EDB-strafferet

2. rev. udg.

Af Vagn Greve

Jurist- og Økonomforbundets Forlag

EDB-strafferet
2. reviderede udgave

Bogen er sat med Times af Inger Hansen Fotosats, Græsted
og trykt hos Mogsø ApS, København
Omslaget er tilrettelagt af John Back
Printed in Denmark 1986.
ISBN 87-574-4452-8

Forord

Denne lille bog handler om de strafferetlige problemer, der kan opstå i forbindelse med brug og misbrug af edb. Den er baseret på et manuskript, som blev udarbejdet til et DJØF-kursus i edb-ret. Jeg har søgt at skrive den på en sådan måde, at også ikke-jurister skulle kunne finde rundt i den; men må straks erkende, at det ikke er lykkedes overalt. Men viljen har været der.

De store ændringer i lovgivningen, som blev gennemført i foråret 1985, har gjort det nødvendigt at foretage en gennemgribende revision. 2. udgave adskiller sig derfor meget betydeligt fra 1. udgave.

For udarbejdelse af registre og foretagelse af citatkontrol takkes Lene Kielgast.

Kriminalistisk Institut
1. marts 1986 *Vagn Greve*

Indhold

I. Indledning

A. Kriminalitetens omfang

Edb-kriminalitet står i en særlig glans i offentlighedens øjne og avisernes beskrivelser. Omtalen er tit præget af den samme uvirkelige science fiction stemning, som findes i James Bond film. Den amerikanske pseudo-faglige litteratur, som dominerer markedet, har samme grundtone. *Svindlerne* beskrives som unge, højtbegavede og veluddannede mænd, der ved hjælp af et formidabelt herredømme over mystiske, skinnende, blinkende og ærefrygtindgydende maskiner får millionerne til at rulle ind på deres bankkonti. Deres bestjæling af samfundets magtfulde pengeinstitutter og kæmpeforetagender sammenlignes med Robin Hoods plyndringer af rige prælater og skatteopkrævere. Afstanden mellem sådanne lovbrydere og de gemene forbrydere understreges ofte. I de empiriske beskrivelser er der dog næppe noget, som tyder på, at de adskiller sig væsentligt fra underslæbere og andre »white collar« forbrydere. En svensk undersøgelse fandt, at de mest markante forskelle var, at de edb-kriminelle meget hyppigere var kvinder, og at de var noget yngre (Artur Solarz 1985 s. 17 og 83 ff.).

I de senere år ses desuden en ganske anden type personer i sagerne. Det er helt unge, som er vokset op med og som lever deres ganske liv i datamaternes verden. Hvor andre unge laver deres drengestreger på gaden, laver de deres ved maskinen. Når de går på opdagelse, er det i fremmede systemer etc.

Eksempel 1: To norske drenge på 13 år indrykkede en falsk bryllupsannonce i en norsk avis ved at bryde ind i bladets edb-system gennem deres hjemmedatamat. Den ene af de »nygifte« var drengenes skolelærer. (Politiken 1985-05-26).

Ingen bestrider, at edb-kriminalitet findes. Men hvor udbredt og omfattende er den? De fleste *skøn over omfanget* hidrører fra folk, der ved hjælp af skrækhistorier søger at sælge sikkerhed inden for edb-branchen. Viden om tyveriers udbredelse bør næppe hentes ukritisk hos forsikringsagenter og sælgere af tyverialarmer. Ligeså på dette område. Vi har da heldigvis også andre kilder. Siden 1958 skal der være registreret ca. 1000 sager – kriminelle og ikke-kriminelle – ifølge en international oversigt udarbejdet af en usa-ner, som længe har beskæftiget sig med området (Donn B. Parker 1983 s. x). Når man betænker dataanlæggenes store udbredelse i dag, er dette tal

meget lille. Forfatteren er knyttet til et vigtigt forskningscenter på det kendte Stanford Universitet, så man burde kunne gå ud fra, at hans adgang til at indsamle oplysningerne har været særdeles god. (Se nedenfor om metoden). Konklusionen synes at måtte blive, at den registrerede edb-kriminalitet er uforståelig sjælden. Og hans definition er endda så vid, at der blandt andet indgår en jugoslavisk sag i materialet, hvor fem studenter trykkede regeringskritisk materiale på et dataanlæg (John K. Taber 1980 s. 292). Sammenhold hermed, at en svensk undersøgelse viste, at en stor del af datakriminaliteten vedrørte tyverier af »datorutrustning« (Hans Wranghult 1983 s. 566). Dermed rører vi ved et meget væsentligt problem. Der findes ingen almindelig anerkendt definition af edb-kriminalitet. De fleste synes dog at anvende meget brede *definitioner,* så det snarere er for meget end for lidt, som kommer med.

Det danske straffelovråd definerer »den egentlige datakriminalitet« som »de strafbare handlinger, der rummer en anvendelse af den for databehandling særegne teknik med hensyn til registrering, opbevaring, bearbejdelse og brug af oplysninger« (strl.bet. 1985 s. 8 og 14 f.). Samtidig forudsættes det, at der også er andre former for datakriminalitet. Det svenske politi har anvendt følgende definition: »ett brott som genomförts mot eller med hjälp av ett datasystem av någon som därvid utnyttjat sina kunskaper i datateknik eller sin kännedom om det aktuella systemet« (Polisens åtgärder mot datakriminalitet s. 6 og 24 ff., spec. s. 33). Den svenske kriminolog A. Solarz bruger denne: enhver kriminalitet, som har tilknytning til datoriseret informationsteknik (1985 s. 14 og 37 ff.). Stein Schjølberg beskriver datakriminalitet som »kriminalitet hvor utnyttelse eller bruk av datateknologi har vært vesentlig ... og som omfatter handlinger som ... bør være straffbare« (1984). Nogle foretrækker i stedet eller desuden at tale om f.eks. computerrelateret kriminalitet. Det gør næppe nogen forskel i denne sammenhæng.

Det er ikke nødvendigvis den samme definition, som det er hensigtsmæssigt at anvende ved afgrænsningen af en bogs emne (som her), i det lovforberedende arbejde, i analysen af politiets behov eller som enhed i kriminalstatistikken. Det kriminologisk og kriminalpolitisk interessante er imidlertid, at uanset hvilken definition, som er blevet lagt til grund, er de vederhæftige skøn over edb-kriminalitetens omfang overraskende små.

Det hævdes ofte, at der er ca. 10 *domme* om året i Danmark (f.eks. Politiken 1984-01-30). Jfr. også strl.bet. 1985 s. 16. Den svenske rigspolitistyrelse kender ca. 5 sager om året fra perioden 1977-83 (Artur Solarz 1985 s. 75 f.). Solarz har selv fundet et betydeligt større antal sager ved en systematisk gennemgang af svensk domsmateriale, men tallet er stadigt lille og definitionen vid (1985). De enkelte sager rummer ofte flere forhold. I »Polisens åtgärder mot datakriminalitet« omtales 33 sager med i alt ca. 400 forhold (s. 6).

Der ses ingen danske undersøgelser over *mørketallet* på edb-området. Kim Eplov har anslået, at én ud af 10 danske dataforbrydelser meldes til politiet. Grundlaget for dette skøn fremgår ikke af artiklen. (Politiken 1984-01-30). I U.S.A. cirkulerer lignende tal. U.S.A.s National Center for Computer Crime Data går dog endnu længere og anslår, at kun 1% af bedragerierne opdages (Flemming Berg 1984). Fra andre områder af kriminologien ved vi, at sådanne gætterier er totalt upålidelige, medmindre der foreligger et empirisk grundlag. Ingen af de nævnte giver nogen form for begrundelse for overslagenes størrelse.

Alt andet lige må man antage, at de store edb-forbrydelser bliver *opdaget* hyppigere - relativt set - end de små. Ved revisioner af regnskaber, lageroptællinger o.s.v. vil et kraftigt »svind« let eller i hvert fald lettere kunne opdages. Der ses ikke tilstrækkelig årsag til at tro, at de store svindlere er så meget dygtigere til at skjule sporene end de små, at dette kan opveje de andre faktorer.

Der kan også være grund til at formode, at de store snarere vil blive *meldt* til politiet. Vi ved, at en del (andre) berigelsesforbrydelser ikke anmeldes, hvis lovovertræderen eller familien betaler erstatning. Det fremgår således af U 1976.604 Ø, at postgirokontoret først meldte en person, som havde tilsvindlet sig mere end 200 000 kr., da han misligholdt en afdragsordning. Det samme er formentlig tilfældet her. Det vil hyppigt være umuligt for den helt store svindler at betale erstatning. På den anden side kan det meget vel tænkes, at det kan være lettere for en højt placeret ansat at slippe med en afskedigelse, end det vil være for den meget underordnede. For eksempel kan firmaet have en større interesse i at handle med disse; lovovertræderen kan slippe med afskedigelse mod at lægge alle kort på bordet o.s.v. Der er også andre forhold, som kan begunstige chefgruppen. Men inden for hver enkelt gruppe, må det være mest sandsynligt, at de store hyppigere anmeldes. Det giver som det samlede resultat, at det snarere vil være de store, som meldes til politiet, kommer for retten o.s.v. (Jfr. også Artur Solarz 1985 s. 21). På en stor engelsk konference oplyste halvdelen af deltagerne, at deres firma ville foretage politianmeldelse (Computer Crime needs international countermeasures s. 3).

I denne forbindelse bør det fremhæves, at mørketallets størrelse afhænger af mangt og meget i det pågældende land. Det gøres fra forskellig side gældende, at en usa-nsk bank aldrig offentligt ville vedgå, at den var blevet snydt. Det er næppe sandsynligt, at danske banker uden videre (altid) vil vige tilbage fra at melde en kasserers underslæb eller en kundes bedrageri o.s.v. En ny svensk undersøgelse viste, at mere end 1/3 af de dataforbrydelser, som indgik i undersøgelsen, var anmeldt til politiet af en bank (Artur Solarz 1985 s. 21 og 134). I denne forbindelse kan forsikringsselskabernes

holdning til politianmeldelser blive ganske afgørende. Den nye datamisbrugsforsikring, som kan tegnes hos Baltica, giver udtrykkeligt forsikringsselskabet ret til at kræve politianmeldelse.

Der findes mig bekendt ingen danske undersøgelser af *tabet* ved edb-kriminalitet. Donn B. Parker analyserede alle de af ham kendte tilfælde i U.S.A. fra begyndelsen af 1960-erne til midten af 1970-erne (1976). I det sidste år i hans undersøgelse var der 59 sager, som i alt medførte et tab på $ 6,21 mio., svarende til gennemsnitligt ca. $ 100 000. Hans materiale er imidlertid i vidt omfang registreret ud fra avis- og tidsskriftsudklip, og de vil selvfølgelig fortrinsvis omhandle de spectacle sager. Der var på ingen måde en klar tendens (stigning/fald) i udviklingen gennem årene. - Den usa-nske regering undersøgte i 1976 arkiverne i de 10 vigtigste »agencies« et godt stykke tilbage. Blandt disse »agencies« var militæret, socialforsorgsområdet, »Internal Revenue Service« og FBI. Den fandt i alt 69 tilfælde. De samlede økonomiske skader blev opgjort til $ 2,6 mio. Halvdelen af sagerne vedrørte beløb under $ 6749 (John K. Taber 1980 s. 282). Disse tal skal ses på baggrund af, at man regner med, at der alene i U.S.A. i 1975 var 150 000 datamater, og at 2¼ mio. personer havde en direkte arbejdskontakt med dem (Krister Malmsten 1979 s. 253 f.). U.S.Secret Service har opgivet, at gennemsnittet af de 150 sager, som den kendte til, var ca. $ 4 000 (Polisens åtgärder mod datakriminalitet s. 7). - I Donn B. Parkers seneste bog er der kun 42 sager fra 1980 og 16 fra 1981 (1983 s. 26). På den baggrund og ud fra rimelige formodninger om mørketallets størrelse virker en del påstande og gætterier om de årlige tab aldeles utroværdige. FBI påstår, at der årligt begås datasvindel for 3 mia. dollars (Politiken 1984-01-02), Stein Schjølberg nævner muligheden af 1 mia. dollars om året i U.S.A. (1980 s. 441), og en repræsentant fra Interpols sekretariat hævder, at der i U.S.A. årligt anmeldes edb-forbrydelser for $ 100 mio. (J.N. Meetarbhan 1983). (Se hertil Ulla Høg 1981). På den anden side oplyser Interpols generalsekretariat, at det overhovedet ikke modtog nogen indberetning om edb-kriminalitet i 1983 (International Criminal Police Review 1984.278). Artur Solarz har beregnet det gennemsnitlige udbytte i sit materiale af underslæb m.m. til godt 200 000 s.kr. (1985 s. 81), svarende til et årligt beløb på over 3 mio. s.kr. Det samlede beløb kan givet et indtryk af edb-kriminalitetens omfang. Derimod har gennemsnitstallet en meget lav informationsværdi. Hans materiale blev fundet ved en gennemgang af de grove tilfælde af 'förskingring' (underslæb), hvilket selvfølgelig kan sætte gennemsnitsudbyttet betydeligt i vejret. Smh. også Report on Computer Crime 1984.

Konklusionen af dette synes at være, at der begås forbavsende få edb-forbrydelser, men at nogle af dem medfører meget store tab for ofrene, således at det alene af den grund er rimeligt at interessere sig for dette område – såvel kriminalpræventivt som strafferetligt.

Fremtiden er usikker. Antallet af personer med kendskab til edb og med adgang til datamater er stærkt stigende. I Danmark var der i 1979 ca. 5 terminaler for hver 1000 ansatte; i 1987 forventes tallet at være mere end 3 gange større (Artur Solarz 1985 s. 29). Robert Courtney har talt om, at en sådan udvikling medfører »the democratization of white-collar crime« (Donn B. Parker 1983 s. 103). Når mulighederne for at begå en form for kriminalitet øges, ses der hyppigt en forøget kriminalitet. Samtidig er der dog i de senere år blevet indbygget større sikkerhed i systemerne. Vi ved ikke, om dette vil kunne opveje eller sågar overveje betydningen af de i andre henseender øgede muligheder.

Underslæb, mandatsvig, bedrageri o.s.v. må i fremtiden i et vist omfang begås ved hjælp af edb. Når »nøglen til pengeskabet« er tastaturet på et edb-anlæg, vil det blive brugt, når svindelen skal begås. Derved vil den tekniske udvikling næsten uvægerligt medføre en forøgelse af edb-kriminaliteten. På den anden side er der måske grund til at tro, at antallet af traditionelle underslæb, arbejdspladstyverier o.s.v. vil falde. Når penge erstattes af plastkøbekort, svinder muligheden for gammeldags tyverier og røverier. Personer, der ikke kender til edb, har ikke længere de samme kriminelle muligheder. På den anden side vil visse edb-færdigheder blive lige så udbredte, som en del basal viden er i dag. Artur Solarz fandt i sin svenske undersøgelse, at gerningspersonerne typisk ikke var højt kvalificerede dataeksperter, men terminaloperatører med et vist kendskab til systemet (1985 s. 20). Igen må vi sige, at det er umuligt at forudse, om edb-teknik totalt set vil vise sig at være kriminalitetsøgende eller -begrænsende.

Nogle erfaringer synes at vise, at når en person med held har udtænkt og gennemført en edb-forbrydelse, vil der være et kraftigt invitament til at prøve på ny. Det kan tale for, at der formentlig hyppigt vil være et større antal forhold (eller en 'fortsat forbrydelse') hos den enkelte lovovertræder i fremtiden. Det synes bekræftet gennem Solarz undersøgelse. Tilsvarende kan forekomme på andre kriminalitetsområder, men edb-området adskiller sig fra disse, ved at den nye situation ofte vil være fuldstændig lig den tidligere.

Derimod hævder Donn B. Parker - på yderst spinkelt grundlag - at edb-forbryderne meget sjældent recidiverer (1983 s. 105 f.).

B. Edb og den danske strafferet

I datamaternes barndom var der ingen grund til at diskutere de særlige juridiske problemer. Senere blev man angst for »registersamfundets« uhyggelige muligheder for at udvikle sig til et orwellsk 1984. De første love på om-

rådet drejede sig derfor meget naturligt om grænserne for edb-registreringer af borgernes privatliv og om tavshedspligten for personalet i datacentralerne. Med den tekniske udvikling har datamaterne og deres udløbere, terminalerne, spredt sig. Først til banker og andre storforetagender, siden ud i de små håndværksvirksomheder og hjemmene. Det har skabt muligheder for nye former af berigelsesforbrydelser, og har på det seneste foranlediget gennemførelsen af straffelovsændringer på bedrageriområdet m.m. (Lov om ændring af straffeloven nr. 229 af 6. juni 1985).

I udlandet er der også fremkommet speciallove på en række områder, hvor det endnu ikke er blevet anset for nødvendigt her. Denne tilbageholdenhed skyldes ikke, at den strafferetlige lovgivning i øvrigt er så moderne, at der er blevet taget hensyn til sådanne spørgsmål. Tværtimod er kernen så gammel, at det ville have krævet clairvoyance at gøre dette. Grunden til, at der ikke er fremkommet flere lovforslag, er, at de almindelige, generelt formulerede regler formodes at kunne dække de tilfælde, hvor der i praksis vil vise sig et strafbehov.

