage over bestemte virksomheder.

11. Intranet

De kommunikationsformer, tekniske grænseflader, protokoller og programmer, der understøtter Internettet, kan også anvendes ved kommunikation mellem parter, der i forvejen kender hinanden. Når virksomheder eller organisationer anvender Internet-teknologi internt i en organisation i stedet for eksterne forbindelser til Internettet, taler man om, at der opbygges *intranet*. De informationer, der kan spredes på denne vis, er f.eks. prislister (der kan produceres, distribueres og opdateres på dertil indrettede lokale "hjemmesider"), virksomhedsspecifikke biblioteker, f.eks. med manualer til betjening af udstyr (der på samme måde kan opdateres, når der indvendes nye erfaringer herom), samt elektronisk post eller anden form for intern informationsudveksling.

Den megen tale om Intranet i disse år har ikke nævneværdige forbrugerretlige perspektiver. At virksomhederne anvender de teknologier, der er udviklet til ét kommunikationsmedium med henblik på intern anvendelse, har ikke større betydning for den enkelte forbruger, end at virksomheden anvender et hvilket som helst andet værktøj i sin produktionsproces. Derimod kan virksomhedernes fokus på Internet-teknologi i deres egen informationshåndtering gøre dem mere motiverede til også at benytte denne teknologi overfor omverdenen.

Virksomhedernes interesse for at fastholde og tiltrække nye kunder, bl.a. ved hjælp af loyalitets- og bonusordningskoncepter, forstærkes og understøttes af de nye stærke databehandlingsystemer benævnt "datawarehousing" og tilsvarende. Mulighederne for en betydelig mere koncentreret og målrettet markedsføring overfor enkeltindivider eller nærmere afgrænsede grupper af personer gennem en ny og mere intensiv udnyttelse af allerede eksisterende data ses under stærk udbygning. Dette kan være i modstrid med almindelige konkurrenceretlige principper og ønsker og dermed være til ugunst for forbrugeren.

12. Betalingsformerne

a. Betalingsbegrebet og Internet-betaling

Et særligt problem ved elektronisk handel er *betalingen*. I generel betydning taler man om betaling, når en transaktion resulterer i, at kreditor med rette kan anse sig for fyldstgjort, således at der ikke længere består noget gældsforhold mellem kreditor og debitor. Dette begreb er imidlertid for vidt, idet det også

omfatter tilfælde, hvor kreditor fyldestgøres ved at indtræde i en fordring, som debitor har mod tredjemand. Derfor kan man udskille begrebet kontantbetaling som de tilfælde, hvor betalingstransaktionen indebærer, at kreditor får rådighed over rede penge eller stilles i en position, så han umiddelbart får en sådan rådighed (f.eks. ved modtagelse af en check eller overførelse af et beløb til kreditors konto).

Når spørgsmålet om "betaling på Internet" rejses, er det værd at bemærke, at Internettet i sig selv kun er et kommunikationsmiddel. Går betalingstransaktionen kun ud på, at debitor beder sin bank om at overføre et beløb til kreditor, er der ingen *principiel* forskel mellem en sådan betaling og en betaling, hvor debitor pr. brev anmoder sin bank om at udføre en bestemt transaktion, men derimod den *praktiske*, at der ved Internet-kommunikation består en langt højere risiko for, at en sådan betalingsanmodning læses - og måske forvanskes - af udenforstående.

Baggrunden for denne risiko ligger i den måde, hvorpå Internet-meddelelser transmitteres, nemlig ved, at den oprindelige meddelelse splittes op i mindre meddelelser, og sendes fra afsender til modtager via en række mellemstationer (routere) som den passerer undervejs, og hvorpå meddelelsen lagres.

Det er imidlertid ikke de tilfælde, hvor parterne i et køb indgår aftale på Internet og i den forbindelse aftaler, at køberen skal sende en check eller overføre et pengebeløb, når han har modtaget varen, der spiller den største rolle, når man diskuterer betaling på Internettet. Først og fremmest er det relevant at behandle de tilfælde, hvor betalingshandlingen indgår som led i et system, der specielt tager sigte på at løse de særlige sikkerhedsproblemer m.v., der er forbundet med Internet-kommunikation, herunder usikkerheden om, hvem der "gemmer sig" bag Internet-adresser og om, hvad der sker med informationen undervejs. Hvis banken på forhånd har tilkendegivet, at den vil udvirke en kontooverførelse, når betalingsanmodningen er afgivet via Internettet ved hjælp af en digital signatur, eller ved brug af et andet særligt betalings-system, hvortil der hører en kode m.v., kan man med rette tale om Internet-betaling.

b. Mikro- og makro-betalinger

Enhver betalingstransaktion er forbundet med omkostninger af økonomisk art. Derfor vil valget af betalingsmetode til enhver tid bero på en afvejning mellem *omkostningerne* ved at gennemføre betalingstransaktionen (f.eks. betale et checkgebyr) overfor 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 kontanter (mønter og sedler) er velegnede til småpengebetalinger (også kaldet "mikro-betalinger") som f.eks. køb af dagligdagens livsfornödenheder, men upraktiske ved større betalinger (også kaldet "makro-betalinger") 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 betalings slip via et kreditkort) når det drejer sig om ørebeløb.

Det store problem ved Internet-betaling er, at der ofte er et uforholdsmæssigt papirarbejde forbundet med at betale ved hjælp af kontooverførelser m.v. Dette skyldes, at det jo skal registreres et sted, at pengene flyttes fra A til B etc. Et andet stort problem består i at sikre betalerens anonymitet. Den forbruger, der lægger sin betaling ved supermarkedets kasseapparat, afgiver ikke dermed sin identitet, og de fleste forbrugere vil nok ikke ønske at afgive deres identitet ved en sådan betaling. Derfor vil parterne i den digitale betaling typisk ønske, at betalingen ikke efterlader "elektroniske spor".

Der er imidlertid et stort behov for at kunne udføre egentlige småpengebetalinger via Internettet, hvor udgifterne ved selve betalingshandlingen nærmer sig 0 kr., hvor selve betalingshandlingen er ligeså enkelt gennemført som de "klik", brugeren i forvejen vil udføre fra sin edb-skærm, og hvor betalerens identitet bevares. Behovet for denne enkelhed, fleksibilitet og prisbillighed skyldes at en række ydelser på Internettet - f.eks. ydelser med ophavsretsbeskyttet information - ikke kan udbydes, hvis ikke der erlægges en beskeden betaling herfor (efter princippet om "mange bække små"). Det er i høj grad tænkeligt, at der vil komme et mere massivt udbud af værdifuld information på Internettet, herunder i form af professionelt drevne fuldt opdaterede underholdnings- og nyhedstjenester m.v., når der er mulighed for at gennemføre anonyme, enkle og sikre småpengebetalinger for denne information.

c. Ideelle krav til Internet-betalingsystemer

Ovenfor er allerede skitseret et par af de ideelle krav, man vil stille til et betalingssystem på Internettet. Som det gælder på andre områder, hvor det digitale medium tages i brug i stedet for papirmediet, er der tale om, at man søger at simulere papirmediets - her de fysiske penges - egenskaber.

Først og fremmest skal betalingssystemet være *fleksibelt*, d.v.s. anvendeligt i relation til forskelligartede betalingsformer og over for flest mulige betalingsmodtagere. Ligeledes må der i kravet om fleksibilitet lægges, at flest muligt har adgang til og mulighed for at anvende betalingssystemet. Jo mere udbredt betalingssystemet er, des mere værdifuldt er det.

En anden væsentlig interesse angår den faktiske, økonomiske og juridiske *sikkerhed* i betalingssystemet. Parterne må være sikret mod *tekniske* fejl, der kan indebære, at betalingen kommer til at koste dem mere end planlagt.

Et elektronisk betalingssystem må være således indrettet, at der findes muligheder for parterne for efterfølgende at kunne dokumentere og sandsynliggøre, at betalingerne er sket, og pengene er modtaget.

Sikkerhedsmålsætningen i Internet-baserede betalingssystemer søges bl.a. tilgodeset gennem en standard (Secure Electronic Transactions (SET)), der anvender teknikker til kryptering og digital signatur ved brug af en troværdig tredjepart (herhjemme PBS). Der tænkes indledt et pilotprojekt, der vil omfatte udvalgte forretninger, der vil kunne tilbyde deres kunder at anvende dette system når de handler på nettet.

For det tredje skal betalingssystemet kunne sikre parternes *fortrolighed*. I de systemer, der betjener sig af PIN-koder (hemmelig kode) eller kontonumre m.v. er der dernæst en interesse i, at sådanne værdifulde oplysninger ikke kompromitteres.

De systemer til Internet-betaling, der findes i øjeblikket, kan inddeles efter vidt forskellig kriterier: Hvem står bag systemet? Hvilke betalingstransaktioner understøtter det? Er systemet baseret på hardware eller software? Anvender det troværdige tredjeparter? Når det lægges til grund som afgørende for Internet-betalingsbegrebet, at betalingstransaktionen udvirkes gennem udveksling af digitale meddelelser, må det afgørende for inddelingen synes at være, hvordan de forskellige systemer forvandler kontante penge (mønter og sedler) til digitale meddelelser og omvendt. Ud fra en sådan betragtning kan man sondre mellem følgende tre betalingssystemer:

- * Konto-til-konto-betalinger (homebankingsystemer)
- * Kreditkort-baserede betalinger
- * Electronic purses (den elektroniske pung, "digital cash")

Udover de teknisk begrundede forskelle mellem disse betalingsformer, rummer de hver for sig visse retspolitiske implikationer. Konto-til-konto-betalingen, der forudsætter en række oplysninger om modparten samt overførsel af identifikation til homebanking-systemet, vil tillige typisk være forbundet med en gebyrbetaling og kan derfor være problematisk at anvise som grundlag for almindelige forbrugertransaktioner. Omvendt er kreditkortbetalingen kun til rådighed for kreditværdige forbrugere, hvorved disse systemer kan siges at vende den tunge ende nedad. Den elektroniske pung sikrer en høj grad af anonymitet, samtidigt med at de kan erhverves af enhver, der er i stand til at præstere den betaling, kortet repræsenterer.

d. Konto-til-konto betalinger

Ved en konto-til-konto-betaling flyttes penge fra debtors konto til kreditors konto ved hjælp af en digital meddelelse. Denne betalingsform kendetegnes ved, at pengeinstituttet råder over det beløb, der skal fyldestgøre kreditor. Betalingen sker da ved, at debitor *giver meddelelse* til denne tredjepart (banken) om, at betaling skal ske.

Homebanking er i sig selv en kendt betalingsform, eftersom betalingen sagtens kan udvirkes - og daglig bliver udvirket - ved hjælp af papirbaserede betalingsanmodninger. De særlige problemer, der er forbundet med at gennemføre konto-til-konto-betalinger på Internettet, ligger i risikoen for, at betalingsanmodningen uberettiget læses eller forvanskes undervejs. Problemet kan løses gennem kryptering eller digital signatur. Det ligger derfor klart, at sådanne betalingssystemer kan drage fordel af, at der opbygges almindelige rutiner og systemer til sikker identifikation. Om dette også er ensbetydende med, at lovgivningen om kortløse betalingssystemer med kode finder anvendelse, diskuteres nedenfor i kapitel III.4.

Home-banking-systemer

En række pengeinstitutter tilbyder i dag homebanking-systemer, der gør det muligt for brugeren at overføre penge fra og til konti med dette og andre pengeinstitutter fra sin terminal. Disse systemer er oprindeligt ikke udviklet med henblik på Internet-anvendelse. De mest udbredte af dem anvender telefonen som kommunikationsmiddel. Brugeren identificerer sig med en indtastet PIN-kode, indtaster herefter oplysninger om det kontonummer, hvorfra og -til pengene skal overføres og bekræfter herefter transaktionen, hvorefter denne udføres.

De mere avancerede af disse systemer giver brugeren mulighed for at foretage sådanne overførelser via PC'en. Mange banker har i dag sådanne systemer. De kommunikerer oftest via telenettet, men homebankingsystemer, der kan anvendes via Internettet, er under udarbejdelse. Brugeren installerer sit system og genererer i den forbindelse et nøglepar (d.v.s. offentlig og privat nøgle). Den offentlige nøgle indsendes herefter til registrering hos banken, idet brugeren herved identificerer sig med en på forhånd udleveret PIN-kode. Når nøglen er registreret, bruges den til at identificere brugeren ved de kommende transaktioner. Den krypteringsløsning, der anvendes i bankernes home-banking systemer er baseret på TeleSeC-systemet, som er udviklet af PBS på grundlag af dansk software fra firmaet Cryptomathic.

PaymentLink

Paymentlink er - i modsætning til ovennævnte - et rent Internet-betalingsystem, der baserer sig på konto-til-konto overførelser. Kunden (betaleren) giver PaymentLink fuldmagt til at debitere en af kunden udpeget konto for de betalinger, kunden foretager. Kunden igangsætter sin betaling ved at afgive en betalingsmeddelelse til betalingsmodtageren om enten at udskrive en fysisk check eller overføre et beløb fra kundens bankkonto, fratrullet et gebyr. Herefter igangsættes betalingen. Udover at sikre betalerens identitet har systemet knyttet en forbindelse fra de traditionelle bankkanaler til Internettet.

Netcheck

Netcheck tilbyder en tilsvarende løsning, omend uden forudgående fuldmagt fra kunden. Netcheck-systemet understøtter i øvrigt kun udstedelse af papirchecks.

e. Kreditkort-baserede betalinger

Den anden form for betaling kendetegnes ved at *effektuere* selve betalings-handlingen ved træk på et kreditkort. Som praksis er i dag, er de eksisterende betalingskort hyppigt anvendte betalingsformer på Internettet. Betalingen baseres her på betalerens *underretning* til betalingsmodtageren om, at der i tilknytning til en bestemt konto består en ret til at overføre et beløb til betalingsmodtageren. Betalingen sker via *kortudstederen*.

Svagheden ved disse rene kreditkortbetalinger ligger i, at betalingsmodtageren kun har begrænsede muligheder for at kontrollere rigtigheden af de oplysninger, betaleren afgiver om sit kreditkort og om sin kompetence til at råde over dette. Når betalingsmodtageren leverer sine varer på grundlag af forbrugerens oplysning om, at han råder over et betalingskort, at dette har et bestemt

nummer og udløbsdato, og *at* han ønsker sit køb debiteret den til kortet hørende konto, sker dette i tillid til, at disse tre forhold kan bevises. Der består en vis risiko for, at kortet er kompromitteret, hvorved forbruget debiteres med urette. Ifølge reglerne i Betalingskortloven og Forbrugerombudsmandens retningslinier, hæfter betalingskortindehaveren ikke for disse køb, jf. reglerne om kortindehavers- og kortudsteders ansvar i Betalingskortlovens §§ 21 og 22.

For at overkomme disse bevisvanskeligheder, for at minimere transaktionsomkostningerne, og for at sikre betalingens fortrolighed, har man udviklet en række systemer, der baserer sig på kreditkortbetalingen, således at forstå at selve betalingen til syvende og sidst debiteres den konto, kortet "hører til".

Et sådant eksempel er betalingssystemet *First Virtual*. Systemet er beregnet til brugere, der har en e-postadresse, som de bruger til at "betale fra", og et kreditkort, som der betales med. I stedet for, at betaleren sender sine kreditkortoplysninger til betalingsmodtageren over Internettet (med fare for, at disse informationer snappes op undervejs og misbruges), sender betaleren en meddelelse om, hvilket beløb, han ønsker at betale, samt en særlig kode, kaldet en VirtualPIN, som First Virtual udstyrer ham med. VirtualPIN-koden udleveres til betaleren efter en automatiseret procedure, der indebærer, at betaleren aldrig afgiver sine kreditkortoplysninger over Internettet men i stedet taster dem ind til First Virtual via telefonen. Koden anvendes til at identificere den konto, brugeren anvender, uden at disse oplysninger kommer til betalingsmodtagerens kendskab.

Foruden den fortrolighed og sikkerhed, man dermed opnår, indebærer systemet den stordriftsfordel, at First Virtual kan samle de enkelte "mikro-betalinger" i større bundter, der samlet debiteres kreditkortet, og som dermed gør dette mere fleksibelt. Sammenfattende kan man sige, at First Virtual fungerer som en mellemmand mellem betaler og betalingsmodtager, der løser de umiddelbare praktiske problemer, der ellers ville være forbundet med at skulle anvende sit kreditkort til betaling på Internettet.

Systemet har flere svagheder. For det første er det kostbart, da det inkorporerer de omkostninger, betalingskortsystemet er forbundet med. For det andet rummer det en vis usikkerhed, eftersom også de betalingskortoplysninger, kunden afgiver ved sin indtastning, kan tænkes aflyttet af tredjeparter.

f. Den elektroniske pung

De førnævnte Internet-betalingsystemer mangler en række af de egenskaber, der kendetegner egentlige kontantbetalinger, nemlig muligheden for umiddelbart at overføre likvide beløb uden tredjeparters mellemkomst. Man sonderer mellem de hardwarebaserede og de softwarebaserede electronic purses. Fordelen ved den softwarebaserede purse er, at den er enkel at implementere for brugeren. Den software, der styrer systemet, kan ubesværet hentes ned over Internettet og installeres umiddelbart med et minimum af omkostninger. Ulempen består i, at brugeren til gengæld er låst fast til den terminal, hvor programmet er installeret, når han skal betale. Da brugeren dernæst ikke kan forventes at befinde sig ved

sin terminal altid, består der dernæst en risiko for, at tredjeparter uberettiget gør brug af systemet.

Fordelen ved en hardwarebaseret purse (d.v.s. i praksis en chipcard-løsning) ligger først og fremmest i dens fleksibilitet. Besiddelsen af chipkortet er nødvendigt for at kunne betale. Dette er på den anden side også chipkortets styrke, eftersom denne portabilitet gør det muligt at betale fra forskellige terminaler, f.eks. såvel fra brugerens egen PC (udstyret med chipkort-læser) eller fra en betalingsautomat (f.eks. en telefon).

Der findes to former for chipkort. For det første et hukommelseskort, der fra start af har en bestemt værdi og som herefter kun kan nedskrives. I disse situationer skal forbrugeren løbende holde rede på forbruget af denne værdi. Den anden form er et processorkort, som kan genoplades, og som dernæst kan forsynes med andre funktioner (f.eks. digital signatur el.lign.).

For begge typer af løsninger er der tale om, at betaleren lader et informations-system 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 betalingsoverførelser.

Digicash

En softwarebaseret løsning tilbyder Digicash, der er udviklet af Deutscher Bank. Systemet markedsfører sig under sloganet "numbers that are money": Forud for sin betaling har betaleren anmodet sit pengeinstitut om en digital *ecash*-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, honoreres den.

Ecash-meddelelsen sikrer anonymiteten således, at en betaling ikke kan henføres til en bestemt kunde. Betalingsmodtageren skal kun verificere hvilken bank, der står bag den elektroniske pengeseddel. Det er altså kun betalerens identitet, der er skjult. Den, der har trukket *ecash*-pengene, optræder som sådan overfor sit pengeinstitut. Anonymiseringen gennemføres ved hjælp af såkaldt "blind digital signatur." Denne teknik er baseret på public key kryptering til at verificere betalerens identitet, at kommunikation til og fra pengeinstituttet foregår i fortrolighed, og at den involverer de rette parter.

Ecash kan kun bruges en gang. Når den enkelte "mønt" er brugt, sendes den umiddelbart til den udstedende bank, hvor den verificeres on-line og "logges" (d.v.s. registreres), så de samme penge ikke kan bruges to gange. Hvis betaleren alligevel skulle bruge en *ecash*-pengeseddel to gange, kompromitterer systemet ham, og betalingen vil blive afvist. Den udstedende bank kender altså den totale værdi af den udstedte *ecash*, hvorimod den ikke kan godtgøre, hvorfra indkomne *ecash*-meddelelser hidrører. Når en *ecash*-betaling er gennemført, krediteres modtagerens bankkonto

CyberCoin

CyberCoin er et andet softwarebaseret betalingssystem. Fra CyberCash's hjemmeside henter forbrugeren et program, der fungerer som en såkaldt tom elektronisk pung ("wallet"). Programmet indeholder et krypteringsprogram, der krypterer brugerens kreditkortnummer og dermed skaber fortrolighed mod angreb på dette nummer, samtidig med, at det sikrer betalerens identitet. Dette program lægges ind på harddisken på brugerens PC, hvorfra den nu kommunikerer med hans pengeinstitut (som råder over et tilsvarende CyberCoin kommunikationsprogram) og indhenter de nødvendige bankoplysninger. Når identifikationen er sikret, kan forbrugeren debitere beløb fra sit pengeinstitut og kreditere den elektroniske tegnebog disse beløb. Herfra kan pengene nu overføres i små bidder i forbindelse med enkeltbetalinger. Betaling med CyberCoin kan herefter ske til modtagere, der også har installeret det nødvendige programmel.

Finansieringen af CyberCoin sker ved gebyrer, der er forholdsvis høje ved små betalinger, men tilsvarende lavere jo højere betalinger der er tale om. Det ventes, at CyberCoin inden længe vil møde konkurrence fra andre udbydere, herunder amerikanske pengeinstitutter. Når denne konkurrence kommer, vil priserne utvivlsomt falde drastisk.

Mondex

En hardwarebaseret purse-løsning er det engelske Mondex-system, der er udviklet i England af National Westminster Bank, men for nylig (efteråret 1996) overdraget til Mastercard. Systemet er baseret på et chipkort, som betaleren og betalingsmodtageren får udleveret, og som lagrer informationer om de betalinger, der skal udføres. Dette chipkort "tømmes", når der betales, og "lades op", når det sættes i forbindelse med en bankkonto, hvorfra der er givet autorisation til overførelse af beløb.

Hver gang Mondex-kortet anvendes, genererer kortet en unik digital signatur, som kan genkendes af det andet Mondex-kort, der er involveret i betalingstransaktionen. Denne signatur indebærer sikkerheden for, at der er tale om et originalt Mondex-kort, og at der ikke er sket ændringer af data undervejs. Indtræder sådanne ændringer, bremser transaktionen, og der udvirkes hverken nogen hævnning på det betalende kort eller kreditering af betalingsmodtagerens.

Mondex-kortet er designet til at kunne håndtere op til fem møntsorter samtidigt. Der kan kun betales til modtagere, der også råder over Mondex-kort. Gør han det, kan parterne sætte sig i forbindelse med hinanden via nettet; kortene identificerer herefter hinanden, og det beløb, som betaleren ønsker at betale, trækkes da - under iagttagelse af en række sikkerhedsrutiner - fra debitors kort og krediteres kreditors kort, fra hvilket det nu senere kan tjene som betaling. Brugeren kan bestemme, om han vil "lukke" kortet med en PIN-kode.

Da selve betalingen sker uafhængigt af de pengeinstitutter, fra hvilke beløbene er trukket, tillader Mondex-konceptet minimale transaktionsomkostninger. Derimod indebærer konceptet det problem, at brugeren har mistet sine penge, hvis han mister Mondex-kortet, eller dette af forskellige grunde bliver funktionsudygtigt.

I sit præsentationsmateriale udtaler Mondex, at kortet lever op til eksisterende internationale standarder for korttolerance, og herunder for de mere skræppe regler for GSM-kort til mobiltelefoni.

Omkostningerne ved Mondex-kortet afholdes af brugeren, når han erhverver kortet. Da de enkelte betalinger imidlertid er gratis, er kortet særdeles velegnet til mindre småpengebetalinger. Konceptets succes vil afhænge af, om tilstrækkeligt mange vælger at tilslutte sig. For tiden er systemet ikke anvendeligt i Danmark.

Danmønt-kort

Danmønt-kortet er et dansk småpengekort, som er blevet til i et samarbejde mellem bl.a. TeleDanmark A/S og PBS. Baggrunden for projektet var, at der var udviklet en række kort-baserede betalingssystemer, der udelukkende understøttede bestemte typer af ydelser (HT-rabatkort, telefonkort m.v.), men som anvendte den samme teknologi (chipkort, kryptering m.v.). Den praktiske afvikling af systemet varetages af selskabet Danmønt A/S, der både står for planlægning og koordinering (vedtagelse af standarder og specifikationer for kort og terminaler m.v.), for den driftsmæssige afvikling og overvågning og for selve betalingsclearingen. Danmønt ejes i dag fuldt ud af PBS.

Når kortet produceres, indbetaler kortudstederen (f.eks. et pengeinstitut) kortets pålydende værdi til Danmønt, der herefter registrerer og krediterer forbruget af varer og tjenester på grundlag af kortet. Konceptet er stærkt stigende. I 1994 var der aktiveret 120.500 kort, der i alt udførte 963.400 transaktioner. I 1995 var 258.900 kort aktiveret, og disse kort udførte i alt 2,14 millioner transaktioner.

Secure Electronic Commerce

I juli 1996 har PBS, IBM, MasterCard International og Europay International etableret udviklingsprojektet Secure Electronic Commerce (SET), der skal udvikle teknikker til sikker betaling på Internettet ved hjælp af MasterCard og EuroCard. Teknologien bygger på SET-standard, og sikrer dermed betalingernes integritet og fortrolighed ved at kryptere alle elementer i transaktionen. PBS skal optræde som 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 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 mellemlid.

SET-systemet indebærer en række fordele både for de forbrugere og forretninger, der vil bruge det. Forbrugerne vil være beskyttet imod uønsket afsløring af kortoplysninger. Systemet vil sikre, at ordre er modtaget og accepteret af forretninger, som er blevet kvalificeret af PBS til at bruge systemet. For erhvervsdrivende betyder SET tillid til at betalingerne er foretaget med gyldige kort.

III. Forbrugerrisici

1. Nye afgrænsningsspørgsmål

I takt med, at digital informationsspredning bliver mere effektiv, kommer det digitale medium til at overtage en række klassiske forbrugerområder (f.eks. bog- og avisudgivelser, rådgivningsydelser, underholdning og TV, undervisning o.m.a.). Hermed falder grænserne for en række af de retlige begreber, som lovgivningen er bygget op om, og der opstår et "*beskrivelsesproblem*": Retsreglerne giver ikke nogen klar vejledning for, hvilke fænomener de tager sigte på. Problemet er analyseret hos Mads Bryde Andersen: Edb og ansvar (1988). Blandt de praktiske problemer, der udspringer af dette problem, kan følgende fremhæves:

a. Produkt- og lølørebegreberne

Når en stigende del af omsætningen sker ved, at der kun overføres digital information fra leverandør til forbruger, opstår spørgsmålet om, hvorvidt de regler, der knytter an til materielle begreber som "produkter", "genstande", "varer" etc. uden videre kan anvendes, og om købeloven finder anvendelse, når man handler på nettet.

Problemet er, at den digitale information overføres anderledes end papirinformation (manifesteret i bøger el.lign.), idet der ikke nødvendigvis overdrages noget medium men derimod sker en kopiering. Problemet opstår f.eks. i købeloven, der handler om køb af løløre, herunder immaterialrettigheder: Hvornår er levering sket? Er en informationsmangel en køberetligt relevant mangel, eller er der fri adgang til at fraskrive sig ansvaret herfor i forbrugerkøb?

Et andet eksempel er produktansvarsloven, der giver hjemmel for et objektivt erstatningsansvar for forbrugertingsskader m.v. forvoldt af defekte produkter. I den forbindelse er det afgørende at få fastlagt, hvad der forstås ved "produkt". Vil en virusfejl, der fører til datatab, være omfattet af dette objektive erstatningsansvar?

Et tredje eksempel er reglerne i lov om produktsikkerhed, der giver hjemmel for tilbagekaldelse eller andre retsmidler mod farlige "produkter". Kan man med hjemmel heri tilbagekalde programmel, og hvordan skal dette i så fald ske, hvis det pågældende programmel er "distribueret" som freewareprogrammel (d.v.s. uden ophavsretlige bånd af nogen art) via Internettet?

Afklaringen af sådanne spørgsmål bør ske i relation til hver enkelt retsområde. Det lader sig næppe gøre at opstille et produktbegreb, der som sådan kan anvendes på tværs af de krydsende regelsæt og hensyn, der gør sig gældende.

b. Fuldbyrdseshandlinger

Regulering af dispositioner vedrørende digital information, f.eks. gennem strafansvar, må tage stilling til, hvornår den pågældende handling er fuldbyrdet. Også dette spørgsmål kan løses forskelligt alt efter hvilken lovgivning, der er tale om at bringe i anvendelse. Derimod kan det være nyttigt på forhånd at udsønde nogle situationer, som en regulering kan *tænkes* at knytte sig til. Hermed opnås der et overblik over de reguleringsmuligheder, der gør sig gældende.

Man kan sondre mellem på den ene side den regulering, der angår *information* (f.eks. i form af et forbud mod visse former for anstødelig markedsføring) og på den anden side den, der angår det anvendte *medium* (f.eks. således at markedsføring via papirpost og telefax er tilladt, hvorimod markedsføring via telefon til forbrugeren er forbudt). Hvor afgrænsningen af de forskellige informationstyper i sig selv ikke frembyder beskrivelsesproblemer, kan der tænkes vidt forskellige reguleringsvarianter over mediet. Også her kan man anlægge en tvedeling mellem *afsenderen* henholdsvis *modtageren* af denne information.