I det følgende vil jeg på grundlag af den eksisterende litteratur om edb-svindel prøve at skitsere, hvilke situationer der vil kunne komme til bedømmelse. Det vil i et vist omfang ske ved hjælp af udenlandske eksempler. Derpå vil jeg søge at rubricere situationerne i den danske forbrydelseskatalog. I det omfang der ikke er særregler, må de almindelige bestemmelser fortolkes. Grænserne for tolkninger afstikkes som altid af strl. § 1, der forbyder udvidelser, der går længere end til lovbestemmelsens fuldstændige analogi.

I det følgende omtales fremmed ret i et vist omfang. Det er dels til orientering for personer, som har kontakt med virksomheder i udlandet, dels for at antyde, hvad der kunne overvejes retspolitisk. Løsningen i f.eks. usa-nsk ret har i sig selv næsten aldrig interesse for fremstillingen af gældende dansk ret. På dataområdet er der dog større grund end ellers til at skabe overensstemmelse med udenlandsk ret. Edb-kriminalitet vil formentlig ret hyppigt have internationale træk. Det er i så fald vigtigt, at det let kan konstateres, om forholdet er strafbart i begge (alle) landene. Det har betydning for gennemførelsen af udleveringssager og ved afgørelsen af om danske domstole er kompetente (strl. § 7, stk. 1, nr. 2).

Systematikken har taget udgangspunkt i situationerne og ikke i reglerne. Det betyder, at der er ret mange krydshenvisninger og nogen dobbeltdækning. Til gengæld skulle det gøre bogen lettere at anvende for brugerne.

Litteraturen fra udlandet er meget omfattende. Det meste af den ikke-nordiske litteratur har kun ringe interesse fra en strafferetlig synsvinkel. En

sober fremstilling af misbrugsformerne findes i Adrian R.D. Norman 1983. I øvrigt kan Ulrich Sieber 1980 fremhæves.

Fra de øvrige nordiske lande er der kommet vigtige betænkninger inden for de sidste år. Af litteraturen vil den danske læser formentlig have størst interesse af at begynde med Krister Malmsten om Sverige, Lauri Lehtimaja om Finland og Stein Schjølberg om Norge for så vidt angår edb-straffe-retten i snæver forstand.

II. Den egentlige edb-kriminalitet

Den egentlige edb-kriminalitet er rettet direkte mod selve edb-systemet (datamat, programmel, lagrede data og transmissionsledninger m.m.). Angrebene kan have karakter af ødelæggelse, kopiering og tilegnelse. Eftersom angrebsobjektets art kan være afgørende for den retlige bedømmelse, må de fire dele af edb-systemet behandles hver for sig.

Hvis et angreb samtidig rammer flere dele, f.eks. hvis datamaten sprænges i luften sammen med programmel og data, må det først undersøges, om angreb på de isolerede led ville have ført til bedømmelse efter samme bestemmelse. I så fald vil der som udgangspunkt foreligge én 'enhedsforbrydelse'. Hvis de isoleret set ville have ført til forskellige rubriceringer, må det i den givne situation afgøres, om der foreligger 'idealkonkurrence', så alle (flere af) bestemmelserne skal citeres, eller om en eller flere af dem absorberer en eller flere af de andre. Det får betydning for strafudmålingen (strl. § 88), forældelsesreglerne (strl. § 93, stk. 4), dommens retskraft m.m. (Jfr. Hurwitz: Alm. D. s. 11 ff.).

A. Datamaten m.m.

Datamater (datamaskiner, »computers«, »elektronhjerner«) er en slags maskiner. Inden for datalogien benyttes f.eks. definitioner som: maskine, der kan udføre udskiftelige programmer. Der findes ingen autoritativ definition i dansk ret, og det har hidtil heller ikke været nødvendigt at prøve at opstille en sådan. Ved straffelovsændringen i 1985 indføjedes der bestemmelser, som dels talte om »databehandlingsanlæg« (§ 193), dels om »anlæg til elektronisk databehandling« (§ 263). Andre paragraffer forudsætter sådanne anlæg, jfr. § 279 a (»elektronisk databehandling«). Disse bestemmelser gør det nødvendigt at foretage nogle afgrænsninger. Lovforarbejderne rummer ikke mange relevante bidrag til dette. Sprøgsmålene er henskudt til besvarelse i retspraksis, som formentlig vil lade dagligsproget være afgørende. Umiddelbart er der grund til at tro, at de ovennævnte udtryk i §§ 193, 263 og 279 a skal forstås på samme måde, til trods for forskellene i formuleringerne.

Ved afgørelsen kan der hentes en vejledning i strl.bet. 1985 s. 11 ff., hvor Straffelovrådet beskriver de indretninger, som det har i tankerne. En vis inspiration kan også findes i en us-amerikansk legal definition:

»... udtrykket 'datamat' omfatter elektroniske, magnetiske, optiske, elektrokemiske og andre meget hurtigt arbejdende databehandlingsanlæg, som udfører logiske, aritmetiske eller oplagringsfunktioner; det omfatter ethvert datalagringsanlæg og datakommunikationsanlæg; det omfatter ikke automatiske skrivemaskiner eller sættemaskiner, ej heller lommeregnemaskiner eller andet lignende udstyr.« (Min oversættelse fra Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 § 1030 (e)).

»Oxford Dictionary of Computing« (1983) definerer en computer som et »device or system that is capable of carrying out a sequence of operations in a distinctly and explicitly defined manner«.

I det følgende er udgangspunktet for tanken de større anlæg, men hovedparten af det sagte gælder også for de mindre og mere »målrettede«.

1. Tilegnelse, ødelæggelse m.m.

Datamater adskiller sig som udgangspunkt ikke i strafferetlig henseende fra de maskiner, som vi i øvrigt omgiver os med. Det særlige ved hine er blot, at de ad elektronisk vej behandler data. De regler, der gælder om dispositioner over skrivemaskiner, fjernsynsapparater, biler o.s.v., kan også bruges her. Med den tekniske udvikling indeholder de i øvrigt allerede i dag hyppigt »chips« etc.

Tilegnelse af datamater eller edb-udstyr kan være *tyveri* (strl. § 276) eller *underslæb* (strl. § 278) (strl.bet. 1985 s. 30 f.). Disse forbrydelser har en voksende betydning. Fra 1982 til august 1984 blev der i Sverige registreret 300 sådanne tyverier med en samlet værdi af 11 mio. s.kr. (Polisens åtgärder mot datakriminalitet s. 6).

Ødelæggelse skal normalt straffes som *tingsødelæggelse* efter strl. § 291 (strl.bet. 1985 s. 36 f.).

Eksempel 2: En københavnsk direktør for et edb-firma er blevet sigtet for at have smadret dataskærme m.m. til en værdi af 5 mio. kr. (Politiken 1984-08-13).

Eksempel 3: En ansat ødelagde en datamat med sin skruetrækker for at få arbejde til overtidsbetaling. (Engelsk sag. Polisens åtgärder mot datakriminalitet s. 51).

2. Uvedkommendes brug af edb-systemet

a. Udfinding af kodeord

Så længe anvendelsen af maskinen forudsatte en direkte, nær fysisk kontakt, var sikkerhed et spørgsmål om dørlåse, vagthunde o.s.v. Med »fjernbetjening« over telefonnettet og indførelsen af tidsdelingssystemer

(»timesharing«) opstår der et behov for at beskytte anlægget og brugerne mod misbrug fra udenforstående eller andre brugere.

En del systemer er sikret mod uvedkommendes indtrængen og brug af anlægget på den måde, at der skal bruges et særligt kodeord (»pass word«, »feltråb«, kendeord, »nøgleord«), før maskinen fungerer. Det kan f.eks. være 8 selvvalgte og tilfældige bogstaver og/eller tal.

Der kan være en særlig kode for den enkelte kunde. I sådanne tilfælde vil det som regel være mest naturligt at se koden som kundens »ejendom«. Der kan også være en fælles kode for en gruppe eller alle kunder. I så fald vil det være mest naturligt at betragte den som »tilhørende« anlægget. Det kan eventuelt få en vis, om end mindre betydning for den retlige rubricering af krænkelsen af hemmeligheden. (Hvem er offeret for fredskrænkelsen og dermed påtaleberettiget? Etc.).

Hvis kendskabet til koden opnås *over telefonnettet* af en uberettiget person, som prøver sig frem, - en såkaldt »hacker« - overtræder denne *strl. § 263,* der blandt andet handler om at gøre sig bekendt med indholdet af en datamat. Jfr. nærmere nedenfor og s. 20 og 39 ff.

Der vil også kunne være tale om *strl. § 264, stk. 2 om industrispionage,* hvis kendskabet fås ved en husfredskrænkelse. Jfr. nærmere nedenfor 26 ff.

Såfremt personen har en arbejdsmæssig tilknytning til firmaet, kan det bedømmes som en overtrædelse af *markedsføringsloven,* jfr. nærmere nedenfor s. 28 ff.

»*Hæleri*« med hensyn til sådanne, ulovligt fremskaffede oplysninger er kriminaliseret. Ansatte m.fl., som på lovlig måde har fået sådan kundskab, gør sig også skyldig i et strafbart forhold, hvis de videregiver den. Jfr. nedenfor s. 31 f. Det hævdes, at 75% af de kodeord, som »hackerne« anvender, er overgivet til dem af medarbejdere ved virksomheden (Jan Carlsen 1984).

Hvis en udenforstående på lovlig måde har fået et sådant kendskab, f.eks. ved at høre medpassagerers samtale i et tog, er en videreudbredelse næppe altid en overtrædelse af strl. § 264 d om videregivelse af meddelelser vedrørende en andens private forhold. Under en eventuel straffesag må man så i øvrigt falde tilbage på at anse det som medvirken (til forsøg) på en eller anden forbrydelse, typisk en fredskrænkelse, et »brugstyveri« eller en berigelsesforbrydelse.

b. Brugen af kodeord

Gennem brugen af det rette kodeord »åbner« dataanlægget sig for den pågældende. En uberettiget person vil herved overtræde strl. § *263, stk. 2,* om »den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk data-

behandling«. Forbrydelsen er fuldbyrdet i samme øjeblik, der skabes forbindelse, på samme måde som en krænkelse af brevhemmeligheden fuldbyrdes ved opsprætningen af brevet. Bestemmelsen kræver forsæt. Det betyder blandt andet, at det ikke er strafbart at skabe forbindelse ved et uheld. Men det er i så fald strafbart efter den samme bestemmelse at opretholde forbindelsen, efter at det med sikkerhed eller med overvejende sandsynlighed er konstateret, at der er skabt adgang til oplysninger eller programmel, som den pågældende ikke er berettiget til at have adgang til. Straffen er bøde, hæfte eller fængsel indtil 6 måneder. Under særligt skærpende omstændigheder, f.eks. ved industrispionage, kan straffen stige til fængsel indtil 2 år. (Jfr. strl.bet. 1985 s. 22 ff.).

Ophavsretsloven giver ingen beskyttelse mod brugen af et fremmed kodeord (Jon Bing 1985 s. 41).

I avisdebatten har det været gjort gældende, at selve brugen af et kodeord skulle være en ulovlig brug, jfr. strl. § 293, stk. 1. Et sådant ord er imidlertid ingen »ting«. At maskinen giver adgang, gør ikke i sig selv anvendelsen af koden til et »brugstyveri« (§ 293, stk. 1). Det er ingen overtrædelse af denne bestemmelse at prøve sin bilnøgle i døren på en tilfældig fremmed bil, hvis man ikke vil gøre andet og mere.

Maskinen bruger eventuelt en minimal mængde strøm som reaktion på koden. Dette er ikke selvstændigt strafbart. Heller ikke efter strl. § 276, 2. pkt., om tyveri af energi. (Strl.bet. 1985 s. 30 f. og 34 f.; NOU 1985:31.16 og 19).

Hvis datamaten ikke tillader brugerne at »komme ind« uden at have identificeret sig med navn, kodenummer, arbejdsplads eller lignende, og en bruger har opgivet falsk identitet o.s.v., kan forholdet i usa-nsk ret bedømmes som 'forgery' (»falsk«) (Edward H. Coughran 1976 s. 9).

I det omfang adgangen skabes ved hjælp af et (falsk) 'credit card' (kontokort), kan der i U.S.A. eventuelt anvendes særlige 'credit card fraud sanctions' (straffe for kontokortsfalsk) (s.st.). Disse findes ikke i dansk ret. Her vil det også kun sjældent være muligt at bruge dokumentfalsk-bestemmelsen, medmindre den pågældende samtidig skriver f.eks. en kvittering under med det falske navn. I så fald er det imidlertid ikke naturligt at sige, at det er edbsvigen, som bedømmes som dokumentfalsk. Derimod kan brug af en tredjepersons (ægte) kort eventuelt straffes efter strl. § 174 om dokumentbestemmelsesmisbrug.

c. Brugen af maskinen m.m.

1°. Den *uberettigede brug* må som udgangspunkt straffes efter strl. § *293, stk. 1* (strl.bet. 1985 s. 33). At maskinen i sig selv er kostbar, gør ingen forskel. »Brugstyveri« af en supertanker eller en jumbojet er ligefuldt »brugstyveri«. At den uberettigede brug ikke udelukker en samtidig berettiget brug, kan ikke medføre, at forholdet falder uden for § 293, stk. 1. Det er ikke et led i denne bestemmelses gerningsindhold, at den berettigedes rådemuligheder skal indskrænkes gennem lovbruddet. Smh. hermed, at der kan begås »brugstyveri« med hensyn til en ting, der lovligt er i gerningspersonens egen varetægt.

Eksempel 4: En student brugte højskolens datamat, som var knyttet til en datacentral. Den pågældende havde manipuleret med tælleværket, så det registrerede for lidt eller slet intet. Dømt for 'olovligt brukande'. (Göteborg 1980. Polisens åtgärder mot datakriminalitet s. 43 f.).

Den nye bestemmelse i strl. § 263, stk. 2, omhandler kun fredskrænkelsen, ikke formuekrænkelsen (brugen). Hvis brugen sker ved hjælp af eget programmel og egne data, kan der kun straffes efter § 293. Hvis gerningspersonen også anvender offerets specielle programmel og data, kan begge bestemmelser bruges (sammenstød).

Nutidens store dataanlæg er meget kostbare i anskaffelse. Driften er derimod overordentlig billig. Flere personer kan anvende anlægget samtidig, og strømforbruget er minimalt. En datamat i år 1952 krævede lige så megen energi som et lokomotiv. Nutidens kræver ikke mere end en glødelampe. (Artur Solarz 1985 s. 27). »Skaden« (brugen) har derfor langt mindre betydning for offeret, end den tomme benzintank har i en normal bilbrugstyverisituation. Brugen af benzinen straffes ikke særskilt. Allerede af denne grund skal der heller ikke straffes særskilt for strømforbruget m.m. (Strl.bet. 1985 s. 34 f.).

Se om norsk ret NOU 1985:31.17, 18 f., 33 og 35.

Den nugældende svenske bestemmelse (BrB 10:7) om ulovlig brug kræver, at gerningspersonen har »annans sak ... i besittning«. Regeringen foreslår nu besiddelseskravet sløjfet for at kunne ramme al »tidsstöld« (lagrådsremiss 1985-09-19).

Efter usa-nsk ret kan brugen bedømmes som 'theft' (tyveri) (Model Penal Code 223.7 og Edvard H. Coughran 1976 s. 9), 'theft of services' eller 'interference with use' (Computer Crime s. 6 f. og 7 f.).

Eksempel 5: T fik fra sin telefon i hjemmet adgang til en regeringsdatamat i California i ca. 190 timer, svarende til en værdi af $ 2000. Under sagen blev det antaget, at »the consumption of computer time and the use of computer storage capacity were inseparable from the physical identity of the computer itself«, hvorfor den tiltalte havde krænket 'property', (Computer/Law Journal 1980.780). Tilsvarende den canadiske straffelovs § 287, hvorefter det er tyveri, hvis en person uberettiget bruger »a telecommunications service«. Det er klart - efter dansk ret - at datamaten er en ting (»property«); men det gør ikke brugen til et tyveri.

Der findes endvidere i U.S.A. særlige bestemmelser om 'wire fraud' (»telefonledningssvig«) over statsgrænserne (Computer Crime s. 12 f.).

I Virginia er »computer time« ifølge loven en ting i relation til tyveribestemmelsen.

I schweizisk ret taler man om 'Zeitdiebstahl' (tyveri af tid). Louis Rohner (1976) vil henføre dette under schweizisk StGB art. 143 om 'Sachentziehung' (d.v.s. unddragelse af en rørlig ting til skade for den berettigede). Dens nærmeste modsvarighed i dansk ret er strl. § 291 eller § 293, stk. 2. Rohner erkender dog samtidig, at denne subsumption kræver »eine extensive Interpretation der Tatbestandsmerkmale« (s. 28). I dansk ret ville udvidelsen ganske sprænge grænserne for de nævnte bestemmelser, allerede fordi den berettigedes brug ikke i sig selv nødvendigvis hindres af andres samtidige brug.

'Unauthorized use of a computer' er blevet foreslået særskilt kriminaliseret i Canada. Jfr. nærmere Christopher J. Millard 1985 s. 161 ff.

2°. Hvis den uberettigede gennem anvendelsen af en tredjepersons kodeord eller andre identitetsoplysninger giver maskinen »opfattelsen« af, at den arbejder for hin tredjeperson, vil *regningen* til tider blive udskrevet og sendt til tredjepersonen ganske automatisk. Denne vil muligvis lide et økonomisk

tab på grund af svindelen. Afgørende vil blandt andet være, om svindelen overhovedet opdages, eller om den blot skjules i det almindelige mellemværende. Og selv om den opdages, vil bevisbyrderegler, risikosynspunkter o.s.v. eventuelt kunne føre til, at der må betales for svindlerens misbrug. Nedenfor i afsnit III behandles spørgsmålet om, hvilke formueforbrydelser der kan tænkes anvendt, når berigelsen er det direkte mål. Tilsvarende vil kunne gælde, hvor berigelsen - som her - er et sekundært element.

En anden situation foreligger, når regningen ikke kan betragtes som reel, fordi der er identitet mellem »kreditor« og »debitor«, f.eks. to afdelinger af samme firma. I så fald bruges regningen alene som et bilag i den interne regnskabsføring. Der skal dømmes efter § 293 for den ulovlige brug, men ikke samtidig for en berigelsesforbrydelse.

Eksempel 6: I en californisk sag havde T tidligere været ansat i et firma. Han brugte dets filialers koder med den virkning, at filialerne blev »afkrævet« $ 15 000 for 143 timers drift.

Ovenfor omtaltes et helt tredje spørgsmål, da det blev nævnt, at edb-anlæggets ejer kun fik et minimalt tab ved en tredjepersons uberettigede brug. Til sammenligning kan nævnes, at en flyvebillet til New York er dyr, fordi maskine m.m. skal afskrives, men det direkte tab, ved at en blind passager skjuler sig ombord, er en ganske lille forøgelse af benzinforbruget. Det er ingen berigelsesforbrydelse, som den blinde passager begår - hverken på flyet eller på edb-anlægget - medmindre andre momenter kommer til.

3°. Hvis en vis brug er berettiget, men vilkårene ikke overholdes, kan den overskydende anvendelse være strafbar. Der må dog være et vist spillerum. Forholdet skal have nogen grovhed, før det bliver naturligt at supplere de civilretlige reaktioner på kontraktbrud med strafferetlige sanktioner. Dette kan også udtrykkes således, at fortolkning af lovregler, evt. *den almindelige retstridighedsklausul,* meget let kan føre til straffrihed i sådanne situationer. (Smh. Hurwitz: Alm. D. s. 8 f.).

Strl. § 293, stk. 1, om ulovlig brug kan også dække nogle situationer, hvor en lejer benytter en ting efter den aftalte periode.

Eksempel 7: T havde lejet en bil, som han beholdt nogle dage ud over lejeaftalen. Dømt efter § 293, stk. 1. (VLD 1971, Domme 1968-1972 s. 225).

Strl. § 298, nr. 4 i.f., handler om den, som »uden erlæggelse af den fastsatte betaling tilsniger sig adgang ... til benyttelse af anden almentilgængelig indretning«. Det forudsættes, at den pågældende ikke direkte har vildledt en kontrollør, idet det ellers vil (kunne) blive bedrageri (strl. § 279) (jfr. Hurwitz: Sp. D. s. 454 og Waaben: Sp. D. s. 159 f. og 171 f.).

Bestemmelsen stammer fra Torps udkast til en forseelseslov § 37 (strl.bet. 1917). Forarbejder, teori og trykt retspraksis er meget magre. Det er derfor noget tvivlsomt, hvad den dækker.

I denne forbindelse bliver det første spørgsmål, om en *indretning* kan være et edb-anlæg. Sprogligt er der ingen hindring herfor (jfr. ODS IX.422 1.2). I den givne sammenhæng ville det måske være nærliggende at kræve, at indretningen skulle være af en ikke helt ringe størrelse. Smh. at nr. 4 i øvrigt handler om forestilling, udstilling, forsamling og offentlig samfærdselsmiddel. Det synes dog ikke at være et tvingende argument.

I br-tysk ret findes der en noget lignende bestemmelse i StGB § 265 a om 'Erschleichen von Leistungen' (tilsnigelse af ydelser eller præstationer). Den handler blandt andet om tilsnigelse af adgang til en »Einrichtung«. Herunder hører f.eks. badeanstalter, museer, kuranlæg og betalingsparkeringshuse (Schönke-Schröder s. 1719). Den samme paragraf omhandler også automatmisbrug. Tilegnelse af ting fra automater var og er tyveri, men uberettiget brug af »Leistungsautomaten«, der spiller musik, viser billeder eller personvægt o.s.v. var tidligere straffri. Sådant misbrug blev derfor kriminaliseret ved en ændring af straffeloven. Tysk ret kan i det mindste tages til indtægt for, at der er en nær sammenhæng mellem de forhold, som givet behandles i strl. § 298 og nogle former for maskinmisbrug. Og med den nære sammenhæng og den sproglige mulighed må det nok antages, at danske domstole vil acceptere, at sådanne automatmisbrug henføres under § 298.

Den noget lignende bestemmelse i BrB 9:2 om 'bedrägligt beteende' ligestiller også automatmisbrug med forhold, der svarer til strl. § 298s. (Jfr. Nils Jareborg 1978 s. 182). (Den vil dog være umulig at anvende i de fleste af de her omtalte situationer, eftersom ydelsen skal »tilhandahålles under förutsättning av kontant betalning«).

Det næste spørgsmål bliver, hvad der skal forstås ved *almentilgængelig* i § 298. Den naturligste sproglige tolkning er, at alle skal have adgang (ODS I.461 ff.). Det kan dog næppe afvises, at det kan være nok, at en meget stor gruppe, f.eks. studenterne ved Københavns Universitet, har adgang.

Af dette vil det fremgå, at der er et uklart grænseområde mellem § 293 og § 298. Hvis retten til brugen er begrænset, vil § 293 eventuelt skulle anvendes. Hvis enhver har adgang til at bruge anlægget mod betaling m.m., men en person finder en måde at undgå betalingen på, må de nærmere omstændigheder afgøre, hvilken af bestemmelserne, der skal bruges. Smh. til illustration eksempel 4.

Se også NOU 1985:31.14 om anvendelsen af fredskrænkelsesbestemmelser i lignende situationer. S.st. foreslås en ændring af den til § 298 svarende bestemmelse i norsk strl. § 403, så den klart kommer til at omfatte edb-misbrug, jfr. NOU 1985:31.31 f. og 35.

4°. At *ansatte leger* med anlægget eller i øvrigt bruger det på anden måde, end det egentlig var meningen, forekommer nok ganske hyppigt. For at kunne straffe misbruget, må det kræves, at det er af en vis grovhed. Selv om to ansatte fordriver en pause i arbejdet med at sænke slagskibe, skrive julekort eller tegne Marilyn Monroe ved hjælp af edb-anlægget, er der ikke grundlag for at straffe. »Minima non curat praetor«. (Retsvæsenet skal ikke tage sig af bagateller). (Jfr. strl.bet. 1985 s. 33 f.). Det svarer til, at en kontorassistent skriver nogle privatbreve på arbejdspladsens skrivemaskine. Retlige reaktioner mod overdrevent brug, må - hvis de er nødvendige - som udgangspunkt findes i ansættelsesretten, erstatningsretten eller den øvrige civilret.

Hvis forholdet bliver særligt groft, f.eks. hvis en ansat *opbygger sin egen private, konkurrerende virksomhed* ved hjælp af den uberettigede brug af ansættelsesstedets datamat, kan der tænkes et strafansvar. Der vil dog kun sjældent være tage om en berigelse, som det vil være naturligt at føre ind under strl. kap. 28 om berigelsesforbrydelser (f.eks. § 280 om mandatsvig). Jfr. herved det ovenfor sagte om, at den ansattes brug af maskinen ikke direkte påfører ejeren noget tab. Udgangspunktet må også her være strl. § 293, stk. 1, om ulovlig brug. (Jfr. Ulla Høg 1981 s. 63). Hvis ansættelsen direkte er søgt med henblik på at gennemføre dette misbrug, kan der være tale om bedrageri i ansættelsessituationen (strl. § 279). Endvidere kan nogle af de konkurrenceretlige regler eventuelt bruges, jfr. nærmere nedenfor om markedsføringsloven.

Eksempel 8: I U.S.A. var 47 ingeniører udstyret med terminaler, der tillod dem at udføre beregninger og skitser. 16 af ingeniørerne påtog sig private opgaver, som kom til at omfatte en femtedel af maskintiden. Firmaet opgjorde sine skader til $ 2,8 mio. (Louis Rohmer 1976 s. 11).

3. Standsning af driften

1°. Hvis de centrale edb-systemer ikke fungerer, bliver store dele af det moderne samfund lammet. Ved ændringen af straffeloven i 1985 kriminaliserede man derfor i § *193* den situation, hvor der på retstridig måde fremkaldes *omfattende forstyrrelse i driften af databehandlingsanlæg.* (Jfr. strl.bet. 1985 s. 9, 40 ff. og 76 f.). Lovbestemmelsen stiller ingen krav til størrelsen eller karakteren af det beskyttede anlæg som sådant. Afgørende er dets betydning. Efter bestemmelsens placering i strl. kap. 21 om almenskadelige handlinger og efter forarbejderne til lovændringen skal der være tale om særlig vigtige databehandlingsanlæg. Straffelovrådet nævnte som eksempler på paragraffens anvendelsesområde angreb, der helt lammer eller i betydeligt omfang forstyrrer registrering, behandling og transmission af data inden for værdipapircentralen, kildeskattedirektoratet, politiets motorregister eller lignende. Til illustration af disses størrelser kan det nævnes, at værdipapircentralen gennemsnitligt behandler for 15 mia. kr. om dagen. (Politiken 1985-07-31). Inden for den private sektor blev der peget på tilsvarende forstyrrelser af den centrale elektroniske databehandling hos banker, sparekasser, realkreditinstitutter o.s.v. Bestemmelsen kan næppe bruges, hvis virkningerne alene føles inden for den pågældende virksomhed selv. Det er »almenskadeligt« at standse postgirokontorets arbejde, men ikke at tvinge Danfoss eller andre store virksomheder til at ophøre med produktionen. I sådanne tilfælde må de nedenfor omtalte bestemmelser bruges i stedet.

Bestemmelsen stiller ingen krav om brug af bestemte midler til at forårsage forstyrrelsen. Det er imidlertid ikke alle forstyrrelser, som er retstridige i denne sammenhæng. En standsning af driften, der er en følge af en lovlig (overenskomstmæssig) strejke, kan næppe straffes efter § 193. Det er derimod mere tvivlsomt, hvordan ulovlige (overenskomststridige) strejker skal betragtes. (Jfr. diskussionen i Komm. strl. II s. 184, Waaben: Sp. D. s. 222, FT 1984/85.10703 og B.1915 ff.).

Straffen er efter lovændringen i 1985 hæfte eller fængsel indtil 4 år eller under formildende omstændigheder bøde.

Uagtsomme overtrædelser straffes efter stk. 2 med bøde eller hæfte. (Jfr. strl.bet. 1985 s. 20). Under dette vil også kunne høre afbrydelser, som skyldes ødelæggelse af kabler under vejarbejde eller lignende. I praksis kan der kun forventes rejst tiltale i de særlig grove tilfælde, jfr. Komm. strl. II s. 185. En vis begrænsning kan også findes i de almindelige krav om adækvans.

Se også s. 44 ff. nedenfor.

Smh. NOU 1985:31.32 f.

2°. Det er kun de færreste anlæg, der er beskyttet af § 193, og de fleste forstyrrelser må derfor bedømmes efter andre regler.

Eksempel 9: Et firma i New York havde en central datamat, der hver nat over telefonnettet kaldte datamater i firmaets filialer og fik overspillet dagens regnskab, ordrer m.m. Under en strejke hos leverandøren af edb-systemet lod nogle ingeniører en anden datamat kalde nogle af filialernes datamater på et tidligere tidspunkt, end hovedsædets datamat skulle gøre det. Filialernes datamater fik den sædvanlige ordre om at afspille deres indhold. Ingeniørerne optog ikke dette. Virkningen var alene, at båndene kørte. Eftersom de ikke automatisk spoledes tilbage efter kørslen, var det ikke muligt for dem at aflevere indholdet til hovedsædets datamat, når denne på et senere tidspunkt kaldte og afgav den sædvanlige ordre. Efter fire ugers søgen efter »fejlen« lykkedes det at finde årsagen. Da offeret ikke ønskede tiltale rejst, skete der intet med ingeniørerne.

Eksempel 10: I en anden sag spillede nogle strejkende et kassettebånd over telefonen til firmaets kunder, så disses maskiner spyede dynger af ligegyldigt papir ud.

Det antages i den usa-nske strafferetlige teori, at det havde været muligt at straffe for 'aggravated harassment' (grov chikane) i disse tilfælde. Denne bestemmelse bruges ellers i almindelighed over for personer, der foretager obskøne telefonopringninger (Ulrich Sieber 1977 s. 93 og Donn B. Parker 1983 s. 229 f.). Vi har ingen tilsvarende bestemmelse i dansk ret. Sådanne telefonopkald straffes her efter nogle bestemmelser, der ganske ville savne mening i de nævnte sager, strl § 232 om blufærdighedskrænkelse eller § 265 om overtrædelse af polititilhold.

Eksempel 11: Et meget stort tysk firma havde dårlig plads i sine bygninger. En del arbejdere måtte gå gennem datacentralen på vej til og fra deres arbejdsplads. En af dem gjorde sig til vane at trykke på en bestemt knap, hver gang han passerede, for at genere. Det medførte, at datamaten standsede, og det tog hver gang flere timer at bringe anlægget i fuld gang igen. Dette anses for straffrit efter tysk ret. (Mohr 1984).

Situationen i eksemplerne kan anskues på to måder. For det første kan man se den således, at de pågældende uberettiget brugte fremmede maskiner. I så

fald vil strl. § 293, stk. 1, som nævnt ovenfor, kunne anvendes. Det er imidlertid en noget anstrengt subsumption. Formålet med det hele er jo ikke at bruge maskinerne, men at hindre andre i at gøre det. Det gør det nærliggende at overveje *strl. § 293, stk. 2.* Som nævnt nedenfor (s. 50 ff.), handler den om *hindringer for, at nogen udøver sin ret til at råde over en ting.* Under bestemmelsen hører blandt andet tilfælde, hvor gerningspersonen ved »Afspærring eller paa lignende Maade hindrer en anden i at *benytte* sin Raadighedsret« (Krabbe s. 722).

Overtrædelser af § 293, stk. 2, straffes med bøde eller hæfte eller under skærpende omstændigheder med fængsel indtil 6 måneder. En del kunne tale for, at denne strafferamme blev justeret, f.eks. således at den kom i overensstemmelse med strl. § 285.

Se også nedenfor om afbrydelser af datatransmissionen.

3°. Hvis en *operatør* ved fysisk magt eller grove trusler tvinges til at ophøre med sit arbejde, vil forholdet også kunne straffes efter *strl. § 260* om ulovlig tvang. De almindelige bestemmelser om legemsangreb, trusler på livet o.s.v. kan selvsagt også blive aktuelle i denne sammenhæng. Derimod er § 260 uanvendelig, hvis operatørens arbejde umuliggøres på grund af angreb rettet mod selve edb-anlægget.

§ 260 er efter sin placering i strl. kap. 26 begrænset til krænkelser af den personlige frihed til at handle. Den omfatter ikke egentlige angreb på personen selv eller på ting, selv om der herved sker en faktisk indskrænkning i personens handlemuligheder. (Smh. Komm. strl. II s. 283). Hurwitz fremhæver således, at en nedbrydning af en servitutindretning og lignende, der har karakter af en fysisk magtanvendelse, men som ikke involverer personlig overlast, falder udenfor. (Sp. D. s. 285. Ligeledes Krabbe s. 589. Men cfr. strl.bet. 1971 s. 221).

4. Kopiering m.m.

a. Industrispionage m.m.

1°. Opnåelse af viden om konkurrenters produktionsmetoder, konstruktioner o.s.v. er ikke i sig selv en krænkelse af interesser, der er beskyttet af strafferetten. Det afgørende for strafansvaret er i denne forbindelse ikke målet, men midlerne. Hvis kundskaberne opnås gennem læsning af faglitteratur, demontering af en datamat købt i den almindelige handel o.s.v., er dette fuldt lovligt. En fabrikant kan ikke - selv ikke ved udtrykkelige forbud - hindre andre i at *undersøge en købt maskine* indgående.

Hvis maskinen derimod er lånt, lejet, leaset o.s.v. er ejeren berettiget til at plombere den eller til at foretage andre foranstaltninger, som sammen med et klart og udtrykkeligt forbud vil kunne have den virkning, at en åbning og undersøgelse efter omstændighederne kan blive strafbar, f.eks. efter de nedenfor behandlede regler.

2°. Hvis kendskabet til konstruktionen fås gennem indbrudsvis tilegnelse af tegninger, komponenter m.m., er de almindelige bestemmelser i straffeloven om *tyveri, husfredskrænkelse m.fl.* selvfølgelig anvendelige.

Nedenfor s. 31 omtales særligt det tilfælde, at en af firmaets ansatte uberettiget bruger firmaets fotokopieringsmaskine til at kopiere tegninger m.m. med henblik på at tilegne sig fotokopierne. Det antages dér, at en sådan brug af maskinen og tilegnelse af produktet næppe i sig selv bør være tilstrækkelig til at statuere tyveri, når en affotografering med eget kamera og film ikke ville være det. (Smh. RT 1938/39 A. 3782).

En del kunne tale for at behandle den natligt indtrængende fremmede på samme måde i denne relation. Med de eksisterende strafferammer i strl. § 264, stk. 2, ville der ikke være betænkeligheder ved at lade denne bestemmelse absorbere det tvivlsomme tyveriansvar.