I relation til *afsenderen* kan der sondres mellem følgende tilfælde, der navnlig kan være relevante i relation til lovregler om god markedsføringsskik, krænkelse af forretningskendetegn, spredning af ulovlig information el.lign.:

1. Afsenderen holder information passivt tilgængelig på en web-server (f.eks. i strid med regler i markedsføringsloven, registerlovgivningen eller særlige strafferetlige regler).
2. Informationen holdes passivt tilgængelig på en web-server, men andre henviser hertil (med en hypertext-link) uafhængigt af afsenderen.
3. Afsenderen holder informationen passivt tilgængelig på en Web-server, men således, at der er en vis kommerciel aktivitet, f.eks. traditionelle markedsføringstiltag i modtagerlandet (web-serveren befinder sig f.eks. i Tyskland, markedsføringstiltagene sker ved direct mail til forbrugere i Danmark, idet der heri henvises til web-serveren).
4. Informationen spredes til på forhånd afgrænsede grupper, f.eks. til kundeemner, personer på bestemte lokaliteter (der står anført i officielle e-postadresser), tidligere kunder, medlemmer af "newsgroups" el.lign.

I relation til modtageren kan der sondres mellem følgende handlinger:

1. Informationen modtages på en e-postadresse på fremmed medium (f.eks. hos en Internet-leverandør), men læses ikke af forbrugeren.
2. Informationen modtages på en e-postadresse, forbrugeren læser den præsentation af e-postmeddelelsen, som afsenderen har forsynet den med, men derimod ikke selve meddelelsen.

3. Informationen modtages på en e-postadresse, forbrugeren læser selve informationen, men sletter herefter e-postmeddelelsen.
4. Informationen modtages på en e-postadresse, forbrugeren læser selve informationen, sletter e-postmeddelelsen men udfører samtidigt en kopi til eget medium. Hvis forbrugeren herefter foretager en videre spredning af den pågældende information, optræder han som afsender, hvorved henvises til den første gruppe.

Lovgivningen har på et enkelt område forholdt sig til disse fuldbyrdelses-handlinger, nemlig i forarbejderne til den ændring af straffeloven, der fandt sted ved lov nr. 1100 af 21. december 1994. Lovændringen gjorde det bl.a. strafbart at "besidde" fotografier, film eller lignende af børn, der har samleje eller anden kønslig omgængelse end samleje. I bemærkningerne til lovforslaget siges det, at et billede, der overføres fra en database til egen edb-skærm ikke er i forbrugers besiddelse, men at dette er tilfældet, hvis forbrugeren lagrer billedet, herunder til harddisk eller diskette, således at den pågældende kan fremkalde det igen.

Sondringen forekommer ikke overbevisende, eftersom den peger på to forholdsvis tilfældigt afgrænsede typer af datamedier (en skærm-buffer, henholdsvis et fast lagermedium). Den synes heller ikke at ramme det reelle beskyttelsesbehov (forstået som ønsket om at ramme dem, der profiterer af at sprede den slags information). Væsentligt er det imidlertid, at man gør sig klart, hvad der bliver virkningen af at regulere på den ene eller anden måde.

c. Forbrugerbegrebet

Ifølge den gældende definition er en forbrugeraftale en aftale, som en erhvervsdrivende indgår som led i sit erhverv, når den anden part (forbrugeren) hovedsagelig handler uden for sit erhverv. Den erhvervsdrivende har bevisbyrden for, at en aftale ikke er en forbrugeraftale.

Når aftalen indgås mellem parter, der optræder overfor hinanden, er den erhvervsdrivendes bevisbyrde forholdsvis enkel at overskue. Den erhvervsdrivende kan henvise til en række ydre forhold, som bidrager til at "placere" aftalemodparten som forbruger eller erhvervsdrivende. Situationen er anderledes, når der handles via åbne netforbindelser. Parter, der kun har identificeret sig overfor hinanden med navn, evt. suppleret med deres Internet-identifikation (e-postadresse eller web-adresse), har ikke dermed signaleret, hvilken rolle de optræder i, medmindre dette fremgår af omstændighederne (f.eks. parternes korrespondance om formålet med ydelsen). Hertil kommer, at en ganske stor del af den samlede mængde af e-postadresser, er udstedt til enkeltpersoner i deres rolle som ansatte i en virksomhed. Undertiden vil de oplysninger, der kan give den erhvervsdrivende formodning om, at han står overfor en forbruger, tilmed kun blive modtaget af hans edb-system, uden at han altså selv har subjektiv viden om dem og dermed om forbrugerrelationen. Dette er f.eks. tilfældet, når ordren afgives ved ren maskinel indtastning af ydelse, leveringssted og betalingsform på virksomhedens hjemmeside.

Den her beskrevne usikkerhed kan afklares inden for rammerne af den gældende lovgivning og gør sig i øvrigt også gældende i en række andre situationer. At man tidligere har klaret sig uden nævneværdige vanskeligheder, viser, at man også vil gøre det igen. Det må her tages i betragtning, at den erhvervsdrivende på grund af sin bevisbyrde har et særligt incitament til at få forholdet afklaret. Forholdet bør derfor ikke give anledning til regulering.

Et særligt, og måske vanskeligere, problem opstår i relation til de regler, der knytter særlige begrænsninger i adgangen til at sprede information m.v. til *mindreårige*. Medens en persons alder ofte afslører sig ved fremtoning, stemmeleje eller håndskrift, kan det være noget vanskeligere at erkende, hvilken alder afsenderen af en digital meddelelse har. Ligeså vanskeligt er det at konstatere, om information, der er tiltænkt voksne personer, fejlagtigt - og med skadevirkninger - tilgår mindreårige. De heraf følgende spørgsmål har bl.a. været drøftet i en EU-arbejdsgruppe om Harmful and Illegal Content on Internet, se herom nedenfor i kapitlerne III.7.g. og IV.2.b.

En variant af dette problem er risikoen for, at aftaleparter lider skuffelser m.v. ved at indgå aftale med mindreårige eller umyndige. Dette spørgsmål bør afklares i en kommende lovgivning om digital signatur. Således kan ordningen indebære praktiske løsninger på problemet for dem, der vil benytte sig af digital signatur. I Forskningsministeriets hidtidige overvejelser vedrørende en sådan lovgivning har man åbnet mulighed for, at indehaveren af det "nøglepar", der skal udvirke den forpligtende digitale signatur, på forhånd kan erklære, at han kun kan forpligte sig med digital signatur i relation til bestemte transaktioner m.v. Ligeledes lægges der op til, at der kan ske registrering af nøglepar udelukkende med henblik på identifikation (men altså uden mulighed for, at der udvirkes en binding). Det skitserede problem kan løses i praksis ved, at man kun giver myndige personer muligheder for at opnå certificering af sådanne nøglepar til identifikation. For at understøtte umyndiges adgang til at råde over selverhverv kan det eventuelt komme på tale at udvirke certificering af nøglepar med begrænset dispositionsadgang.

d. Markedsbegrebet

Internet betragtes af mange som et selvregulerende rum ("Cyberspace"). Grænseoverskridende rum kendes allerede fra medier som radio, tv og telefoni, der traditionelt har været genstand for offentligretlig kontrol såvel med hensyn til vilkårene for udbud af information som med hensyn til indholdet af denne information. Men disse medier har hidtil kun i begrænset omfang dannet rammerne for "markeder", som bringes erhvervsdrivende og forbrugere sammen. Når Internet-hjemmesider f.eks. anvendes til målrettede markedsførings tiltag, hvor hele verdens Internet-brugere har adgang, kan der imidlertid være grund til at genoverveje de traditionelle markedsbegreber.

Den danske markedsføringslov gælder for markedsførings handlinger, der udfolder sig på dansk territorium, jf. nærmere i kapitel III.7. En markedsførings handling, der retter sig mod det danske marked, vil derfor være omfattet af markedsføringsloven, uanset hvilket medium den anvender, uanset hvor dette medium er placeret, og uanset hvem der kommunikerer til og fra det. Dette udgangspunkt fører allerede med klassiske informationsteknologier til praktiske vanskeligheder, hvis den erhvervsdrivende udfolder sin markedsføring fra

fremmed territorium, f.eks. ved direct mailing i strid med danske markedsføringsregler, der rettes mod danske forbrugere fra Tyskland. I det omfang de pågældende virksomheder ikke også begår noget kriminelt i afsenderlandet, har danske myndigheder begrænsede mulighed for at afskære sådanne aktiviteter.

Problemerne om kontrol med internationaliseret markedsføring har optaget den danske forbrugerombudsmand op gennem 90'erne. Problemerne er nøjere beskrevet i Forbrugerstyrelsens Juridiske Årbog 1992, side 11 ff, hvor det bl.a. anføres, at det i sidste ende alene er internationalt samarbejde, som kan løse problemet. Det har været foreslået, at markedsføringen skal ske i overensstemmelse med reglerne i det land, som markedsføringen retter sig imod, uden at der foretages en harmonisering af lovgivningsmodellerne. Det har imidlertid vist sig meget svært at gennemføre konkrete regler med et sådant indhold.

Der er således allerede i årbogen for 1992 omtalt en sag, der involverede en hollandsk erhvervsdrivende, der markedsførte sig over for danske forbrugere i strid med markedsføringsloven. Markedsføringen blev foretaget ved direct mail fra Holland til Danmark og det hollandske firma var ikke etableret i Danmark. Efter henstilling fra Forbrugerombudsmanden besluttede Rigsadvokaten at rejse tiltale ved Sø- og Handelsretten i København mod det hollandske firma. Firmaet har i februar 1997 anerkendt tiltalepunkterne og har i Sø- Handelsretten vedtaget en bøde på 100.000 kr. for overtrædelse af den danske markedsføringslov. Firmaet er endvidere, efter henstilling fra Forbrugerombudsmanden, indgået på, at firmaets fremtidige markedsføring lovliggøres efter forhandling med Forbrugerombudsmanden.

Sagen er et eksempel på, at det ved retsforfølgning er muligt at få et udenlandsk firma, som ikke er bosiddende i Danmark, men som markedsfører sig i Danmark, til at anerkende at skulle indrette sig efter dansk lovgivning, og at der kan ifaldes strafansvar.

Håndhævelsen begrænses af kravet om, at de pågældende handlinger skal være strafbare både i afsenderlandet og i modtagerlandet, da markedsføringsreglerne i forskellige lande varierer meget. En nærmere gennemgang af markedsføringsreglerne i de europæiske lande i EU er foretaget i Kommissionens grønbog om kommerciel kommunikation i det indre marked udsendt i foråret 1996 (KOM(96)192).

Som beskrevet nærmere i kapitel III.6.d. er der fremsat et direktivforslag, der, ved at forbedre mulighederne for at få nedlagt forbud for grænseoverskridende overtrædelser af en række direktiver, skal sikre en bedre beskyttelse af forbrugernes kollektive interesser. Forslaget skal gøre det muligt at tilsynsmyndigheder eller forbrugerorganisationer fra det land, hvor overtrædelsen har virkning, kan sagsøge virksomheden i dens hjemland.

I en rapport udarbejdet af prof. Bogdan, Lunds Universitet, anføres det, at denne løsning ikke er særlig hensigtsmæssig. Det fremhæves således, at det vil være vanskeligt for en dommer i en medlemsstat at tage stilling til om eksempelvis markedsføring i et andet land og på et andet sprog er vildledende. Han foreslår derfor, at man i stedet arbejder for, at Lugano- og Bruxelles-

konventionerne ændres, således at offentligretlige domme afsagt i det krænkede land, vil kunne anerkendes og fuldbyrdes i virksomhedens hjemland.

Endelig vil det ofte være således, at uetisk markedsføring i enkelte lande, bl.a. Danmark, ikke reguleres via strafbelagte bestemmelser. Hovedbestemmelsen i Danmark er således generalklausulen om god markedsføringsskik, som ikke sanktioneres med straf. Bestemmelsen giver derimod mulighed for, at Forbrugerombudsmanden kan få nedlagt forbud mod forskellige handlinger. I andre lande er der helt andre systemer, og det er ofte ganske kompliceret at sammenligne de forskellige landes systemer og relatere disse til gældende internationale konventioner og andre regler på området.

Når det drejer sig om de særlige problemer, der opstår ved brug af offentlige telenet, kan det volde tvivl, hvilke konkurrenceretlige og immaterialretlige regler, der skal anvendes, eftersom det *marked*, der afgrænses af sådanne net, ikke er lokalt afgrænset. I en vis forstand må man sige, at et værk, der stilles til omverdenens rådighed via en almindeligt tilgængelig hjemmeside, dermed er "udgivet" over hele verden, eftersom enhver kan få adgang til værket. At værket dermed er udgivet betyder bl.a., at en række ophavsretlige undtagelsesregler træder i kraft, f.eks. i medfør af den danske ophavsretslovs aftalelicensregler. Det må formodes, at dette spørgsmål på et tidspunkt vil blive søgt underlagt en EU-regulering.

Et lignende problem opstår ved håndhævelse af varemærkerettigheder og andre immaterialrettigheder via Internettet, idet lovgivningen her bygger på territorielt afgrænsede enerettigheder. Inden for varemærkets gyldighedsområde kan indehaveren forbyde andre virksomheder at markedsføre deres ydelser under varemærket, f.eks. ved at markedsføre varer eller tjenester under angivelse af mærket. Emnet er nærmere behandlet af Knud Wallberg i UFR 1997 B, p.23 ff. Se også Henrik Villumsen i UFR 1997 B, p.188 ff.

Denne nationalitetsforankring mister sin praktiske betydning, hvis den "uberettigede" brug af et varemærke sker via en hjemmeside på Internettet. Her vil udgangspunktet formentlig være, at indehaveren af et varemærke i land X kun kan rette sit krav mod en krænker, der er bosat i land X og som herfra udvirker krænkelsen, hvorimod reglerne i land X ikke kan håndhæves i land Y, hvor varemærket ikke er gældende. Og der er ikke meget vundet ved at gennemføre et forbud mod anvendelse af varemærket i land X, hvis krænkeren ubesværet og med samme mulighed for at nå den pågældende Web-målgruppe kan opnå samme resultat fra land Y.

2. Beskyttelse af forbrugerens person

a. Kompromittering

Når en forbruger ringer til en erhvervsdrivende for at bestille en ydelse, eller den erhvervsdrivende via almindelig post fremsender et tilbud, sker der en kommunikationshandling, som er nogenlunde sikret mod at blive kompromitteret af tredjepart. TCP/IP-protokollen har fremkaldt en række af de sikkerheds-

problemer, der gør sig gældende på Internettet (men som derimod ikke gør sig gældende på andre sammenlignelige, omend ikke ligeså udbredte nettyper, som f.eks. det såkaldte X.400-net): Når en elektronisk meddelelse sendes fra sin afsender og til sin modtager, passerer den en række mellemstationer undervejs, nemlig de ovenfor i kapitel II.3. omtalte routere. På hver mellemstation lagres meddelelsen midlertidigt, hvorved der opstår risiko for, at den kompromitteres af udefra kommende.

b. Almindelig databehandlingsbeskyttelse

Når en forbruger bestiller en ydelse hos en erhvervsdrivende ved brug af edb, sker der et antal registreringer hos den erhvervsdrivende, som - alt efter ydelsens beskaffenhed - sammenstykket med andre informationer kan røbe forhold vedrørende forbrugerens person og privatliv. Disse kan med rette forlanges unddraget almenheden. Forbrugeren har derfor et rimeligt behov for, at disse dele af hans transaktion beskyttes mod kompromittering fra tredjemands side (f.eks. ved at en hacker udnytter et svagt punkt i leverandørens edb-system til at tilegne sig de pågældende transaktionsdata). Dette *sikkerhedsbehov* er varetaget i generalklausulen om edb-sikkerhed i lov om private registre § 6, stk. 4, som pålægger, at der "skal træffes de fornødne sikkerhedsforanstaltninger mod, at oplysninger i et edb-register misbruges eller kommer til uvedkommen- des kendskab." Bestemmelsen drøftes i øjeblikket i Justitsministeriets registerudvalg, idet det bl.a. kan diskuteres, om denne sikkerhedspligt burde gøres mere præcis.

Et sådant tilfælde af kompromittering af personlige oplysninger på Internettet skete for nylig (marts 1997), da Den Danske Bank tilgængeliggjorde en række fortrolige data, som flere bankkunder havde sendt til banken på Internettet i forbindelse med lånansøgninger. Banken har forklaret, at der var tale om en menneskelig fejl og ikke fejl i bankens edb-program på Internettet. Forbrugerombudsmanden fastslog, at der forelå en overtrædelse af markedsføringslovens § 1, idet banken burde sikre sig, at fortrolige og følsomme oplysninger om kundernes økonomi ikke kunne gøres tilgængelige for tredjemand. Det forhold, at oplysningerne har været tilgængelige for en bred og udefineret personkreds, gjorde forholdet særligt kritisabelt. Da der var tale om mulige overtrædelser af bank- og sparekasseloven og lov om private registre, var både Finanstilsynet og Registertilsynet gået ind i sagen.

I denne sag var der ingen grund til at betvivle, at der var tale om fejl fra bankens side. Anderledes forholder det sig, når udenforstående skaffer sig adgang til private data. Hacking - ulovlig indtrængen i fremmede edb-systemer, oftest via et modem tilsluttet det offentlige telefonnet - er strafbart efter straffeloven. Således blev seks hackere, der blandt andet havde skaffet sig adgang til USA's sikkerhedscenter Pentagon og andre databaser, dømt i december 1996 ved Roskilde Byret. De tiltalte modtog betingede fængselsstraffe, samfundstjeneste og bøder. I straffeloven er der hjemmel til at straffe disse og lignende handlinger i § 193 om retsstridig fremkaldelse af omfattende forstyrrelse i driften af databehandlingsanlæg, § 263 om uberettiget at skaffe sig adgang til en andens oplysninger eller programmer, der er bestemt til elektronisk databehandling og §279a om databedrageri.

Tilsvarende ulovlige handlinger vil utvivlsomt kunne straffes på samme måde, f.eks. på linie med et tilfælde ved årsskiftet 96/97 i Tyskland. I denne sag har en gruppe tyske hackere vist på tysk TV, hvordan et bestemt edb-program kunne smugles ind i en privat computer via Internettet. Derefter kunne hackerne overflytte penge fra en almindelig hjemmebank til deres egne konti. På baggrund af sagen blev der i Folketinget rejst et spørgsmål til Erhvervsministeren (S 1635 af 6. marts 1997) vedrørende mærkning af edb-programmel, der vil sikre, at programmet ikke indeholder virus eller andet sikkerhedsrisici. Foreløbig har ministeren afvist kravet om lovpligtig mærkning af edb-programmel, da den form for risiko kan håndteres ved eksisterende lovgivning - markedsføringslovens forskrifter om forsvarlig vejledning og god markedsføringsskik - og forbrugernes opmærksomhed og kendskab til risiciene ved benyttelse af Internettet.

c. Elektroniske spor

Et særligt problem knytter sig til den form for registrering, der almindeligvis omtales som "elektroniske spor". Hermed menes den registrering af visse ydre tekniske forhold, som brugeren af et digitalt baseret system efterlader sig under brugen, men som ikke har direkte betydning for den pågældende tjenesteydelse. Et eksempel herpå kan være oplysninger om, hvordan et kreditkort er benyttet, eller hvordan en hjemmeside, som efterfølgende anvendes som led i en direct marketing-indsats eller kompromitteres, er anvendt.

Betalingskortlovens § 24 opstiller en almindelig regel om, at der kun må registreres oplysninger om kortindehavers brug af kortet til betalingskortfunktioner, som er nødvendige for gennemførelse af betalingstransaktioner og for at hindre misbrug. Oplysninger om kortindehavers brug af kortet til betalingskortfunktioner, som er defineret i lovens § 2, må kun anvendes og videregives, når dette er nødvendigt til gennemførelse af betalingstransaktioner, korrektioner og retshåndhævelse, eller når dette er hjemlet ved lov. Oplysninger om misbrug må kun videregives i det omfang, det er nødvendigt for at hindre misbrug, jf. § 24, stk. 2. Disse regler gælder ikke for hævetransaktioner, der foretages hos kortudsteder, eller for oplysninger, der ikke kan føres tilbage til fysiske eller juridiske personer. Oplysninger om betalingsmodtagers omsætning, antal betalingstransaktioner, beløbsstørrelser og lignende forhold hos betalingsmodtager må kun registreres, anvendes og videregives, når dette er nødvendigt til gennemførelse af betalingstransaktioner, korrektioner og retshåndhævelse. Oplysninger må i øvrigt kun videregives i det omfang, det er bestemt i anden lovgivning, se lovens § 2, stk. 3.

EU-direktivet om persondatabeskyttelse går ikke lige så langt. Direktivets artikel 14 (b) berettiger den registrerede til efter anmodning og uden udgifter, at *modsætte sig* en behandling af personoplysninger, der vedrører den pågældende, og som den registeransvarlige agter at foretage med henblik på markedsføring, eller at *blive underrettet*, inden personoplysningerne første gang videregives til tredjemand eller anvendes på tredjemands vegne med henblik på markedsføring.

Man kan sætte spørgsmål ved, om de beskrevne regler går vidt nok. Betalingskortloven angår kun betalingstransaktioner og rammer derimod ikke de elektroniske spor, der efterlades som led i almindelig "browsing". I det straks nedenfor omtalte ISDN-direktivforslag er der som nævnt sket en vis regulering af disse spørgsmål i relation til telesektorens registrering, men udenfor dette område er der ingen regulering af falde tilbage på.

En yderligere regulering af disse spørgsmål er foreslået i Kommissionens forslag til direktiv om beskyttelse af personoplysninger og beskyttelse af kommunikationshemmeligheden i forbindelse med digitale telenet, herunder det tjenesteintegrerede digitalnet (ISDN) og digitale mobilnet (KOM(94) 128 af 13. juni 1994), EFT C 1994 200/4.

Direktivforslaget har til formål at sikre en tilfredsstillende beskyttelse af både borgernes privatliv og juridiske personers legitime interesser, især med hensyn til tjenesternes sikkerhed, netsikkerheden, telekommunikationshemmeligheden, trafik- og debiteringsdata.

Det hedder bl.a. heri, at *debiteringsdata* (altså de data, der er nødvendige for debiteringen for teletrafikken) kan behandles, men kun af de personer, der har ansvar for debiteringen (artikel 6, pkt. 4), og at *trafikdata*, der har været nødvendige for at opsætte samtaler, og som lagres i teleselskabernes centraler, skal slettes, så snart de ikke længere er nødvendige for at stille den pågældende tjeneste til rådighed (artikel 6, pkt. 1). Direktivforslaget drøftes nærmere i kapitel III.7.c.

Rådet fastlagde en fælles holdning til dette direktiv (den 12. september 1996), hvorefter der på dette spørgsmål blev tilføjet to aspekter: For det første tjenesteleverandørers adgang til at anvende trafik- og debiteringsdata til markedsføring af deres egne tjenesteydelser mod forhåndstilladelse fra abonnenten i overensstemmelse med det generelle direktiv om databeskyttelse. For det andet myndigheders adgang til trafikdata, når de har ansvaret for bilæggelse af tvister om debitering eller samtrafik.

Europa-Parlamentet vedtog den 16. januar 1997 en udtalelse, som indeholdt 11 ændringsforslag til Rådets fælles holdning. Bl.a. foreslogs der en indskrænkning af medlemsstaternes mulighed for individuelt at beslutte, at visse af bestemmelserne udelukkende skulle omfatte fysiske personer. Europa-Parlamentet ønskede, at bestemmelserne generelt skulle gælde for juridiske personer dog med undtagelse for de tilfælde, hvor forbrugerhensyn måtte tale imod dette. Angående Rådets fælles holdning, der åbnede mulighed for, at en operatør kunne kræve en rimelig betaling for, at særlige oplysninger vedrørende en abonnent ikke optages i en fortegnelse, ønskede Europa-Parlamentet, at denne bestemmelse i den fælles holdning udgik.

Kommissionen havde meddelt, at den ikke kunne tiltræde alle Europa-Parlamentets ændringsforslag, og da der ikke kunne opnås enighed blandt medlemsstaterne, blev forslaget henvist til behandling i Forligsudvalget.

Hvis man anser den beskyttelse, som EU-registerdirektivet og forslaget til ISDN-direktiv giver den registrerede mod behandling af data, der kan udgøre "elektroniske spor", for principiel, bør det overvejes at indføre en tilsvarende beskyttelse af de "spor", der efterlades ved brug af hjemmesider på Internettet.

I mangel af en regulering på dette område vil forbrugeren opleve et misforhold mellem den forholdsvis intense forbudsregulering, som den gældende betalingskortlovgivning er udtryk for, og den frihed, der i så fald måtte anerkendes på det stadigt større område for Internet-handel og -markedsføring.

Et særligt problem knytter sig til det forhold, at kommunikation på Internettet ofte inddrager routere, der er placeret i tredjelande, og som derfor falder uden for såvel dansk ret som EU-rettens jurisdiktion. Dette problem er i direktivforslaget løst gennem en regel om *gensidighed*. Reglen løser imidlertid ikke problemet fuldt ud. I forbindelse med Internet-transmissionen kopieres disse informationer ofte uden nogen enkeltpersons vidende. Selvom regler om reciprocitet gennemføres, vil det derfor være vanskeligt at håndhæve sådanne regler.

Til denne problemstilling hører det nye fænomen "cookies", hvorved forstås et softwareprogram, der automatisk registrerer en række oplysninger, når en forbruger besøger en bestemt hjemmeside. Når forbrugeren vender tilbage til den samme hjemmeside, vil personen bag Web-adressen (typisk erhvervsdrivende) have en lang række informationer om forbrugeren til rådighed. Oplysningerne bliver lagret på forbrugers egen PC og kan indgå i udbyderens markedsføringsstrategi i forhold til den pågældende forbruger, hvis præferencer udbyderen kender på forhånd.

Registertilsynet har taget stilling til cookies-problematikken ved besvarelse af folketingets spørgsmål nr. S. 1303 af 3/2-1997. Registertilsynet vurderede, at spørgsmålet, om en eventuel registrering af informationer gennem brug af cookies ville være omfattet af lov om private registre, ville afhænge af, om det var muligt for personen bag website at fastlægge brugerens identitet. Efter lov om private registre § 3, stk. 1, må erhvervsvirksomheder, erhvervsdrivende, institutioner, foreninger og lignende kun foretage registrering som nævnt i lovens § 1 - oplysninger om private, økonomiske eller personlige forhold (f.eks. personnumre) - i det omfang, registreringen er et naturligt led i den normale drift af virksomheder m.v. af den pågældende art.

Bestemmelsen har karakter af en retlig standard, og spørgsmålet om, hvornår registrering af oplysninger må anses for at være "et naturligt led i den normale drift" beror på en konkret vurdering i det enkelte tilfælde. På denne baggrund fandt Registertilsynet ikke, at det var muligt at udtale sig generelt om, hvorvidt brugen af cookies indebar tilsidesættelse af denne lov.

Som omtalt ovenfor, kan oplysninger om forbrugernes person, handlemønstre og præferencer, som meget besværligt kan samles, når man handler anonymt i supermarkedet og betaler kontant, meget enkelt og billigt frembringes, når man handler på nettet. Adgangen til personlige oplysninger vil tage til i takt

med indførelsen af identifikationssystemer, hvorefter anonymiteten vil forsvinde.

Nøglebegreber for at angribe dette misbrugspotentiale er forbrugernes underretning og accept. I dag er der næppe mange, der er opmærksomme på, om deres optræden på nettet bliver registreret. Forbrugerne bør derfor have krav på at vide, hvilke informationer om dem, der bliver registeret, og hvordan og til hvilket formål disse oplysninger vil blive brugt. Samtidig bør det overvejes, om de web-sites, der foretager registreringer, ud over meddelelsen at her registreres oplysningerne, skal bede om forbrugernes udtrykkelige samtykke til at bruge informationerne til kommercielle formål.

Et eksempel på en løsning af dette problem er "eTrust"-initiativet, der praktiseres i USA. Dette bygger på den forudsætning, at virksomhederne vil betragte "eTrust"-logo på deres web-sites som en fordel i konkurrence om kunderne, og derfor af egen vilje vil forpligte sig til at overholde programmets retningslinier. Disse går ud på, at virksomhederne skal offentliggøre deres behandling af informationer om kunder, informere kunden om - inden registreringen - at informationen registreres og bruges, tillade kunden at slette eller korrigere tidligere modtagne oplysninger, og undlade at offentliggøre informationerne. Når forbrugeren støder på "eTrust"-logoet på en tilfældig web-site, kan han klikke på den og derefter få "link" til en anden site, der forklarer, hvad logoet betyder.

Et særligt problem i så henseende er mindreåriges adgang til at forpligte sig eller hente bestemte informationer, der kun er tilladt for voksne. Dette kan bl.a. løses gennem identifikationssystemer som f.eks. digital signatur, hvorefter sælgeren vil få adgang til bestemte oplysninger om medkontrahenten, heriblandt den pågældendes kontraheringsevne.

d. Direkte markedsføring

Direkte markedsføring kan forekomme enten i form af henvendelse til bestemte forbrugere, hvis adresse udbyderen kender på forhånd, eller gennem henvendelse til en større kreds af tilfældige forbrugere, som befinder sig bag et afgrænset adressefelt, f.eks. beboere på en bestemt gade eller i en bestemt by, eller personer med et bestemt telefonnummers endetal osv. (omtales også som "cold calling").

For de erhvervsdrivendes markedsføring er viden om, hvor forbrugeren befinder sig, og hvilke faktorer, der vil bestemme forbrugsvalget, altafgørende. På den anden side kan en udstrakt anvendelse af data om forbrugeradfærd m.v. true forbrugers privatliv, enten således at selve registreringen af disse data anses som integritetskrænkende, jf. ovenfor, eller således at selve markedsførings-handlingen anses som en slags fredskrænkelse.

Lovgivningen har på et par områder taget stilling til dette skisma.

Efter § 4b i lov om private registre gælder der en hovedregel om, at virksomheder ikke må videregive registrerede oplysninger om forbrugere til andre

virksomheder til brug ved markedsføring. Dette forbud fraviges dog, jf. bestemmelsens stk. 2, under to betingelser. For det første skal betingelserne for videregivelse af oplysninger, jf. lovens § 4, være opfyldt. For det andet skal den virksomhed, som ønsker at videregive oplysningerne, ved kundeforholdets begyndelse eller på et senere tidspunkt have givet den registrerede tydelig skriftlig meddelelse om, at videregivelse kan finde sted, og den registrerede skal have givet sit udtrykkelige samtykke til videregivelsen.