3°. *Straffeloven* indeholder i *§ 264, stk. 2,* en særlig regel om *industrispionage* og lignende. Paragraffen omfatter - efter ændringen i 1985 - det forhold, at en person »uberettiget« »skaffer sig adgang til fremmed hus eller andet ikke frit tilgængeligt sted« »med forsæt til at skaffe sig eller gøre sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder eller under andre særlig skærpende omstændigheder«.

Bestemmelsen omfatter kun uvedkommende personer, som fysisk skaffer sig ind i fremmede laboratorier, værksteder, kontorer m.m. Ansatte i firmaet og dets håndværkere skal i almindelighed bedømmes efter markedsføringsloven, jfr. nedenfor s. 28 ff. Efter omstændighederne kan dataenheden dog være så adskilt fra virksomhedens øvrige bygninger og rum, at strl. § 264 må anvendes på personale fra andre afdelinger. (Strl.bet. 1985 s. 24).

Besøgende og kunder er bevidst blevet holdt uden for begge sæt regler, fordi virksomheden har bedre muligheder for at beskytte sig mod, at sådanne personer misbruger besøget til at opnå kendskab til oplysninger og produktionsforhold, som firmaet ikke ønsker udbredt. Og under alle omstændigheder er det mest naturligt, at dette ses som firmaets eget problem og egen risiko. (FT 1971/72 A.563).

'Virksomhed' skal forstås som et vidt begreb. Straffelovrådet har formentlig forudsat, at den nye bestemmelse også lader sig anvende på foreninger og offentlige myndigheder (strl.bet. 1985 s. 24). Og hvis man kommer uden for virksomhedsbegrebets område, er det i hvert fald muligt at lade sådant være omfattet af den generelle regel om andre særligt skærpende omstændigheder i paragraffens slutning (s.st. s. 79).

Ved lovændringen i 1985 valgte Straffelovrådet bevidst at beskrive angrebsobjektet - »erhvervshemmeligheder« - på samme måde, som det er sket i markedsføringslovens § 9. (Jfr. strl.bet. 1985 s. 28 og nedenfor s. 28 ff.). En erhvervshemmelighed kan meget vel være den tekniske indretning af datamaten.

Se nedenfor s. 38 ff. om § 263, stk. 3, som normalt vil være udgangspunktet, når krænkelsen rammer programmel og data.

Forbrydelsen fuldbyrdes, når personen har skaffet sig adgang (med det videregående forsæt). Hvis det sker gennem smadrede ruder, opdirkede døre o.s.v., er det klart, at den pågældende har »skaffet sig adgang«. Hvis området er tilstrækkeligt afgrænset, kan det imidlertid være strafbart blot at gå derind (med det videre forsæt). En person, som går ind i en kontorbygning ad en dør, som han tilfældigt ser er åben, da han kører forbi om natten, kan også straffes for at have skaffet sig adgang. Med den anvendte formulering tilsigtede man endvidere at dække tilfælde, hvor personen kommer ind gennem et aktivt svigagtigt forhold, f.eks. hvis industrispionen udgiver sig for at være en tilkaldt reparatør eller vinduespudser. (Smh. U 1956.158 Ø, der endog vedrørte en ældre og snævrere formulering.) (Jfr. Straffelovrådets bet. 601/1971 s. 34 og 35.) Derimod er det ikke tilstrækkeligt, hvis personen blot fortier sin identitet eller baggrund og derfor får mulighed for at komme ind sammen med andre besøgende, f.eks. en skoleklasse på studiebesøg eller en rundskuedagsomvisning.

Bestemmelsen kræver forsæt, såvel til indtrængningen som til formålet.

Som nævnt flere gange, kan bestemmelsen også anvendes under andre særligt skærpende omstændigheder. Det vil f.eks. kunne blive aktuelt, hvis gerningspersonen har skaffet sig adgang til offentlige registre med henblik på at påføre offentlige eller private interesser betydelig skade, jfr. strl.bet. 1985 s. 79.

Straffen er efter lovændringen i 1985 bøde, hæfte eller fængsel i indtil 2 år.

Industrispionage har altid været af betydning for erhvervslivet. Et af de klassiske danske eksempler er brygger J.C. Jacobsens. Der er al grund til at tro, at industrispionage i fremtiden vil få voksende, og for mange virksomheder afgørende, betydning for overlevelses- og vækstmulighederne. Nutidens produktudvikling stiller meget store krav til personalets kvalifikationer og til virksomhedens økonomiske ressourcer. Samtidig løber den tekniske udvikling så hurtigt, at selv særdeles veletablerede firmaer på forbavsende kort tid kan sakke bagud. Industrispionen skaffer viden om konkurrenternes produktions- og markedsforhold, om deres fremtidige produkter og reklamefremstød o.s.v. Dette er ikke blot teoretiske muligheder. I Sverige har man spurgt 1560 virksomheder, om de havde været udsat for industrispionage. 206 vidste, at de havde været det. Sovjetunionen vurderede selv værdien af sin industrispionage i 1980 til mere end 400 mio. rubler sparet i udviklingsudgifter, svarende til ca. 4 mia. kr. I 1976 ansloges værdien til det halve. (Information 1985-08-05).

Industrispionage har større betydning for mange af vore virksomheder, end nogen berigelsesforbrydelse nogensinde vil kunne få. På det sidste har den svenske arbejdsgiverforening indledt et samarbejde med det kriminalpræventive råd om disse risici. Nationaløkonomisk set, kan der næppe tænkes en berigelsesforbrydelse, som kan få nogen interesse. Derimod kan man meget vel forestille sig, at industrispioneri kan få konsekvenser for handelsbalancen.

På den baggrund må det forbavse, at Folketinget i 1985 satte maksimumstraffen for industrispionage ned fra 4 års fængsel til 2 års. I særdeleshed undrer det, når det erindres, at højestestraffen for databedrageri samtidig blev sat til 8 års fængsel (strl. § 286). (Sml. strl.bet. 1985 s. 27 f. og 83 f.).

Ved siden af den civile spionage foregår der omfattende militære spionerier på det elektroniske område, jfr. f.eks. U 1978.167 H og strl. kap. 12.

Hvis den uberettigede viden opnås ved hjælp af andre metoder, kan de almindelige regler om fredskrænkelser eventuelt bruges. Indtrængen i magnetbåndsarkiver over telefonnettet kan straffes efter strl. § 263. Udspionering af ingeniører med kikkert fra et nabohus omfattes af strl. § 264 a.

Hvis spionen får sit kendskab til virksomhedens forhold ved at gennemrode affaldet derfra, jfr. eksempel 55 nedenfor, er der en begrænset beskyttelse i strl. § 263 om at gøre sig bekendt med indholdet af (tidligere) lukkede meddelelser. Men sædvanligvis vil det være straffrit. Derimod kan en senere brug efter omstændighederne straffes, jfr. nedenfor under b, s. 32.

4°. Siden 1912 har konkurrencelovgivningen indeholdt en bestemmelse om krænkelse af forretnings- og driftshemmeligheder. Den er udtryk for, at erhvervsvirksomheder har krav på, at visse forhold vedrørende produktionen eller indkøbs- og salgsorganisationen, der har særlig betydning for virksomhedens konkurrenceevne, bevares for virksomheden selv, og ikke af dens funktionærer eller medindehavere benyttes uden for virksomheden eller gives videre til andre. (Smh. Mogens Koktvedgaard 1965 s. 296 ff.).

Markedsføringslovens § 9 beskytter erhvervshemmeligheder, tekniske tegninger m.m. mod sådanne krænkelser. *Stk. 1 og 2* drejer sig om *erhvervshemmeligheder.* De kan angå tekniske foranstaltninger, som er anvendelige i produktionen; der kan være tale om en opfindelse, som ikke ønskes patenteret, eller som ikke kan patenteres; det kan sågar være viden om en produktionsmåde, der i og for sig er en nærliggende løsning for fagfolk (U 1930.246 H). Erhvervshemmeligheder kan være kendskab til kundeemner, indkøbsmuligheder, markedsanalyser og andre kommercielle forhold. Beskyttelsen omfatter således ethvert lidet kendt teknisk og merkantilt forhold, som der er en reel interesse i at kunne holde hemmeligt (Mogens Koktvedgaard 1965 s. 304). Det må formentlig kræves, at oplysningen har formueværdi (SOU 1983:52.284 f.). Hvis oplysningen let og billigt kan (gen-)skabes af en branchekyndig, er der en formodning mod beskyttelse.

Personen, som skal have strafferetlig beskyttelse, må have en tilsvarende civilretlig. Hvis en ansat har retten til en opfindelse eller ophavsretten til et programmel, kan firmaet selvfølgelig ikke hindre, at det bringes ud.

Den, der vil gøre krav på beskyttelse af sine hemmeligheder, må normalt selv – gennem sikkerhedsforanstaltninger eller på anden måde – have tilkendegivet interessen i beskyttelse, f.eks. således at oplysninger om forholdet kun gives til personer, som nødvendigvis må have denne viden for at kunne fylde deres plads i firmaet. Anerkendelse af beskyttelse er særlig nærlig-

gende, når forholdet kun er kendt af en enkelt person eller af en meget begrænset kreds af personer inden for virksomheden.

Uden for det beskyttede område falder viden om forhold, som er almindeligt kendt i branchen. Udenfor falder også almindelige kundskaber, selv om denne viden er opnået på den pågældende virksomhed. (Jfr. bet. 416/1966 s. 30 og Børge Dahl i Karnov s. 2786 n. 63 og 64.)

Stk. 3 indeholder er særregel om tekniske tegninger, beskrivelser, opskrifter m.m., som er blevet betroet til en person i anledning af udførelsen af arbejde m.m. Derimod næppe mundtlige instruktioner (SOU 1983:52.220). Disse tegninger m.m. behøver ikke at være erhvervshemmeligheder.

Stk. 1 og 2 rammer krænkelser af erhvervshemmeligheder, som begås af *personer,* »der er i tjeneste- eller samarbejdsforhold til en virksomhed eller udfører et hverv for denne«. Hovedeksemplet er ansatte på den pågældende virksomhed. Reglerne dækker disse personer, selv om de bevæger sig ind på et område inden for firmaet, som er uvedkommende i forhold til dem. (FT 1971/72 A.563.) Bestemmelserne omfatter også tilfælde, hvor ansatte foretager krænkelser under »besøg« uden for arbejdstiden, eller hvor de først skaffer sig kendskabet m.m. efter samarbejdsforholdets ophør, men i kraft af dette. (Jfr. Børge Dahl i Karnov s. 2786 n. 60.) Der kan eventuelt straffes i sammenstød med bestemmelserne om husfredskrænkelse (sml. SOU 1983:52.128). Der behøver ikke at foreligge en udtrykkelig aftale om pligt til hemmeligholdelse. En vis hemmeligholdelsespligt er blandt de biforpligtelser, der påhviler en kontrahent, selv uden udtrykkelig aftale herom. Aftalen eller erklæringen kan dog vise, hvad firmaet - også uden for konfliktsituationen - betragter som hemmeligheder, jfr. ovenfor. Den kan endvidere få betydning ved vurderingen af tilregnelsen. Medejere af virksomheden kan være omfattet af reglerne (Jørgen Bull 1973 s. 18). De vigtigste eksempler på »samarbejdsforhold« er underleverandører, repræsentanter og servicearbejdere. Stk. 3 kan desuden omfatte personer, som endnu ikke er i et sådant forhold til virksomheden, men som f.eks. skal afgive tilbud. Det vil dog hyppigt være rimeligt at udvide stk. 1 og 2 ved fortolkning, så de også kommer til at omfatte sådanne personer. Derimod omfatter bestemmelsen ikke andre folk, der har lovlig adgang til en virksomhed, f.eks. som besøgende, selv om de bruger lejligheden til at skaffe sig kendskab til eller rådighed over erhvervshemmeligheder (FT 1971/72 A.563).

En kriminel *handling* begås *for det første,* når en af de nævnte »på utilbørlig måde skaffe[r] sig eller forsøge[r] at skaffe sig kendskab til eller rådighed over virksomhedens erhvervshemmeligheder« (stk. 1). Der kræves en aktiv indsats fra den pågældendes side, jfr. »skaffe sig«. Indsatsen skal desuden være odiøs, jfr. »på utilbørlig måde«. I denne forbindelse må udgangspunktet være, at de ansatte i nutidens virksomheder har ret til at in-

teressere sig for, hvad virksomheden foretager sig. (Smh. Poul Dam FT 1971/72.1103.) Hvis personen har fået sin viden ved at høre en diskussion på et stort medarbejdermøde, eller fordi nogen post ved en fejltagelse blev sendt til den pågældende, er vi uden for stk. 1. Dermed er det ikke udelukket at bruge stk. 2, jfr. nedenfor.

Det er ikke ganske klart, hvad der skal forstås ved, at personen *forsøger at skaffe sig kendskab*. Efter de almindelige regler i strl. § 21, jfr. § 2, ville forsøg alligevel være strafbare uden denne særregel.

Formuleringen synes at stamme fra konkurrencelovudvalget af 1959 (bet. 416/1966 s. 92). Her var en særregel om forsøg velbegrundet, eftersom udvalget forestillede sig, at strafferammen ikke skulle indeholde mulighed for fængsel. Og i sådanne situationer kræver forsøgsstraf en særlig lovhjemmel, jfr. strl. § 21, stk. 3. (Smh. bet. 416/1966 s. 84.) Straffelovrådet (bet. 601/1971 s. 56) videreførte formuleringen. Det nævnte behovet for frihedsstraf, men det fremgår ikke, om Straffelovrådet dermed alene tænkte på hæftestraf - som i den dagældende konkurrencelov. Ministeriet og Folketinget har næppe overvejet spørgsmålet. På den baggrund ville det nok være mest rimeligt nu at fortolke indskuddet som en (ex tuto) henvisning til de almindelige forsøgsregler. Det vil især sige, *at* det er dansk strafferets meget vide forsøgsbegreb, som skal anvendes, *at* der skal kræves forsæt, *og at* der er mulighed for strafophør ved frivillig tilbagetræden, jfr. strl. §§ 21, 22 og 24.

Imod en sådan tolkning taler, at konkurrencelovudvalget skrev: »Forsøg må ved anvendelsen af lovforslagets regel forstås i overensstemmelse med almindelig sprogbrug som alle nærmere forsøgshandlinger.« (S. 97). Hvis dette lægges til grund, bliver forsøgsområdet snævrere end det ville være efter strl. § 21. Det er ikke foruroligende; men det bliver derefter nærliggende at spørge, om der kan straffes for uagtsomhed, og om strafophør ved frivillig tilbagetræden er udelukket på det snævre forsøgsområde. Se om et lignende problem Vagn Greve 1979 s. 169 ff. Dette vil være særdeles betænkeligt uden klarere støtte i forarbejderne. Reelt ville det betyde, at man behandlede forholdet strengere efter specialreglen, end det ville være blevet efter de almindelige regler, selv om det eneste grundlag herfor var en halvgammel motivudtalelse, der var baseret på en afstandtagen fra vor almindelige, meget vidtgående lære. Det må derfor fastholdes, at indskuddet er en ex tuto henvisning til de almindelige forsøgsregler.

Smh. norsk strl. § 405 a med NOU 1985:31.17 f.

Markedsføringsloven kriminaliserer krænkelsen af hemmelighederne uanset metoden. Den fremgangsmåde, der anvendes af den pågældende person ved krænkelsen, kan være selvstændigt kriminaliseret, f.eks. i straffelovens kapitler om fredskrænkelser og formueforbrydelser, så der skal straffes i sammenstød (FT 1971/72 A.563). Opbrydning af gemmer skal således også straffes efter strl. § 263. Tilsvarende gælder med hensyn til overtrædelser af strl. § 263, stk. 2, om data m.m. (strl.bet. 1985 s. 73 f.). Hvis tegninger, modeller osv. fjernes, kan der efter omstændighederne (også) straffes for tyveri (strl. § 276) eller underslæb (strl. § 278). Hvis den opnåede rådighed over erhvervshemmelighederne viser sig i, at informationen »føres bort« i den ansattes hukommelse eller lommebog, på den ansattes egne film i et kamera, etc. er straffelovens §§ 276-278 imidlertid uanvendelige.

Hvis der tages en fotokopi af tegninger m.m., og det er denne kopi, der fjernes, medens originalen lægges tilbage på plads, opstår spørgsmålet, om fjernelsen af fotokopien kan konstituere tyveri/underslæb. I usa-nsk ret antages det, at fotokopien er 'property', som er beskyttet

af de almindelige regler om tyveri, hæleri m.m. (Edward H. Coughran 1976 s. 31). Tilsvarende antages i fransk retspraksis. Efter dansk ret ville der også foreligge en 'ting', som *kan* være beskyttet. Spørgsmålet er imidlertid, om dette ville være den mest naturlige måde at anskue handlingen på.

Som nævnt ovenfor, er der ikke tale om tyveri, hvis en ansat tegner en konstruktionstegning af i sin egen notesbog eller lignende. Hvis han mod at erlægge 25 øre per kopi må tage private fotokopier på firmaets kopimaskine, er det også givet, at disse kopier er hans egne i relation til strl. § 276. Hvis han unddrager sig sin betaling af de nævnte 25 øre per kopi, er vi uden for de situationer, som det er naturligt at bedømme efter strafferetten. Hvis han havde kopieret en sølvbryllupssang, ville ingen drømme om at straffe. Og det gælder, hvad enten han undlod at betale sine 25-ører, eller der var et generelt forbud mod at bruge kopimaskinen til private formål. »Minima non curat praetor.« (Retssystemet skal ikke tage sig af bagateller). Der bør i hvert fald højest blive tale om civilretlige sanktioner.

At det kopierede ikke er sølvbryllupssange, men firmaets konstruktionstegninger, bør næppe gøre nogen forskel. Den reelle krænkelse er jo ikke knyttet til brugen af fotokopieringsmaskinen, men til tilegnelsen af informationen - og den straffes selvstændigt efter markedsføringsloven.

Noget andet er, hvis der ikke er tale om noget ligegyldigt papir, som ud fra en dagligdags betragtning ikke tillægges nogen værdi, men f.eks. om en overspilning på et af firmaets magnetbånd, som derpå fjernes. Her skal der også straffes for tyveri/underslæb af denne ting. (Men tilsvarende betragtninger fører til, at der er en formodning for, at § 286 ikke skal anvendes.)

Efter markedsføringslovens § 9, *stk. 2,* er det *for det andet* forbudt under samarbejdet m.m. og i 3 år derefter at *viderebringe* eller *erhvervsmæssigt at benytte* virksomhedens erhvervshemmeligheder. Jfr. også stk. 3 om tegninger m.m., som ikke indeholder nogen tidsgrænse. Bestemmelsen i stk. 2 får især selvstændig betydning ved siden af stk. 1, når personen lovligt har den relevante viden. Forbuddet mod viderebringelse gælder selvsagt kun videregivelse til uvedkommende, jfr. nærmere Mogens Koktvedgaard 1968, s. 166 f.

Eksempel 12: Kort tid før T skulle fratræde sin stilling som ingeniør, sendte han med benyttelse af firmaets papir og skrivemaskine et brev til 15 interessentskaber, som firmaet udførte vandværksanlæg for. I brevene gav han blandt andet oplysning om firmaet indkøbspris på materialer. Straffet for overtrædelse af den dagældende konkurrencelovs § 11, der i nogen grad svarer til den nugældende markedsføringslovs § 9. (HRT 1941.519.)

Det har stor praktisk betydning, at det strafferetlige forbud gælder 3 år efter, at arbejdsforholdet er ophørt. I U.S.A. antages det, at skift af arbejdssted er den største »utæthed« i edb-firmaerne. Til illustration kan det nævnes, at 24% af de ansatte i Californias berømte Silicon Valley skiftede plads i 1982 (Time 1983-09-19).

Eksempel 13: T ledede udviklingen af skibsradioanlæg i en virksomhed. Han opsagde sin stilling til fratræden den 31. juli og begyndte sin egen produktion af skibsradioer. Allerede den 9. september udsendte han salgsmateriale og tilbød levering i januar. På grundlag af skønserklæringer om det tidsrum en udvikling af et sådant anlæg kræver, og om lighedspunkter med det tidligere ansættelsessteds anlæg, blev det antaget, at T havde nydt fordel af den viden, som han havde erhvervet under sin ansættelse. Straffet efter den dagældende konkurrencelovs § 11. (U 1975.1049 H.)

Se finsk frifindende højesteretsdom i Lauri Lehtimaja 1979 n. 4.

Både *forsætlige og uagtsomme* overtrædelser af § 9 er strafbare (strl. § 19 og bet. 416/1966 s. 85).

Overtrædelser *straffes med* bøde, hæfte eller fængsel indtil 2 år, jfr. markedsføringslovens § 19, stk. 5. Ifølge § 19, stk. 6, kan der pålægges kollektive enheder bødeansvar. Se om strafudmålingen bet. 416/1966 s. 84 ff. og bet. 681/1973 s. 25, samt rigsadvokatens meddelelse 7 8.7.1975.

I det nye finske straffelovsudkast af 31. maj 1984 foreslås 'företagsspionerí' og nogle krænkelser af 'företagshemlighet' straffet med bøde eller fængelse i højest 2 år (30. kap. 3.-5. §§). Se om Sverige SOU 1983:52 med forslag til »lag om skydd för företagshemligheter«.

b. Efterfølgende brug

Efterfølgende brug af oplysninger, der er fremkommet gennem industrispionage (strl. § 263, stk. 3, og § 264, stk. 2) eller ved en overtrædelse af markedsføringslovens § 9, stk. 1-3, kan efter omstændighederne straffes efter henholdsvis strl. § 264 c og markedsføringslovens § 19, jfr. § 9, stk. 4. I begge tilfælde forudsættes det, at modtageren ikke kan straffes for medvirken til førforbrydelsen, jfr. strl. § 23 (og § 2). Det vil f.eks. være tilfældet, hvis modtageren har overtalt spionen/den ansatte til at fremskaffe nogle bestemte oplysninger,

Strl. § 264 c kræver *forsæt,* medens markedsføringslovens § 9 i overensstemmelse med det almindelige princip i strl. § 19 også rammer *uagtsomt* forhold. (FT 1971/72 A.565). Tilregnelse (viden m.m.), som opnås senere, og medens f.eks. en produktion er i gang, er efter omstændighederne tilstrækkelig til at gøre fortsættelsen af produktionen strafbar (cfr. bet. 416/1966 s. 98). Hvis hemmeligheden går over til at blive almindelig faglig viden, f.eks. gennem en (tredjepersons) artikel i et fagblad, kan »hæleren« siden hen - på samme måde som alle andre - bruge den retmæssigt. (Smh. bet. 416/1966 s. 98.)

Strafferammen for overtrædelse af strl. § 264 c, jfr. § 263, stk. 3/§ 264, stk. 2, er bøde, hæfte eller fængsel indtil 2 år (efter lovændringen i 1985). Efter markedsføringslovens § 19, stk. 5, jfr. § 9, stk. 4, er den ligeledes bøde, hæfte eller fængsel indtil 2 år.

Det er næppe ganske afklaret, hvorfra *forældelsesfristen* efter strl. § 94 skal regnes i sådanne tilfælde. (Smh. Vagn Greve, Ole Ingstrup og Minna Bloch 1977 s. 20 ff.)

Hvis den oprindelige krænkelse (desuden) kan straffes som f.eks. tyveri eller underslæb, kan den efterfølgende erhvervelse m.m. straffes som *hæleri* (strl. §§ 284 og 303).

Eksempel 14: En fabrikant, der ville begynde på en fremstilling af grebe, modtog nogle halvfabrikata af en arbejder, som søgte plads hos ham. De havde isoleret set en værdi af 20-30 øre per styk, men det var let at fremstille det fornødne værktøj efter dem. Fabrikanten, der forstod, at emnerne var stjålet hos en konkurrent, blev dømt for hæleri. (U 1931.243 H.)

c. Eftergørelse m.m.

1°. »Angrebet« kan have karakter af en uberettiget eftergørelse. Tusindvis af Apple-kopier er eksporteret fra Taiwan under navne som »Pear« og »Orange« (Göteborgs-Posten 1984-12-27). Sovjetunionen har kopieret en datamat fra IBM så grundigt, at selv ledningernes farver er de samme (Time 1985-06-17). Fra midten af 1982 til foråret 1984 anlagde Apple Computer (California) 45 plagiatsager mod fabrikanter i 16 lande fra UK til Taiwan (Time 1984-05-28).

Edb-anlæggets »isenkram« kan som andre maskiner *patentbeskyttes*. Forsætlige indgreb i den patentbeskyttede eneret kan straffes med bøde eller under skærpende omstændigheder med hæfte i indtil 3 måneder. En skærpende omstændighed kan være, at der er foregået en grov udnyttelse af en særlig ringe mulighed for opdagelse (Ane Boe i Karnov s. 2725 n. 151). (Når krænkelsens alvor tages i betragtning, er strafferammen absurd lav sammenlignet med f.eks. tyveris.) Kollektive enheder kan pålægges bødeansvar. Jfr. patentlovens § 57. Patentlovens straffebestemmelser anvendes (næsten) ikke i praksis. Ane Boe oplyser (s.st.), at straf ikke ses anvendt under den nugældende patentlov, dvs. 1967-1982.

Se om de særlige regler vedrørende »chips« bet. 1064/1986.70 ff. og SOU 1985:51.113 ff.

2°. Ifølge *markedsføringslovens* § 1, 2. pkt., må erhvervsvirksomheder ikke foretage »handlinger, som strider mod god markedsføringsskik«. Denne *generalklausul* giver grundlaget for en vis civilretlig beskyttelse mod efterligning, snyltning og anden udnyttelse af andres indsats, men den er ikke sanktioneret med straf. Hvad der også ville have været stridende mod det væsentlige strafferetlige princip, at der ikke bør være vage og upræcise straffebestemmelser (bet. 416/1966 s. 84). I strafferetten må vi falde tilbage på den ovenfor omtalte snævrere § 9 i markedsføringsloven.

B. Programmel

1. Indledning

Programmel (programmer, »software«) er det sæt af specificerede kommandoer, der direkte eller indirekte styrer og sikrer gennemførelsen af den elektroniske databehandling. (Smh. U.S. Copyright Act s. 101). Inden for datalogien ses f.eks. følgende definitioner: Programmel er programmer, som kan køre på en datamaskine. Program er ordrer, der entydigt kan transformere inddata til uddata. Så længe datamaten er uden sådanne instruktioner, er den ude af stand til at fungere. Programmellet kan være integreret i maskinen (ROM, »firmware«, integrerede kredse), men behandles alligevel ophavsretligt som andet (løst) programmel - i hvert fald som udgangspunkt. (Se dog Agne Henry Olsson 1985 og Jon Bing 1985 s. 46 ff. og 179 ff., samt

SOU 1985:51.113 ff. og bet. 1064/1986 s. 70 ff., 86 og 93 om »chips«). Af dette følger ikke nødvendigvis, at alt programmel strafferetligt skal behandles på samme måde i alle sammenhænge. Programmellet kan være indlæst permanent eller midlertidigt i maskinen eller/og det kan have en ydre selvstændig fysisk fremtræden. I dette fald kan det findes på et magnetbånd, som en stak hulkort, trykt eller skrevet i en bog o.s.v.

Programmel adskiller sig juridisk set i nogle relationer markant fra data, selv om de to ting datateknisk set har eller kan have stor indbyrdes lighed.

2. Ødelæggelse

a. Angreb på den fysiske genstand

Hvis den fysiske bærer af programmellet (magnetbånd, disketter, chips, bøger o.s.v.) angribes, foreligger der som udgangspunkt en tingsødelæggelse (strl. § 291). »Ting« er fysiske genstande af enhver art (Komm. strl. II s. 415 og strl.bet. 1985 s. 30).

b. Andre former for ødelæggelse

Hvis programmellet er indlæst på et magnetbånd, en diskette (»floppy disk«) eller tilsvarende, kan »indholdet« ødelægges, uden at båndet, disketten etc. beskadiges som sådant.

Eksempel 15: I 1969 trængte modstandere af den usa-nske krig i Vietnam ind i firmaet DOW's Chemical Corporations forskningscenter. Med magneter slettede de 1000 magnetbånd i den tro, at båndene indeholdt oplysninger om de kemiske våben, der blev brugt i Vietnam. Rekonstruktionen kostede $ 100 000. (Ulrich Sieber 1977 s. 91 f.)

Eksempel 16: Et usa-nsk forsikringsselskab opsagde lederen af dets magnetbåndsamling. Som hævn slettede hun alle båndene. Skaderne for firmaet beløb sig til omkring $ 10 mio. (Ulrich Sieber 1977 s. 88.)

Eksempel 17: En programmør foretog tilføjelser og sletninger i et programmateriale som hævn for firmaets bortvisning af hans kollega. Straffet efter strl. § 291, stk. 2. (Hillerød 1983-04-21).

Efter en konflikt slettede leverandøren af programmellet ved hjælp af telefonmodem programmel, så edb-anlægget ikke længere kunne udskrive checks til de berettigede. Straffet efter strl. § 291, stk. 2. (Frederiksberg 1985-08-09; anket).

Eksempel 18: I samme frederiksberske sag havde T kendskab til, hvilket programmel fra en anden virksomhed, som man ville kunne anvende som reserve. I dette indlagdes også sletteinstruktioner. Ligeledes henført under § 291, stk. 2.

Eksempel 19: I den pågældende sag ændrede T i midten af juli et programmel på en sådan måde, at det ville slette en række filer, hvis det blev anvendt efter 25. august. Man taler til tider om sådant som »en bombe i systemet«. Også henført under § 291, stk. 2.

Sådanne former for ødelæggelse af programmel og andre indkodede data har fysisk set kun karakter af en anden indstilling af maskinen eller »indholdet« af båndet. Det svarer til, at man går hen til et bord, hvor der ligger

nogle terninger, og vender rundt på dem. Det, der ødelægges, er ikke tingen, men strukturen. Hvis terningerne havde været udstillet som et kunstværk på Louisiana, ville der ikke være tvivl om, at en ændring af terningernes placering ville kunne være en destruktion af kunstværket. Hvis en uvenlig person skiller sin nabos bil fuldstændigt ad - lige til mindste møtrik - ville det utvivlsomt være en tingsødelæggelse, selv om alle løsdelene isoleret set er fuldstændig intakte.

I californisk ret har det været diskuteret, om sådanne sletninger af magnetbånd m.m. bør bedømmes som 'malicious mischief' (hærværk), 'burglary' (indbrud) og/eller 'misuse of telephone services' (misbrug af telefonsystemet) (Edward H. Coughran 1976 s. 11 f.). En fjerde mulighed er 'altering of records', der nævnes nedenfor. De fleste U.S.A.-stater afviser at bedømme det som hærværk (Computer Crime s. 2).

I Sverige anses det for 'skadegörelse' (SOU 1983:50.182 f.). I br-tysk ret er det den overvejende opfattelse, at sådanne sletninger er omfattet af StGB § 303 om 'Sachbeschädigung' (tingsødelæggelse) (Ulrik Sieber 1977 s. 191 f.). Derimod anser Stein Schjølberg det for »et særlig tvivlsomt spørsmål«, om det også gælder efter norsk ret (1983 s. 482). Det norske straffelovråd henfører det under 'skadeverk' gennem reglen om »gjort ubrukelig« (NOU 1985:31.10.).

'Tingsødelæggelse' synes også at være den naturlige subsumption efter dansk ret, når programmellet tilhører en anden og er knyttet til en fysisk ting (strl.bet. 1985 s. 37), jfr. eksemplerne 17-19. Men ikke f.eks. § 293 om ulovlig brug, der vil blive absorberet. Det giver mulighed for at straffe med bøde, hæfte eller fængsel indtil 4 år.

Programmellet kan anses for ødelagt i og med, at den »logiske bombe« indlægges i programmellet. Ødelæggelsen kan også anses for knyttet til »sprængningen«, hvor programmel og/eller data udslettes. Straffelovrådet peger på den første løsning for strl. § 291, stk. 1, og den anden løsning for stk. 2. Endelig nævner det muligheden for i visse relationer at bruge firmaets første kørsel med programmellet. (Strl.bet. 1985 s. 38). Straffelovrådet begrunder den første løsning med, at der på »dette stadium sker ... et indgreb i anlæggets tilbehør, som derfor kan siges at være beskadiget«. De to andre løsninger begrundes ikke. Den frederiksbergske byretsdom i eksemplerne 17-19 anvendte den første mulighed ved § 291, stk. 2.

Det giver den enkleste og mest hensigtsmæssige løsning, hvis man i alle sammenhænge vælger den anden løsning, »sprængningen«. - Det giver en bedre overensstemmelse med reglernes brug i andre forhold. Hvis en terrorgruppe anbringer en bombe på et turisthotel, er der ingen, som vil være i tvivl om, at det er selve sprængningen, som realiserer § 291. Og det vil ikke gøre nogen forskel, om det er en lille bombe (stk. 1) eller en stor bombe (stk. 2). - »Logiske bomber« kan være indrettet, så de først skal fungere efter meget lang tid. I denne forbindelse vil det være mest naturligt at lade forældelsesfristen løbe fra »sprængningen«, jfr. strl. § 94, stk. 2. - Vi kan bevare incitamentet til den kriminelle persons tilbagetræden (strl. § 22) længst muligt ved at vælge denne løsning. - Endelig giver den de mest rimelige løsninger, hvor en ansat programmør har indlagt »bomben« under den oprindelige opbygning af programmellet. I denne forbindelse må det betænkes, at programmellet, som bruges i virksomheder m.m., i praksis er under stadig revision. Det er ikke naturligt at sige, at en produktion af en farlig genstand har karakter af ødelæggelse af samme genstand. Og det er vanskeligt at følge Straffelovrådet og tillægge det tilfældige tidspunkt for den første kørsel betydning i denne sammenhæng.

Hvis sletningen sker med berigelsesforsæt, er udgangspunktet strl. § 279 a, jfr. nedenfor s. 65 ff.

Hvis programmellet leveres fra et udenforstående firma med »bomben« indbygget, kan det til tider være nærliggende i stedet at bedømme forholdet som bedrageri (strl. § 279) (strl.bet. 1985 s. 38). Se nedenfor s. 44 om »bomber« indlagt som beskyttelse mod kopieringer. Hvis »bomben« kun kan »springe« efter en senere aktivering, kan det efter omstændighederne være naturligt at straffe i sammenstød mellem § 279 og § 291.