Det almindelige krav i lovens § 4 indebærer nærmere bestemt, at videregivelse af følsomme oplysninger - der ikke er lovlig i kraft af særskilt lovhjemmel - enten kræver samtykke fra den registrerede eller den, som handler på hans vegne, eller tilladelse fra Registertilsynet. Tilladelse kan gives, når videregivelse sker til varetagelse af offentlige eller private interesser, herunder hensynet til den pågældende selv, der klart overstiger hensynet til de interesser, der begrundet hemmeligholdelse.

Selv om indsamling og registrering af oplysninger ved en forbrugers tilmelding til et loyalitetsprogram ikke er i konflikt med registerlovgivningen, kan et register over kundernes forbrugsadfærd over en længere periode imidlertid danne grundlag for detaljerede profiler, der kan give adgang til en særdeles intensiv og individualiseret markedsføring.

Det er derfor nærliggende at antage, at selv om tilmelding fra forbrugerens side sker på frivilligt grundlag, og det samtykke, der umiddelbart meddeles herved, ligeledes omfatter den efterfølgende registrering af indkøbsadfærd, vil den erhvervsdrivendes opsamling og anvendelse af profiler som led i markedsføringen efter omstændighederne kunne være i strid med markedsføringslovens generalklausul. Spørgsmålet bliver behandlet i et igangværende projekt om "Loyalitetsprogrammer i Norden og forbrugerbeskyttelse" under Nordisk Embedsmandskomite for konsumentspørgsmål.

3. Sikkerhedsspørgsmål

a. Fysisk sikkerhed

Information i digital form kan under visse betingelser være skadevoldende. Hvis en forbruger fra en hjemmeside overfører en programfil, der er inficeret med en virus, kan denne fil påføre forbrugeren en tingsskade i form af datatab og under visse omstændigheder (f.eks. hvis der inficeres programmel til kontrol med fysiske indretninger m.v.) muligvis også personskaade. Spørgsmålet er, om forbrugeren efter den gældende lovgivning er tilstrækkeligt værnet mod sådanne skader.

Lov nr. 364 af 18. maj 1994 om produktsikkerhed (PSL) gælder for "ethvert produkt, der bringes i omsætning", samt - modsat produktansvarsloven - for tjenesteydelser, der har tilknytning til et produkt. Hvor det efter produktansvarsloven kan give anledning til tvivl, om digital information (f.eks. edb-programmel) udgør et produkt, er der næppe nogen tvivl om, at dette spørgsmål må besvares bekræftende for produktsikkerhedslovens vedkommende, når vi ser på den digitale information, der er inkorporeret i et edb-system.

Begrebet produkt er i loven defineret som "enhver løsøregenstand, uanset om den er en råvare eller et naturprodukt" (PSL § 3). Det kan diskuteres, hvad denne definition dækker over.

På den ene side kan det hævdes, at loven omfatter både produkter i form af et såkaldt fysisk medium og de transmitterede informationer, som knytter sig til det fysiske produkt, mediet. Hvis ikke mediet eksisterede, ville informationen heller ikke kunne formidles til brugeren, og i tilfælde af en sundheds- og sikkerhedsfare er det følgelig vanskeligt klart at skelne, om det er det ene eller det andet forhold, der giver anledning til, at produktet må siges at falde ind under loven. Hvis man befinder sig i en situation, hvor programmet sender visuelle påvirkninger eller udsender lyde, som indebærer en sådan sundheds- eller sikkerhedsfare for personer eller ejendom, må lovens indgrebsmuligheder (forbud, tilbagekaldelse) kunne finde anvendelse.

På den anden side kan det påstås, at lovens definition bør forstås således, at ren information, i modsætning til f.eks. programmet, ikke falder inden for loven; et resultat, der da også understøttes af, at nogle af lovens centrale bestemmelser vil være vanskelige at håndhæve i relation til rent digitale informationsprodukter (f.eks. reglerne om tilbagekaldelse m.v. i lovens § 11).

Man kan drøfte, om en eventuel manglende produktsikkerhedsregulering på det digitale område efterlader et uacceptabelt vakuum. For et benægtende svar taler det forhold, at de hjemmesider, der drives af anerkendte virksomheder m.v., i praksis følger en sikkerhedspolitik, hvorefter der sker løbende scanning for virus. De mindre seriøse af slagsen kan efter omstændighederne rammes af de almindelige generalklausuler i markedsføringsloven, produktansvarsloven og de almindelige erstatningsretlige regler. Dernæst har mulighederne for at blive ramt af erstatningsretlige sanktioner (eventuelt efter en objektiv ansvarsregel i produktansvarsloven) formentlig virket stærkt motiverende overfor de erhvervsdrivende, der i givet fald vil være målet for en særregulering.

b. Pengeværdier

Et andet særligt sikkerhedsspørgsmål aktualiserer brugen af hardwareenheder, der fungerer som ultimative symboler for pengeværdier, se f.eks. ovenfor i kapitel II.12.f. om det engelske Mondex-kort. Tillader man sådanne systemer, er det nærliggende at sikre, at den anvendte hardware tilvejebringer en rimelig grad af sikkerhed for, at kortet - og dermed værdien - ikke går til grunde som følge af dagligdagens påvirkninger med temperatur, fugt, elektromagnetisme eller andet. Betalingskortlovens § 22 og lovgivningen vedrørende Elektromagnetisk Kompatibilitet, se lovebekendtgørelse nr. 475 af 1. juni 1994 om beskyttelse mod elektromagnetiske forstyrrelser, indeholder et muligt hjemmelsgrundlag for ansvarsplacering i sådanne tilfælde.

4. Betaling og finansiering via Internettet

a. Økonomisk sikkerhed

Reglerne i den finansielle lovgivning (lovgivningen om forsikringsselskaber, banker og sparekasser, fondshandlere etc.) har til formål at beskytte forbrugeren mod utilsigtede følger af, at leverandøren af en finansiell ydelse viser sig insolvent og dermed ikke kan honorere sine forpligtelser overfor forbrugeren. Et af de problemer, der hurtigt vil aktualisere sig, er spørgsmålet om, hvornår udbydere af de elektroniske betalingssystemer driver bankvirksomhed. Problemet er ikke aktuelt lige nu, eftersom de systemer, der er i praktisk udbredelse, netop knytter sig til bankvirksomhed, men i takt med standardiseringen på området kan problemet opstå.

De nationale retsregler herom udspringer af en direktivregulering, der har til formål at harmonisere dette tjenesteydelsesmarked inden for EU. Forbrugeren kan dermed påregne en vis fælles beskyttelse, uanset hvor i fællesskabet han disponerer. Da reglerne derimod ikke gælder for finansielle institutioner i tredjelande, kan der opstå problemer, når en forbruger i Danmark eller et andet EU-land kommer i kontakt med en finansiell institution, der ikke er bundet af sådanne regler. En kontakt kan f.eks. tænkes realiseret ved, at forbrugeren lader et beløb overføre til en institution, der herefter skal varetage clearingfunktioner for en efterfølgende betaling, jf. redegørelsen nedenfor om de eksisterende betalingssystemer.

Kommissionen har den 4. juni 1996 fremsat forslag til et direktiv, der skal fastlægge minimumsregler for EU-bankernes betalingssystemer med henblik på at forbedre sikkerheden omkring disse systemer. Baggrunden herfor er, at den nuværende opbygning af betalingssystemerne, der udelukkende er baseret på national lovgivning, efter Kommissionens opfattelse frembyder en række risici, der kan true stabiliteten af de finansielle markeder og hindre kapitalens frie bevægelighed. Direktivforslaget skal bl.a. sikre, at ingen national konkurs- eller insolvenslovgivning giver mulighed for at omstøde eller anfægte betalinger, der er foretaget i henhold til eksisterende regler for betalingstransaktioner. Tilbagekaldelse af gennemførte transaktioner skal forbydes, og hvis der er sket fejl i overførselen, må denne ikke annulleres men derimod korrigeres ved en separat transaktion. Endelig foreslår Kommissionen, at princippet om netting (d.v.s. aftaler mellem pengeinstitutter, der er involveret i en betalingsoverførelse, om at man kun modregner nettobeløb) lovfæstes og dermed gives bindende virkning overfor tredjemand. Regler herom er allerede indført i dansk ret ved kapitel 18 i værdipapirhandelsloven.

Dernæst har Kommissionen den 22. maj 1996 offentliggjort en *grøn bog* om virkningerne for forbrugeren af gennemførelsen af fri bevægelighed af finansielle tjenesteydelser. Det fremgår bl.a. heraf, at Kommissionen undersøger, om det er nødvendigt at udstede særlige EU-regler for fjernsalg af finansielle tjenesteydelser svarende til dem, der er ved at blive vedtaget vedrørende fjernsalg af varer og andre tjenesteydelser.

Spørgsmålet om reguleringen af de virksomheder, der udsteder *electronic purses* er behandlet i en rapport, som EU-centralbankerne udsendte i maj 1994. Rapporten analyserer ikke forbrugerproblemerne men derimod de konsekvenser, sådanne kort har for overvågningen af betalingssystemerne, for pengepolitikken og for brugen af mønter og sedler. Rapporten konkluderer, og det Europæiske Monetære Institut har tiltrådt denne konklusion, at det alene skal være tilladt for kreditinstitutter at udstede småpengekort, idet de enkelte EU-centralbanker dog under særlige tilfælde kan dispensere fra dette krav og tillade udstedere, som ikke er kreditinstitutter. I sådanne tilfælde forudsættes det dog, at systemet alene opererer i hjemlandet, at udstederen er underkastet behørig regulering, samt at udstederen i de fleste tilfælde er under tilsyn af samme myndighed, som i det pågældende land fører tilsyn med kreditinstitutter. I overensstemmelse hermed er loven om sparevirksomheder og udstedere af forudbetalte betalingskort ændret ved lov nr. 375 af 22. maj 1996.

b. Betalingskort

Anvendes et betalingskort til betalinger over internettet, f.eks. ved afgivelse af kortnummeret, er dette reguleret gennem betalingskortloven, herunder navnlig ansvars- og tabsbegrænsningsreglerne i lovens kapitel 5. Da kortene i disse tilfælde benyttes uden de sædvanlige kontrol- og sikkerhedsprocedurer, og da misbrugsrisikoen herved er væsentligt forøget, har Forbrugerombudsmanden efter forhandlinger med branchen udstedt "Retningslinier vedrørende fjernsalg m.v. i betalingssystemer med betalingskort" (december 1996). Disse sikrer sammen med betalingskortlovens bestemmelser kortindehaverne en rimelig retsstilling i tilfælde af misbrug.

Visse former for betaling via netforbindelser er reguleret gennem betalingskortlovens regler om betalingssystemer uden kort men med kode.

Betalingskortlovens regulering af betalingssystemer (og betalinger) via de åbne net bør give anledning til en nærmere udredning i forbindelse med lovens revision.

Landene inden for OECD arbejder for tiden med en code of practice vedrørende brugen af kortnumre via digitale net. Så vidt vides foreligger der ingen sådan udredning fra anden side. Derimod foreligger der et EU-projekt (kaldet TEDIS), der generelt har undersøgt den retlige beskaffenhed af elektroniske betalinger i fællesskabet. TEDIS-projektet har bl.a. publiceret en større rapport herom i slutningen af 1993. Herudover har UNCITRAL udarbejdet en modellov om International Credit Transfers.

c. Småpengekort

Ved lov nr. 375 af 22. maj 1996 om sparevirksomheder og udstedere af forudbetalte betalingskort er der taget højde for en del af de spørgsmål, der har at gøre med "den elektroniske pung". Loven indfører et tilsyn med udstedere af forudbetalte betalingskort, der kan benyttes som betalingsmiddel hos andre end kortudstederen. Danmønt-kort er eksempelvis omfattet af loven. Formålet er dels at beskytte køberen af sådanne kort mod tab som følge af en kortud-

steders konkurs, dels at beskytte de betalingsmodtagere (herunder småhandlende), der modtager forudbetalte betalingskort som betaling. Loven er indført på baggrund af den førnævnte anbefaling af maj 1994 fra det Europæiske Monetære Institut (EMI).

Efter lovens § 8 skal sådanne udstedere have en aktiekapital på 20 millioner kroner, hvis det samlede pålydende ikke overstiger 200 mio. kr. Ligger pålydende over dette beløb, skal udstederens aktiekapital være på mindst 40 millioner kroner svarende til kapitalkravet efter bank- og sparekasseloven for pengeinstitutter. De øvrige regler for udstedere af forudbetalte kort vil blive fastsat ved bekendtgørelse af Finanstilsynet med udgangspunkt i de regler, der gælder for pengeinstitutter. Disse regler kan bl.a. angå forhold vedrørende stiftelse, minimumsolvens, midlernes anbringelse, revisionserklæringer og systemrevision.

Loven indfører i § 2, stk. 3 en maksimal beløbsgrænse på 1.000 kr. på forudbetalte kort, svarende til den maksimale størrelse på danske pengesedler. Udstedere må ikke have andre aktiviteter end udstedelse af forudbetalte betalingskort, herunder rådgivning om forudbetalte betalingssystemer. Ved genopladning af et kort må den samlede værdi på et kort inklusive restbeløbet ikke overstige 1.200 kr. Til gengæld gælder der en bagatelgrænse for udstedere, der kun udsteder forudbetalte betalingskort med et pålydende på 500 kr. eller mindre, og såfremt det samlede pålydende beløb på de kort, som udstederen har i cirkulation, er mindre end 1 mio. kr. pr. seneste 31. december, jf. § 2, stk. 4. Disse udstedere falder uden for loven og således uden for Finanstilsynets tilsyn med overholdelse af loven, jf. §11.

5. Aftaleindgåelse

a. Den digitale viljeserklæring

Reglerne om aftaleindgåelse har traditionelt formet sig med baggrund i kendte omgangsformer. Man møder hinanden på markedet og giver håndslag, eller man forhandler en aftale under et møde og enes herefter om en aftaletekst, som man underskriver. Man tager varen ned fra hylden og indicerer dermed et ønske om at købe den.

I relation til den digitale aftaleindgåelse har der endnu ikke dannet sig tilsvarende omgangsformer. Dette er i sig selv ikke noget særsyn. Sådan forholder det sig for så vidt hver gang, en ny branche og heraf følgende nye handleformer opstår. Men problemet vanskeliggøres af, at denne usikkerhed træder frem på tværs af kulturelle skel og på tværs af retssystemer. Hvor man mellem danske aftaleparter har en fælles kulturtradition og heraf følgende fælles "typeforudsætninger" at falde tilbage på, er dette ikke nødvendigvis tilfældet i den internationale Internet-handel. Ofte vil formodningen være for det stik modsatte.

En viljeserklærings gyldighed er uafhængig af, om den er repræsenteret ved digitale medier. Dette princip følger af en fæstnet dansk retsopfattelse om, at

aftaler er gyldige uden formkrav. Princippet er ligeledes nedfældet i artikel 5 i UNCITRALs modellov om Electronic Commerce. Spørgsmålet er imidlertid, hvornår den fornødne "vilje" er til stede, f.eks. fordi den handling, hvormed "afgiveren" udvirker afgivelsen af en digital meddelelse, er udført isoleret fra den tekniske hændelse, hvorved denne handling manifesteres overfor omverdenen. Modtageren oplever f.eks., at "nogen" via elektronisk post har sendt en digital meddelelse om, at en vare bestilles, men om denne bestilling fremtræder som resultatet af en erkendt disposition, eller om der foreligger en fejltagelse hidført ved fejlbetjening af udstyret eller fejlprogrammering af systemet, vides ikke. Derimod er det klart, at nogen vil lide skuffelse ved enten at blive forpligtet af eller stole på den pågældende meddelelse.

Er der tale om, at en *tredjepart* retsstridigt udvirker afsendelse af en meddelelse i nogens (pseudo-hovedmandens) navn, fører dansk rets almindelige regler om falsk til, at afgiveren ikke bindes. Dette udgangspunkt må dog nok modificeres i løbende aftaleforhold, idet der her påhviler pseudo-afgiveren en pligt til at reagere overfor modtageren, såfremt pseudo-afgiveren ikke ønsker at være bundet af erklæringen. En sådan reklamlationspligt opstiller aftaleloven således for en række tilfælde, hvor der kan opstå en sådan usikkerhed om aftaleindgåelsen.

UNCITRALs modellov om Electronic Commerce indeholder følgende bestemmelse herom:

Article 13. Attribution of data messages

(1) A data message is that of the originator if it was sent by the originator itself

(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or

(b) by an information system programmed by or on behalf of the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:

(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

(4) Paragraph (3) does not apply:

(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or

(b) in a case within paragraph (3) (b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. 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.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

Er der derimod tale om, at *afgiveren* har fejlbetjent udstyret, f.eks. ved uforvarende at komme til at "klikke" på et felt i menuen, som effektuerer afsendelse af en meddelelse, afsenderen ikke havde tænkt sig at afgive, befinder vi os inden for rammerne af afl. § 32, stk. 1. Denne bestemmelse regulerer aftaleforpligtelsen i tilfælde af "fejlskrift eller anden fejltagelse" og fastslår, at afgiveren hæfter for sådanne fejltagelser, medmindre modtageren er i ond tro. Til dette regelsæt hører også afl. §39, hvorefter man, inden det fastslås at aftalen er bindende, også skal se på, om den fejlbehæftede viljeserklæring har virket bestemmende på modtagerens handlemåde på det tidspunkt, han gøres bekendt med fejlen. Hvis ikke modtageren (i denne sammenhæng sælgeren) nåede at handle i tillid til erklæringen, bør forbrugerens retsbeskyttelseshensyn bevirke, at der tages hensyn til dette forhold i retning af en eventuel lempelse af forbrugerens forpligtelser.

Ved at programmere edb-systemer til at afgive og modtage forpligtende digitale meddelelser (f.eks. EDI-meddelelser) uden umiddelbar menneskelig kontrol, kan man etablere aftaleretlige forpligtelser, der ikke har tilbudets og acceptens subjektive kendetegn. Stadig flere brancher anser EDI for at være en væsentlig forudsætning for at kunne overleve i det moderne samfund, men den elektroniske meddelelse rejser det problem, at den ikke i sig selv fremkommer i konsekvens af "vilje" endsige modtages med "kendskab". Hvis A har fremsendt en EDI-meddelelse til B's edb-system, som han ønsker at kalde tilbage efter dens fremkomst, kan han så det? Ifølge afl. § 7 beror dette på, om B har fået kendskab til den, men B selv kender intet til meddelelsen, og tilbagekaldes meddelelsen ikke, vil den typisk udvirke en ordrehåndtering (produktion, forsendelse og efterfølgende debitering), der ganske svarer til, at A havde afgivet ordren telefonisk overfor B. Forskellige synspunkter har været anført om, hvad man bør sidestille med dette "digitale" kendskab. Er forholdet ikke afklaret ved parternes aftale, bør tilbagekaldelse formentlig kunne ske frem til det tidspunkt, hvor B har fået kendskab om meddelelsen (f.eks. ved at modtage underretning om, at varen er på vej), men således at A ud fra et culpasyndspunkt vil være forpligtet til at udrede B's tab ved tilbagekaldelsen (negativ kontraktsinteresse).

Var resultatet blevet modsat, ville der ingen grænser være for, hvad A kunne blive forpligtet til: Computere kan som bekendt behandle data med ekstrem effektivitet, og dermed også afgive fejlagtige data med en sådan effektivitet! Spørgsmålet er dog omtvistet. I U1994B.395 foreslår Birgitte Kofod Olsen et bearbejdningskriterium, hvorefter det tidspunkt, hvor computeren har afsluttet bearbejdningen af de indkomne data, skulle være afgørende. 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. Problemet er ikke afklaret i UNCITRALs modellov om Electronic Commerce.

Spørgsmålet tegner sig anderledes efter CISG, FN's Konvention om Internationale Købsaftaler ("Convention on Contracts for the International Sale of Goods"). Ifølge CISG art. 16 kan et tilbud tilbagekaldes, indtil en aftale er indgået, såfremt tilbagekaldelsen kommer frem til tilbudsmodtageren, før han har afsendt et antagende svar. Da "antagende svar" ikke behøver at udgøre en umiddelbar manifestation af en menneskelig vilje (viljeserklæring), vil aftale kunne indgås, selv om svaret udspringer af en fejltagelse. Er dette tilfældet, opstår i stedet spørgsmålet, om aftalen kan erklæres ugyldig p.g.a. fejlskrift m.v., jf. for dansk ret afl. § 32, stk. 2.

b. Web-pacts

Den førnævnte usikkerhed om, hvornår nogen er bundet af en viljeserklæring, har fremkaldt et betydeligt behov for regulering, og i mangel af lovregulering har mange virksomheder søgt at skabe det fornødne reguleringsgrundlag i såkaldte "web-pacts".

Med betegnelsen *web-pact* sigtes der almindeligvis til aftalevilkår, der træder frem på en hjemmeside, og som informationsudbyderen (i en forbrugertransaktion, den erhvervsdrivende) ønsker sin aftalemodpart (forbruger) bundet af. Web-pacten er i familie med den såkaldte *shrink wrap*-aftale, der er hyppigt anvendt ved salg af edb-programmer. En *shrink wrap*-aftale er et sæt aftalevilkår, der er placeret på en vare på en sådan måde (typisk bag krympefolien, deraf navnet), at brugeren kan orientere sig om indholdet i forbindelse med købet. Vilkårene indeholder typisk klausuler om, at forbruger tiltræder disse vilkår, hvis han bryder krympefolien, idet man hertil føjer, at brugeren blot kan returnere varen igen, hvis han ikke ønsker sig bundet (og således ikke har brudt folien). Tilsvarende vil en web-pact f.eks. kunne knytte licensbegrænsninger til den information, der hentes ind fra en hjemmeside. Web-pacts kan også anvendes til at etablere et mere fintmasket aftalegrundlag for elektronisk handel.

Det er i "automatiseringen" af aftaleforpligtelsen, at *shrink wraps* og web-pacts volder ensartede problemer. Problemet består i, at den handling, der som viljeserklæring angivelig skulle udløse aftalepligten (bruddet på folien) udfolder sig *efter* parternes forhandling og ofte også efter ydelsernes udveksling. 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 m.v.) det fulde retsgrundlag mellem parterne. Skal dette retsgrundlag modificeres, kræves

tiltrædelse fra begge parter. En ensidig fremsendelse af vilkår er ikke tilstrækkelig, jf. senest dommen i *U1996.1125SH*.

Shrink-wrap aftalens problem har i dansk retspraksis foreligget i forbindelse med de såkaldte reverssystemer (d.v.s. distributionssystemer med vilkår for videresalg), man har anvendt ved ugebladsdistribution. I *U1943.1119H* 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 *U1935.1066H*, der lagde til grund, at forbudet ikke i sig selv var forpligtende. Se ligeledes *U1942.963V* og i det hele Blomqvist (1987), s. 114 f. med henvisning til yderligere praksis samt for svensk ret NJA1949.645, hvor et tilsvarende forbehold på en grammofonplade ikke bandt Sveriges Radio.

En nyligt afsagt amerikansk appelretsdom afsagt den 20. juni 1996 af 7th. Circuit i sagen *Pro-CD v. Zeidenberg*, 86 F.3d 1447 (7th Cir., 1996), har taget et væsentligt skridt i retning mod anerkendelse af shrink wrap-licensvilkår. I april 1995 købte Martin Zeidenberg CD-ROM-produktet *Select Phone*, som indeholdt en database indsamlet fra et stort antal telefonbøger. Sådanne oplysninger kunne næppe i sig selv beskyttes ophavsretligt, men ifølge de medfølgende shrink-wrap vilkår, som kom til syne på skærmen, når programmet blev anvendt, men hvis indhold ikke var synlige på pakken, måtte oplysningerne kun anvendes til privat, ikke-erhvervsmæssige formål. Desuagtet stillede Zeidenberg de pågældende 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 ved efter brugerens formelle accept af købet. I så henseende fandt retten lighedspunkter med 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 billetens fremsendelse) får kendskab til de nærmere vilkår. Førsteinstansen (se 908 F.Supp., W.D. Wis, 1996) havde antaget, at købet var indgået på de vilkår, kunden kunne læse på programpakken yderside, hvorimod kunden ikke var bundet af de klausuler, som yderteksten henviste til, men ikke gengav.

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.

En skotsk Court of Session er i en dom fra december 1995 gået endnu videre, se sagen *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.

Problemstillingen er imidlertid anderledes for web-pacts, hvor vilkårene lægges frem for brugeren på en måde, der giver ham mulighed for at erkende sin retsstilling inden aftaleindgåelsen. Her afgives den relevante viljeserklæring

nemlig med fuld viden om de vilkår, der er gældende for transaktionen. Fremgår det f.eks. af en hjemmeside, at et materiale, der ikke er ophavsbeskyttet, ikke må anvendes til erhvervsmæssig brug, må en sådan begrænsning respekteres som en del af parternes aftale. 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.

Den her beskrevne form for kontrahering giver anledning til flere principielle overvejelser. Når en pakket digitalvare med aftalevilkår på "forsiden" når forbrugeren, skal han overveje, om tilbudet accepteres, inden han åbner pakken. Spørgsmålet er, om man bør tillade sælgeren adgang til en ubegrænset ansvarsfraskrivelse i denne specielle form for aftaleindgåelse. Samme problemstilling gør sig gældende når det aftaledokument, som forbrugeren agter at (elektronisk) underskrive, henviser til andre dokumenter, der indeholder yderligere aftalevilkår. Spørgsmålet her er, om forbrugeren vil blive bundet af disse "usynlige" vilkår. I forlængelse heraf bør det overvejes, hvordan man løser problemstillingen vedrørende omfanget af aftalematerialet, specielt med hensyn til vanskelighederne ved at overskue mængden af elektroniske dokumenter.

c. Inkorporering

Problemerne ved den digitale aftaleindgåelse får en særlig dimension, når der rejses spørgsmål om at skulle inkorporere aftalevilkår i certifikater eller andre meddelelser, der udveksles under en digital kommunikationsproces. Problemet kan bl.a. tænkes at opstå i forbindelse med certificering af nøglepar som led i public key krypteringssystemer: For at undgå at blive pålagt et strengt ansvar, ser afgiverne af sådanne certifikater en interesse i at begrænse ansvaret for eventuelle fejl i selve certifikatet. Sådanne ansvarsreguleringer er imidlertid ganske vanskelige at formulere, fordi de bevæger sig på knivens æg: Enten fraskrives ansvaret, hvorved troværdigheden forsvinder, eller også påtager man sig et garantilignende ansvar, hvorved virksomheden som certificeringscenter bliver mindre attraktiv (mere risikabel). Skal disse interesser afbalanceres, må der formuleres præcise - og ofte ordrige - regler. Men typisk vil det føles som en belastning at skulle give plads for sådanne regler i selve certifikatet.

For at kunne overkomme disse problemer - "puste og have mel i munden" - har visse udbydere af disse certifikater ønsket at kunne inkorporere aftalevilkår i selve certifikatet ved kun at angive en kortfattet betegnelse, som er tilstrækkelig til at kunne identificere den fulde aftaletekst. Dette problem om "incorporation by reference" rejser imidlertid en række principielle spørgsmål: Har løftegiveren (den, der læser og følgelig ventes at blive forpligtet af vilkårene) den fornødne "vilje" til at blive bundet?

Spørgsmålet blev drøftet i UNCITRALs EDI-arbejdsgruppe under forberedelsen af modelloven om Electronic Commerce, og under mødet i UNCITRAL i maj-juni 1996 vedtog man, at lade incorporation by reference være et af de punkter, der overvejes i den arbejdsgruppe, der udarbejdede UNCITRAL-modelloven.

Under de uformelle drøftelser af spørgsmålet blandt EDI-arbejdsgruppens medlemmer har det bl.a. været foreslået, at der burde indføres en mellemøsning til at løse den modstridende interesse mellem på den ene side at sikre, at den forpligtede kender sin forpligtelse, og på den anden side at undgå, at digitale meddelelser unødigt belastes med meget omfattende forskrifter af standard-karakter, som parterne i forvejen vil anse for gældende. Mellemøsningen skulle bestå i, at et vilkår kun er gyldigt inkorporeret i den digitale meddelelse, hvis vilkårets væsentligste retsvirkninger er angivet i den tekst, der inkorporerer det. Systemet kendes fra det danske tinglysningssystem - omend i en noget andet variant - nemlig ved de angivelser af et tinglyst dokumentets retsvirkninger, der finder vej til tingbogen. Der har ikke været almindelig tilslutning til tankegangen. Den strider noget mod den formalisme, der præger aftaleskrivningen i common law-lande, for hvilke det vil stå som en betydelig usikkerhedsfaktor, *hvor* meget af den forpligtende tekst, der skal præsenteres i den inkorporerende tekst, og i hvilken *form*.

6. Retsstilling og retsbeskyttelse i øvrigt

a. Overblik over komplekse transaktioner

En stor del af forbrugerbeskyttelseslovgivningen søger at sikre forbrugeren mod uventede følger af at indlade sig på komplekse transaktioner. Dette almene retspolitiske ønskemål kan give anledning til at overveje, om man på IT-området bør indføre en særlig sikring af forbrugers retsstilling.