Der kan også straffes i sammenstød med en fredskrænkelsesbestemmelse. I eksempel 15 kunne den almindelige bestemmelse om husfredskrænkelse (strl. § 264, stk. 1, nr. 1) anvendes, hvis forholdet havde været begået i Danmark.

I de ovennævnte eksempler var der hensigt til at slette båndene. Det kan imidlertid også gøres ved uheld. Ulrich Sieber oplyser således, at langt de fleste ødelæggelser i BRD skyldes betjenings- eller installationsfejl (1977 s. 97). I graverende tilfælde af denne art kan strl. § 291, stk. 3, om groft uagtsomt hærværk af betydeligt omfang anvendes i Danmark (strl.bet. 1985 s. 20). Civilretlige reaktioner vil dog som regel være mere nærliggende.

Jfr. også strl.bet. 1985 s. 9.

c. Fordølgelse

Ulla Høg mener, at tingsødelæggelsesbestemmelsen også skal anvendes, hvis programmel og data ikke slettes, men flyttes til et andet sted på databæreren, hvor de (i praksis) kun kan findes af den, der har flyttet dem (1981 s. 64). Således også URD Frederiksberg 1985-08-09 (anket) og Straffelovrådet under henvisning til strafferammerne (strl.bet. 1985 s. 37 f.).

Det kan ikke afvises, at forholdet kan bedømmes som en bortskaffelse efter strl. § 291. Mig forekommer det dog i visse tilfælde, ud fra straffelovens ordvalg, mindst lige så nærliggende at lade det bedømme som en overtrædelse af strl. § 293, stk. 2, om faktiske hindringer for, at ejeren udøver sin ret til at råde over materialet. Se i øvrigt nedenfor s. 50 ff.

Det norske straffelovråd anser det for 'skadeverk', jfr. »gjort ubrukelig« (NOU 1985:31.10).

3. Ændring

a. Mod brugerens/ejerens interesse

Ændringen af programmellet kan være af mere eller mindre indgribende karakter. Hvis den er meget omfattende, kan den ses som en ødelæggelse af hele programmellet. I så fald anvendes strl. § 291, jfr. ovenfor. Hvis ændringen sker med berigelsesforsæt, er udgangspunktet strl. § 279 a, jfr. nedenfor s. 65 ff. Jfr. også ovenfor om strl. § 193. Dette gælder, når datamaten ganske standser, men også, hvor den synes at fungere, men producerer

åbenbart forkerte resultater, så det kontrollerende personale nødsages til at indstille driften.

Det er forudsat, at ændringen foretages af en uvedkommende tredjeperson. Hvis den udføres af ejeren, som har leaset o.s.v. programmel m.m. til brugeren, er tingsødelæggelsesreglen ikke anvendelig. I nogle af disse tilfælde kan strl. § 283, stk. 1, nr. 1, om skyldnersvig måske bruges (berigelsesforsæt forudsat!). I URD Frederiksberg 1985-08-09 (anket) anvendtes analogien af § 291 i et tilfælde, hvor ejeren af datamaten havde en tidsubegrænset brugsret til programmellet.

Hvis den foretages af brugeren i en lejeperiode, kan den stride mod ejerens interesser i en sådan grad, at tingsødelæggelsesbestemmelsen bliver anvendelig. I almindelighed må konflikten dog ses som civilretlig.

Hvis ændringen er mindre omfattende, og den ikke tilsigter at medføre en standsning af driften, men tværtimod måske forventes at bevirke urigtige resultater eller andet i en kortere eller længere periode, kan det blive et spørgsmål, dels om hvordan ændringen i programmellet skal bedømmes, dels om forvanskningen af uddata er strafbar i sig selv.

Et programmel kan næppe være et dokument i straffelovens forstand. Det har ikke den funktion, som strl. § 171, stk. 2, kræver. Deraf følger, at ændringen ikke i sig selv kan betragtes som dokumentfalsk. Det mest nærliggende bliver i disse tilfælde at falde tilbage på den almindelige regel om tingsødelæggelse (strl. § 291).

Andre bestemmelser kan efter omstændighederne komme på tale. F.eks. kan det være en statsforbrydelse at ændre programmellet i en militær datamat.

Hvis ændringen skal frembringe forkerte udskrifter m.m. i en periode, vil det formentlig i almindelighed være rigtigst at se den som en forsøgshandling i relation til den forbrydelse, som fuldbyrdes ved udskrivningen m.m. af de forkerte uddata. Hvis det er urigtige eksamensbeviser, kan det være forsøg på dokumentfalsk, hvis det er pengeoverførsler, kan det være databedrageri o.s.v.

b. Mod programmørens interesse

Indgrebene i programmellet kan krænke programmørens eller andres ophavsret. Se herom nedenfor under 4.d., s. 41 ff.

4. Kopiering m.m.

a. Tilegnelse

Programmeller kan være ganske simple, men også yderst komplicerede. De kan have et meget bredt anvendelsesområde eller være tilpassede en enkelt brugers helt specielle behov. Udvikling af programmel kan være en meget langvarig og særdeles kostbar proces. Man skønner, at den tyske industri

anvender mere end 8 mia. DM om året på udvikling af programmel (Oertel 1984). Det kostede BOAC £ 43 mio. at udvikle et billetbestillingssystem i midten af 1960-erne (Ulrich Sieber 1977 s. 101). I det nedenstående eksempel 20 blev værdien af de 59 dokumenter med programmeller opgivet til $ 2,5 mio. VisiCorp har solgt mere end 700 000 af et programmel beregnet til økonomisk analyse siden 1979 å ca. $ 200 (Time 1984-04-16). Leasing af et enkelt programmel vedrørende bankforretninger kan koste $ 200 000 om året (Time 1984-04-16). Det hævdes, at der sælges for ca. 5 mia. kr. piratsoftware om året i den vestlige verden (af en sælger af disketter, der ikke kan kopieres. Politiken 1984-06-20). Når programmellet er skrevet på papir, indkodet på magnetbånd o.s.v., vil en tilegnelse af papirerne, magnetbåndet o.s.v. være tyveri (strl. § 276) eller underslæb (strl. § 278).

Eksempel 20: T var ansat hos Texas Instruments i Texas og tog 59 dokumenter med edb-programmel. Han forsøgte at sælge dem til Texaco, der imidlertid orienterede Texas Instruments. T blev dømt for tyveri. (Computer/Law Journal 1980.777).

Hvis der ikke samtidig sker en tilegnelse af den fysiske bærer af programmellet, er vi uden for tyveri/underslæbsbestemmelserne, jfr. disses krav om, at genstanden skal være en »fremmed rørlig ting« (strl.bet. 1985 kap. 3). Se i øvrigt ovenfor om fotokopieringer m.m.

I Sverige er der forslag fremme om at ændre mandatsvigsbestemmelsen 'trolöshet mot huvudman', BrB 10:5), så den kommer til at omfatte personer, som »självständigt handha kvalificerad teknisk uppgift eller .. övervaka ... sådan ... uppgift«. Der tænkes alene på personer, der er i særlig ansvarsfulde stillinger, og som udleverer foretagendets hemmeligheder, f.eks. programmel. Under bestemmelsen skal ikke blot falde ansatte, men også f.eks. konsulenter. (Lagrådsremiss 1985-09-19. Jfr. også Polisens åtgärder mot datakriminalitet s. 109 f.).

b. Fredskrænkelsen

Ovenfor behandledes industrispionage (strl. § 264, stk. 2) og ansattes krænkelser af erhvervshemmelighederne (markedsføringslovens § 9). Disse bestemmelser kan også anvendes her. Det må antages, at erhvervshemmelighederne i nogen grad vil miste deres beskyttelse, når programmel distribueres vidt og bredt uden kontrol med brugen m.m. (Jfr. Christopher J. Millard 1985 s. 121). Af særlig interesse derudover er imidlertid *»tapninger«* af data-anlæggene *over telefonnettet.* Det kaldes til tider »hacking«. (Udtrykket skal stamme fra Tech Model Railroad Club på MIT, hvor studenterne i slutningen af 1950-erne brugte »hack« om en smart og fræk drengestreg (Sal Alfano 1984)). Hvis der kan opnås tilstrækkeligt kendskab til programmeller ad den vej, kan de anvendes på det egne dataanlæg, eller det fremmede anlæg kan udnyttes til beregninger m.m. Endvidere kan det kopierede programmel eventuelt videresælges. (Smh. SOU 1983:52 s. 357).

Eksempel 21: T var over telefonnettet »trængt ind« i Federal Energy Administrations datamat og havde skaffet sig sådanne oplysninger om programmellet, at han kunne tappe anlægget for vigtige oplysninger om olieudvinding m.m. Han blev tiltalt for 'wire fraud' (telefonsvig). (Los Angeles Times 1976-07-17).

Eksempel 22: Lignende sag, hvor T uden held gjorde gældende, at et programmel ikke var 'property' i den forstand, som det kræves for at straffe for 'wire fraud'. (Computer/Law Journal 1980.781).

Eksempel 23: Et edb-firma, ISD, havde udviklet et programmel, som gjorde det muligt at yde en service, som konkurrenten, UCC, ikke kunne give. En ansat i UCC kendte (lovligt) et kundenummer hos ISD. Ved hjælp af dette kaldte han over telefonnettet ISD og fik udskrevet alle deres programmeller, herunder det pågældende.

Spørgsmålet under retssagen var, om dette var en 'theft of secret' (tyveri af erhvervshemmeligheder), der ifølge californisk ret forudsatte, at der forelå en 'tangible article' (rørlig ting). Det skriftlige programmel, som var blevet skrevet ud på UCCs maskiner antoges at være en sådan 'tangible article'.

(Ulrich Sieber 1977 s. 111 f. og Computer/Law Journal 1980.783).

Christopher J. Millard (1985 s. 149) antager, at den pågældende ville være blevet frifundet, hvis han alene havde gennemset programmet på sin skærm. Sådant er imidlertid nu omfattet af en ny bestemmelse i den californiske straffelov.

Smh. også samme sted s. 117 f. om forretningshemmeligheders karakter af 'property' inden for common law.

Når krænkelsen af tredjeperson sker over telefonnettet, er det efter dansk ret udelukket at bruge tyveri/underslæbsbestemmelserne. Udskriften i eksempel 23 ville selvfølgelig også efter dansk ret være en 'rørlig ting', men den er ikke 'fremmed' i §§ 276-278s forstand.

Det har tidligere været den almindelige antagelse, at sådanne fredskrænkelser kunne straffes efter strl. § 263, (stk. 1), nr. 1. (Jfr. 1. udgave af denne bog s. 49). For at fjerne enhver tvivl, indsatte man ved straffelovsændringen i 1985 et nyt *stk. 2 i § 263.* (Jfr. strl.bet. 1985 s. 8, 21 ff. og 78 ff.). Det lyder:

»Med bøde, hæfte eller fængsel indtil 6 måneder straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling«.

På dette sted er interessen koncentreret omkring programmellet. Oplysninger behandles nedenfor s. 46 ff.

Krænkelsen skal være 'uberettiget'. Vurderingen heraf er konkret. Politiet kan med hjemmet i retsplejelovens kap. 71 (som ændret i 1985) foretage lovlige aftapninger. (Jfr. bet. 1023/1984 s. 57). I øvrigt vil en udefrakommendes forsætlige indtrængen næsten altid være uberettiget. Det gælder også, selv om den pågældendes motiv har været pænt. Journalister må ikke trænge ind i andres edb-anlæg uden tilladelse, selv om de blot vil vise, hvor dårlige sikkerhedsforanstaltningerne er (Peter Seipel 1984). Men der kan selvfølgelig tages hensyn til motivet i forbindelse med strafudmålingen (strl. § 80). Smh. U 1982.1005 H.

Ansatte og reparatører, som har til opgave at beskæftige sig med dele af anlægget, kan straffes efter § 263, hvis de går længere, end de har lov. Det forudsætter dog i almindelighed, at de klart har bevæget sig ind på områder, hvor de intet har at gøre. Hvis de blot bruger maskinen længere tid, end de har tilladelse til, jfr. studenten i eksempel 4, er vi uden for § 263. Også i øvrigt er der et grænseområde, hvor ikke enhver aftalestridig brug er strafbar. Hvis en ansat i almindelighed har adgang til fortrolige oplysninger, men han i den givne situation skaffer sig den pågældende viden med henblik på ulovligt salg, skal forholdet snarere henføres under strl. § 264 c. (Smh. NOU 1985:31.19).

Jfr. strl.bet. 1985 s. 25 og 26.

Adgangen kan skaffes fra en terminal, ved hjælp af aflytning af andres kommunikation o.s.v. Det er uden betydning, om gerningspersonen står lige ved siden af maskinen, eller om kontakten er skabt ved hjælp af telefonnettet eller andet over lang afstand.

Der kræves en aktiv indsats fra gerningspersonens side, jfr. »skaffer sig«.

Angrebet skal rettes mod »en andens« programmel m.m. Det er ligegyldigt, om gerningspersonen selv ejer edb-anlægget, eller om han i øvrigt har ret til at bruge det pågældende anlæg. (Strl.bet. 1985 s. 26).

Under »programmer« hører formentlig også dokumentationen af sådant programmel. Efter bestemmelsen er programmellet beskyttet uanset dettes fysiske fremtrædelsesform. Det kan være indlæst i datamaten, men det kan også findes på et magnetbånd eller i en bog, som står fjernt fra enhver datamat (strl.bet. 1985 s. 23). Hvis den retmæssige indehaver lader det ligge og flyde, kan den strafferetlige beskyttelse falde bort (smh. Waaben: Sp. D. s. 238).

»Programmer« vil per definition være udarbejdet med henblik på »at bruges i et anlæg til elektronisk databehandling«. Det betyder næppe noget i denne forbindelse, om de fortsat agtes (»er bestemt til« at blive) brugt således. Derimod kan beskyttelsen udtrykkeligt eller forudsætningsvis være opgivet. (Ren teoretisk programmering falder antagelig uden for paragraffens anvendelsesområde).

Efter ordlyden af § 263 omfatter den alle former for programmel. I det omfang programmellet har karakter af uforanderlige maskininstruktioner (ROM eller »firmware«), forudsætter en almindelig brug af datamaten ofte en anvendelse af dette programmel. I disse tilfælde absorberes strafansvaret efter § 263 af § 293 m.m. Hvis der ikke er tale om en almindelig brug, men om en kopiering må der dog i stedet straffes efter § 263.

Der findes ingen dansk legal definition af »et anlæg til elektronisk databehandling«. Det er nærliggende at bortfortolke små lommeregnemaskiner

o.s.v., men den nærmere afgrænsning er overladt til domstolenes frie retskaben. (Se strl.bet. 1985 s. 14 og ovenfor s. 16 f.).

Lovovertrædelsen fuldbyrdes, når gerningspersonen har skaffet sig adgang. Også selv om han ikke har tilsigtet eller fået noget kendskab til det pågældende programmel. Hvis personen er ubekendt med det nødvendige kodeord eller lignende og derfor kun kommer til at se et blokerende skærmbillede, kan der højest straffes for forsøg. Hvis gerningspersonen ønsker kendskab til et bestemt programmel, men alene får kontakt med andet programmel, er det mest nærliggende at bedømme forholdet som et forsøg. (Jfr. Hurwitz: Alm. D. s. 240 om »aberratio ictus«, cfr. strl.bet. 1985 s. 26 f.).

Bestemmelsen kræver forsæt, jfr. strl. § 19.

Se i øvrigt nedenfor s. 46 ff. om de øvrige led i paragraffen.

Straffen for overtrædelse af § 263, stk. 2, er bøde, hæfte eller fængsel indtil 6 måneder. Såfremt forholdet er begået med forsæt til at skaffe sig eller gøre sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder eller under andre særlig skærpende omstændigheder, kan straffen stige til fængsel indtil 2 år, jfr. *stk. 3.* Med hensyn til fortolkningen af de enkelte led i dette stykke, kan der henvises til bemærkningerne om de tilsvarende led i § 264, stk. 2, jfr. ovenfor s. 26 ff., samt strl.bet. 1985 s. 27 ff. og 78 ff.

Andre personers senere udnyttelse af de oplysninger, der er fremkommet ved overtrædelsen, kan straffes efter *strl. § 264 c.* Den omfatter desuden personer, som gennem en aktiv indsats »skaffer« sig den pågældende viden fra den umiddelbare gerningsperson. Derimod er passive modtagere af oplysninger straffri - når de ikke senere udnytter deres viden.

Straffen efter § 264 c afhænger af, om »førforbrydelsen« er § 263, stk. 2, eller stk. 3. Den afhænger således mere af førforbryderens forhold end af gerningspersonens egne.

I Sverige er 'dataintrång' kriminaliseret i datalagen, jfr. Nils Jareborg 1984 s. 285 f. og Jan Freese 1983 s. 162 ff.

Der foreligger et forslag om ændring af denne, så den med sikkerhed kommer til at omfatte »uppgifter som är under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för automatisk databehandling« (lagrådsremiss 1985-09-19).

c. Brug

Hvis en uberettiget brug af fysiske genstande indbefatter en brug af programmel, som er lagret på disse genstande, kan forholdet være strafbart efter strl. § 293, stk. 1 (strl.bet. 1985 s. 9). Hvis det alene er brugen af programmellet - ikke af dets fysiske bærer - der er uberettiget, må det strafferetlige værn som udgangspunkt søges i lovgivningen om enerettigheder, jfr. umiddelbart nedenfor.

d. Krænkelse af enerettigheder

Utilladt kopiering og videresalg af edb-programmel er et stort problem. På verdensplan anslår branchen(!), at den årligt taber 7 mia. kr. på grund af piratkopier. Tekstbehandlingsprogrammellet Wordstar er solgt i 800 000 eksemplarer, men det antages, at det kører på ca. 3 mio. datamater. Tabstallet må sammenholdes med, at årsomsætningen antages at være 1400 mia. kr. (SOU 1985:51). Tabet er således 0.5%. I Danmark skønner branchen, at det drejer sig om ca. 50 mio. kr. om året. I Danmark har klagerne især drejet sig om spil til hjemmedatamater. Det hævdes, at 70-80% af dem, der er i omløb, er illegale. De populære spil kopieres på billige kassettebånd, som sælges for en lav pris gennem små annoncer. Direktøren for Commodore har oplyst, at de fleste kopister, som han har kendskab til, er drenge i 13-års alderen, som sidder hjemme og supplerer deres lommepenge på den måde. Der er dog også »voksen« kriminalitet her i landet. Der verserer en erstatningssag om et millionbeløb. En københavnsk »hacker« skal have kopieret et jysk administrativt system og solgt det gennem det jyske firmas konkurrent. (Politiken 1984-11-27, 1985-02-20, 1985-03-03, 1985-05-01 og 1985-09-23).

Kopieringen kan være sket gennem en fredskrænkelse, jfr. reglerne ovenfor. Hvis programmellet er frit tilgængeligt for kopisten, f.eks. fordi han selv har købt det hos en autoriseret forhandler, kan reglerne om fredskrænkelser ikke anvendes. Retstridige kopieringer må i så fald rammes af enerettighedslovgivningen. Hvis begge sæt regler er overtrådt, kan der straffes efter dem begge ('i sammenstød').

Programmel kan normalt *ikke patentbeskyttes* som sådant, jfr. patentlovens § 1, stk. 2, nr. 3. Det kan derimod efter den herskende opfattelse være beskyttet af *ophavsretslovgivningen,* jfr. ophavsretslovens § 1, stk. 1, i.f. og bet. 1064/1985 s. 42 ff. Spørgsmålet har endnu ikke været prøvet for domstolene. (Et meget omtalt fogedforbud (Københavns Byret 1985-01-02) har næppe nogen væsentlig præjudikatsværdi). Ophavsretsbeskyttelse forudsætter, at programmellet er resultat af en individuel skabende åndsvirksomhed. Det skal have en egenartet og en selvstændig karakter, men det behøver ikke at være »nyt«. (Mogens Koktvedgaard 1968 og 1983 (spec. s. 322), W. Weincke & Jørgen Blomqvist i Karnov s. 2690, Gunnar Karnell 1984, Jon Bing 1985 og SOU 1985:51.85 ff.). De nævnte krav afstikker ikke nogen snæver ramme, som det vil ses af et eksempel fra et ganske andet livsområde.

Eksempel 24: En køreplan for Randers og omegn var forfatterretligt beskyttet. Denne ret blev krænket gennem udgivelsen af et lignende hæfte for Horsens og opland. (JD 1944.237 U).

Jon Bing konkluderer, at man i praksis kan gå ud fra, at ethvert program, som ikke er ganske trivielt, har tilstrækkelig 'værkshøjde' til at få ophavsretlig beskyttelse (1985 s. 32).

Det er kun fysiske personer, der kan frembringe værker i ophavsretslovens forstand. Udgangspunktet er, at retten tilkommer den person, der har fremstillet værket (her: programmellet). Hvis flere har skabt det i fællig, er retten - med visse undtagelser - også fælles. Juridiske personer (aktieselskaber m.m.) kan eje ophavsretten, hvis denne er blevet overdraget til dem. En aftale om overdragelse kan indgås på forhånd, f.eks. som led i en ansættelseskontrakt, jfr. lovens § 27. Aftalen behøver ikke at være udtrykkelig. Ophavsretten kan også gå over til virksomheden som følge af deklaratoriske branchesædvaner. (Mogens Koktvedgaard 1983 s. 324 f., W. Weincke & Jørgen Blomqvist i Karnov s. 2690, strl.bet. 1985 s. 70 og Jon Bing 1985 s. 50 ff.).

Efter lovens § 2 krænkes ophavsretten, når der fremstilles eksemplarer af det beskyttede værk, eller når det gøres tilgængeligt for almenheden. Jfr. også § 55 b om udenlandske krænkelser. Derimod er det ikke en ophavsretskrænkelse at købe en piratkopi eller at bruge en sådan på anden måde end nævnt i § 2. Reglen om fremstilling af kopier får en ganske særlig betydning inden for dataretten. Brug af programmel (som ikke er integreret i datamaten) forudsætter, at det indlæses i den datamat, der ønskes benyttet. Det antages i den herskende ophavsretlige teori, at en sådan indlæsning er tilstrækkelig til at realisere § 2s regel om ulovlige fremstillinger. Hvis dette synspunkt - som umiddelbart synes meget vidtgående - accepteres af de danske domstole, vil enhver uautoriseret brug af programmel blive en krænkelse af ophavsretten, medmindre indlæsningen (kopieringen) anses for lovlig med hjemmel i § 11 om kopieringer til rent privat brug. (Mogens Koktvedgaard 1983 s. 323, strl.bet. 1985 s. 70 og SOU 1985:51.54 ff. og 71 ff.).

Strafansvar pådrages ikke nødvendigvis, når der realiseres et gerningsindhold. Handlingen skal også være 'retstridig'. Det er muligt, at man ved hjælp af denne almindelige begrænsning kan nå frem til, at visse andre kopieringer end de rent private er straffri. Kopieringer med henblik på arkivering og som sikkerhed (sikkerhedskopier, »backup«) er antagelig straffri, selv om de måtte være aftalestridige. (Smh. Jon Bing 1985 s. 69).

Det er givet, at slaviske kopieringer af hele det beskyttede programmel, er en lovovertrædelse. Når der kun bruges en del af det, eller når der sker en udnyttelse af ideerne i det, afhænger det af handlingens beskaffenhed, om der er hjemmet for sanktioner. Disse afgrænsningsspørgsmål må henvises til ophavsretten.

Efter lovændringen i 1985 er normalstraffen bøde, jfr. § 55, stk. 1. Subjektivt kræves mindst grov uagtsomhed. Se om tilregnelses- og vildfarelsesproblemer Mogens Koktvedgaard 1966. Forsøg er straffri, jfr. strl. § 21, stk. 3. Kollektive enheder kan pålægges et bødeansvar.

Under særligt skærpende omstændigheder kan forsætlige overtrædelser, der er begået ved erhvervsmæssigt at fremstille eller sprede værket, straffes med hæfte eller fængsel indtil ét år. Særligt skærpende omstændigheder vil navnlig kunne være frembringelse af et betydeligt antal eksemplarer eller frembringelse, salg m.m. for at opnå betydelig vinding. Disse bestemmelser kan blive aktuelle med hensyn til edb-programmel (strl.bet. 1985 s. 70 f.). I disse tilfælde er forsøg også strafbare (strl. § 21 og FT 1984/85 A.4373 ff.).

Efter ophavsretslovens § 57 kan ulovlige kopier inddrages, når de er erhvervet til andet end privat brug, eller når de er erhvervet i ond tro. Desuden kan straffelovens almindelige konfiskationsregler eventuelt benyttes.

Se om norsk ret NOU 1985:31.18. I Finland blev maksimumsstraffen sat op fra 6 måneders til 2 års fængsel i 1984. Det er samme maksimum som for simpelt tyveri.

Tidligere anså man de civilretlige sanktioner for tilstrækkelige. Alvorlige krænkelser af ophavsret forudsatte et større apparat. Nu har den tekniske udvikling gjort det muligt for enhver at blive pirat, Dermed har de strafferetlige reaktionsmuligheder fået en øget betydning (FT 1984/85 A.4373 nr. 14). Opdagelsessandsynligheden er dog næppe særlig stor. Dertil kommer, at mange kopieringer af programmel er fuldt lovlige, fordi de sker til privat brug. Producenterne har derfor i stedet søgt at opbygge tekniske værn. Politiken har bragt et interview med en datalog, som fortalte, at hans administrative programmel var blevet ændret. »Nu er der anbragt en slags bombe i programmet. Disketten er i sig selv en nøgle, og forsøger nogen at kopiere, slettes hele programmet på få sekunder...« (1984-10-10). I dette ligger der nye juridiske problemer. Et programmel til en værdi af adskillige (måske mange) tusinde kroner kan blive slettet som følge af en hændelig fejlbetjening eller af et ikke lovstridigt forsøg på kopiering til privat brug. Mindstekravet - for at undgå et spørgsmål om ansvar for bedrageri eller tingsødelæggelse - må være, at køberen på købstidspunktet får klar besked om denne tekniske konstruktion.

C. Data

Datamaten fodres med inddata (»input«), lagrer data og afgiver uddata (»output«). I alle tre situationer kan der komme spørgsmål om ødelæggelse, om ændring og om kopiering. 'Data' er enhver form for repræsentation af kendsgerninger eller ideer, der kan kommunikeres eller behandles gennem en eller anden proces. I edb-verdenen til tider begrænset til oplysninger i form af tal og/eller symboler.

1. Inddata

'Inddata' er alle data, der indgår til databehandling.

a. Ødelæggelse

Hvis inddata er knyttet til et fysisk objekt, f.eks. spørgeskemaer, skemaer med aflæsninger eller fakturaer, er det en overtrædelse af *strl. § 291* at ødelægge det fysiske objekt. I teori og praksis antages det, at også ting, der er uden formueværdi, er omfattet af denne paragraf (Komm. strl. II s. 415). På

samme måde, som det blev antaget ovenfor, må det lægges til grund, at destruktion af information på maskinlæsbare magnetbånd og lignende kan straffes efter § 291, selv om det fysiske objekt (bæreren) for så vidt forbliver intakt. Der kan i stedet eller desuden være et strafansvar efter en specialbestemmelse, f.eks. strl. § 279 a om databedrageri, strl. § 178 om dokumentødelæggelse, strl. § 125 om bevisdestruktion eller bogføringslovgivningen.

Hvis ødelæggelsen ikke umiddelbart rammer et fysisk objekt, er strl. § 291 om tingsødelæggelse ikke anvendelig. Hvis man drikker en medarbejder fuld, så den pågældende glemmer de oplysninger, som skulle indlæses i maskinen, kan der (højst) være tale om et forsøg på et eller andet. Hvilken bestemmelse - om nogen - der kan straffes efter, vil afhænge af intentionen. I så henseende sættes grænserne kun af ens fantasi. Hvis der f.eks. pilles ved instrumenterne i et hospitals datamat, så den ikke reagerer på ændringerne i en patients blodtryk, skal der måske straffes for en personforbrydelse.

I Canada er der 1984-02-07 fremsat et lovforslag, hvorefter det er strafbart, hvis en person: »*(a)* destroys or alters data; *(b)* renders data meaningless, useless or ineffective; *(c)* obstructs, interrupts or interferes with the lawful use of data«.

b. Forvanskning

En delvis ødelæggelse af grundmaterialet kan bedømmes som en ødelæggelse af helheden eller af den pågældende del (strl. § 291). I mange tilfælde vil det dog kunne være mere naturligt at se krænkelsen som en forvanskning end som en ødelæggelse. I sådanne tilfælde kan ændringen i stedet straffes som databedrageri (strl. § 279 a), dokumentfalsk (strl. § 171), bevisforvanskning (strl. § 125), en overtrædelse af bogføringslovgivningen o.s.v. Personen kan også i kraft af sin stilling pådrage sig et strafansvar for tjenesteforsømmelse.

Eksempel 25: En politibetjent bortskaffede akterne i en sag mod en person, der var sigtet for spirituskørsel. Dømt efter strl. § 155, 2. pkt., om misbrug af offentlig tjeneste for at skaffe andre uberettiget fordel. (U 1982.1078 Ø.)

Det særlige i forbindelse med edb-behandlingen er, at dele af inddata let kan springes over i forbindelse med indlæsningen, eller at der uagtsomt eller forsætligt kan indlæses andet, end der skulle have været indlæst (»data diddling«).

Eksempel 26: På Brooklyn College indlæste studenter, som arbejdede med dataanlægget, eksamenskaraktererne. Der blev indlæst andre, end der stod på bedømmernes papirslister. (Computer World 1976-04-05).

Eksempel 27: I California forbigik en kontorassistent, der skulle indkode ubetalte parkeringsafgifter, de rapporter, der vedrørte hendes venner.

Eksempel 28: En ansat i et schweizisk skattevæsens regnskabscentral hullede fiktive indbetalingskort for sig selv og sine venner. Han blev dømt for 'Urkundenfälchung' (dokumentfalsk) (Ulrich Sieber 1977 s. 50 f.).

Eksempel 29: T var ansat i et engelsk credit card-firmas svenske filial. Fra en terminal i Sverige gav han hovedsædet besked om, at en lukket konto for LL skulle genåbnes, og at LL nu havde bopæl på en anden adresse. Et nyt kort blev automatisk udskrevet og kuverteret i England uden nogen manuel medvirken. Den opgivne adresse var Ts forlovedes. Da de blev anholdt af det schweiziske politi, havde de købt varer for 200 000 s.fr. i Basel. (Artur Solarz 1985 s. 120).

I eksemplerne 27 og 28 - og måske 26 - synes der efter referaterne at have været begået en embedsforbrydelse, jfr. eksempel 25. I eksempel 28 ville der også efter dansk ret kunne have været mulighed for at bedømme hulkortene som dokumenter og dermed forholdet som dokumentfalsk (smh. Komm. strl. II s. 137). På mange måder er eksemplerne 26 og 29 imidlertid mere karakteristiske. Det afgørende er jo ikke, hvad der kommer ind i maskinen, men hvad der kommer ud af den. I dette tilfælde skal de lagrede data danne grundlaget for senere udstedelse af eksamensbeviser, credit cards m.m. Indlæsningen er en *forberedelseshandling (evt. en iværksættelseshandling)* til det senere delikt. (Strl.bet. 1985 s. 59 f.).

c. Kopiering

1°. Kopiering af data kan være strafbar, hvis der derved sker en krænkelse af en tavshedspligt eller af andres fred. Der findes en række bestemmelser i lovgivningen. Se f.eks. strl. kap. 27. Ved ændringen af straffeloven i 1985 indføjedes der her et nyt *stk. 2 i § 263.* Det omhandler blandt andet det forhold, at en person »uberettiget skaffer sig adgang til en andens oplysninger«. Oplysningerne behøver ikke at være hemmelige eller at vedrøre særligt følsomme forhold. Det må anses for givet, at eftersætningen - »der er bestemt til at bruges i et anlæg til elektronisk databehandling« - også knytter sig til »oplysninger«. Alligevel er det en vidtfavnende forbrydelse. I dag vil næsten alle oplysninger på en eller anden måde blive brugt i et anlæg til elektronisk databehandling. En bogbestilling hos en boghandler, en tegning af et avisabonnement, en mekanikers timeseddel, en check som lommepenge til ens datter, en hospitalspatients temperatur, ankomsttiden for Oslo-flyet o.s.v., o.s.v. vil alle være oplysninger, som (også) er bestemt til at bruges i et anlæg til elektronisk databehandling. Og det er ikke muligt at udskille en kategori, som alene er bestemt hertil - det er i hvert fald ikke relevant. Det er heller ikke muligt at foretage en indskrænkning ved hjælp af de subjektive krav. Alle ved, at alt bliver edb-behandlet. Den svenske bestemmelse om 'dataintrång' kræver, at informationen alene skal kunne læses ved hjælp af datateknik (Nils Jareborg 1984 s. 286). Det norske forslag dækker kun »data som er lagret« (NOU 1985:31.31). Det er næppe muligt at indfortolke en sådan begrænsning i den danske bestemmelse, selv om den

på mange måder ville give en rimelig afgrænsning. Når straffelovrådet (strl.bet. 1985 s. 78) og justitsministeriet (FT 1984/85 A. 4373 ff.) omskriver bestemmelsens ordlyd til »dataanlægs oplysninger«, er der dog nogen støtte for, at der skal være en snævrere forbindelse mellem oplysningerne og edb-behandlingen.

Visse oplysninger er i udpræget grad bestemt til at *kunne* bruges, men ikke til at blive brugt. Det gælder f.eks. sikkerhedskopier, der, hvis alt går vel, er bestemt til at havne i en eller anden form for brokkasse efter en passende tid. Sådanne er utvivlsomt også omfattet af § 263, stk. 2.

Den usa-nske Counterfeil Access Device and Computer Fraud and Abuse Act af 1984 § 1030 er begrænset til visse særligt beskyttelsesværdige data. En tilsvarende begrænsning kan ikke indlægges i den danske lovregel.

2°. I privatregisterlovens § 20, stk. 2, er der et forbud mod, at edb-servicebureauer anvender de modtagne oplysninger i andet øjemed end til udførelse af den opgave, aftalen vedrører, og mod, at de lader oplysningerne opbevare eller bearbejde hos andre eller i udlandet.