Overvejelser i denne retning har allerede været gjort i USA, hvor man i øjeblikket drøfter indførelsen af en ny "article 2B" til den uniforme køberetslovgivning, Uniform Commercial Code (UCC). Et af problemerne er, om man skal opfatte software som en vare ("goods"). Det forslag, der for øjeblikket diskuteres, tager bl.a. stilling til, hvem af parterne, der skal have ret til den information, der indgår i transaktionen, f.eks. hvis parternes samarbejde har frembragt nye data. Ligeledes opstiller den principper, der skal sikre, at frembragt information ikke kompromitteres overfor tredjepart. Endelig tager forslaget stilling til, under hvilke omstændigheder leverandørens ensidigt fastsatte licensvilkår forpligter kunden. Forslagets ambition er at tage højde for de særlige karaktertræk ved information, herunder hvorledes man forholder sig til de ophavsretlige restriktioner, hvornår der er sket korrekt opfyldelse, pligt til at modvirke uautoriseret anvendelse, samt gyldigheden af shrink wrap-aftaler. Antallet af repræsentanter fra softwareindustrien er forholdsvis stort i dette forberedende arbejde.

Se nærmere om forslaget Raymond T. Nimmer, Donald A. Cohn & Ellen Kirsch: License Contracts Under Article 2 of The Uniform Commercial Code: A Proposal. 19 Rutgers Computer & Technology Law Journal 283 (1993).

Ændringsovervejelserne i USA udspringer af, at USA hvad køberetlig lovgivning angår tilhører en anden tradition end Danmark. Dansk formueret og dermed også dansk køberet, baseres i vid udstrækning på ulovbestemte regler. Der er relativt langt mellem de formueretlige lovinitiativer (når bortses fra dem, vi er nødt til at indføre i kraft af EU-samarbejdet), og behovet herfor er beskedent, når det tages i betragtning, at domstolene ofte kan nå fleksible

fortolkningsresultater, der imødekommer eventuelle beskyttelsesbehov, på grundlag af den eksisterende lovgivning og veletablerede retsgrundsætninger.

Dertil kommer, at behovet for at beskytte forbrugeren i forbindelse med Internet-baserede transaktioner ikke er markant anderledes end behovet for at sikre forbrugere i relation til andre IT-ydelser. Dog må det erkendes, at når en forbruger køber IT-systemer, erhverver han en ydelse, der er kompleks med heraf følgende behov for særlig vejledning.

I stedet for at analysere dette almene problem forekommer det mere tjenligt at se på de enkelte lovgivningsområder, hvor forbrugers retsstilling og retsbeskyttelse kan tænkes påvirket af de nye digitale medier.

b. Købeloven

Det er tvivlsomt, om købeloven også gælder digital information, der spredes uden samtidig overførelse af et medium, f.eks. ved indlæsning af en programfil fra en hjemmeside på WWW. Dette spørgsmål har været drøftet i litteraturen i relation til edb-programmel og med sigte på købeloven og produktansvarsloven. På nuværende tidspunkt findes der ingen domspraksis - hverken herhjemme eller i udlandet - der klart tager stilling til, om kbl. gælder for informationsprodukter. Spørgsmålet har været diskuteret i den juridiske litteratur, men heller ikke her finder man noget klart svar.

Mads Bryde Andersen i "Lærebog i edb-ret" (1991) s. 455 ff. foreslår, at man besvarer spørgsmålet under hensyntagen til, hvorledes den leverede information optræder over for brugeren. Er der tale om information, der fungerer i systeminterne tekniske sammenhænge, som brugeren ikke oplever som kommunikationsprocesser (f.eks. programmel indlejret i apparater), bør man efter forfatterens mening nå til, at kbl. gælder. Er der derimod tale om information, der indgår i et samspil med brugeren, på samme måde som oplysninger i en bog (f.eks. en informationsdatabase), taler meget for at trække paralleller mellem programmel og andre informationsprodukter (f.eks. litteratur), hvilket fører til, at købeloven ikke finder anvendelse. (Se også Bryde Andersen: Edb og ansvar (1988) s. 320 ff.)

Ifølge denne sondring er det uden betydning for retsgrundlaget, hvilket *medium*, der understøtter transaktionen. Når det gælder digital information, som netop kendetegnes ved at skulle læses maskinelt, og altså ikke af forbrugeren selv, er mediets rolle udtømt, når informationen er gjort maskinlæsbar. Valget af medium har derfor primært betydning for, om ydelsen er leveret rettidigt og på en måde, der gør den digitale information læsbar. Når dette er tilfældet, vil alle yderligere retsspørgsmål knytte sig til selve informationen.

c. Leveringsbegrebet

Derimod ligger det klart, at overdragelse af information giver anledning til praktiske og retlige vanskeligheder, der adskiller sig fundamentalt fra dem, vi kender i den klassiske formueret. Et af disse spørgsmål angår leveringsbegrebet. Ifølge den almindelige regel i købelovens § 9 skal sælgeren levere salgsgen-

standen på det sted, hvor han ved køkets afslutning havde sin bolig. Drev han på dette tidspunkt forretning, og stod salget i forbindelse dermed, skal levering ske på forretningsstedet. Befandt genstanden sig ved køkets afslutning på et andet sted end ovenfor nævnt, og var parterne eller burde de være vidende derom, anses dette som leveringssted. Denne regel giver ikke mening, når det solgte skal leveres via et digitalt kommunikationsnet. Således er bestemmelsens forudsætning om, at det solgte "befandt" sig enten hos sælgeren eller køberen irrelevant, eftersom den leverede digitale informationsmængde bliver leveret ved at blive *kopieret* fra et medium, som sælgeren har rådighed over, og til et medium, som køberen har rådighed over.

I Mads Bryde Andersens "Lærebog i edb-ret" (1991), s. 399 f., tilkendegives den opfattelse, at den part, der har det i sin magt at træffe opfyldelsesvalget, bærer ansvar og risiko for, at dette valg viste sig ufrugtbart. Denne opfattelse fører bl.a. til, at risikoen for, at en transmitteret informationsmængde går tabt på sin vej fra sælger til køber, påhviler sælger indtil informationerne kopieres over til et af modtageren valgt medium. Hvis køberen f.eks. har ønsket, at en tekstfil leveres til køberens e-mail adresse hos TeleDanmark, må risikoen for, at filen går tabt forinden dette er sket, påhvile sælgeren.

Retsvirkningerne af levering i købeloven er ens, uanset på hvilken måde levering er sket. Når man fjerner sig fra den køberetlige regulering kan det imidlertid tænkes, at der må påregnes forskellige leveringsbegreber alt efter hvilke retsvirkninger, der er tale om at knytte til leveringshandlingen (forsinkel-se, mangelsbedømmelse ydelsesrisiko, vederlagsrisiko).

EU-Kommissionen har den 18. juni 1996 fremsat forslag til et direktiv om garanti ved forbrugerkøb, se KOM(95) 520 endelig udg. Direktivet, der supplerer direktiv 93/13/EØF om urimelige kontraktvilkår i forbrugerftaler, vil fastlægge en minimumsgarantiperiode for forbrugeres køb af varer samt udstikke retningslinier for supplerende garantier udstedt af sælgere eller producenter. Der lægges op til en ufravigelig garantiperiode på 2 år regnet fra leveringstidspunktet, art. 3, stk. 1, dog kun 1 år for så vidt angår krav på reparation. Der er tale om et minimumsdirektiv, der altså ikke afskærer medlemslandene fra at opretholde strammere forbrugerbeskyttelsesregler.

d. Lovvalg og værneting

Ved elektronisk handel via Internettet over landegrænser kan det hyppigt forekomme, at en dansk forbruger træder i aftaleforhold med en udenlandsk erhvervsdrivende. I sådanne forhold gælder den internationale privatrets regler om lovvalg og værneting.

I spørgsmålet om *lovvalg* gælder et udgangspunkt om aftalefrihed, jf. artikel 3, stk. 1, i lovvalgskonventionsloven, hvorefter en aftale er underkastet den lov, som parterne har vedtaget. Hovedreglen fraviges ved artikel 5, der finder anvendelse på forbrugerftaler om levering af løsøregenstande eller tjenesteydelser eller om ydelse på kredit til et forbrugerformål. Uanset hovedreglen i artikel 3 fastslår denne artikel, 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.

Artikel 5 lyder som følger:

1. Denne artikel finder anvendelse på aftaler om levering til en person ("forbrugeren") af løspøregenstande eller tjenesteydelser med henblik på en anvendelse, der må anses at ligge uden for hans erhvervsmæssige virksomhed, eller om ydelse på kredit til et sådant formål.

2. Uanset artikel 4 [der peger på det land, som aftalen har sin nærmeste tilknytning til, når andet ikke er aftalt] kan parternes lovvalg ikke 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, eller

- såfremt den anden part eller dennes repræsentant har modtaget forbrugers bestilling i dette land, eller

- såfremt aftalen angår salg af løspøregenstande, og forbrugeren er rejst fra dette land til et andet land og har afgivet sin bestilling dér, under forudsætning af at forbrugers rejse var arrangeret af sælgeren med det formål at formå forbrugeren til at afslutte køb

3. Uanset artikel 4 er en aftale, der er omfattet af nærværende artikel, i mangel af et lovvalg i henhold til artikel 3 undergivet loven i det land, hvor forbrugeren har sin bopæl, såfremt den er indgået under de i stk. 2 nævnte omstændigheder.

4. Denne artikel finder ikke anvendelse på

- a) transportaftaler;
- b) aftaler om levering af tjenesteydelser, såfremt disse udelukkende skal præsteres i et andet land end det, hvor forbrugeren har sin bopæl.

5. Uanset stk. 4 finder denne artikel anvendelse på aftaler, hvorved der for en samlet pris ydes en kombination af rejse og ophold.

Når disse bestemmelser overvejes anvendt i relation til Internet-baserede transaktioner, er det springende punkt, hvornår den erhvervsdrivende kan siges forud for aftalens indgåelse at have "foretaget reklamering". Begrebet "reklame" tager almindeligvis sigte på handlinger, der har karakter af opsøgende informationsvirksomhed, der tager sigte på salg m.v., sml. definitionen i rådsdirektivet om reklame for humanmedicinske lægemidler (92/28, EU-Karnov, 5. udgave 1996, s. 1221), artikel 1, stk. 3. Som nævnt ovenfor, kan det være vanskeligt at opretholde forestillingen om, at der udøves en sådan form for opsøgende virksomhed i relation til enhver bruger, der er forbundet med Internettet.

For at anse, 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 Internettet 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 hypertext-forbindelser til den fremmede hjemmeside. En sådan retstilstand synes bl.a. forudsat ved den nyligt afsagte amerikanske dom i "Playmen-sagen", se herom nedenfor i kapitel IV.5.

Forbrugerombudsmanden har for nylig taget stilling til lovligheden af internationale virksomheders markedsføringskampagne på Internettet, der har virkning på danske forbrugere, i forhold til den danske markedsføringslov. Når det vurderes, om en virksomheds reklamemateriale på Internettet kan siges at være foretaget i Danmark - og dermed underlagt de danske regler, herunder markedsføringsloven - må to kriterier være opfyldt. For det første, skal reklamerne være tilgængelige og have relevans for danske forbrugere. For det andet lægges der vægt på, om virksomheden har en så stor kommerciel aktivitet i Danmark, at det er naturligt for virksomheden at iværksætte markedsføringsforanstaltninger i Danmark. Hvis begge kriterier er opfyldt, anser Forbrugerombudsmanden sig kompetent til at håndhæve forbrugernes beskyttelsesregler over for den pågældende udenlandsk virksomhed og kræve at de danske regler respekteres.

I tillæg til lovvalgskonventionsloven indeholder afl. § 38d en generel ugyldighedsregel om *lovvalgsaftaler* i forbrugerforhold, der peger på lovgivningen i et land uden for EU/EØS. Sådanne aftaler gælder nu ikke, for så vidt angår urimelige aftalevilkår, såfremt den relevante EU/EØS ville have givet forbrugeren en bedre retsstilling.

Hvad angår *værneting* inden for EU-området gælder EF-Domskonventionen, jf. rpl. § 247. Domskonventionens artikel 2 opstiller en hovedregel om, at personer, der har bopæl på en kontraherende stats område, uanset deres nationalitet skal sagsøges ved retterne i denne stat. Personer, som ikke er statsborgere i den stat, hvor de har bopæl, er undergivet de kompetenceregler, der gælder for landets egne statsborgere. Konventionens artikel 5, stk. 3 foreskriver at man i sager om erstatning uden for kontrakt skal anlægge sag ved retten på det sted, hvor skadetilføjelsen er foregået. Udlændinge, der er bosat uden for EU-området og uden for det nordiske område, hvor Den Nordiske Domskonvention finder anvendelse, kan sagsøges her i landet, hvis et af retsplejelovens undtagelsesværneting kan anvendes på sagen, se rpl. § 246, stk. 1.

Kommissionen har den 24. januar 1996 fremlagt et direktivforslag til Rådsdirektiv om søgsmål med nedlæggelse af påstand om forbud inden for området "beskyttelse af forbrugeres interesser", se EFT 1996 C 107/3 og den bagvedliggende handlingsplan, KOM(96) 725, endelig udg. Forslaget, der bygger på Kommissionens grønbog "Access to justice" og tilhørende høringssvar, har til formål at koordinere medlemsstaternes lovgivning med henblik på at forbedre mulighederne for at nedlægge forbud mod handlinger, som skader forbrugernes

interesser, og som strider mod en række forbrugerbeskyttende direktiver. Disse direktiver fremgår af et bilag til direktivforslaget. Det drejer sig bl.a. om direktivet om vildledende reklame, direktivet om aftaler indgået uden for fast forretningssted, direktivet om forbrugercredit, visse bestemmelser i direktivet om udøvelse af tv- og radiospredningsvirksomhed, direktivet om pakkerejser, direktivet om reklame for humanmedicinsk lægemidler, direktivet om urimelige kontraktvilkår i forbrugeraftaler, direktivet om timeshare og det kommende direktiv om fjernsalg. Bilaget forventes udbygget.

Direktivforslaget skal åbne mulighed for, at en erhvervsdrivende kan sagsøges i sit hjemland for overtrædelser, der har virkning i en anden medlemsstat. Herved skulle myndigheder/organisationer, der varetager forbrugernes interesser, få bedre muligheder for at standse overtrædelser af direktiverne og dermed sikre en mere effektiv håndhævelse af lovgivningen.

Det har således vist sig vanskeligt at komme overtrædelser til livs ved gennemførelse af en retssag, såfremt virksomheden, der overtræder reglerne i en medlemsstat, ikke er bosiddende i samme land. Myndigheden vil tillige ofte være afskåret fra at kunne anlægge en sag i virksomhedens hjemland, ligesom den ikke vil kunne få assistance fra hjemlandets tilsynsmyndighed, der alene kan behandle sager, der har virkning over for dets egne borgere.

Direktivforslaget indebærer som minimum, at hver medlemsstat skal udpege en domstol/administrativ myndighed (herhjemme domstolene), der skal have kompetence til at træffe afgørelse i en sag om nedlæggelse af et forbud. Medlemsstaterne skal samtidig tillade, at en udenlandsk organisation/myndighed, der af sin hjemstat er udpeget som kompetent til at anlægge sådanne sager, rejser sager ved domstolen/myndigheden.

Reglerne om lovvalg og de processuelle rammer for sager, der rejses efter dette direktiv, fastlægges af de gældende konventioner, de internationale privatretlige regler og den nationale retsplejelovgivning i medlemsstaten.

Herudover kan medlemsstaterne beslutte, at en udenlandsk myndighed/organisation først kan rejse sag, hvis den forinden har rettet henvendelse til den lokale tilsynsmyndighed/organisation i den erhvervsdrivendes hjemland og givet denne mulighed for at rejse sagen.

e. Fortrydelsesret

Det indgår som et grundfæstet element i den civilretlige lovgivning om forbrugerbeskyttelse, at forbrugeren bør beskyttes mod sine egne dispositioner, når han indlader sig på komplekse transaktioner. Dette hensyn bør spille en særlig rolle, når der er tale om forbrugerdispositioner, der eksekveres ved hjælp af digitale medier: Med den effektive informationsbehandling, disse systemer tilbyder, opstår risikoen for, at den enkelte forbruger gennem enkle tastetryk m.v. forpligtes i et uforudset omfang.

En række love beskytter derfor allerede i dag forbrugeren mod "sig selv" i denne betydning. Det gør f.eks. forbrugeraftaleloven, pakkerejseloven, og nu

også lov om forbrugerbeskyttelse ved erhvervelse af fast ejendom, hvor fortrydelsesretten dog er kombineret med en pligt til at svare en godtgørelse på 1 procent af købesummen, se lovens § 11.

Forbrugeraftalelovens kapitel 3 giver bl.a. regler om fortrydelsesret ved aftaler indgået uden for fast forretningssted. Efter § 2 må erhvervsdrivende ikke uden forudgående anmodning herom rette *personlig eller telefonisk henvendelse* til en forbruger på dennes bopæl, arbejdsplads eller andet sted, hvortil der ikke er almindelig adgang, med henblik på straks eller senere at opnå tilbud eller accept på tilbud om indgåelse af aftale. Et løfte afgivet i strid med dette forbud er ikke bindende, jf. lovens § 3. Det er ikke ganske klart, om denne bestemmelse også omfatter markedsføring af varer og tjenesteydelser via Internettet. Gennem WWW kan forbrugere bestille en mangfoldighed af ydelser uden at rejse sig fra terminalen. Informationsydelser i form af edb-programmel, adgang til telelinjer og databaser og tilrådgivelsesstillelse af anden software (video-on-demand) præsteres på stedet. Så længe forbrugeren selv efterspørger disse ydelser, volder loven ingen problemer, men det gør den, når forbrugeren udsættes for en overrumpling.

Selv om forbudet mod telefoniske henvendelser kan siges at åbne døren på klem til en regulering af den uanmodede *digitale* henvendelse, er der næppe grundlag for at anlægge en sådan udvidende fortolkning. Baggrunden for forbudet ligger primært i den psykologiske overrumpling, der gør sig gældende i en samtale. Denne risiko består ikke i samme omfang, når en henvendelse sker via Internettet. Heller ikke telegrafiske meddelelser m.v. falder indenfor reglen, se hertil Karnovs Lovsamling (1995) s. 4624, note 18. Resultatet er dog ikke utvivlsomt. Det har med en vis styrke været gjort gældende, at den bruger, der handler fra sin terminal, er i en mindst lige så udsat situation, som den, der opsøges på sin bopæl/arbejdsplads, idet han ikke altid vil have overblik over de retsvirkninger, han kan udløse herigennem. Ved terminalen har forbrugeren f.eks. ingen fysisk kontakt med varerne, hvilket kan give grundlag for uoverlagte dispositioner.

Den uanmodede digitale henvendelse må derimod håndteres efter reglerne om fortrydelsesret ved *fjernsalg* i forbrugeraftalelovens kapitel 4. Efter forbrugeraftalelovens § 10 defineres dette som "en aftale om salg af varer, ifølge hvilken varen skal sendes til køberen, når sælgeren i katalog, annoncer *eller ved andet læsbart medie* har tilbudt at sende varen efter bestilling pr. telefon, brev *eller andet læsbart medie*, og køberen har afgivet bestilling på denne måde". Efter de udhævede ord er det åbenbart, at markedsføring via Internettet udgør fjernsalg. Virkningen heraf er, at køberen kan træde tilbage fra aftalen i overensstemmelse med de særlige regler herom i lovens §§ 11 og 13.

Et væsentligt anvendelsesområde for denne bestemmelse har været den såkaldte *teleshopping*, hvor den erhvervsdrivende får kontakt med forbrugeren via tv-apparatet. Grundlaget for forbrugers bestilling kan her være en såkaldt "informercial", hvor den erhvervsdrivende på tv - ofte udenfor prime time-sendetiden - giver information om produktet på en måde, der går langt mere i dybden end i den almindelige tv-reklame. Forbrugeren kan herefter bestille varen ved at ringe op på telefonen.

Europa-Parlamentets og Rådets direktiv 97/7/EF om forbrugerbeskyttelse i forbindelse med aftaler vedrørende fjernsalg blev vedtaget den 22. januar 1997. Direktivets formål er at tilnærme medlemsstaternes retsregler om forbruger aftaler vedrørende fjernsalg, "der med indførelsen af nye teknologier medfører en mangedobling af de midler, som forbrugeren råder over til at gøre sig bekendt med kommercielle tilbud overalt i Fællesskabet." Direktivet indeholder bestemmelser om fortrydelsesret, ligesom det sikres, at forbrugerne modtager relevante informationer i forbindelse med fjernsalgstilbud og bestillinger. Disse informationer skal bekræftes skriftligt eller på et andet varigt medium, som er til forbrugers rådighed og tilgængeligt for ham.

Direktivet indeholder endvidere bestemmelser om effektivering af fjernsalgsbestillinger og et forbud mod levering uden forudgående anmodning. Forbrugernes privatliv beskyttes ved bestemmelser, der begrænser brugen af visse fjernkommunikationsteknikker. Brug af telefax og automatisk opkaldssystem kræver således forbrugers forudgående samtykke. Andre fjernkommunikationsteknikker, som tillader individuel kommunikation, må kun anvendes, hvis forbrugeren ikke klart modsætter sig det. Medlemslandene har en frist på 3 år til gennemførelse af direktivet. Til direktivet henhører en henstilling (92/295/EØF), der opfordrer de berørte brancher til at supplere direktivets minimumsbestemmelser med kutymeregler.

ICC retningslinjer om Interactive Marketing Communications af 11. juni 1996 indeholder en række generelle principper og et antal specifikke guidelines om salg via åbne interaktive medier.

De *generelle principper* fastslår, at kommerciel kommunikation gennem interaktive medier bør overholde "the spirit of the principles set forth in the ICC's Codes on Advertising Practice, Sales Promotions, Direct Marketing, Environmental Advertising, and Sponsorship, as well as the ICC-ESOMAR Code on Marketing Research Practices." Sådanne markedsføringsskridt skal være "legal, decent, honest and truthful", idet "legal" her forstås som "consistent with the laws of that country in which the dissemination of such communication originates".

I de *specielle guidelines* fastslås det, at erhvervsdrivende altid skal røbe deres identitet, at de skal respektere brugernes ønske om ikke at modtage kommercielle meddelelser, og at de skal give oplysning, hvis anvendelsen af meddelelser eller tjenesteydelser er forbundet med betalingspligt. Ligeledes bør de erhvervsdrivende respektere, at visse kommunikationsformer (newsgroups, bulletin boards etc.) er offentlige mødesteder, der kan have særlige forventninger om, hvorledes kommerciel information distribueres. Sådant information må kun spredes til den slags grupper, hvis de angår kommercielle aktiviteter, eller hvis der i øvrigt foreligger et særligt samtykke. Herudover skal virksomhederne respektere privatlivets fred og i den forbindelse kun registrere nødvendig information samt besvare anmodninger fra registrerede personer om, hvad man har registreret om dem. På grund af mediets globale karakter skal en særlig omhu udvises overfor information, der kan blive opfattet som voldelig, racistisk eller sexistisk.

f. Selvreguleringens implikationer

Svaret på problemerne omkring regulering og beskyttelse af forbrugerne i informationssamfundet er ofte selvregulering. Selvregulering har de positive konsekvenser, at reguleringen accepteres af virksomhederne, som i fællesskab har vedtaget dem. Indholdet af reguleringen kan til enhver tid ændres uden omfattende bureaukrati. Offentlig regulering skal så forbeholdes mere kvalificerede bud på grundlæggende regler i samfundet, såsom forbud mod børneporno.

Accepten af selvregulering beror på den forudsætning, at der er et sammenfald mellem kommercielle interesser samt samfunds- og forbrugerinteresser. Det må således fremstå som givet, at virksomhederne ikke frivilligt vil acceptere en regulering, der strider imod virksomhedernes interesser. Det må nok anses for tvivlsomt, om en sådan forudsætning kan anses for at være opfyldt i alle tilfælde. Både interesser i den enkelte virksomhed og i en bestemt branche kan stride imod mere generelle samfunds- og forbrugerinteresser. Forbruger- og samfundsinteresser kan tilgodeses ved at inddrage organisationer og myndighederne i forhandlingerne om reguleringens udformning. Det er imidlertid spørgsmålet, hvor langt en sådan deltagelse kan gå.

Under alle omstændigheder forudsætter selvregulering, at reguleringen er rimeligt branchedækkende, og at reguleringen ikke får konkurrencebegrænsende effekter. Det er nok sandsynligt, at en selvregulering vil kunne være branchedækkende inden for visse sektorer af erhvervslivet, men det er sikkert, at den ikke vil kunne være tilstrækkelig inden for alle brancher. Det er endvidere en historisk kendsgerning, at selvregulering har en tendens til, at veletablerede virksomheder i en bestemt branche bliver de dominerende ved regelfastsættelsen.

Det er fra mange sider påpeget, at informationssamfundet som en meget positiv konsekvens kan betyde en øget konkurrence ved, at mindre og mellemstore virksomheder får adgang til rent faktisk at konkurrere med større - men mindre dynamiske - organisationer. Selvregulering vil derfor i vidt omfang kunne tænkes at kunne bremse den konkurrenceskærpelse og teknologiudvikling, som ønskes etableret gennem udviklingen af informationssamfundet. Det vil derfor under alle omstændigheder være en "offentlig opgave" at sikre, at enhver form for konkurrencebegrænsning ikke accepteres.

g. Formkrav

Det er efterhånden blevet en tradition på forbrugeraftaleområdet og lønmodtagerområdet, at komplicerede transaktioner skal foreligge på skrift. De fleste af de regler, vi har herom, knytter ikke gyldighedsvirkning til de særlige *formkrav*. Tilsidesættelse kan derimod få virkning for bevisbedømmelsen eller måske ligefrem være strafsanktionerede.

Når man overvejer behovet for at beskytte forbrugere mod virkningerne af komplicerede transaktioner, der indgås ved hjælp af digitale medier, kan et middel hertil være at indføre lignende formkrav. I en sådan drøftelse må man

på den ene side tage hensyn til forbrugerhensynet, men på den anden side til, at det digitale medium i disse år er ved at erstatte papirets funktioner ud fra et alment ønske om at understøtte dette medium i samfundet. En pligt til at understøtte digitale transaktioner med en papirafale ville være ensbetydende med en frakendelse af det digitale mediums gyldighed. Ligeledes må det tages i betragtning, at man på visse områder allerede har anerkendt, at skriftlighedskrav kunne opfyldes gennem brug af digitale medier. Ved vedtagelsen af pakkerejsedirektivet blev der således afgivet en råds- og kommissionserklæring om, at direktivets skriftlighedskrav, der indebærer, at erklæringen skal foreligge "skriftligt eller på anden for forbrugeren klar og tilgængelig måde", også omfatter elektroniske medier. Se herved Betænkning om Pakkerejser, nr. 1240/1992, s. 142 og 244.

Direktiv om grænseoverskridende pengeoverførsler (vedtaget den 27. januar 1997, 97/5/EF), der har til formål at sikre hurtige, sikre og billige grænseoverskridende betalinger, indeholder bl.a. regler om oplysningspligt ved sådanne transaktioner. Direktivets artikel 3 bestemmer, at udbyderne "stiller skriftlige oplysninger om vilkårene for grænseoverskridende pengeoverførsler til rådighed for deres ... kunder i en let forståelig form, eventuelt ad elektronisk vej."

Når man ud fra et forbrugerbeskyttelsesperspektiv kan være forbeholden overfor at lade digitale dispositioner forpligte i samme omfang som papirdispositioner, og tilsvarende være tilbageholdende med at lade krav om "digital skriftlighed" erstatte "papirskriftlighed", hænger det sammen med, at der endnu ikke har dannet sig samme generelle opfattelse af, at et museklik på et skærmbillede manifesterer en vilje til at være forpligtet, som f.eks. en underskrift på et stykke papir gør det. UNCITRAL's modellov om Electronic Commerce udtaler udtrykkeligt, at den ikke skal tilsidesætte lovgivning om forbrugerbeskyttelse. Heri ligger en forudsætning om, at man i relation til forbrugere ikke (endnu?) kan forudsætte, at der gælder samme forventning om at være forpligtet som på det erhvervsmæssige område. Disse vil ændre sig i takt med, at det digitale medium bliver dagligdagens kommunikationsform, men de bør tages i betragtning, når spørgsmålet om digital skriftlighed diskuteres.

Denne udvikling vil givetvis blive påvirket af en kommende lovgivning om digital signatur. En sådan lovgivning planlægges p.t. i Forskningsministeriet, og et af dens problemer er netop vanskeligheden ved at tage stilling til, hvornår afgiveren af en digital signatur hæfter for indholdet af det signerede. Det må antages, at der på områder, hvor man for at advare forbrugere m.v. kunne tænkes at indføre regler om skriftlighed, i almindelighed bør kunne lade dette krav være opfyldt ved hjælp af digitale meddelelser.

Hvis man herefter indsnævrer blikket til de tilfælde, hvor man overvejer at lade et skriftlighedskrav være opfyldt ved digitale meddelelser, må det tages i betragtning, at en række af de argumenter, der ellers kunne tænkes at tale imod indførelsen af sådanne regler, taler med mindre vægt. Navnlig er omkostningerne og besværet ved at skulle afgive information i digital form om vilkårene for at erhverve bestemte ydelser m.v. langt mindre, end når denne information skal afgives skriftligt: Skriftlighedskravet opstår således i det

digitale miljø, d.v.s. der er allerede baseret en teknisk, automatiseret ramme for transaktionen.

De områder for formkrav, lovgivningen i øjeblikket indeholder på forbrugerområdet, retter sig alle mod bestemte transaktionstyper (dørsalg, pakkerejser etc). På det generelle forbrugeraftaleområde, jf. de særlige regler om forbrugeraftaler i afl. kapitel IV, er der i øjeblikket ingen formkrav. Ønskes en formregulering af de forbrugeraftaler, der indgås i digital form, kan en sådan regulering imidlertid knyttes til dette kapitel i afl., eventuelt således, at den erhvervsdrivende har pligt til forudgående - eventuelt i digital form - at meddele forbrugeren de vilkår, der er gældende for den således indgåede aftale.

Spørgsmålet om formkrav findes at være et principielt problem, også i en bredere sammenhæng.

Det må antages, at udviklingen og benyttelsen af åbne net i praksis i vidt omfang mindsker brugen af papir i forbindelse med forskellige former for aftaleindgåelser og information i øvrigt over for forbrugerne. Dette må umiddelbart give problemer i relation til de love, hvor der stilles krav om skriftlighed ud fra et forbrugerbeskyttelseshensyn, men må også antages at svække forbrugerens muligheder for at sikre sig bevis for en aftales vilkår og forudsætninger samt de egenskaber, der måtte være "lovet" forbrugeren i forbindelse med et eventuelt køb. Udover de eksempler på lovgivning, der er nævnt overfor, skal der peges på kreditaftalelovens krav om skriftlighed i forbindelse med indgåelse af kreditaftaler.

h. Immaterialretlige begrænsninger

Den omstændighed, at digital information (og dermed alle de ydelser, der kan præsteres på denne vis) overføres til forbrugeren ved at blive *kopieret* (hvorved der i ophavsretlig forstand fremstilles eksemplarer af denne information), indebærer, at der ved enhver transaktion af denne art er et ophavsretligt problem, der kan give anledning til skuffelser eller tab for forbrugere. Ophavsretten har dermed fået en direkte forbrugerdimension, idet immaterialretlige begrænsninger kan betyde, at forbrugeren ikke får den forudsatte nytte af et produkt.

Når information opfylder de krav, *ophavsretsloven* stiller til "værkshøjde", vil enhver eksemplarfremstilling, visning og transmission m.v. af disse *værker* kræve samtykke fra ophavsmanden eller den, han overdrager retten til. For den, der ønsker at bruge digitale værker, er den ophavsretlige eneret ganske vidtgående, eftersom enhver læsning af det digitale værk forudsætter brug af digital teknologi, og dermed eksemplarfremstilling. Med andre ord vil enhver læsning fra skærm (og dermed kopiering til hukommelsesenheden på brugerens system), downloadning på eget medium, spredning og offentlig visning m.v. kun kunne ske lovligt med samtykke fra ophavsmanden eller den, som ophavsmandens ret er overgået til.

At man tillader enerettigheder med så omfattende virkninger, hænger for det første sammen med, at ophavsretten udgør et incitament til, at ophavsretligt

beskyttede værker m.v. frembringes, produceres og distribueres. Dernæst spiller det ind, at de ophavsretligt beskyttede værker typisk bliver tilgængelige på markedsvilkår: Hvis en rettighedshaver forsøger at misbruge sin eneret, og denne rettighedshaver ikke har stilling som monopolist el.lign., vil markedet vende sig til andre udbydere. Selv om ophavsmanden selv bestemmer, om han ønsker sit værk offentliggjort eller på anden måde udnyttet overfor omverdenen, begrænser loven hans rettigheder i de tilfælde, hvor han vælger at sætte sit produkt på markedet med en udgivelseshandling. Ifølge lovens § 19 kan sådanne værker herefter spredes videre. Om en sådan spredningsret består, kan volde tvivl, når der er tale om, at værket stilles til rådighed via en hjemmeside. (Se om disse spørgsmål Mads Bryde Andersen i NIR 1995.616 ff.)

Immaterielretlige rettigheder over digitale produkter kan skabe mangelslignende problemstillinger for forbrugeren. Dette kan f.eks. tænkes, når rettigheden afskærer brugeren fra selv af *afhjælpe fejl* i programmer eller digitale data. Man kan kun rette fejl i et program m.v. ved at tage en kopi af det: Kun ved at få programmet "op på skærmen" kan man se, hvad der skal afhjælpes. Herved sker der en kopiering. Når afhjælpningen herefter har fundet sted, skal programmet herefter kopieres ned i en maskinlæsbar form, d.v.s. en anden kopi.

Det kan bemærkes, at sammenslutningen af europæiske forbrugerorganisationer, BEUC, ofte har givet udtryk for forbrugerinteresser, når ophavsretlige lovforslag m.v. har været til behandling, f.eks. i forbindelse med Kommissionens Grønbog om Ophavsret i Informationssamfundet (KOM(95) 382 endelig udg. Heri fremsættes bl.a. ønsket om, at forbrugere ikke skal betale for enhver information, der modtages, og der efterlyses en retsøkonomisk analyse af ophavsrettens konsekvenser for brugerne.

En del af disse spørgsmål er der taget højde for i ophl. § 36, der lyder således:

§ 36. Den, der har ret til at benytte et edb-program, må

1) 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 rettelser af fejl,

2) fremstille et sikkerhedseksemplar af programmet, for så vidt det er nødvendigt for benyttelsen af det, og

3) besigtige, undersøge eller afprøve edb-programmet for at fastslå, hvilke ideer og principper der ligger til grund for de enkelte elementer i programmet, hvis dette sker i forbindelse med sådan indlæsning, visning på skærm, kørsel, overførsel, lagring eller lignende af programmet, som vedkommende er berettiget til at udføre.

Stk. 2. Bestemmelserne i stk. 1, nr 1 og 2, finder tilsvarende anvendelse på andre værker i digitaliseret form, hvis anvendelse styres af et edb-program. Det er dog ikke tilladt at foretage ændringer i værkerne.

Stk. 3. Bestemmelserne i stk. 1, nr 2 og 3, kan ikke fraviges ved aftale.

Bestemmelsen sikrer programbruger en vis "forbrugerbeskyttelse", idet ophavsretten ikke hindrer *afhjælpning af fejl* i et programprodukt. Derimod tillader bestemmelsen ikke, at brugeren ændrer programmet med henblik på

forbedringer af det, endsige almindelig vedligeholdelse (f.eks. opdatering af afgiftssatser i et skatteberegningsprogram, der ændrer sig med lovgivningen).

Et andet problem er forbrugerens adgang til at *sikkerhedskopiere* (tage "et sikkerhedseksempplar") edb-programmel. Hvis denne kopi mistes samtidigt med arbejdskopien, mister forbrugeren dermed programmet. Der er imidlertid almindelig enighed om, at "et sikkerhedseksempplar" ikke udgør et ultimativt tal for, hvor mange eksemplarer, der kan udføres. Man kan så sige tage "et" sikkerhedseksempplar flere gange! Derfor er der næppe grundlag for at tage disse bestemmelser op til revision. Behovet for fejlrettelse består primært i relation til erhvervsmæssige programlicenser m.v., og i disse tilfælde er det typisk forudsat, at leverandøren skal vedligeholde det leverede i kraft af særskilt aftale. Ændringer af disse regler forudsætter ændringer i det direktiv, der ligger til grund herfor (91/250/EEC). Dertil kommer at brugeren har ret til at ændre programmet med det formål, der i praksis har størst betydning, nemlig med henblik på rettelse af fejl.

Bestemmelsen løser imidlertid ikke det problem, der opstår, hvis brugeren *ikke* har foretaget en sådan privatkopiering. Gældende aftale- og køberetlige regler giver ikke forbrugeren en udvidet kopieringsret (som f.eks. kunne tænkes udøvet ved i en sådan situation - manglende privatkopiering - at udføre en kopiering via tredjemands eksemplar af programmet) ved beskadigelse af mediet, selvom dette resultat kan påtvinge køberen en ny og i en vis forstand uforholdsmæssig udgift til genanskaffelse af denne licens. Dette gælder, selvom det er åbenbart, at betalingen primært vederlægger leverandøren for en immaterialret, snarere end for det medium, hvorpå den solgte information overdrages til forbrugeren.

Denne konklusion begrundes dog næppe, at man bør revidere disse regler for at sikre forbrugeren i disse henseender. Den erhvervsdrivende vil ofte være tilskyndet til at ordne forholdet i mindelighed med brugeren, f.eks. således at et nyt medium erhverves mod betaling af et mindre gebyr el.lign. Den erhvervsdrivende undgår dermed, at forbrugerens frustration vendes mod ham som badwill eller udvirker ulovlige kopieringer med selvtægtspræg, hvortil kommer at denne tjeneste i sig selv kan være profitabel for den erhvervsdrivende.

Et tredje problem angår forbrugerens mulighed for at *videresælge* edb-programmel. Er anden aftale ikke indgået (hvilket ophl. giver fuld aftalefrihed til at gøre), har erhververen af et program ret til at videreoverdrage programmet. Dette følger af ophl. § 19, der taler om at "et eksemplar af et værk med ophavsmandens samtykke er solgt eller på anden måde overdraget til andre." Der er næppe tvivl om, at bestemmelsen har de tilfælde for øje, hvor eksemplaret overdrages ved, at overdrageren giver erhververen et medium i hænde, f.eks. en "programpakke". Når erhververen har fået dette medium i hænde, vil han i kraft af denne råden "have ret til at benytte" programmet, jf. § 36. Overdrages eksemplaret, bortfalder brugerens ret til at anvende det, jf. § 36, herunder retten til at anvende de sikkerhedskopier m.v., der er udført inden overdragelsen.

Der er imidlertid intet i ordlyden, der afskærer brugeren fra at opnå denne ret på anden måde, f.eks. ved, at brugeren mod betaling henter et program ned fra Internet. Er i disse tilfælde andet ikke aftalt, må det antages, at brugeren også kan videreoverdrage sådanne eksemplarer. Gør han det, ophører hermed hans ret til at anvende de kopier af programmet, han foretog inden overdragelsen.

Endelig kan man som et fjerde forbrugerproblem vedrørende programlicenser nævne de anordninger, der beskytter programmer mod uautoriseret kopiering. Dette spørgsmål har bl.a. givet anledning til sager hos Forbrugerombudsmanden, se f.eks. afgørelsen i FSÅ 1991, s. 38 om elektroniske ordbøger.

Sagen drejede sig om kopibeskyttelse af standard software til edb ("dåseprogrammel"). Forbrugeren ønskede en afgørelse af, hvorvidt den anvendte kopibeskyttelse af programmet var direkte lovhjemlet, og i mangel heraf, om kopibestemmelsen var i overensstemmelse med købelovens almindelige regler, herunder reglerne om forbruger køb.

Forbrugerombudsmanden udtalte her, at han efter omstændighederne ville kunne anse det for at være i strid med god markedsføringsskik, hvis sælger, importør eller fremstiller ikke havde etableret procedure til at afhjælpe fejl i forbindelse med installering af kopibeskyttet "dåseprogrammel".

Sagen blev dog på grund af sit principielle indhold henvist til afgørelse ved domstolene.

Kopibeskyttelsesanordninger nyder en vis retsbeskyttelse ved ophavsretslovens § 78, der med bøde straffer den, som 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. Overtrædelser af denne bestemmelse påtales af det offentlige. Bestemmelsen har rod i Rådsdirektivet af 1991 om retlig beskyttelse af edb-programmer. I de nedenfor omtalte WIPO-forslag findes bl.a. regler, der forbyder anordninger, der udelukkende har til formål at omgå kopispærreanordninger.

Det må antages, at ophavsretlige begrænsninger i brugerens adgang til at benytte digital information (programmer, databaser, kunstneriske og litterære værker m.v.) i stigende omfang vil give anledning til lovregulering. På europæisk plan er en sådan lovregulering allerede gennemført ved direktivet om retlig beskyttelse af edb-programmer (91/250/EØF), der blev indført i dansk ret (bl.a. nu ved ophl. § 36) i 1989, og ved det nyligt gennemførte direktiv om retlig beskyttelse af databaser (96/9/EF). Kommissionen følger imidlertid området nøje og har for nylig fremlagt en grønbog, hvor man inviterer til en debat om behovet for yderligere regler af denne art, særligt i relation til værksanvendelsen på Internettet.

Et andet initiativ i retning mod en global regulering er fremlagt af WIPO den 30. august 1996 med sigte på en diplomatisk konference i Geneve i december måned 1996. WIPO har fremlagt i alt fire papirer, der tilsigter at kunne danne grundlag for en mulig protokol til Bernerkonventionen om beskyttelse af

kunstneriske og litterære værker. Grundet vanskelighederne med ændring af selve Bernerkonventionen, havde Wipo vedtaget 2 selvstændige traktater og et teknisk papir - "Administrative and final clauses", hvis formål var at bringe overensstemmelse med hensyn til de tekniske og juridiske bestemmelser i de fremlagte traktater. De vedtagne traktater er (1) beskyttelse af fonogramproducenter og udøvende kunstnere og (2) beskyttelse af kunstneriske og litterære værker. I dette dokument præciseres det bl.a. hvilke digitale værker, der er beskyttet - herunder edb-programmer m.v. - samt hvilke former for net-anvendelse m.v., der omfattes af den ophavsretlige beskyttelse. Der kunne ikke opnås enighed om et tredje traktatforslag vedrørende beskyttelse af databaser.

WIPO-traktater om beskyttelse af kunstneriske og litterære værker indeholder en række præciseringer, der tager stilling til, hvornår man er inden for de ophavsretlige grundbegreber (vedrørende et edb-program, uddrag af informationer, retten til distribution af værker, retten til at leje værker, regler om "Rights Management Information" m.v.) ved brug af værker i digital form. Traktatens artikel 8 fastslår, for så vidt angår retten til tilgængeliggørelse, at rettighedshaveren har eneret til at forbyde "communication to the public". Hertil hører bl.a. det forhold, at værket gøres tilgængelig som ovenfor anført om databaser, d.v.s. "by wire or wireless means, in such a way that members of the public may access these works from a place and at a time individually chosen by them."

i. Bevisproblemer

En række af de problemer, der har været berørt i det foregående, påvirkes af forbrugers mulighed for at føre bevis for, hvad han har gjort i forbindelse med en digital disposition, f.eks. i forbindelse med afgivelse af en digital signatur, læsning af en digital meddelelse eller disposition over et betalingskort. Disse bevisproblemer må formodes at få stigende betydning. Problemerne vil muligvis blive påvirket af, hvilke generelle sikkerhedstiltag, der vil vinde indpas i samfundet, f.eks. som led i et fremtidigt borgerkort eller som led i de løsninger, der udbydes i forbindelse med et regelsæt om digital signatur.

Der kan være et behov for at få afklaret bevisproblemer og fastlagt klare og rimelige krav til bevisbyrder m.m. I modsat fald vil der nemt kunne brede sig en almen mistillid til brugen af digitale systemer. Der er i øjeblikket et projekt under Nordisk Ministerråd, som skal belyse bevisproblemer ved elektroniske betalinger.

Den danske betalingskortlovs § 22 har været på forkant med denne udvikling ved principielt at pålægge systemudbyderen bevisbyrden. Spørgsmålet er dog, hvor langt man kommer via lovbestemte bevisbyrderregler, da det relevante spørgsmål i forskellige sammenhænge vil være, hvilke konkrete krav domstolene vil stille til beviset i den enkelte situation i forhold til det konkrete medium.

Bevisproblemer af denne art har allerede givet anledning til en del debat i Danmark. Et sådant område er de sager, hvor der har været tvivl om, hvorvidt et Dankort er blevet anvendt til at hæve beløb. (Se hertil Mads Bryde Andersen: Lærebog i edb-ret (1991), s. 383 med henvisning til praksis fra Pengeinstitutankenævnet.) Et andet eksempel er sager, hvor der har været tvivl

om rigtigheden af en telefonregning fra TeleDanmark A/S. Disse spørgsmål har givet anledning til en rapport fra Telestyrelsen (dateret 1. september 1994) med titlen "Hovedrapport - Undersøgelsen vedrørende regningsklager m.v.".

Med nedsættelsen af Telebrugernævnet ved lov nr. 466 af 12. juni 1996, § 15, er der skabt et forum for afgørelsen af disse sager. Det var på et tidspunkt på tale, at der i denne lov skulle indsættes regler om omvendt bevisbyrde til fordel for brugeren, hvor denne kunne godtgøre, at en regning var uforholdsmæssigt høj. Sådanne regler er dog endnu ikke blevet indført.

7. Markedsføringsspørgsmål

a. Problemstillingen

Internettet har vist sig som et særdeles velegnet medium for erhvervsmæssig markedsføring. Værdien af dette medium stiger med antallet af nye Internetbrugere og med disse brugeres afhængighed af dette nye medium i forbindelse med dagligdagens gøremål som f.eks. betaling, indkøb, informationssøgning og underholdning. Når Internettet bliver den enkelte forbrugers naturlige kontakt med disse dele af omverdenen, vil virksomhederne naturligt intensivere mediet som grundlag for henvendelser m.v. til forbrugerne.

Det er langt fra givet, at sådanne nye anvendelsesformer vil basere sig på den nuværende PC-teknologi. I Kommissionens Working Document "Commercial Communications in the Internal Market" (XV/9579/96), s. 39, tegnes følgende perspektiv for den fremtidige elektroniske markedsføring:

"New on-line commercial communication services may well rely on a combination of telephone distributors, specialised software driven network providers and broadcasters or publishers who will extend their business into interactive services. Until a set-top box has been commercialised the growth of interactive advertising received via TV screens is difficult to appreciate." Se ligeledes Kommissionens Grønbog om Kommerciel Kommunikation i det indre marked, KOM(96) 192, s. 11 ff.

Grundlaget for den danske regulering af erhvervsmæssig markedsføring findes i m.fl. § 1, der lyder således:

§ 1. Loven gælder i privat erhvervsvirksomhed og offentlig virksomhed, som kan sidestilles hermed. Der må i sådan virksomhed ikke foretages handlinger, som strider mod god markedsføringsskik.

Bestemmelsen, der er suppleret af 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 mulighed for at ramme overtrædelser af reglerne om god markedsføringsskik, der begås under anvendelse af digitale netforbindelser, på ganske samme måde, som hvis disse markedsføringshandling var udført på traditionel vis (annoncering, direct marketing etc.).

Foruden disse markedsføringsforbud findes der særlige regler om markedsføring på bestemte områder. Visse af disse regler er baseret på EF-direktiver. Det gælder således reglerne om vildledende reklame (direktiv 84/450/EØF), om mærkning af og præstationsmåder for levnedsmidler (79/112/EØF), om livsforsikringsvirksomhed (talrige direktiver) og om humanmedicinske lægemidler (92/28/EØF).

Som nævnt ovenfor, gælder loven inden for de territoriale grænser, som loven sætter. Det burde overvejes nøje at diskutere, i hvilket omfang en eventuel udvidelse af lovens territoriale anvendelsesområde kan være relevant i forhold til den teknologiske udvikling, som betyder stigende grænseoverskridende markedsføring.

Radio- og TV-reklamer skal opfylde markedsføringsloven samt de særlige regler om Radio- og TV-reklamer i lov om radio- og fjernsynsvirksomhed og i kulturministeriets bekendtgørelse nr. 108 af 8. februar 1994 om reklame og sponsoring i radio og fjernsyn.

Radio, og ikke mindst TV, er stærke medier, og det er baggrunden for, at der gælder særlig skærpede regler for reklamer i disse medier. Reklamerne skal klart kunne identificeres og skal være klart adskilt fra programmerne gennem lyd og for fjernsyns vedkommende tillige ved billedmæssig angivelse. I fjernsyn må reklamer kun udsendes i blokke. Der gælder omfattende regler i nævnte bekendtgørelse, som bl.a. har til formål at beskytte børn og unge under 18 år. Det er forbudt at reklamere for alkoholholdige drikkevarer, tobaksprodukter og lægemidler.

En revision af radio- og fjernsynsloven er under forberedelse. De særlige regler om reklamer i radio og fjernsyn forventes imidlertid ikke ændret. Det forventes, at nævnet får mulighed for at tage sager op af egen drift om identifikation af reklamer.

Reglerne om Service 900: Bekendtgørelse nr. 917 af 18. oktober 1996 om service 900-tjenester er trådt i kraft den 1. november 1996. Der er af Forskningsministeriet nedsat en arbejdsgruppe vedrørende den fremtidige service-900 regulering.

Den eksisterende bekendtgørelse indebærer bl.a., at udbydere i modsætning til teleudbydere kan afsætte ydelser til overtaksering (limiteret både hvad angår tid og takst), idet teleudbyderen på vegne af "sælgeren" varetager registrering af forbrug, fakturering og opkrævning af betaling.

Udbydere af tjenester registreres i Service 900-Nævnet under forudsætning af at betingelserne herfor er opfyldt. Selve udbudet er underlagt en række krav vedrørende såvel indhold (f.eks. pornografi) som markedsføring (f.eks. ej rettet mod børn under 16 år), herunder prisoplysning.

Direktiv nr. 89/552/EØF om grænseoverskridende fjernsyn: Direktiv 89/552/EØF om samordning af visse love og administrative bestemmelser i medlemsstaterne vedrørende udøvelse af TV-spredningsvirksomhed udgør

retsgrundlaget for tv-spretningsvirksomhed i det indre marked. Der arbejdes for tiden med en revision af direktivet.

TV-direktivets reklameregler ligger generelt på et betydeligt lavere beskyttelsesniveau end de tilsvarende danske regler. Det gælder fx reglerne om reklameafbrydelser, reglerne om børn og unge og reglerne om alkoholreklamer.

Forskellen mellem tv-direktivets regler om tv-reklamer og de tilsvarende danske regler indebærer, at TV-stationer beliggende i forskellige lande er underlagt forskellige regler, idet TV-direktivet eksplicit siger, at en udsendelse alene skal opfylde direktivets bestemmelser samt de regler, der gælder i det medlemsland, hvorfra opsendelsen sker. Det er således ikke modtagerlandets regler, der skal overholdes. Dette bevirker en svækkelse af det generelle beskyttelsesniveau, som modtagerlandet ønsker, samt en konkurrenceforvridning i forhold til TV-stationerne i modtagerlandet.

Sverige har indbragt en sag for EU-domstolen vedrørende denne problemstilling. Spørgsmålet i denne sag er, om de svenske myndigheder kan forbyde reklamer i TV3, der strider mod det svenske forbud om TV-reklamer. Det svenske forbud retter sig mod børn under 12 år. Problemet er, at den pågældende TV-station opsender dets program fra England og som sådan alene skal opfylde de engelske regler om TV-reklamer.

Direktivet indfører en ordning, hvorefter hvert enkelt radio- og TV-selskab kun kan være underlagt lovgivningen i den medlemsstat, hvor det er etableret, og under hvis retsområde det derfor hører. Dernæst opstiller direktivet visse minimumsregler (de såkaldt "samordnede områder"), som skal overholdes i hele fællesskabet. Disse områder drejer sig nærmere bestemt om TV-reklamer og sponsorering. Endelig skal medlemsstaterne sikre borgernes ret til fri modtagning. De må altså ikke hindre transmission af TV- og radioudsendelser fra andre medlemsstater under henvisning til forhold, der er omfattet af de samordnede områder.

I de foreslåede ændringer til TV-direktivet, indgår teleshopping på lige fod med TV-reklamer, således at direktivets reklameregler også kommer til at omfatte denne særlige form for reklame.

Senderlandsprincippet fastholdes i ændringsforslaget til direktivet.

b. Identifikation af den forretningsdrivende

Der opstår nye forvekslingsproblemer. På den ene side er risikoen for at forveksle én virksomhed med en anden reduceret betydeligt, fordi netadresser skal afgives med fuldstændig præcision. På den anden side betyder nettets globalisering, at forbrugeren ofte ikke ved, hvor den forretningsdrivende befinder sig. Dette problem er størst i relation til virksomheder, der er registreret under root-domænet "com", hvorimod det er noget mindre for de, der er registreret med nationalitetsbetegnelsen som root-domæne.

For så vidt angår den forveksling, der kan opstå, når den erhvervsdrivende placerer sit varemærke eller forretningskendetegn som en grafisk figur på selve hjemmesiden, er problemerne derimod helt sammenfaldende med dem, vi kender fra den traditionelle markedsføring.

I relation til de egentlige forbrugertransaktioner er disse identifikationsproblemer dog næppe større end dem, man kender i forvejen, f.eks. når udenlandske virksomheder ved direct marketing kontakter kunder i Danmark. I begge tilfælde har forbrugeren ingen direkte kontakt med den erhvervsdrivende, idet aftalens ydelser udveksles over afstand og uden umiddelbar personlig kontakt. Det må dog påpeges, at mulighederne for at løse dette problem er større i Internettet end på det almindelige direct-mail område, fordi Internet-virksomheden nødvendigvis indgår i et aftaleforhold med en Internet-operatør. Efter gældende danske retsplejeregler vil Internetoperatøren kunne tilpligtes at udlevere en sådan aftale på grundlag af en såkaldt editionsbegæring, jf. retsplejelovens § 299. Problemerne opstår dermed kun i tilfælde, hvor den indgåede aftale ikke kan fremlægges (f.eks. fordi aftalen er indgået mundtligt), eller hvor aftalen vel foreligger, men med en uklar partsbetegnelse. Hertil kommer, at man også kan anvende Internettet til at løse disse problemer, f.eks. ved at bruge Internettet som grundlag for en slags online-undersøgelse af den erhvervsdrivende, se hertil ovenfor i kapitel II.12.d. om det amerikanske NetCheck-initiativ.

Som påpeget af Knud Wallberg i U97B.23 ff, har Internettets fremkomst i sig selv kun skabt enkelte nye problemer. Markedsføring, køb, salg og reklame m.v. på tværs af grænserne er kendte fænomener. De fleste virksomheder præsenterer sig på nettet under deres kendteste varemærke, som således ikke blot fremstår i grafisk form på hjemmesiderne, men som også indgår i virksomhedernes domænenavne. Da mærket ofte vil være forbrugernes eneste bindeled til producenten af den pågældende vare eller tjenesteydelse, er det vigtigt, at eksisterende varemærkeretlige principper, der sikrer mod forvekslelighed og dermed mod potentiel vildledning af forbrugerne, kan overføres til nettet.

Der har været mange tilfælde, hvor kendte varemærker er blevet registreret som domænenavn af andre end den berettigede virksomhed eller bruges uberettiget af andre på deres hjemmesider. Søger en forbruger frem til virksomheden bag mærket ved at bruge mærket som søgekriterium, vil man altså kunne risikere at få fat i den "forkerte", og er dennes hjemmeside tilstrækkeligt professionelt lavet, eller giver den sig, som der har været flere eksempler på, direkte ud for at være "den officielle hjemmeside for ...(mærket)", kan det være ganske svært for forbrugeren umiddelbart at opdage dette.

c. Påtrængende markedsføring m.v.

Anvendelse af digital telekommunikation mellem forbruger og erhvervsdrivende giver den erhvervsdrivende større muligheder for effektivt og direkte at nå den enkelte forbruger. Internettet er velegnet som medium for markedsføring på grund af sine lave udgifter til transmission af kommunikation. Mediets fordele viser sig navnlig for nichevirksomheder, der ellers vil have vanskeligt ved at

nå forbrugeren gennem traditionelle kommunikationskanaler som f.eks. aviser, ugeblade, TV-reklamer, omdelte brochurer eller direct marketing.

Når de digitale kommunikationsformer automatiseres, opstår nye og mere effektive muligheder for at foranstalte påtrængende markedsføringshandlinger. I relation til telefaxområdet har spørgsmålet tidligere været rejst af Forbrugerombudsmanden (i en sag fra 1988), men med udbredelsen af Internettet er problemet blevet mere påtrængende. Kombineres disse teknikker med registrering af enkelte brugeres forbrugsprofiler, åbner dette mulighed for en langt mere personlig og påtrængende, markedsføring.

Europa-Parlamentets og Rådets direktiv 97/7/EF om fjernsalg indeholder en beskyttelse mod aggressive kommunikationsteknikker. Efter artikel 10 kræver en leverandørs brug af telefax og automatisk opkaldssystem således et forudgående samtykke fra forbrugeren. Andre fjernkommunikationsteknikker, som tillader individuel kommunikation, må kun anvendes, hvis forbrugeren ikke klart modsætter sig det.

I Kommissionens forslag til direktiv om beskyttelse af personoplysninger og privatlivets fred inden for telesektoren, navnlig det tjenesteintegrerede digitalnet (ISDN) og digitale mobilnet KOM(94)128, jf. Rådets fælles holdning af 12. september 1996 (EF nr. 57/96), er der indsat en bestemmelse mod uønskede telefoniske henvendelser (art. 12). Artiklen har følgende ordlyd:

"1. Anvendelse af automatiserede opkaldsanordninger uden menneskelige indgreb (automatisk opkaldsmaskine) eller telefaxmaskiner (fax) med henblik på direkte markedsføring kan kun tillades over for abonnenter, som forudgående har givet deres tilladelse hertil.

2. Medlemsstaterne træffer de fornødne foranstaltninger for gebyrfrit at sikre, at uønskede telefoniske henvendelser, hvis formål er direkte markedsføring med andre midler end dem, der er nævnt i stk. 1, forbydes, medmindre... (samtykke.)".

Via Internettet kan der sendes informationer af al mulig art. Når forbrugeren vælger at bosætte sig i et bestemt geografisk område, kan forbrugeren påregne, hvilke typer reklamer, annoncer og tilbud familien udsættes for af de omkring liggende forretninger og gade skilte. Tilsvarende kan myndighederne sørge for at fjerne uønsket materiale fra bestemte gader/distrikter. Dette bliver illusorisk på Internettet. Når ens computer er koblet op på nettet, modtager terminalen alt det, der står til rådighed på et givet tidspunkt over hele verden.

En mulig løsning kan f.eks. være indførelse af et elektronisk "Nej Tak" klistermærkersystem i forbrugernes egne computere, som kendes og respekteres af annonceudbydere og reklameomdelere. Herefter vil forbrugerne kunne opnå større kontrol over kvaliteten og kvantiteten af de reklamer, annoncer og andet kommercielt materiale, der havner på deres E-post terminal.

Et lignende problem kan opstå, når erhvervsdrivende ved hjælp af "cookies" samler informationer om forbrugernes handlemønstre, og disse informationer

derefter bruges til direkte markedsføring af diverse materialer. Det kan være hensigtsmæssigt at arbejde hen imod en løsning, hvorefter teknologien giver forbrugerne mulighed for at efterlade sådanne "cookies" med omvendt indhold, nemlig at bestemte materialer nægtes adgang til forbrugernes computer, men derimod "skubbes" tilbage til afsenderen.

d. Sponsorering

Ifølge et kodex fra ICC om kommerciel kommunikation gennem interaktive elektroniske medier fra 1996, defineres "sponsorship" som "any kind of communication through which a sponsor, on the basis of a contract, provides the financial or other type of support in order to establish a positive association between the sponsors' image/brand/products or services and the sponsored event, activity, organisation or individual." Man sonderer almindeligvis mellem sponsorering af begivenheder (f.eks. støtte til en koncert) og mediesponsorering (f.eks. angivelse af firmanavn og varemærke i en TV-transmitteret fodboldkamp).

Det må ventes, at en betydelig del af den erhvervsmæssige markedsføring på Internettet vil ske gennem en sponsorering, hvorefter den erhvervsdrivende betaler for at have deres forretningskendetegn eller annoncer m.v. placeret på en hjemmeside. En sådan form for markedsføring kender man ikke alene på Internettet, men også i relation til Tekst-TV. Sponsorering spiller i det hele taget en stigende rolle i radio- og TV-spredningen.

Der er næppe andre problemer knyttet til sponsorering af hjemmesider end dem, der kendes vedrørende sponsorering af andre medier. Den problemstilling, der kendes i relation til presseområdet om afgrænsningen mellem redaktionelt stof og reklamemateriale, har ikke samme tyngde i relation til Internet-information, hvor der næppe kan siges at være nogen typeforudsætning om, at informationen har enten redaktionel eller kommerciel art. Befinder man sig på hjemmesiden for et dagblad, vil formodningen være for, at man læser redaktionelt stof, indtil forretningskendetegnet for en annoncør dukker op. Formodningen vil være omvendt, hvis man befinder sig på en salgsvirksomheds hjemmeside.

e. Overblik, oplysning og gennemsigtighed

Der er både en almindelig konkurrenceretlig og en speciel forbrugerretlig interesse i, at forbrugerens dispositioner træffes på et så klart grundlag som muligt. Er der risiko for, at de nye medier slører beslutningsgrundlaget for forbrugerens dispositioner, bør der overvejes initiativer. Dette kan f.eks. tænkes, hvis selve teknologien vanskeliggør et overblik over ydelsernes beskaffenhed.

Ifølge m.fl. § 3 skal der ved afgivelse af tilbud, 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 Internettet og dermed også når danske forbrugere. Men der kan tænkes situationer, hvor man vil anse en virksomheds interesse i det danske marked som så naturligt og relevant, at virksomhedens materiale på Internettet vil være omfattet af markedsføringsloven, selv om sproget måtte være fremmed (men almindeligt kendt i Danmark) som f.eks. det engelske sprog, smh. Forbrugerombudsmandens stillingtagen til spørgsmålet i kapitel III.6.d.

Diskussionen ovenfor tog alene udgangspunkt i den kendsgerning, at en erhvervsdrivende *kan* nå en dansk forbruger. Indsnævrer man derimod blikket til de tilfælde, hvor den erhvervsdrivende mere aktivt henleder danske forbrugeres opmærksomhed på sin hjemmeside (f.eks. ved annoncering i Danmark), rammer man en situation, der formentlig allerede i dag må anses for omfattet af loven. Ved at udpege et medium, hvor en markedsføringshandling fuldbyrdes, og som den erhvervsdrivende har kontrol over, kan den erhvervsdrivende siges at inkorporere de oplysninger, der findes her. M.fl. § 3 giver derfor næppe anledning til revision i henseende til disse spørgsmål.

f. Lighed, konkurrence og rimelighed

Det konkurrenceretlige hensyn er allerede nævnt. Afledede funktioner heraf er ønsket om, at markedet udfolder sig under lige vilkår, og således at aftaler indgås på afbalancerede vilkår. EU-myndighederne overvåger løbende disse markedsforhold og kan tænkes at skride ind overfor uacceptable handleformer gennem undtagelsesforordninger fra art. 85-86 eller ved at stille forslag om regulering ved direktiver.

Det må imidlertid påpeges, at Internettet også har en positiv betydning for forbrugerens konkurrencemæssige stilling, idet nettet giver forbrugeren muligheder for at styrkes sin position overfor den erhvervsdrivende. Der er eksempler på, at forbrugere har fået tilforhandlet sig betydelige rabatter ved - via nettet - at samle sig i store grupper, der er parat til at afgive ordre om storindkøb (f.eks. 15 samtidige køb af en bil). Ligeledes kan forbrugerne anvende Internet til effektive prissammenligninger, der undertiden understøttes af dertil udviklede søgeprogrammer. Et eksempel herpå er programmet BargainFinder, der automatisk screener nettet for priser på bestemte varer og tjenester.

g. EU-tiltag

EU-Kommissionen har den 8. maj 1996 fremlagt en Grønbog om Kommerciel Kommunikation i det Indre Marked, KOM(96) 192 - endelig udg. Grønbogen udspringer af en beslutning, Kommissionen tog i 1992 om at tage sin fremtidige strategi op på dette område. Grønbogen inviterer til en debat, idet den fremlægger nogle foreløbige undersøgelsesresultater, herunder *at* grænseoverskridende kommercielle kommunikationstjenester inden for det indre marked vil blive et mere og mere udbredt fænomen, *at* divergerende nationale regler kan skabe hindringer for virksomheder og problemer for forbrugerne, og *at* det derfor har betydning, at der er information til rådighed om lovforanstaltninger og markedsudvikling.

I grønbogen drøftes behovet for et antal EF-initiativer på forskellige lovgivningsområdet. Forbrugerområdet omtales - kort - på s. 19, hvor de hertil hørende problemer anses for omfattet af konkurrencelovgivningen. Senere, s. 23 ff., påpeges imidlertid en række områder, hvor divergerende lovgivninger vedrørende reklamering antages at skabe problemer.

Et andet initiativ har Kommissionen taget med sit Green paper fra 1996 "on the Protection of Minors and Human Dignity in the Audiovisual and Information Services". Papiret, der bl.a. bygger på anbefalinger fra Information Society Forum, betoner det problem, at en stigende del af den audiovisuelle kommunikation nu foregår via globale net, som det er vanskeligt at regulere, og hvis skadevirkninger kan få uforholdsmæssige følger netop for børn og mindreårige. Behovet for at gennemføre en sådan styring diskuteres herefter overfor hensynet til ytringsfriheden. Herefter lægges en række spørgsmål frem til diskussion om, hvorvidt der er et behov for at beskytte mindreårige m.v., og hvorledes denne beskyttelse i givet fald skal finde sted (frivilligt, gennem "labelling" eller ved forbud og påbud). Papiret konkluderer, at EU bør spille en rolle for at sikre de nødvendige globale løsninger på disse problemer.

Papiret om mindreåriges beskyttelse er offentliggjort samtidigt med en grønbog om "Illegal and harmful content on the Internet", (COM 96) 487. I dette papir præsenteres de beskyttelsesbehov, der kunne tænkes at give anledning til regulering. Forbrugerbeskyttelseshensynet er ikke omtalt som sådant, men derimod indirekte under emnerne economic security (som dog afgrænses til fraud og instructions on pirating credit cards), information security (malicious hacking) og protection of privacy.

Papiret er interessant i sin analyse af de problemer, der er forbundet med at identificere og retsforfølge ulovlig information på Internet, se navnlig s. 11 ff. Derfor er der behov for internationalt samarbejde samt for en klar angivelse af den "chain of responsibilities", som resulterer i, at retsbrud overhovedet kan forekomme. Rapporten er nærmere omtalt nedenfor, kapitel IV.2.b.

8. Konkurrencespørgsmål i øvrigt

a. Standardisering

Det kendetegner hovedparten af de systemer og komponenter, der anvendes i den digitale teknik, at de kun fungerer sammen, hvis de lever op til visse tekniske standarder. At standardiseringen spiller en central rolle for edb-området viser den personlige computers historie med al ønskelig tydelig. Først da IBM i begyndelsen af 1980'erne lancerede Microsofts operativsystem DOS (Disk Operating System) som sin standard, opstod der for alvor et PC-marked. Med denne standard kunne andre PC-producenter konkurrere med IBMs PC (idet kunderne kunne købe DOS-styresystemet hos Microsoft), ligesom programudbydere kunne skrive deres programmer, så de passede til DOS-standard. Det deraf følgende gigantiske marked har været en væsentlig drivkraft bag de seneste års edb-udvikling.

At disse tekniske *standards* spiller en betydelig rolle for IT-udviklingen kan også iagttages på andre områder af denne sektor. 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. Et fjerde eksempel er de standarder vedrørende digitale TV-signaler, der er omfattet af det førnævnte direktiv 95/47/EF, og som vil blive indført i dansk ret med lov om standarder for transmission af TV-signaler m.v.

I en række tilfælde kan det tænkes, at sådanne tekniske standarder beskyttes efter immaterialretlige eneretsregler, f.eks. ophavsret eller patent, der herefter udøves til skade for (for)brugerne. Bl.a. det har været diskuteret, om rettighedshaveren skal kunne opretholde et patent i en standard (f.eks. et teknisk krav om, at alle GSM-basisstationer skal følge dette sorteringsprincip). En sådan eneret kommer nemlig til at fungere således, at patenthaveren kommer til at "eje" reglerne om den pågældende teknologi - en situation, der strider mod retsopfattelsen i dansk ret, hvorefter love ikke er undergivet ophavsret.

Spørgsmålet har givet anledning til en intens debat ved Den Europæiske Standardiseringsorganisation for Telekommunikation, ETSI. Denne diskussion er indtil videre afsluttet ved ETSIs vedtagelse af en Intellectual property Rights Policy, dateret 24. november 1994, der slår fast, at indehavere af immaterielle rettigheder (kaldet IPR) "should be adequately and fairly rewarded for the use of their IPRs in the implementation of standards". Ifølge reglerne er alle medlemmer af ETSI forpligtede til at orientere ETSI om essentielle immaterialrettigheder, de er eller burde være opmærksomme på (pkt. 4.1), inden rimelig tid. Hvis et medlem selv fremlægger forslag til en teknisk løsning i en standard, skal medlemmet selv give oplysning om immaterialrettigheder, som måtte være essentielle herfor (pkt. 4.2). Viser det sig, at tredjemand råder over en immaterialrettighed, skal direktøren for ETSI omgående tage kontakt med denne med henblik på at få oplyst, om tredjemand er indstillet på uigenkaldeligt at give standarden i licens på rimelige og ikke-diskriminerende vilkår (pkt. 6.1). Nægtes dette, tages der skridt til at reformulere standarden, således at den pågældende immaterialret ikke længere bliver essentiel.

Ser man imidlertid sagen fra immaterialrets-indehaverens synspunkt, kan det også føles urimeligt, at en teknologisk løsningsmetode, som har været kostbar at udvikle, og som samtidigt har så betydelige økonomiske nyttevirkninger for brugeren, at den ophøjes til standard, dermed skal 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 kombinere to typer af standarder, de såkaldte eneretsstandarder ("proprietary standards"), og de standarder, der kvalificeres af et standardiseringsorgan under en officiel og åben vedtagelses-procedure (undertiden kaldet de facto-standarder). At ETSI-politikken har givet

anledning til en så forholdsvis omfattende debat skyldes, at det almindeligvis betragtes som hovedreglen, at de jure-standarder er i public domain (ganske som lovgivning og anden officiel information er det). Derimod er det den almindelige opfattelse, at private virksomheders eneretsstandards netop kan holdes i eneret ganske som andre enerettigheder, idet prisen for denne eneret til gengæld er, at sådanne standarder ikke blåstemples som officielle, f.eks. i forbindelse med offentlige myndigheders indkøb.

b. EU-ret, herunder konkurrenceret

EF-domstolen har ved flere afgørelser fastslået, at reklame må betragtes som en tjenesteydelse i medfør af EF-traktatens regler om fri udveksling af tjenesteydelser (art. 59-60), se bl.a. *Sacchi*, sag C-155/73, saml. 1974 (1), s. 409, og *Debauvre*, sag C-52/79 (saml. 1980, s. 833). Derfor har EF-domstolen kompetence til at erklære indgreb i erhvervsdrivendes reklamepraksis for EU-retsstridige, jf. Kommissionens Fortolkende meddelelse om fri udveksling af tjenesteydelser på tværs af landegrænserne, EFT 1993 C 334/3.

IV. Principielle reguleringsovervejelser

1. Ressortafgrænsning

Den foregående udredning har vist adskillige eksempler på, at de problemer, der angår beskyttelse af forbrugere ved digitale grænseoverskridende markedsføringshandlinger, berører forskellige ressortområder. De heraf følgende afgrænsningsproblemer viser sig på nationalt, på EU-retligt såvel som på globalt plan.

a. Nationalt

Herhjemme har Forskningsministeriet i kraft af de vedtagne regeringshandlingsplaner indtil videre "Fra vision til handling" (marts 1995) og "Info-samfundet for alle - den danske model" (marts 1996), placeret sig som det tværgående ministerium, der søger at koordinere de generelle bestræbelser på IT-området. Handlingsplanerne har rod i den rapport om Info-samfundet år 2000, som det såkaldte Dybkjær/Christensen-udvalg afgav i 1994.

På grund af denne placering er det f.eks. Forskningsministeriet, der har ført OECD-forhandlingerne vedrørende kryptering og vedrørende Content Control på Internettet. Ligeledes vil ministeriets overvejelser om lovgivning vedrørende digital signatur få principiel betydning for en række af de lovområder, der er berørt i det foregående, samt for den heraf følgende EU-kontakt.

b. EU

Flere dele af EU-Kommissionen har taget såvel generelle initiativer som konkrete lovgivningsinitiativer, der tilsigter at føre EU frem i en førerposition, når det gælder udvikling og anvendelse af moderne IT. På det principielle plan blev processen igangsat i 1994 med fremlæggelsen af den såkaldte Bangemann-rapport, men inden da har Kommissionen taget adskillige initiativer med henblik på at styrke unionens IT-industri. Under sit møde i Corfu i juni 1994 besluttede Det europæiske Råd, at informationssamfundets problemer burde gøres til genstand for permanent overvejelse. På grundlag af disse overvejelser vedtog Kommissionen i juli 1994 en handlingsplan med titlen "Europe's way to the Information Society", i hvilken Kommissionen bl.a. annoncerede sit reformforslag om fuld liberalisering af telekommunikationsområdet pr. 1. januar 1998. I 1995 nedsatte Kommissionen en permanent tænketank med navnet Information Society Forum, der afgav sin første - generelt holdte - rapport i juni 1996 med titlen "Networks for People and their Communities - Making the Most of the Information Society in the European Union."

Den 24. juli 1996 udsendte Kommissionen en meddelelse til Rådet, Parlamentet og det Økonomisk-Sociale Udvalg med titlen: "The Information Society: From Corfu to Dublin - The new emerging priorities" (KOM(96) 395 final. Dokumentet indeholder fire konkrete forslag, hvoraf det ene ("The Implications of the Information Society for European Union Policies") bl.a. beskæftiger sig med

beskyttelsen af forbrugerinteresser (s. 9). De forslag, der her diskuteres, har dog kun forberedende karakter. Kommissionen vil støtte forskning i mere brugervenlige systemer og vil sørge for en højere inddragelse af forbrugerinteresser i standardiseringsprocessen. Dernæst rejses spørgsmålet om "unwanted or offensive information content disseminated on on-line services", samt problemet om "the protection of minors". Som nævnt ovenfor i kapitel III.7.g., er disse emner siden taget op i en særlig arbejdsgruppe. Endelig peges på behovet for at lette grundlaget for forbrugers valg.

En særlig EU-retlig problemstilling med sigte på medlemsstaternes IT-lovgivning foreligger med et forslag fra Kommissionen om ændring af direktivet om en informationsprocedure med hensyn til tekniske standarder og forskrifter (83/189/EØF) med sigte på "Forskriftsmæssig gennemsigtighed i det indre marked for informationssamfundets tjenester", se KOM(96) 392 endelig udg. Hvis dette forslag gennemføres, vil det pålægge medlemsstaterne helt nye og hidtil ukendte begrænsninger i muligheden for selv at lovregulere på de områder, der er omfattet af nærværende udredning.

1983-direktivet har sikret en koordination af medlemsstaternes arbejde med udstedelse af tekniske standarder og forskrifter. En medlemsstat, der forbereder indførelsen af en ny standard, har pligt til at underrette Kommissionen og de øvrige medlemsstater om det udkast hertil, som den agter at vedtage. Kommissionen og de øvrige medlemsstater har herefter en periode på tre måneder til at vurdere dette udkast. De bemærkninger, som måtte fremkomme, skal medlemsstaten herefter tage videst muligt hensyn til.

Ifølge forslaget skal 1983-direktivets ordning også omfatte "ethvert udkast til forskrifter" herunder "frivillige aftaler, som de offentlige myndigheder er kontraherende part i, samt fagkodekser eller kodekser for god praksis, hvis overholdelse giver formodning om, at der er overensstemmelse med de krav, der er fastsat i en række bestemmelser." Senere fremgår det dog, at KOM-dokumentets "forskrifter" også omfatter "lovgivning". På s. 38 anføres som eksempel på et område, der kunne være omfattet, et tysk lovforslag om rammer for informations- og telekommunikationstjenester, og sammesteds omtales det, at forslaget ikke vil omfatte "medlemsstaternes love eller administrative bestemmelser ... hvis medlemsstaterne dermed opfylder bindende EF-retsakter ...", men - underforstået - kun da. Selve teksten til direktivforslaget synes dog kun at medtage administrative bestemmelser, se forslaget til nyt nr. 12 til art. 1.

Baggrunden for det stillede forslag er et ønske om at sikre, at de nye tjenester, der vil blive formidlet i informationssamfundet, kan udnytte fordelene ved det grænseløse marked. De nye tjenester, der tænkes på, er bl.a. elektroniske aviser, fjernundervisning, telemedicin, elektroniske turistinformationstjenester, elektronisk fjernsalg af varer og tjenester, elektronisk betaling, elektroniske væddemålsforretninger, interaktive spil, underholdningstilbud og fritidstilbud m.v., (se nærmere KOM-dokumentet s. 4 f. og 36 f.) Da der imidlertid kan tænkes en række barrierer mod den frie spredning af sådanne tjenester, er der et potentielt harmoniseringsbehov: Medlemsstaterne kan tænkes at indføre divergerende barrierer ud fra nationale overvejelser og dermed hæmme den fælleseuropæiske udvikling af disse teknologier.

Dette harmoniseringsbehov vil Kommissionen søge løst ved at videreføre den samordningsprocedure, der er skabt på grundlag af 1983-direktivet. Proceduren består dels af en *informationsprocedure*, hvorefter udkast til standarder m.v. fremsendes til Kommissionen, dels en *høringsprocedure*, hvorefter de øvrige medlemsstater kan fremsætte deres bemærkninger hertil. Kommissionen foreslår, at dette anvendelsesområde udvides til også at omfatte udkast til forskrifter vedrørende informationssamfundets tjenester. Herigennem vil man reducere behovet for EU-forskrifter, sikre en bedre beskyttelse af almene interesser (et mål, der skulle opnås gennem mere intense drøftelser om reguleringsbehovene), lette det administrative samarbejde, og bidrage til at sikre forskrifternes stabilitet. Forslaget må ses i tilknytning til Kommissionens grøn bog om Kommersiell kommunikation, der bl.a. indeholder et forslag om "Informationsprocedure".

2. Retspolitisk udgangspunkt

a. "Læren om digital fartbegrænsning"

Den digitale teknik har skabt et sikkerhedsmæssigt hastighedsproblem, der modsvarer det, man kender inden for færdselsområdet. Jo hurtigere trafikken afvikles, desto større er behovet for at regulere køretøjernes indretning samt den tilladte fart. Jo mere intense retsvirkninger, forbrugerne kan udvirke gennem dispositioner, der udvirkes ved hjælp af digitale medier, og jo mere intenst forbrugeren bombarderes med markedsføring ved hjælp af digitale teknikker, i desto højere grad kan der være grundlag for at overveje beskyttelse.

Denne effektivitet ved det digitale medium giver anledning til at overveje, om man bør indføre mere restriktive særregler på det digitale område. Registerlovgivningen er et væsentligt eksempel på, at man forbyder en digital informationsbehandling (edb-registrering), som er tilladt på papir (almindelig usystematisk databehandling). Et andet eksempel er det særlige forbud mod digital privatkopiering, der følger af ophavsretslovens § 12. Et tredje eksempel er de særlige regler om reklamer på TV.

Det bør overvejes, om der kun bør indføres regler om digital fartbegrænsning, hvis der er et notorisk beskyttelsesbehov, som ikke forventes løst på anden måde. I den forbindelse må det tages i betragtning, at det bliver stadigt vanskeligere at adskille forskellige typer af teknologier fra hinanden, idet teknologien (f.eks. gennem effektiv udprintning, scanning og optisk læsning m.v.) gør det stadigt lettere at flytte information fra det digitale medium til det klassiske papirmedium og omvendt. Ligeledes må man tage i betragtning, at den vidtgående "digitale fartbegrænsning" meget let kan komme på kollisionskurs med de politiske meldinger om intensiv anvendelse af digital teknologi, der f.eks. er udtrykt i handlingsplanerne.

b. Regulering eller selvregulering

I det omfang, der ses et behov for at regulere, opstår spørgsmålet, hvorvidt denne regulering skal ske gennem retsregler, eller om man skal forsøge at lade

branchen regulere sig selv ad frivillighedens vej f.eks. ved vedtagne branchestandarder el.lign.

Valget mellem lovregulering eller selvregulering beror på, hvilken jurisdiktion man ønsker at regulere for og hvilke aktører, der er inde i billedet. Ønskes en regulering på europæisk eller globalt plan, kan selve proceduren med at vedtage en regel være så vanskelig, at man i første række forsøger en selvregulering. En sådan fremgangsmåde er lettere, og den harmonerer med det *subsidiaritetsprincip*, der er nedfældet i TEF art. 3B. Den er imidlertid kun farbar, hvis der praktiseres en vis selvdisciplin blandt de aktører, der skal leve op til den.

Internet-branchen er i disse år ved at finde sammen i brancheorganisationer, der befatter sig med disse spørgsmål, bl.a. inden for rammerne af FIL. Efter det oplyste er det almindelig praksis, at Internet-leverandører umiddelbart tager skridt til at lukke hjemmesider m.v., som de kan kontrollere, hvis det konstateres, at der begås ulovligheder herpå. Her hjemme har TeleDanmark A/S efterkommet en begæring fra politiet og besluttet at lukke et antal nyhedsgrupper, der indeholdt børnepornografisk materiale. I et andet tilfælde i januar 1997 besluttede den statsejede edb-virksomhed UNI-C at fjerne forskellige emner, der handlede om sex med børn, fra nyhedsgruppen. I Tyskland har der været flere sådanne sager.

En mellemform mellem regulering og selvregulering er den regulering, der sker ved godkendelse eller anmeldelse af de erhvervsdrivendes standardaftaler. Sådanne regler findes f.eks. i lov om omsætning af fast ejendom § 10. Et andet eksempel på en sådan regulering er Forbrugerombudsmandens retningslinier for markedsføring, der udstedes efter forhandling med de relevante erhvervs- og forbrugerorganisationer med hjemmel i markedsføringslovens § 17 og betalingskortlovens § 12 a.

På europæisk plan har selvreguleringstanken vundet gehør henholdsvis i Kommissionens Communication to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions om "Illegal and harmful content on the Internet" ("Ulovligt og skadeligt indhold på Internet" COM(96) 487, den 16. oktober 1996), samt i den arbejdsgruppe vedrørende Internettet, der i november måned 1996 afsluttede sit arbejde vedrørende Harmful and Illegal content on Internet. Begge papirer lægger op til, at der i første række ikke bør indføres europæiske løsninger på problemet vedrørende ulovligt indhold. I stedet bør man sigte mod frivillige løsninger, der inddrager den berørte branche, idet man samtidigt undersøger de faktiske muligheder for at ramme kritiske former for informationsspredning.

Frankrig har i forskellige internationale sammenhænge tilkendegivet et ønske om at kunne regulere informationsstrømmen på Internettet. I begyndelsen af året pegede den franske minister for telekommunikation, Françoise Fillon, på de særlige håndhævelsesproblemer, som udspringer af Internettets grænseoverskridende natur. Initiativet har angiveligt rod i en ulovlig Internet-spredning af en bog - "Le Grand Secret"- om afdøde præsident Mitterand, skrevet af dennes læge. Den franske holdning blev præsenteret i ministerråds-mødet for telekommunikationsministrene i februar 1996.

Inden for sin suverænitet står det i princippet ethvert land frit for at forbyde sine borgere at koble sig op på nettet eller kun at tillade visse informationer at passere. En sådan kontrol rummer imidlertid såvel juridiske, politiske som praktiske vanskeligheder, som mest er at sammenligne med de vanskeligheder, der ville følge af at skulle overvåge enhver form for telefoni til og fra et land. Rent *praktisk* forudsætter en sådan kontrol, at telefonlinjerne kun passerer ind og ud af landet via et afgrænset (og kontrolleret) antal forbindelser, og at der er fuld kontrol med æterbåren telefoni, idet de således kontrollerede forbindelser herefter skulle gøres til genstand for de nødvendige tekniske tiltag. Det vil dernæst være en nødvendig konsekvens af sådanne tiltag, at de kommunikerende parter ikke må tale i kodesprog (d.v.s. forbud mod kryptering).

Lande, der i forvejen har tradition for censurlovgivning, har allerede taget initiativ hertil. I Kina passerer al Internet-trafik gennem landets ministerium for post- og telekommunikation. Ifølge omtale i dagspressen (Computerworld, 13. september 1996) blokerer man herfra adgangen til visse servere på the World Wide Web, herunder adgang til visse amerikanske nyhedstjenester. Tilsvarende initiativ er taget i Singapore. Kina har ligeledes - som en i og for sig konsekvent følge af sit ønske om at regulere informationsstrømmen ind og ud af landet - forbudt anvendelse af parabolantennor. Spørgsmålet blev drøftet på en ASEAN-konference i begyndelsen af september måned, jf. omtale i Berlingske, 14. september 1996.

Det ville ikke alene være i fundamental strid med dansk tankegang, men tilmed formentlig i strid med censurforbudet i grundlovens § 77, at tænke sig tilsvarende foranstaltninger indført i Danmark. Efter vore traditioner vil sådanne kontroltiltag formentlig alene kunne tænkes, hvis det anvendte udstyr af særlige grunde var undergivet en licensordning el.lign. Men på netop dette område går samtlige tiltag den stik modsatte vej, nemlig mod en øget grad af liberalisering af teleudstyr.

På den anden side må det erkendes, at der er områder af dansk ret, hvor der ved lov er gjort begrænsninger i adgangen til at sprede information til almenheden. Ifølge § 1 i lov om radio- og fjernsynsvirksomhed er det således kun DR, TV 2 og foretagender med særskilt tilladelse, der kan sprede radio- og fjernsynsprogrammer. I relation til DR og TV2 har reguleringen bl.a. til formål at sikre en vis kvalitet af programudbudet. Et tilsvarende krav stilles ikke for de lokale stationer, hvor der på den anden side forlanges en vis lokal tilknytning i programudbudet.

En mulig *teknisk platform* for en sådan selvregulering er den såkaldte PICS-teknologi (PICS = Platform for Internet Content Selection), der er udviklet af the World Wide Web Consortium (W3C).

W3C er en global sammenslutning af mere end 150 medlemsvirksomheder bistået af et sekretariat på ca. 30 medarbejdere. W3C blev oprindeligt etableret i USA, men har nu - bl.a. med støtte fra EU-Kommissionen - fået medlemmer i Europa, Australien og ASEAN-landene.

PICS er en fremgangsmåde, der gør det muligt at give hjemmesider m.v. på Internettet en særlig varedeklaration. Brugeren kan da - f.eks. af hensyn til

børnenes Internet-anvendelse - indstille sin Internet-browser, så den kun kan modtage PICS-varedeklarede hjemmesider. PICS tilbyder herefter en mulighed for at give forskellige labels til en hjemmeside alt efter dennes indhold. De labels, der klassificerer hjemmesiden, kan enten påføres af tekstens ophavsmand, fra dens udgiver eller fra en tredjepart.

3. Jurisdiktionsspørgsmålet

I det omfang man vælger at regulere i lovform, opstår spørgsmålet om, hvorledes retlige forbud og påbud *gennemføres*. Dette spørgsmål må drøftes på den ene side i relation til de forbud og påbud, der kan udledes af formueretlige regler (aftaleretlige, erstatningsretlige, ophavsretlige) og på den anden side de, der har grundlag i strafsanktioneret lovgivning. For så vidt angår de formueretlige retskrav henvises til bemærkningerne ovenfor i kapitel II.6. Når det gælder strafsanktionerede forbud og påbud, er det et almindeligt princip i dansk ret, at afgørelsen såvel om straf som om andre retsfølger af handlingen sker efter dansk lovgivning, strfl. § 10, stk. 1.

Spørgsmålet er imidlertid, hvornår en handling er omfattet af dansk straffemyndighed (jurisdiktion). Dette spørgsmål afgøres af strfl. § 6, som definerer de handlinger, der hører under dansk straffemyndighed. Det gælder handlinger, som foretages 1) i den danske stat, 2) på dansk fartøj, som befinder sig uden for nogen stats folkeretlig anerkendte område, samt 3) på dansk fartøj, som befinder sig på fremmed folkeretligt anerkendt område, af personer, der hører til fartøjet, eller som rejsende følger med dette.

Ifølge straffelovens § 7 omfatter dansk straffemyndighed også visse handlinger, som en person, der har *dansk indfødsret* eller er *bosat* i den danske stat, har foretaget uden for denne. Dette gælder i to tilfælde 1) for så vidt handlingen er foretaget uden for folkeretligt anerkendt statsområde, hvis handlingen af den pågældende art kan medføre højere straf end hæfte, 2) for så vidt handlingen er foretaget inden for sådant område, hvis den er strafbar også efter den dér gældende lovgivning. Disse regler finder tilsvarende anvendelse med hensyn til handlinger begået af en person, der har indfødsret eller bopæl i Finland, Island, Norge eller Sverige, og som opholder sig her i landet. Efter denne regel vil man efter den danske straffelov eller danske strafbelagte markedsføringsregler kunne straffe danske statsborgere m.v. for lovbrud, der via Internettet begås i lande, der giver samme hjemmel for straf.

For så vidt angår de straffelovsbestemmelser, hvis gerningsindhold kræver, at der indtræder en bestemt følge (såkaldt forårsagelsesdelikter), gælder strfl. § 9. Sådanne handlinger betragtes *tillige* som foretaget dér, hvor virkningen er indtrådt eller tilsigtet at skulle indtræde. Det klassiske eksempel herpå er, at en person i land A henover grænsen affyrer et dræbende skud mod en person i land B.

Domstolene har endnu ikke taget stilling til, om denne bestemmelse kan antages at omfatte situationer, hvor virkningen i land B af den handling, gerningsmanden i land A foretager sig, alene indtræder, hvis et offer i land B foretager

sig noget aktivt overfor gerningsmanden i land A, f.eks. kalder op til en hjemmeside, der drives af gerningsmanden i land A. Spørgsmålet er, hvad man skal lægge i bestemmelsens krav om, at "virkningen" er indtrådt. Er der tale om, at en amerikansk statsborger stiller ulovlig information til rådighed via Internet på en sådan måde, at den kan opnå skadevirkning i Danmark, må man konstatere, at gerningsmandens handling er en *nødvendig* men ikke en *tilstrækkelig* betingelse for, at der forvoldes en retsstridig handling. For at opfylde kravet om virkningens indtræden, skal offeret foretage sig noget aktivt, nemlig kalde op til den pågældende hjemmeside. Beskytter straffelovbestemmelsen modtageren af den pågældende information, kan denne aktive handling siges at indebære en form for medvirken eller accept, som efter danske regler vil føre til, at straffen bortfalder.

Vanskelighederne opstår derimod, når vi ser på de straffebestemmelser, der enten beskytter bredere samfundsinteresser (f.eks. forbud mod racistisk eller børnepornografisk information), eller som krænker individuelle interesser (f.eks. ophavsretlige retspositioner). I disse tilfælde vil læren om straffebudets virkning føre til en global strafferetlig jurisdiktion. For den, der ville være sikker på ikke at begå lovbrud nogetsteds i verden, ville moralen være, at der ikke kunne spredtes information på Internet, hvis denne information kunne tænkes at stride mod lovgivningen i blot et enkelt af de lande, fra hvilke den kunne hentes hjem. For internationalt arbejdende informationsvirksomheder, for hvem det er afgørende, at der ikke kan rejses sådanne krav, ville denne retstilstand føre til en slags princip om laveste fællesnævner. Således ville det f.eks. kunne tænkes, at et dansk kunstmuseums drift af en hjemmeside med kunstværker med nøgne kvindelige skikkelser kunne udløse et hårdhændet strafansvar i visse muslimske lande.

En sådan retsopfattelse kan næppe anses for gældende i dansk ret. Når man afgrænser de forbrydelser, der er omfattet af strfl. § 9, bør man se på, om der er tale om et "forårsagelsesdelikt". Når dette spørgsmål rejses i relation til informationsforbrydelser, bør det tillægges afgørende betydning, hvilke modtagere, gerningsmanden (informationssprederen) havde i tankerne, da han spredte den pågældende information. Når reklameinformation f.eks. affattes på dansk og med sigte på et lokalt publikum (f.eks. reklame for et lokalt supermarked), er det åbenbart, at der ikke tilsigtes virkninger i relation til amerikanske forbrugere. Det samme gælder formentlig også, selv om der ikke sigtes lokalt.

Når *kommerciel* information spredes på Internettets almindelige sprog - engelsk - i en form, hvor der ikke sigtes lokalt eller regionalt, kan man muligvis anlægge et kriterium, der tager højde for, hvorfra kunderne melder sig ved bestilling og betaling. Medfører Internet-markedsføring af varer eller tjenesteydelser under et varemærke, der kan påtales i USA, at der melder sig amerikanske kunder, vil det følge heraf, at udbyderen har pligt til at vise disse kunder fra sig. Denne pligt er nemlig en logisk konsekvens af, at kundebehandlingen udspringer af en markedsføringshandling, der p.g.a. varemærkekrænkelsen er ulovlig i USA.

Disse overvejelser er i virkelighedens verden undergivet afgørende praktiske begrænsninger. Om en straffesag bliver aktuel, beror imidlertid på, om gerningsmanden rent faktisk kan bringes for retten. Denne mulighed står i almindelighed kun åben, hvis man antræffer ham her. Udenfor disse tilfælde forudsætter strafforfølgning, at gerningsmanden kan udleveres i kraft af bilaterale aftaler med hans hjemland. Sådanne aftaler vil sjældent foreligge i relation til de særlovsovertrædelser, der her er tale om, og der er heller ingen planer om at etablere et strafferetligt samarbejde, der med sigte på Internet-problemerne skulle tage højde herfor. Problemerne har dog været medvirkende til, at Kommissionen i øjeblikket forbereder det ovenfor i kapitel II.6. nævnte direktivforslag vedrørende koordinering af love og administrative bestemmelser vedrørende effektiv håndhævelse af fællesskabslovgivning, der beskytter forbrugernes økonomiske interesser.

4. Styringsproblemerne

Danmarks muligheder for at påvirke beslutningsprocedurerne vedrørende Internettet og andre digitale kommunikationsnet er forholdsvis begrænsede. Det siges, at nettet ikke er "kommercielt", og der er den sandhed i dette udsagn, idet Internettet ikke er skabt for at generere noget overskud hos nogen investor. Dets udspring i de akademiske forskningsmiljøer har betydet, at der i nettets styrende organer hersker en betydelig grad af selv-regulering. Man kan med andre ord ikke forvente noget *centralt* initiativ i retning af at kontrollere den trafik, der udfolder sig.

Dette udelukker imidlertid ikke, at man kan udøve en sådan kontrol på *decentralt* niveau.

Et eksempel på, hvilke styringsproblemer, der kan opstå herved, er en sag, der opstod i december 1995, da den amerikanske televirksomhed CompuServe efter anmodning fra anklagemyndigheden i den tyske delstat Bayern, valgte at blokere adgangen til over 200 Internet-baserede newsgroups og andre Internet-services, som i strid med den bayerske straffelovgivning spredte obscønt materiale, herunder børnepornografisk materiale. Det principielle i denne sag lå i, at beslutningen ikke kun fik betydning i Bayern, men for alle Internet-brugere verden over, eftersom alle uanset nationalitet nu var afskåret fra adgang til disse tjenesteydelser. En lignende sag opstod i begyndelsen af 1996, da det tyske kommunikationsministerium beordrede, at en online-service ved navn "T-online" med nazistisk information skulle lukkes. Den pågældende tjeneste blev drevet fra Canada. I Tyskland har disse sager givet anledning til politiske krav fra flere sider om regulering af informationsstrømmen på Internettet.

5. Ansvarsproblemerne

Det er udgangspunktet i dansk ret, at ansvaret for spredning af ulovlig information reguleres ved efterfølgende at pålægge den ansvarlige sanktioner (straf, erstatning og - i det medieansvarsretlige miljø - berigtigelse). Det er i strid med

den tanke, der finder udtryk grundlovens § 77, at indføre "Censur og andre forebyggende forholdsregler".

Udover grundlovsargumentet er der også et praktisk argument for at sanktionsregulere efterfølgende, nemlig retsanvendelsesargumentet: Det er lettere at få overblik over skadevirkningerne af en kommunikationshandling, når man kan tage stilling til den i en sammenhæng. Dermed bliver det også enklere at ramme handlingens reelle skadelige virkninger.

Man kan herefter stille spørgsmålet, om det ad *retlig* vej er muligt at regulere den informationsstrøm, der flyder via Internettet, f.eks. således at de aktører, der har ansvaret for, at informationen passerer ind i landet, eller ud til den enkelte bruger, får et retligt ansvar for, at der ikke begås retsbrud. Som udgangspunkt har et sådant ansvar kun mening, såfremt den potentielt ansvarlige har reel mulighed for at kontrollere den pågældende information. Spørgsmålet kan derfor kun besvares meningsfuldt, hvis man tager udgangspunkt i, om denne mulighed består:

Ser man først på teleoperatørens (netoperatørens) kontrol over den *løbende strøm af informationer* over nettet, består der ingen sådan mulighed. Netoperatøren optræder her i samme rolle som telefonselskabet, nemlig som formidler af teletrafik fra det internationale telenet og til nationale abonnenter. Kun i de tilfælde, hvor der er særskilt retsgrundlag for at begrænse en informationsstrøm (f.eks. i form af en kendelse om fogedforbud, en aflytningskendelse eller editionsplæg), kan et sådant ansvar komme på tale.

Et eksempel herpå foreligger med en nyere amerikansk afgørelse, *Playboy enterprises Inc. v. Chuckleberry Publishing Inc. et al.* (no. 79 Civ. 3525 SAS (SD NY)). I 1981 havde en amerikansk domstol afsagt forbudskendelse på begæring af Playboy Enterprises mod et italiensk firma Tattilo, der udgav bladet "Playmen". Forbudet, der skyldtes, at "Playmen" krænkede Playboy-varemærket, angik enhver form for distribution af et engelsksproget magasin med navnet "Playmen" i USA. I 1996 opdagede Playboy Enterprises, at Tattilo distribuerede Playmen fra en hjemmeside (med navnet "Playmen.it") i Italien. På denne hjemmeside kunne man mod betaling hente erotiske billeder fra Playmen-magasinet forsider m.v. Betalingen skete således, at brugeren forinden havde modtaget et password. Ved at identificere sig overfor hjemmesiden med dette password, blev forbruget debiteret brugeren.

Havde den italienske udgiver alene drevet denne hjemmeside fra Italien og uden at adressere det amerikanske marked, var sagen næppe opstået. Imidlertid opfordrede udgiveren amerikanske kunder til at melde sig via telefax, således skete der et egentligt salg af passwords (og dermed brug af hjemmesiden) til amerikanske kunder. Retten fandt, at dette udgjorde en distribution, fordi den blev understøttet af aktive markedsføringshandlinger i USA, og at forbudet omfattede denne aktivitet, selvom forbudskendelsen var afsagt, før Internet var taget i kommerciel anvendelse. Retten pålagde herefter den italienske forlægger enten at afbryde sin hjemmeside eller at standse enhver modtagelse af abonnementsaftaler med personer bosiddende i USA samt at anføre på sin hjemmeside, at man ikke kunne tage ordrer fra USA.

Dommen er omtalt i Software Law Bulletin, vol. 9, no. 7, s. 126 f. og i Computer Law Strategist, June 1996, s. 8. Som anført sidstnævnte sted ville dommens problem have været betydeligt vanskeligere, såfremt der ikke havde foreligget en forbudskendelse. I så fald havde det nemlig været nødvendigt først at skulle tage stilling til, om den amerikanske domstol overhovedet var kompetent til at træffe afgørelse overfor den italienske udgiver.

Det måske mest interessante ved dommen er, at den pålægger redaktøren af en hjemmeside udenfor domstolens jurisdiktion (altså udenfor USA) at foretage aktive skridt til at ændre indholdet af en hjemmeside. Den situation, der foreligger i Playmen-dommen, kan tænkes at foreligge i relation til de kommercielle directory-services, der kommer til at spille en stigende rolle for brugen af Internet (f.eks. Ya-hoo, Alta-Vista m.fl.). Da disse services fungerer som elektroniske hypertext-stikordsregistre til nettet, bliver brugen af dem afgørende for, hvorledes brugerne på nettet får tilgang til information. På grund af denne flaskehals-funktion bliver det afgørende, om man kan bremse en ulovlig informationsstrøm ved at blokere henvisningen fra stikordsregisteret til den berørte net-adresse. Kan man det, vil man ramme den væsentligste del af trafikken til denne adresse, omend ikke den samlede mængde.

Et ansvar for underforstået *medvirken* forekommer, når den ansvarlige for en web-site udvirker hypertext-links, hvorved opkald til siden sendes videre til andre sider. Efter straffelovens § 23 omfatter en straffebestemmelse alle, der ved tilskyndelse, råd eller dåd har medvirket til gerningen. En medvirken kan f.eks. bestå i, at man skaber en hypertext-link til en hjemmeside, hvor der findes information, der ikke lovligt kan spredes, f.eks. på grund af markedsføringsretlige eller ophavsretlige begrænsninger. Danske domstole har endnu ikke taget stilling til, om den, der blot stiller et digitalt medium til rådighed på en sådan måde, at andre - i eller uden for vedkommendes organisation - kan downloade information, dermed bærer ansvaret for de mulige retskrænkelser, der kan følge heraf. Spørgsmålet er ret beset, om man har pligt til at modvirke, at der sker ophavsretlige krænkelser. "Man" kan i princippet være enhver person med kompetence vedrørende den pågældende edb-drift.

Spørgsmålet om, hvem der medvirker til den ophavsretlige krænkelse, når værker stilles til rådighed via BBS-systemer har været afgjort i flere amerikanske sager. I *Playboy Industries Inc. v. Frena*, 839 F.Supp. 1552 (1993) havde en BBS-operatør ladet sine kunder oploade retsbeskyttede fotografier til en database. Da Playboy anlagde sag, fjernede BBS-operatøren omgående fotografierne fra basen. Retten fandt desuagtet, at der forelå en retskrænkelser, uanset om BBS-operatøren var sig den bevidst. I *Sega Enterprises, Inc. v. MAPHIA*, (1994) havde BBS-operatøren haft kendskab til det ulovlige materiale. Dommen i *Cubby v. CompuServe*, 776 F.Supp. 135 (1991) angik injurierende udsagn. Retten anså her databasewærten CompuServe som bibliotek, idet den bemærkede, at lavere ansvarskrav ville "impose an undue burden on the free flow of information." Følgelig ville man kun pålægge CompuServe ansvar for den ophavsretlige krænkelse under betingelse af, at CompuServe kendte den eller burde have kendt den. Et tilsvarende resultat har New Yorks Supreme Court (der trods sit navn er en underordnet instans) fastslået i sagen *Stern v. Delphi Internet Servs. Corp.*, omtalt i International Technology Newsletter, vol. 14, no. 1, s. 10 f. Den kommercielle Internet-udbyder Delphi havde placeret fotos af Mr. Stern på sin hjemmeside. Stern fik medhold i, at denne anvendelse var i strid med hans

kommercielle rettigheder til sit navn (se om denne navnebeskyttelse for dansk ret U1965.126H, U1974.952, U1986.272SH, U1986.428Ø og U1989.1146SH). Delphi påstod frifindelse under påberåbelse af, at man drev virksomhed med nyhedsformidling og fik medhold heri. Dommens anvendelse af princippet i Cubby-sagen er ikke uproblematisk, eftersom der var tale om en kommerciel anvendelse af et billede, som Delphi selv havde bragt, og altså ikke om viderespredning af information, som en læser/bruger havde bragt.

En særlig form for medvirken foreligger, når der sker *redaktion* af den information, der ligger på en hjemmeside. Spørgsmålet om hjemmeside-redaktørens ansvar er blevet rejst under flere amerikanske sager, se f.eks. *Stratton Oakmont v. Prodigy Inc.* 1995 NY Misc LEXIS 229: En investeringsbank, Stratton Oakmont Inc., har påstået Prodigy erstatningsansvarlig, fordi nogle udtalelser var spredt via Prodigy's populære "MoneyTalk" BBS. Udtalelserne gik ud på, at Stratton Oakmont skulle have skjult oplysninger i forbindelse med et aktiekøbstilbud, firmaet stod for. Stratton Oakmont påstod, at Prodigy havde pligt til at fjerne de pågældende oplysninger og henviste til, at Prodigys retningslinjer forbød visse upassende udsagn, samt at der var installeret et program, der scannede og rensede indgående meddelelser for udsagn, der kunne anses for fornærmende. Disse forhold gjorde, at Prodigy ansås som "publisher" (udgiver) i relation til de pågældende udsagn.

Ansvarsreglerne i *medieansvarsloven* regulerer ansvarsproblemerne vedrørende periodiske skrifter m.v. Dermed kan den forurettede altid gøre sit ansvar gældende mod den ansvarshavende redaktør, selvom ophavet til en krænkende oplysning m.v. ikke træder offentligt frem i mediet. Loven finder kun anvendelse for visse af de kommunikationsformer, der her er tale om (nærmere bestemt tekster, billeder og lydprogrammer, der periodisk udbredes til offentligheden, såfremt de har karakter af en nyhedsformidling, der kan sidestilles med den formidling, der er omfattet af de almindelige regler om periodiske skrifter samt radio- og TV-udsendelser). Da loven dermed ikke omhandler andre elektroniske medier (f.eks. BBS-systemer), hvor der også kan forvoldes krænkelse, kan man diskutere, om ikke der er behov for en tilsvarende ansvarsregulering.

Dette blev resultatet i den amerikanske afgørelse i *It's In The Cards Inc. v. Fuschetto*, 535 N.W. 2d 11 (1995). Dommen fortolkede en lovbestemmelse i staten Wisconsin om redaktøransvaret for "a newspaper, magazine or periodical". Parterne var enige om, at et bulletin board service hverken var omfattet af ordene "newspaper" eller "magazine", så striden stod om, hvorvidt den i stedet var dækket af "periodical". Retten afviste dette under henvisning til det tilfældige i den informationsstrøm, der går til og fra et BBS, i modsætning til den jævnlige informationsrytme i "periodicals". K.A. Frøbert i U1996B.387 ff.

I sin afsluttende betænkning om Medierne i demokratiet (nr. 1320/1996) har Statsministeriets Medieudvalg drøftet behovet for en særlig ansvarsregulering af informationsstrømmen på Internettet. Udvalget fastslår (s. 433), at medieansvarsloven regulerer ansvarsproblemerne vedrørende periodiske skrifter m.v., men ikke for Internettet, som ikke er et medie i radio- og fjernsynslovens forstand. Reguleringsmæssigt betegnes Internettet som en datatjeneste, idet

udvalget bemærker, at telelovgivningen ikke regulerer indholdet af datatjenester (s. 433).

Medieudvalget anbefaler, at Internet-udgivelser, som kan sammenlignes med traditionelle massemedier, gennem anmeldelse til Pressenævnet lader sig omfatte af medieansvarsloven (s. 433 og 438). Dette er i givet fald en frivillig ordning, og Medieudvalget støtter dette frivillighedsprincip, bl.a. fordi det er vanskeligt på forhånd præcist at afgrænse hvilke internet-udgivelser, det er relevant for. Derimod finder Medieudvalget ikke (s. 439), at der er grund til at ændre på den gældende retstilstand m.h.t. indholdsmæssig regulering af Internettet. En lovgivning som den amerikanske Communications Decency Act - jf. herom straks nedenfor - vil efter udvalgets opfattelse være af censurlignende karakter og kan derfor ikke anbefales. Hertil kommer de vanskeligheder, der måtte forudses med administrationen af sådanne regler.

Som det fremgår af ovennævnte, er det for tiden ikke muligt entydigt at beskrive hvilke "Internet-aktører", der bør være omfattet af medieansvarsloven. Det kan diskuteres, om en frivillig ordning som foreslået er tilstrækkelig, eftersom det forventes, at der inden for en kort tidshorisont vil forekomme aktører, som bør være omfattet af en form for medieansvar. Her tænkes især på Internet-udgivere, der foretager en vis kvalificeret redaktion af det stof, der er på deres Internet-side, og som minder om de traditionelle massemedier.

En diskussion om en eventuel ansvarsregulering for informationsspredning på Internettet må inddrage de relevante aktørers mulighed for og vilje til selvregulering. En række private Internet-udbydere har allerede indført regler, der fastslår hvilket ansvar, der bør være i forbindelse med ulovligheder via Internet-baserede informationssystemer, (smh. f.eks. FIL's regler og Internet Service Providers Association: www.ispa.org.uk)

Herudover har enkelte operatører vedtaget frivillige regler om denne kontrol. Et eksempel herpå er den "Taste and Decency Policy in respect of BT Internet Access Services", som er vedtaget af British Telecom. Heri udtaler BT, at man betragter sig som "common carrier", der i modsætning til en redaktør ikke skal være "the moral arbiter of such third party material". Det hedder videre:

"Given that BT cannot itself ... filter and edit Internet content, ... BT is focusing instead on providing its customers with all possible advice, education, support and guidance regarding the nature of the Internet and is in particular advising them of the need to take precautions when allowing children access to the Internet. ... BT is consulting consumer and other relevant bodies to explore possible solutions to the above issues."

Det fremgår ligeledes, at BT fører kontrol med, hvilke navne dens newsgroups har, hvorimod man ikke befatter sig med den information, der formidles heri.

En sådan ansvarsregulering bør dels fokusere på den personkreds, der i relation til massemediene betragtes som den "ansvarshavende redaktør", dels på den organisation, der på internationalt niveau står bag udbydelser af de digitale net, og som i givet fald måtte yde bistand til at afskære den tekniske adgang til, at en ulovlig tilstand kunne fortsætte. I relation til sidstnævnte spørgsmål kan man

overveje, om ikke det ville være i tråd med den retstradition, der gælder i relation til de elektroniske massemedier, at man formaliserede (d.v.s. lovregulerede) en organisation som Internet Society. En sådan formalisering vil bl.a. kunne understøtte mere præcise regler om markedsføring og annoncering via sådanne netforbindelser.

I USA forsøger myndighederne at lovgive og dermed placere ansvaret for ulovligt indhold på Internettet. I februar 1996 vedtog den amerikanske regering en lov - Communications Decency Act (Kapitel V i The Communications Act) - som forbyder transmittering af uanstændige materialer på nettet. Loven gør det kriminelt at udsætte unge under 18 år for "usømmeligt" materiale, og overtrædelser straffes med bøder på 250.000 dollars og fængsel i op til to år. Dog bestemmes det, at Internet-udbydere frigøres fra ansvar, hvis de tager "fornuftige, effektive og passende skridt" til at forhindre, at børn får adgang til stoffet, f.eks. ved at verificere forbrugerens myndighed eller ved at kræve betaling via et kreditkort, der kun udstedes for myndige o.lign.

Loven mødte imidlertid kraftig modstand fra borgerretsorganisationer, der fandt at der var tale om krænkelse af forfatningens ret til ytringsfrihed, og at det var umuligt at håndhæve den, da ca. 40% af indholdet på nettet kommer ind i USA fra udlandet, det vil sige uden for lovens jurisdiktion. Tillige pegede de på det problem, at "anstændighed" er et vagt begreb, der kan fortolkes forskelligt fra sag til sag og fra stat til stat.

Loven lagde op til sidestillelse af Internettet som medium med transmissionsvirksomhed i modsætning til f.eks. aviserne, således at de regler som gjaldt for radio og TV kom til at gælde også for Internet-udgivelser. Kritikerne mente, at Internettet snarere burde sammenlignes med de trykte medier, da forbrugerne kunne udøve valg vedrørende det de ville have på deres computere, hvorimod de - efter at havde valgt en station - ikke havde kontrol over det, radio- eller TV-stationen udsender.

Kort efter dens vedtagelse blev loven erklæret ugyldig af en underdomstol, og regeringen har straks anket afgørelse til den amerikanske højesteret. Højesteret er begyndt at behandle sagen i marts 1997.

6. Specifikke reguleringstiltag

a. Beskyttelse af forbrugerens person

Justitsministeriet har igangsat et udvalgsarbejde vedrørende ændring af registerlovgivningen. Udvalget skal bl.a. overveje, hvorledes et direktiv om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger (direktiv 95/46/EF af 23. oktober 1995) skal implementeres. Da udvalgets kommissorium ikke er begrænset til implementeringen af dette direktiv, kan også andre registerretlige problemer tages til behandling.

Emner som beskyttelse af forbrugers integritet i relation til de "elektroniske spor", der efterlades på en hjemmeside, eller om den generelle regulering af sikkerheden i Internettet kan eventuelt rejses og drøftes i Registerudvalget.

b. Sikkerhedsspørgsmål

I Forskningsministeriets nuværende arbejde på at bringe Danmark i førerposition hvad angår brugen af digital teknologi spiller sikkerhedsspørgsmålene en central rolle. I januar 1995 besluttede forskningsministeren at nedsætte IT-sikkerhedsrådet. Rådet har i november 1996 fremlagt sine første anbefalinger om grundlaget for en dansk IT-sikkerhedspolitik.

Det igangværende arbejde præges af, at tidligere planer om at indføre et almindeligt, statsligt *borgerkort*, der vil gøre det muligt for enkelte borgere at identificere sig sikkert overfor offentlige myndigheder, indtil videre er lagt på hylden. Planerne herom har haft forskelligt indhold. Bl.a. har det været diskuteret, om et sådant kort også skulle kunne anvendes som betalingskort.

Idéen om et sådant kort er første gang lagt frem i TeknologiNævnets rapport "Plastkort som borgerkort - Anvendelse af ic-kort teknologien til borgerkort" (TeknologiNævnets rapporter 94/2). De bevis- og erstatningsretlige problemer vedrørende anvendelsen af digitale kommunikationsnet er diskuteret i bilag 1 til Telestyrelsens krypteringsudvalgs 1. delrapport vedrørende et eventuelt myndighedsinitiativ på krypteringsområdet (Telestyrelsen, juni 1993).

Forskningsministeriet arbejder på et lovforslag om digital signatur. Udover at understøtte en række af de sikkerhedsproblemer, der er omtalt i det foregående (vanskelighederne ved at identificere sig m.v.), og dermed bane vejen for sikkerhedsfølssomme løsninger, som f.eks. elektronisk betaling m.v., rummer en sådan lovgivning væsentlige sikkerhedsproblemer. Disse problemer kendes i forvejen fra betalingskortområdet, hvor de gav anledning til intense retspolitiske drøftelser i begyndelsen af 1984 forud for vedtagelsen af Lov om betalingskort, men de genopstår nu i en ny skikkelse og med langt større intensitet. I modsætning til de dispositioner, indehaveren af et betalingskort træffer, og som ultimativt set "kun" kan pådrage ham en økonomisk forpligtelse (der tilmed er begrænset i overensstemmelse med lovens hæftelsesregler m.v.), vil indehaveren af en løsning til digital signatur kunne pådrage sig alle de typer af forpligtelser, som han eller hun kunne have pådraget sig ved at sætte sin underskrift på et stykke papir.

c. Forbrugers retsstilling og retsbeskyttelse

Licensproblemerne: De forbrugersyn, der måtte knytte sig til begrænsninger af immaterialretlig art, behandles af Kulturministeriet som led i dette ministeriums varetagelse af ressortansvaret for ophavsretten. Kulturministeriets aktuelle overvejelser vedrørende den digitale udvikling har hidtil været fokuseret på arbejdet inden for EU. I øjeblikket er dette fokus imidlertid flyttet til det igangværende arbejde vedrørende WIPO's traktater, som er nævnt i kapitel III.6.h.

Fra EU-Kommissionen foreligger dels en Grønbog af 19. juli 1995 om ophavsret og ophavsretsbeslægtede rettigheder i informationssamfundet (KOM(95) 382, endelig udg.), dels et papir om Copyright Law Barriers to the Information Superhighway, udarbejdet af en High Level Strategy Group og fremlagt i et såkaldt "Draft (2)". Papiret peger på en række - for ophavsretskyndige velkendte - problemer i forbindelse med spredning af information i digital form. Enkelte af disse spørgsmål (f.eks. om den frie adgang til kryptering, se papirets pkt. 3.7.f.) kan have betydning for forbrugerens sikkerhed m.v. Papiret anbefaler, at der igangsættes en proces, hvorefter Kommissionen i samarbejde med industrien arbejder for at fjerne de eksisterende ophavsretlige barrierer, f.eks. i relation til spørgsmålet om "fair use" samt ved udvikling af systemer til teknisk kopibeskyttelse, kryptering m.v.

Herudover indgår der et vist forbrugerperspektiv i det udvalgsarbejde vedrørende *bibliotekerne i informationssamfundet*, som ligeledes pågår i kulturministerielt regi. Endelig kan nævnes ministeriets ressortansvar for radio- og TV-området, hvor forbrugerhensynet spiller en indirekte rolle i forbindelse med reglerne om *TV-reklame*.

V. Executive Summary

Concluding chapter for a report made by The Danish Ministry of Business and Industry on "The Legal Protection of Consumer Rights in Relation to Transnational Digital Networks":

Conclusions and Recommendations. An Introduction for Debate

1. Introduction and Superior Valuation

The most important purpose of the Internet today is information interchange. The technological development has implied that the Internet has become still more sophisticated and easier to utilize. These facts have resulted in the fact that business and consumers have taken to the Internet.

Increasingly the Internet has become a marketing instrument utilized by business, public authorities and interest groups in order to get into contact with citizens. Concomitantly the Internet is utilized by an increasing number of citizens as a means of communication.

The network is characterized by being applicable for one-way communication - for instance when two persons are sending E-mail to one another or when a person is reading a homepage and for multi communication, for instance in the shape of "bulletin boards"/"contact fora", etc., where a broader and perhaps even boundless circle of persons has access to collect/insert information. The Internet can be used for interactive communication as well.

The Internet is characterized by being "boundless", that is to say, when first information is available on one spot on the network, the information basically becomes freely accessible for everybody simultaneously - wherever in the world information is being searched for. And mind you, this is with no essential costs for the person inserting information. Furthermore, a quick and continuous modification and updating of available information at, for instance a homepage, can be carried out.

Concurrently the Internet is characterized by the fact that it is not possible to point out a central control authority, which ensures that the material inserted on the network fulfills certain regulations. In this way the Internet differentiates markedly from other media - for instance TV and books - where the publisher "supervises" information passed on by the media.

These circumstances imply that the Internet in the popular sense of the word is independent of time and place, and that it has become significantly easier for the individual - not only to collect information, but to spread information as well; including importunate, incorrect, unethical or even illegal information.

It is to be expected that the continuous development of the Internet implies that it will increasingly take on the character of a market place where business and consumers are able to trade directly with one another and where payments will take place directly through the network. Extensively the Internet will be used for commercial purposes. This development demands a lot from both the consumers, business and the authorities. The Internet will take a considerable alteration of existing trade patterns and market structures.

The open digital networks do not only create new markets but new products as well - the so called digital products - which do not exist physically, but delivered only in a digital shape, and which are being transferred to the computer of the consumer through the Internet. As examples of digital products are to be mentioned computer programs and other information products including newsletters, books and music.

The appearance of both new boundless markets and purely digital products raise a number of consumer political challenges. The report draws attention to a number of consumer relevant areas of risks, and it contains a number of considerations of a modern consumer policy proportional to transnational marketing and trade, carried out through open digital networks. Such a policy must balance between consumer and trade interests, and at the same time consider the evident social advantages and promising dimensions of the open networks. Finally, the policy shall consider the fact that the information technology is in a considerable development, which continuously may change the risk points which, seen from a consumer's political point of view, has the highest priority.

If the Internet is to have a future as a successful instrument for efficient, fast and cheap trading activities and services, it is important that initiatives which minimizes the principal risks, currently taken, in such a way that business and industry and the consumers have confidence in the Internet. Simultaneously it is of importance that these initiatives are taken as soon as possible, as it is not appropriate, neither for business nor for the consumers that on central points doubts arise about which rules of the game are valid. Consequently it is not appropriate that a generally "laissez faire" - policy be pursued, in which it is the indicated matters of dispute/problems that first may find their solution by the authorities and the court of justice "who try to" employ the current legislation.

SUPERIOR VALUATION:

The Internet may result in several advantages for the consumers:

- improvement of the consumers possibilities of making rational consumer choices,
- consolidation of the political consumer's influence,

- increasing possibilities of transforming from massproduction into customer-oriented production, and
- an increase in the number of suppliers and introduction of new products - including digital products - which after all may lead to increased competition and consequently lower prices.

On the other hand the Internet's use of digital information interchange raises a number of consumer political doubts, of which the following in particular are to be drawn attention to:

- Business is given quite new possibilities of collecting, adapting, passing on and using information of the individual consumer.
- It becomes substantially easier and cheaper for business to get into contact with the consumers, this will raise the possibilities of employing insistent and unethical marketing activities.
- The boundlessness of the Internet implies that certain persons/business will be able to utilize that some countries do not have a legislation which provides an acceptable protection of the citizens.

Consequently the main consumer political challenges of the Internet are:

- To insure the integrity of the consumer both as regards business' collection and use of information related to an individual and business' use of insistent and unethical marketing activities,
- to make the consumers capable of using the Internet in such a way that the positive aspects of the Internet become a reality.
- to ensure that Danish legislation currently - and as soon as possible - is adapted to the IT-development in progress.

2. Advantages

The advantages of trade on the global network are numerous. The consumer can, in an unknown extent up to the present - get access to information, offers, news etc. which meet his precise area of interest. He is able to receive advertisements and offers from suppliers from the other part of the earth, just as simple as the material from the local shop. The information is accessible day and night, every day of the week - and in principle no matter where the consumer might be. The traditional opening hours of the shops are of secondary importance. The advertisements can be compared quickly and effectively for instance by means of special seeking programs, this makes it easier to sort out in the quantities of advertising materials and find one's way to the cheapest and most advantageous offer. With no major expenses for the advertisers the advertisements contain very detailed information about the characteristics and

contents of the products. Furthermore the information will be kept up to date currently, improving the level of information.

Technology opens up the prospect of the Network containing pictures, sound and three-dimensional graphics. The interactivity of the media means that the consumer by a click on the mouse is able to activate the exhibited product. For instance the consumer is capable of turning over the coat and having a look at its back/lining or experience the moving possibilities of a product. The consumer will also be able to design products which satisfy the exact requirements of the consumer. This can be effected by combining materials, modules, colours etc. It opens up the prospect of quick and simple ordering of goods and the development in progress will be supported by the Internet, which implies that still more goods are being produced in order to satisfy the individual request and needs of the consumer.

As the consumers do not need to appear at the shop they are ensured equal treatment and information irrespective of ethnic origin, colour of skin, sex or religion.

The Internet will create increased competition. Coincidentally a number of business companies will be able to minimize their costs (of offices, depots, advertising etc.) by utilizing the Internet. It is to be expected that the Internet - if utilized in the proper way - will improve the consumers' possibilities of making rational consumer choices. This aspect will probably result in lower prices on a number of products.

3. International Aspects of the Internet

Electronical trade does not only offer advantages for the consumers, it involves significant risks as well. Protection of the consumers' interests against abuse of the new technological possibilities must naturally be made in a manner that does not undermine the Internet's advantages as open and accessible information interchange. After this, the task will be formulating and effectuating a policy, which takes into account the particular "nature" of the Internet with its unique, decentralised and international structure, so that the consumers will benefit from the convenience of technology with maximal law and order.

The boundlessness of the Internet implies that a single country will not be able to legislate and maintain its own rules towards all foreign citizens and business companies. Consequently it is a certainty that the Internet demands a higher priority of international collaboration both regarding preparation of new/harmonized rules and maintenance of the rules.

As the Internet is global, it would be ideal to create a collaboration forum that is as international as possible. This could exist in Nordic framework, EU or OECD. The Nordic forum is - on account of the cultural community, the judicial unity and the close communication channels - suitable for testing the possibilities of common proposals and initiatives at first. The initiatives, agreed upon in the Nordic framework, could be sought promoted afterwards either in EU-framework, OECD-framework or if necessary in UN-framework. Although

international collaboration is advisable, national and regional authorities (for instance Danish authorities and EU) cannot await a "global solution", as these are not realistic within an acceptable time frame. Business must therefore be prepared to have their activities regulated by national or regional authorities - not withstanding that some countries which do not find reasons to criticize or adjust the behaviours in question exist.

Business must be aware that the Internet gives sense to a degree, to the term "the global village". When business find itself on the Internet it gets into contact with consumers and authorities in a great number of countries (villages) interested in what is to be found on the Internet, and are prepared - based on precisely their own ethical, religious and political views - to react to the material that offend them.

For business this implies in practice that when being on the Internet with a homepage - it must be aware that the political consumers in every single country may react when finding the behaviour of the business company (on the Internet) unethical/unacceptable.

4. Challenges

The major part of the problems a consumer comes up against when using the Internet are to be recovered in the "ordinary commercial world", but some of the problems assume another character on account of the special qualities of the Internet. It is hence not a question of whether we are facing a large number of unknown consumer political challenges, rather a question of facing a far new, and a number of unknown, consumer political challenges which nevertheless have assumed altered characteristics on several points.

The fundamental starting point should be to avoid special rules exclusively controlling the Internet as far as circumstances permit. If there is a necessity of a new or revised legislation, the rules should be valid to a great extent whether the act takes place over an open digital network or through other media. Current legislation which is found obsolete shall be revised to a necessary extent and adjusted to technological development. A (new) regulation shall be elaborated to the greatest extent in consideration of the dynamic development existing within information technology, and wherever possible it is to be avoided that the rules have a restrictive influence on a sound technological development.

For a number of years business' use of the Internet will be characterized by "learning by doing", in other words that business for a number of years will be facing a new media, not knowing quite how to "utilize" it. This implies that business proceeds by trial and error and that a number of companies will be committing some errors in this process. Concurrently business will be attempted to make use of various technical possibilities in an unacceptable manner seen from a social point of view, for instance a more direct marketing and increased registration of the consumers' behaviour.

The consumers are facing a new media as well - and new marketing initiatives. This makes increased demands to the "critical sense" of the consumers, as the need for consumer information increases. It is of importance that the consumers take advantage of the possibilities of exchanging information on business/products. They should also realize their advantages given by the Internet in influencing business to act correctly. It must be assumed that a number of the problems arising from the increased transnational trade in the long term will be reduced in consequence of the consumers' own rational behaviour patterns. A raising of the level of the ordinary "consumers' attitude" through education, consumer information and similar should take up an important part.

Based on the problems outlined in the report, it is to be expected that among others the following problems will be of great importance in the years to come:

- Increased registration of information of the consumers' behaviour when surfing and trading on the network (electronical trace) and increased use/passing on of this information in the future marketing.

It will not be possible immediately for the consumers or the authorities to know/control what is being registered and how the registrations are used.

- Insistent and/or camouflaged marketing through the Internet including the use of incentive arrangements (discounts etc.), granted on condition of the acceptance of the consumers, that they submit certain information or "receive" certain advertising spots etc. when utilizing the network or special services offered through the network.
- An expansion in the quantity of marketing material. Simultaneously the marketing material will undergo frequent modifications. These circumstances will create more cases, where the authorities shall assess if the marketing material is in accordance with the legislation.
- Increased use of standard conditions (including by virtue of references) standard and frequent modifications of standard conditions might force the consumers to spend essentially more time considering whether they wish to conclude an agreement on precisely these terms, as the risk of unfair standard conditions increases.
- Cases, where the consumer by an operating error happens to order products, which the consumer did not intend to order.
- Increased number of cases where products, ordered on the Internet, either are not delivered (on time) or are not equal to the expectations the consumer held to the product as a consequence of the marketing material.
- Problems with evidence, as regards to which information the businessman has given through the Internet. Frequent modifications of the

marketing material - and the fact that often the consumers will not be in possession of the marketing material, which they have seen on the network - will increase the number of cases, where there are disagreements about what prospects the company has led the consumer to believe.

PROPOSAL FOR INITIATIVES:

Based on the problems outlined in this report the following initiatives should be considered in particular:

- 1) That the consumers and business get easy and cheap access to the Internet, which is to function dependably and with quick response duration.
- 2) That communication on the Internet can be effectuated in encrypted format and with application of digital signature.
- 3) That the Internet functions uncontrolled.
- 4) That business companies which utilize the Internet commercially always are to establish their identity including their physical address. This is valid both when the Business companies are using the Internet for marketing and when making agreements with consumers/business companies through the Internet.
- 5) To amend the Sale of Goods Act, The Product Liability Act and the Product Safety Act. These acts seem to be "blind" towards the existence of pure digital products.

On account of the legal unity in the Northern countries it will be a natural move to seek the activation of a Northern collaboration on this problem - in particular in relation to the Sale of Goods Act.

- 6) To amend the Canvassing Act in order to make it take into account the new means of communication and marketing practices, provided for by the information technology.

Hereby is referred to the risk of "information pollution", where a company issues marketing material to a large number of persons on the Internet (contrary to marketing directed to specific and relevant consumers), without request from the receivers. In order to meet "information pollution", furthermore there ought to be a possibility for the consumers towards the companies - issuing "targeted" marketing material - to be spared of receiving future marketing material from the company concerned.

Concurrently the purposes of the modifications should partly be to simplify the Canvassing Act, partly to accomplish directive 97/7 about consumer protection in connection with agreements relating to remote-trading.

- 7) To amend the register legislation in order to safeguard consumers against unfair registrations - including use of potential registrations - when surfing or trading on the Network. Concomitantly it should be considered if the area renders possible a sufficient protection of the consumers.

As the Ministry of Justice has appointed a register committee, it will be natural at first to make a request to the committee to investigate whether the current legislation/directive offers the necessary protection, including partly if the legislation offers the necessary knowledge of which registrations the individual company is effectuating, partly if the current possibilities of supervision are sufficient. The IT-Security Council ought to be involved in these investigations as well.

- 8) To amend the Price Labeling Act, in order to make the companies state prices etc., when giving the possibility of remote trading of goods and services through the Internet. Similarly it ought to be considered whether a company, which is on the Internet with a homepage generally should state the same price information etc., on the Internet, which they have to state by posters in the shop.
- 9) To amend the Administration of Justice Act. The criminal code and certain ad hoc acts, for instance the Trade Marks Act, offer the opportunity of confiscating (or destroy) physical material. Supplementary to these rules it ought to be considered introducing a legal remedy, which makes it possible to intervene against digital information and digital products, which are to be found on open digital networks and which are to be reproduced continuously and are placed on the network once more. It ought to be considered whether the criminal code should be amended in order to make it possible for the authorities to force the Internet-suppliers to close access to the Internet of a person/company, when authorities and/or law-courts have intervened several times against illegal material placed on the network by the persons concerned. As it is a question of extensive interventions, it ought to be effectuated only in situations where other legal remedies turn out to be insufficient.
- 10) To introduce a general regulation in EU of fair trading practice. The regulation may correspond to § 1 of the Marketing Act, in such a way that a certain minimum requirement to the business companies' behaviour is valid in all of the EU- countries included when utilizing the Internet for marketing.

- 11) That efforts be directed towards an introduction of international rules, in order to make the authorities and the consumers' organizations capable of proceeding against a company - attending to the collective interests of the consumers - at the law courts in the country of which the company by its marketing breaks mandatory consumer protection regulations. A judicial decision - which issues an injunction/command that provides the consumer a claim for compensation, - or which implies that the company is incurred a monetary penalty - should be directly enforceable in the country, where the company has its domicile.
- 12) That efforts are directed towards the introduction of an international Consumer Sale of Goods Act - for instance in the shape of an EU-Consumer Sale of Goods Act - valid when a consumer from a country and a company from a different country are doing business in the form of remote-sale. As an international Sale of Goods Act has already been elaborated (CISG), valid for trading between businessmen, a certain inspiration is to be taken for these regulations.

Until such regulations are effectuated, the efforts from Danish quarters should be directed towards amending article 5 of "The Convention on Jurisdiction and the Enforcement of Judgement in Civil and Commercial Matters", in such a way that it is clarified that it is the consumer's legislation which is to be applied, when the consumer is making international purchases through the Internet.
- 13) That special regulations which regulate interactive marketing addressed to children and young people are effectuated. These regulations should be valid globally, but Nordic regulations or EU-regulations will for the moment be an essential step in the right direction.
- 14) That authorities and consumer organizations take initiatives which ensure that the consumers are aware of the possibilities and risks of the Internet, and that they are given the possibility of utilizing the Internet for collection/exchange of information about consumer relevant material.

To sum up, it is to be concluded that at this tender stage of the Internet's part as a real global market place of benefit to consumers and suppliers of goods and services, it is hardly possible to solve all conceivable consumer risks through legislation. An additional fertile means in the battle of more loyal marketing, safe products, credible payment systems, preservation of personal integrity and responsibility when trading on the Internet, may be a dialogue and a collaboration between businessmen, industry and consumers, supplemented with a number of simple, necessary rules of the game from authorities.

Considering the fast development, it is not unrealistic to expect that technology, through sorting programs and selection mechanisms, will be capable of offering

the consumers a more efficient control of what kind of information flows into the personal computer through the Internet.

Concurrently the consumers who join together may constitute an economical and commercial force, which may force the suppliers of goods and the Internet-suppliers to ameliorate control and quality of the offered products and to observe certain rules, such as labelling of the dispatched materials, and to provide certain information products with cautioning labels or international approved logos and symbols. Finally the mission of the authorities may be to legislate on areas where practice will indicate the necessity for this, and train the consumers in utilizing and enjoying the advantages of the media, but simultaneously be attentive towards its risks.

Ordforklaringer

Applikation: Fordanskning af det engelske ord "anvendelse", underforstået: edb-anvendelse. Benyttes ofte med tilføjelsen "-programmel" (applikationsprogrammel) for at markere en forskel til systemprogrammel. Kan også betegne en given, bruger-rettet edb-løsning. Et tekstbehandling-program er en applikation.

Asymmetrisk kryptering: Se public key kryptering.

Autentifikation: Den proces, hvorved man udnævner et symbol, der er knyttet til en meddelelse, for dermed at identificere sig med denne meddelelse. Når en person underskriver et dokument, autentificerer han det. Autentifikationen udgør beviset for, at den pågældende havde fysisk kontakt med meddelelsen og at meddelelsen siden er blevet bevaret uforandret.

ARPA: Advanced Research Projects Agency. Betegnelsen for den forskningsinstitution, der stod bag opbygningen af det såkaldte ARPA-net; forløberen for Internet.

BEUC: Bureau Européen des Unions de Consommateurs, den europæiske sammenslutning af forbrugerorganisationer.

Browser: en browser er det program, som anvendes i pc'en, når en bruger etablerer adgang til og henter information fra et website.

CD-ROM: Optisk datamedium til lagring af digitale data.

Certifikat: En meddelelse, der er autentificeret af en person, og som udtaler sig om rigtigheden af et forhold.

Cookie: En cookie er en fil, indeholdende linier af tekst, som et websted ved henvendelse fra en bruger placeret på brugerens harddisk. Som udgangspunkt ske dette uden at brugeren bemærker det. Cookien indeholder en vis information i et standardiseret format, som lagres i et særligt bibliotek på pc'ens harddisk. Ved efterfølgende henvendelser fra denne bruger til samme websted, vil cookien i brugerens pc blive fremsendt sammen med henvendelsen til webstedet, hvorved den lagrede information i cookien kan anvendes af webstedet. En cookie er ikke tilgængelig fra andre websteder end det, som har placeret den på den pågældende pc. Anvendelse af cookies er baseret på en facilitet, som er indbygget i de mest anvendte "browsere".

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.

Digital: Baseret på talsystem. Data betegnes som digitale, når de kan omskrives til "nuller og étaller". Digital information indgår i moderne IT-anvendelse på grund af computerens særlige mulighed for at behandle tal.

Digital broadcasting: Udsendelse af radio- og TV-signaler i digital form. På grund af kompressionsteknikker indebærer denne transmission, at man kan sende flere signaler på mindre båndbredde.

Digital signatur: Matematisk metode, der anvendes til at verificere, hvem der har afgivet eller afsendt en digital meddelelse. Teknikken betjener sig af public key kryptering. Meddelelsens afgiver låser meddelelsen, eller knytter en særlig numerisk værdi til den (hash-værdi) ved hjælp af sin hemmelige nøgle. Hvis modtageren kan låse meddelelsen op (eller verificere hash-værdien) ved hjælp af afgiverens offentlige nøgle, kan han slutte, at meddelelsen må stamme fra afgiveren (originalitet), og at den ikke siden afgivelsen er blevet ændret (integritet). Det store praktiske problem med systemer til digital signatur er sikkerheden for, at det virkelig er afgiveren, der har anvendt den offentlige nøgle. Til at sikre dette anvender man en certificeringsinstans (også kaldet CA, Certification Authority), der med sit certifikat om afsenderens identitet m.v. tilvejebringer denne sikkerhed.

DoD: Department of Defence. Det amerikanske forsvarsministerium.

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, m.v.), læses af et modtagende edb-system, der igangsætter en kommunikationsproces svarende til deres indhold; fakturaen bogføres automatisk, købsordren effektuerer automatisk en produktionsgang ect. 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 udveksling af handelsinformation (f.eks. faktureringer, aftaler, bekræftelser ect.), men der er principielt intet til hinder for, at EDI-løsningerne også kan gøre deres indtog inden for den private sfære.

EDIFACT: Forkortelse for Electronic Document Interchange for Administration Commerce and Transport. Standard, der understøtter elektronisk udveksling af handelsdokumenter ved EDI. EDIFACT blev foreslået i april 1987, men opnåede allerede i september s.å. enstemmig vedtagelse som ISO 9735. Standarden skal føre til en række yderligere standarder og retningslinier for strukturering af brugerens data og tilknyttede servicedata i et åbent EDI-system.

EMI: Det Europæiske Monetære Institut.

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

Host: Betegnelsen for en computer, der er tilsluttet Internet med det formål at kunne lagre programmer og data. Se også router.

Information Society Forum: Permanent "tænketaank" udpeget af EU-kommis-sær Martin Bangemann med henblik på løbende at forholde sig til, hvilke initiativer Kommissionen bør tage for at sikre udviklingen af informationssam-fundet.

IAB: Internet Architecture Board. Arbejdsgruppe, der står for fastlæggelsen af de standarder, der anvendes i Internet.

Internet: Betegnelsen for det verdensomspændende edb-net, der kendetegnes ved at følge et antal særlige protokoller for datatransmission, og som admini-streres af en særlig administration, kaldet Internet Society.

Internet Society: Eller ISOC. Den centrale beslutningsinstans i Internet-samarbejdet.

Internet-browser: Edb-program, der finder hjemmesider på Internet, viser dem på brugerens skærm, og giver brugeren mulighed for at søge i og kommunikere fra og til disse.

Hjemmeside: Database, der er tilsluttet Internet, og som præsenterer sig i grafisk form i overensstemmelse med en af de standarder, der er vedtaget for Internet.

HTML: HyperText Mark-up Language. Standard for strukturering ("op-markering") af hypertekst. Anvendes bl.a. som grundlag for WWW-applikatio-ner.

HTTP: HyperText Transfer Protokol. Standard for, hvorledes information formidles via hypertekst-links. De WWW-adresser, der anvender denne standard, vil indbefatte denne forkortelse, f.eks. "http://www.lego.com".

Hypertekst: Tekst, der på grundlag af særlige koder og ved hjælp af dertil indrettet edb-programmel kan læses på anden måde end lineært, f.eks. ved spring mellem forskellige tekstafsnit m.v.

Hypertekst-link: Skaber en umiddelbar netforbindelse (Hypertekst-link) til en Homepage: Se Hjemmeside

ICC: International Chamber of Commerce - det internationale handelskammer. ICC er en privat sammenslutning bestående af handelskamre i 110 lande, der yder bistand og rådgivning til støtte for den internationale handel. Blandt ICC's bistandsydelser kan nævnes The International Court of Arbitration of the ICC, The ICC Institute of International Business Law and Practice og The ICC Counterfeiting Intelligence Bureau. ICC's rådgivningsydelser kommer først og fremmest til udtryk i en lang række publikationer og standardaftaler, bl.a. om voldgift og sikkerhedsstillelse.

Mus: Betegnelsen for edb-indlæsningsenhed på størrelse med en tændstikker-æske, 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 modsvarer de bevægelser, pilen foretager på skærmen.

Newsgroup: en diskussionsgrupper hvor net-brugere kan kommunikere med hinanden på et bestemt web-site, der har et bestemt emne-titel. Der findes mere end 10.000 forskellige grupper, der bruges til udveksling af tekster, lyd og billeder.

Online: Betegnelsen for den form for kommunikation, der foregår med samtidig frem- og tilbagesendelse af information. En tjenesteydelse, der tilbydes online (f.eks. billetbestilling), kendetegnes således ved, at brugeren umiddelbart får en fuldt opdateret information. I modsætning hertil står tjenesteydelser, der baseres på data, der er adskilt fra deres kilde, f.eks. når disse data lægges ned på en CD-ROM.

Pay-per-view: Tjenesteydelse, der giver forbrugeren mulighed for at vælge, hvilke tv-udsendelser, han vil se, og kun betale for dem. Grundlaget for valget ligger i brugerens mulighed for gennem kryptering at låse op for bestemte dele af et krypteret programudbud.

PCP/IP: Transmission Control/Internet Protocol. Grundstammen for Internet-kommunikation. Protokollen benytter sig af såkaldt "packet-switching": Hver meddelelse ("brev") deles op i et antal mindre meddelelser ("postkort"), der herefter postes 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, kan det tænkes, at nogle postkort må komme frem via andre routere. Først når postkortene er samlet ved modtageren, samles de, så det oprindelige brev igen dannes.

PICS: Platform for Internet Content Selection. Fremgangsmåde til "varedeklaration" af hjemmesider m.v. på Internet. Idéen er, at brugeren (f.eks. af hensyn til børnenes Internet-anvendelse) indstiller sin **Internet-browser** til kun at kunne modtage PICS-varedeklarerede hjemmesider. PICS tilbyder herefter en mulighed for at give forskellige labels til en hjemmeside, alt efter dennes indhold.

Protokol: Betegnelse for det sæt af regler, som må iagttages for at gennemføre en kommunikationsproces mellem to edb-systemer eller moduler, og som angiver betingelserne for, hvornår hver af disse enheder kan påbegynde en transmission, henholdsvis er klar til at afsende eller modtage data.

Public Key Krypteringssystem: Krypteringssystem, der bygger på asymmetrisk kryptering. De kommunikerende parter er hver udstyret med to nøgler, der (i kraft af visse printalsmekanismer) 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.

Router: Betegnelse for computer, der er bygget til at kunne modtage og afsende pakker af data, der sendes via Internettet.

RASAC: Recreational Software Advisory Council. Foreningen, der arbejder for udvikling af frivillige rating af hjemmesider. Som grundlag herfor udfylder informationsudbyderen et spørgeskema, hvorpå der svares ja/nej på en række spørgsmål.

SET: Secure Electronic Transactions, internationalt vedtaget standard for udveksling af information vedrørende betaling og aftaleindgåelse m.v. via Internettet. Standarden, der er udviklet i et globalt samarbejde mellem blandt andre IBM, Microsoft, MasterCard m.fl., anvender teknikker til kryptering og digital signatur.

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

TEDIS: Trade Electronic Data Interchange Systems. EF-Kommissionens program for udbredelsen af **EDIFACT**.

UNCITRAL: UN Commission for International Trade Law. Stående kommission under FN's generalforsamlings 6. udvalg, der arbejder med kodificering af den internationale handelsret.

Video on Demand: Informationssystem, der giver brugeren mulighed for at vælge de programmer, han ønsker at se, inden for et katalog af programmer, der tilbydes permanent. Teknologien, der endnu ikke er bragt i anvendelse herhjemme, giver informationsleverandøren mulighed for at optræde på samme måde som en videoudlejer. Begrebet ligner meget "Near Video on Demand", hvor de forskellige udsendelser sendes ud med vekslende mellemrum for herefter at blive lagret i takt med brugerens behov.

Værtscomputer: Se **host**.

WIPO: World Intellectual Property Organization. Specialized Agency under FN, der arbejder med immaterialret.

World Wide Web: (også kaldet WWW). Det verdensomspændende "spindel-væv", der via Internettet forbinder et antal computere (som servere) på nettet og ved hjælp af grafisk repræsentation af data stiller information til rådighed for enhver bruger, der forsynet med en **browser** kan springe fra database til database.

W3C: En global sammenslutning af mere end 150 medlemsvirksomheder bistået af et sekretariat på ca. 30 medarbejdere. W3C blev oprindeligt etableret

i USA, men har nu - bl.a. med støtte fra EU-Kommissionen - fået medlemmer
i Europa, Australien og ASEAN-landene.

Forkortelser

aftl. Aftalelov, lovbekendtgørelse nr. 781 af 26. august 1996.

CLSR The Computer Law and Security Report (tidsskrift).

FSÅB Forbrugerstyrelsens årsberetning.

kbl. Lovbekendtgørelse nr. 28 af 21.1. 1980 om køb som ændret ved lov nr 733 af 7 december 1988, lov nr 271 af 2. maj 1990, lov nr. 1098 af 21 december 1994 og lov nr. 391 af 14. juni 1995.

mal. Medieansvarslov. Lov nr. 348 af 6. juni 1991, som ændret ved lov nr. 1065 af 23. december 1992 og lov nr. 1208 af 27. december 1996.

NÅR Nordisk Årbog i Retsinformation.

mfl. Lov om markedsføring, jf. lov nr. 428 af 1. juni 1994.

ophl. Lov om ophavsret nr. 395 af 14. juni 1995.

strfl. Staffeloven, jf. lovbekendtgørelse nr. 886 af 30. oktober 1992 med senere ændringer.

Litteraturliste

Mads Bryde Andersen: Lærebog i edb-ret (1991)

Jørgen Blomquist: Overdragelse af ophavsrettigheder (1987)

Dansk EDI-Råd: Hindringer for anvendelse af Elektronisk Kommunikation, herunder EDI (Electronic Data Interchange) (februar 1995)

Eivind Einersen: Elektronisk aftale- og bevisret (1992)

Eivind Einersen: Aftaleindgåelse i net. NÅR 1996.81 ff.

European Monetary Institute: Report to the Council of the European Monetary Institute on Prepaid Card (1994)

Susanne Karstoft: Elektronisk dokumentudveksling - retlige aspekter (1994)

Birgitte Kofod Olsen i U1994B.395 ff.

Kommissionen for de Europæiske Fællesskaber: KOM(95)

Ian J. Lloyd: Liabilities for the Contents of On-line Services. International Journal of Law and Information Technology, Vol. 3, no. 3, p. 273 ff.

Chris Reed: Digital Cash and Internet Payment Systems (paper presented at CLA/IFCLA conference, Bruxelles, June 1996)

Matti Rudanko: Den elektroniske marknad - konsumentens skydd. NÅR 1996.59 ff.

Graham J.J. Smith: Internet Law and Regulation - A specially commissioned Report. Bird & Bird (1996)

Jan Thorndal: Småpengekort. Danmarks Nationalbanks kvartalsoversigt - august 1994, s. 26-31.

Olov Thorvund: Elektronisk marked - særlig om betaling. NÅR 1996.93.