3°. Af særlig interesse for edb-retten er de fredskrænkelser, som er kriminaliseret i *strl. § 152 a.* I den oprindelige straffelov af 1930 handlede § 152 om offentligt ansattes krænkelser af tjenestehemmeligheder. I Danmark overlod det offentlige, da noget sådant blev aktuelt, størstedelen af sine edb-opgaver til virksomheder, der ikke hørte under den offentlige forvaltning, f.eks. I/S Datacentralen af 1959. Mogens Koktvedgaard (1968) påpegede, at ansatte i sådanne virksomheder ikke var omfattet af strl. § 152. Registerudvalget tilsluttede sig dette i en delbetænkning fra 1971 (FT 1971/72 A.579 ff.) og gik ind for en ændring af paragraffen. Det forekom udvalget lidet rimeligt, at det offentliges og borgernes beskyttelse mod videregivelse af oplysninger skulle forringes, fordi staten og kommunerne valgte at dække deres behov for databehandling på denne måde. Registerudvalgets forslag blev med nogle ændringer gennemført som § 152, stk. 4, i 1972. I forbindelse med en generel gennemgang af tavshedspligten for personer i offentlig tjeneste eller hverv blev problemerne taget op på ny i bet. 998/1984. Spørgsmålene blev drøftet af Folketinget sammen med forvaltningsloven og loven om offentlighed i forvaltningen. Ved lov nr. 573 af 19.12.1985 ændredes straffelovens § 152 m.fl. Det tidligere § 152, stk. 4, blev erstattet af en ny § 152 a, 1. pkt. Efter denne skal den almindelige bestemmelse om offentligt ansattes tavshedspligt i § 152 nu også finde »tilsvarende anvendelse på den, som i øvrigt er eller har været beskæftiget med opgaver, der udføres efter aftale med en offentlig myndighed«. Hovedeksemplet er ansatte i edb-virksomheder. Bestemmelsen er dog ganske bred. Den omfatter også personalet i et datamaskinfirma, som udfører service og reparationer på maskinerne. Den

omfatter også vinduespudsere eller rengøringsassistenter, som får deres viden fra papirkurvene m.m. (FT 1985/86 A). Pligten til at holde tæt ophæves ikke med ansættelsesforholdets afslutning.

Reglen kan anvendes, selv om den pågældende ikke har haft retmæssig adgang til oplysningerne, og selv om der desuden kan straffes efter de almindelige fredskrænkelsesbestemmelser.

Efter den tidligere bestemmelse omfattede edb-virksomhedernes tavshedspligt alle oplysninger. Nu defineres området på samme måde som for de offentligt ansatte, d.v.s. at der skal være tale om »fortrolige oplysninger«. Dette defineres nærmere i § 152, stk. 3, som oplysninger, der »ved lov eller anden gyldig bestemmelse er betegnet som sådan, eller når det i øvrigt er nødvendigt at hemmeligholde den for at varetage væsentlige hensyn til offentlige eller private interesser«.

Den kriminaliserede handling er for det første *videregivelse af information.* Det kræves ikke, at der sker offentliggørelse. Det er tilstrækkeligt, at en enkelt anden person får beretningen. Det har normalt ingen betydning for strafbarheden, om videregivelsen sker i forbindelse med tavshedspålæg eller -løfter eller ej. (Jfr. bet. 998/1984 s. 96.) Det antages, at videregivelse kan ske gennem passivitet, f.eks. derved at fortrolige dokumenter ikke opbevares på forsvarlig måde (s.st. s. 156). I denne forbindelse må det dog erindres, at der kræves forsæt til videregivelse.

Oplysningerne skal formentlig i almindelighed have et vist konkret præg. En ansat, der fortæller en anden, at hans arbejde består i at bearbejde oplysninger om skibsrederes skatteforhold, har ikke overtrådt bestemmelsen. Det har han næppe heller, hvis han giver udtryk for, at danske skibsredere synes at have haft store indtægter i det forløbne år.

Videregivelsen skal være *uberettiget.* Berettigelse kan følge af mange forskellige forhold. § 152 e fremhæver de vigtigste tilfælde således: »1) er forpligtet til at videregive oplysninger eller 2) handler i berettiget varetagelse af åbenbar almeninteresse eller af eget eller andres tarv«. Se herved bet. 998/1984 og FT 1985/86 A. Se Mogens Koktvedgaard 1968 s. 166 f. om videregivelse til andre edb-firmaer.

Eksempel 30. Kommune-Data er et interessentskab, der ejes af Amtsrådsforeningen i Danmark og Kommunernes Landsforening. En fotograf var ansat her. Han tilegnede sig et sæt af et landsdækkende sygesikringsregister og søgte at sælge det til en postordreforretning. Han blev blandt andet dømt efter strl. § 291 (om bortskaffelse af ting) og § 152, stk. 4, jfr. § 21 (d.v.s. forsøg). (ØLD 1974. Domme 1973-1977 s. 143 og bet. 998/1984 s. 436).

For det andet er det kriminaliseret at *udnytte* oplysningerne på en uberettiget måde. I dette ligger, at forholdet skal have en vis grovhed. Ikke enhver brug er så graverende, at den bør have strafferetlige konsekvenser. Hvis

en ansat får viden om, at der skal bygges et kæmpekraftværk på en naturskøn odde, vil det være straffrit, at han sammen med sin familie lejer et sommerhus dér for at nyde den sidste chance for at se naturen. Derimod vil det kunne være strafbart, at han giver sig til at spekulere i ejendomshandeler i området. (Smh. bet. 998/1984 s. 98).

Udenforstående personer, som køber en ansat til at fremskaffe information, eller som hjælper den ansatte med råd eller dåd, kan straffes for deres medvirken, jfr. strl. § 23.

Eksempel 31: En person blev straffet efter strl. § 152, jfr. § 23, ved at have tilskyndet en ikke-identificeret person i et landsarkiv til at overlade sig kopier af adoptionspapirer. (Bet. 998/1984 s. 438).

En rent *efterfølgende medvirken* kan ikke straffes efter strl. § 23, men der er en specialbestemmelse herom i § 152 d. Tidligere var den i § 152, stk. 5. Nu lyder den:

»... den, som uden at have medvirket til gerningen uberettiget skaffer sig, videregiver eller udnytter oplysninger, der er fremkommet ved en sådan overtrædelse«.

Eksempel 32: En kriminalassistent videregav efter anmodning oplysninger fra kriminalregisteret til sin svigerinde. Svigerinden blev dømt efter strl. § 152, stk. 5, jfr. stk. 1. Eftersom han gjorde det efter hendes anmodning, burde der formentlig i stedet have været straffet for medvirken. (ØLD 1982. Domme 1978-1982 s. 116).

Se bet. 998/1984 s. 151 f. om de særlige problemer om orientering til den pågældendes organisationer m.m.

En offentliggørelse kan i denne forbindelse efter omstændighederne bedømmes som en udnyttelse.

Eksempel 33: En journalist blev straffet efter strl. § 152, stk. 5, jfr. stk. 1, for at have skrevet en artikel på grundlag af oplysninger fra en tidligere skatterådsformand. (ØLD 1976. Bet. 998/1984 s. 437).

Bestemmelserne kræver *forsæt*. (Smh. bet. 998/1984 s. 113 f. om muligheden for straf i tilfælde, hvor der kun foreligger den laveste forsætsgrad, den såkaldte 'dolus eventualis').

Straffen er bøde, hæfte eller fængsel i indtil 6 måneder. Er krænkelsen sket for at skaffe sig eller andre uberettiget vinding eller foreligger der i øvrigt særlig skærpende omstændigheder, kan straffen stige til fængsel i 2 år. (Denne sidste bestemmelse blev citeret i eksempel 30).
Jfr. strl.bet. 1985 s. 29.

4°. Kopieringen kan ske med henblik på senere misbrug. I disse tilfælde er der (også) tale om *forsøg på et eller andet*. F.eks. kan kopiering af et maskinlæsbart kontokort være en forberedelseshandling til bedrageri.

2. De lagrede data

Som nævnt ovenfor har det næppe nogen betydning, hvordan de pågældende data lagres. De behøver heller ikke at være i umiddelbar tilknytning til maskinen. Et magasin med magnetbånd rummer retligt set den samme art information som et »fast« lager i en maskine.

a. Ødelæggelse

Som nævnt ovenfor kan de almindelige *tingsødelæggelses*regler i strl. § 291 anvendes, såvel når de fysiske objekter (magnetbånd, disketter o.s.v.) ødelægges, som når de blot slettes for det indlæste, jfr. eksempel 19. En trussel om at gøre noget sådant kan ikke straffes som forsøg på tingsødelæggelse, men der kan være et ansvar efter andre regler.

Hvis ødelæggelsen foretages med berigelsesforsæt, er udgangspunktet for den strafferetlige vurdering § 279 a, jfr. nedenfor s. 65 ff.

Eksempel 34: En tysk operatør tog i 1973 et bånd med vigtige data fra sin tidligere arbejdsgiver. Han krævede $ 200 000 for at tilbagegive det. Arbejdsgiveren betalte, da det trods alt var det billigste for firmaet. (Ulla Høg 1981 s. 66).

Dette er et eksempel på *afpresning* (strl. § 281). T truer med betydelig skade på gods for derigennem at skaffe sig en uberettiget berigelse.

Hvis der ikke er berigelsesforsæt, vil »kidnapningen« eventuelt kunne straffes efter en af de umiddelbart nedenfor omtalte bestemmelser.

Hvis handlingen er udtryk for ren chikane, hævn eller lignende, kan det være nærliggende at bruge strl. § 291 om bortskaffelse af ting, der tilhører en anden, eller strl. § 293, stk. 2, der handler om at lægge hindringer i vejen for, at nogen udøver sin ret til at råde over en ting.

Strl. § 291 handler først og fremmest om tingsødelæggelse. For så vidt afløste den strl. 1866 § 296. Denne indeholdt derimod ingen regel om borttagelser (C. Goos 1896 s. 4 f.). Strl.bet. 1912 § 313, stk. 1, medtog også, at nogen »forspilder en Ting«, »saa at f.Eks. ogsaa det Tilfælde, at Tingen bortkastes, saa at den ikke kan faas tilbage, utvivlsomt falder ind under Bestemmelsen« (mot. 274). Torp ændrede ordlyden i sit udkast: »»Bortfjerner« er benyttet i Stedet for det iøvrigt nærliggende »bortkaster«, fordi det formentlig er noget mere omfattende« (strl.bet. 1917 mot. 250 om § 260, stk. 1). Strl.bet. 1923 (§ 265) medtog »udtrykkeligt Bortskaffelse af Ting, hvorved forstaas, at Tingen skaffes af Vejen, saaledes at den ikke eller kun ved vanskelige eller bekostelige Foranstaltninger kan faas tilbage« (mot. 382 f.). Bortskaffelse skal med andre ord være af »den Art, at den paafører Ejeren et definitivt Tab ... eller dog væsentlige Udgifter til Fremskaffelse af Tingen« (Krabbe s. 719).

Strl. § 293, stk. 2, har heller ingen direkte modsvarighed i strl. 1866. (Smh. C. Goos 1896 s. 7 f.). Dens oprindelse må søges i strl.bet. 1912 § 314, nr. 3, der skulle dække »visse negative Indgreb, hvad enten de ramme Ejeren eller en Person, der har en begrænset tinglig Ret over Tingen« (mot. 275). Efter Torps udkastet skulle alene krænkelser af de sidstnævnte være omfattet (§ 262). Torps begrundelse for dette synes at have været, at krænkelsen ellers havde karakter af selvtægt (mot. 249, smh. med udkastet til forseelseslovens § 35, mot. 29). Ligeledes strl.bet. 1923 § 267, stk. 2, med mot. 385, regeringsforslagene af 1924 § 293, af 1927 § 293 og af 1929 § 291. Under Landstingets afsluttende udvalgsbehandling blev bestemmelsen atter ud-

videt, »saaledes at den ogsaa rammer Tilfælde, hvor nogen hindrer Ejeren selv i at raade over sine Ting« (RT 1929/30 B.1875). Udvalgsforslaget blev vedtaget uden debat og uden afstemning. Om handlingen er udført af chikane eller med andet formål, er ligegyldigt (Krabbe s. 722). Den angår fortrinsvis faktiske hindringer for tredjepersons ret over tingen (Hurwitz Sp. D. s. 436 f.).

Ordlyden af de to bestemmelser giver ikke megen vejledning med hensyn til den indbyrdes afgrænsning. Når bestemmelsernes forhistorie tages i betragtning, bliver det nærliggende at lade meget langvarige og byrdefulde bortskaffelser være omfattet af § 291 (f.eks. URD Frederiksberg 1985-08-09 (anket)), og at lade korterevarende fjernelser, som vel er generende, men ikke overmåde byrdefulde, være omfattet af § 293, stk. 2. For dette resultat taler også, at § 291 i øvrigt behandler ødelæggelser af ting, medens § 293 i øvrigt handler om det såkaldte brugstyveri. Endvidere peger et selvtægtsmotiv i retning af § 293, stk. 2. Der er kun få trykte domme. De synes at antyde en større tilbøjelighed til at anvende § 291, end jeg kan se tilstrækkelig grund for.

Eksempel 35: T satte sig i besiddelse af et kommunekontors regnemaskine for at kunne udøve tilbageholdsret i den. Dømt efter strl. § 291. (U 1960.746 U).

Eksempel 36: T, som var ejendomsmægler, havde muligvis et tilgodehavende på 25 000 kr. Ved at knuse en rude trængte han ind hos den formodede skyldner og fjernede tæpper til en værdi af 16 000 kr. Umiddelbart efter ringede han til politiet og oplyste, at han havde »lånt« tæpperne. Dømt efter strl. § 291. Med føje skeptisk over for denne subsumption B. Unmack Larsen i Komm. strl. II s. 415. (ØLD 1973, Domme 1973-1977, s. 316).

Ud fra almindelige retskildebetragtninger havde det nok været mere rimeligt at bruge § 293, stk. 2, (eller selvtægtsbestemmelsen) i disse tilfælde.

§ 293, stk. 2, kræver forsæt (jfr. strl. § 19), medens § 291 også i et vist omfang rammer grov uagtsomhed. Overtrædelse af § 293, stk. 2, straffes med bøde eller hæfte eller under skærpende omstændigheder med fængsel i indtil 6 måneder. Strafferammen i § 291 går fra bøde til fængsel i 4 år; se nærmere i paragraffen.

På edb-området kan en lignende regel i *strl. § 263, nr. 1,* få betydning. Efter denne paragraf straffes den, som uberettiget »unddrager nogen ... anden lukket meddelelse«, herunder f.eks. oplysninger på magnetbånd.

Der er et fælles område for strl. § 263, § 291 og § 293, stk. 2. Afgørende for valget mellem dem vil det være, om lovovertrædelsen har karakter af en formuekrænkelse (§§ 291 og 293) eller af en fredskrænkelse (§ 263).

Er der f.eks. tilstrøbt skabt gener for produktion m.m., eller er der tale om destruktion m.m. af vigtige forskningsresultater, vil de førstnævnte være mest nærliggende. (Smh. også eksempel 34). Er der f.eks. tale om bestyrelsesmødereferater, som indehaveren ikke ønsker ud til andre, er den

sidstnævnte nærliggende. Hvis motivet og de øvrige omstændigheder ikke med tilstrækkelig klarhed peger på det ene eller det andet moment, er det formentlig ofte mere naturligt at bruge § 263 (lex specialis) end at straffe efter begge (sammenstød).

Ødelæggelsen kan også være strafbar efter strl. § 178 (om beviser), bogføringsloven o.s.v. (strl.bet. 1985 s. 61 f.).

b. Ændring

1°. C. Goos skrev for mange år siden, at dokumentfalsk ikke blot er et »Angreb paa den Enkeltes Handlefrihed, men paa den sociale Handlefrihed, fordi et af Samfundslivet skabt og for det uundværligt Bestemmelsesmiddel misbruges« (1895 (II) s. 8). Det sagte gælder næppe om lejlighedsdokumenterne i dag, men det gælder utvivlsomt i stedet om edb-forbrydelserne af denne art. Udskrifter fra sådanne maskiner er som regel ganske uigennemskuelige. Alligevel lægges resultaterne i almindelighed til grund med blind tillid af de personer, som de berører. I et svensk eksperiment var det kun én af otte kontohavere, som protesterede, da banken udsendte en for lav saldoopgørelse (Artur Solarz 1985 s. 153). Det ville på en sådan baggrund være nærliggende med en særlig kriminalisering. Det ville også være hensigtsmæssigt, fordi vi på den måde ville få en mere rammende beskrivelse af forholdet. (Cfr. strl.bet. 1985 s. 62 f.) Det må dog fremhæves, at de eksisterende regler utvivlsomt allerede nu omfatter (næsten) alle de situationer, hvor der er et væsentligt behov for strafferetlig beskyttelse af interesserne.

2°. Den *svenske* datalags § 21 kriminaliserer den, som »olovligen ändrar eller utplånar eller i register för in sådan upptagning«. Sådan 'dataintrång' straffes (som udgangspunkt) med bøde eller fængsel i højst 2 år. Se om denne regel SOU 1983:50 s. 171 f.

Det nye *finske* udkast til straffelov (31. maj 1984) har i kapitlet om 'förfalskningsbrott' (33. kap.) taget særligt hensyn til forfalskning i forbindelse med misbrug af datamater.

I *BRD* er 'Fälschung technischer Aufzeichnungen' (datafalsk) kriminaliseret i StGB § 268. Baggrunden for denne bestemmelse var netop, at man i mellemmenneskelige forhold går ud fra, at maskiner er ubestikkelige, at de arbejder uden at lave fejl, og at de afgiver de fremkomne resultater rigtigt. Bestemmelsen er ganske vidtfavnende. I tysk teori er det f.eks. blevet påpeget, at det kan være betænkeligt, at den omfatter alle maskiner, også sådanne som ikke er undergivet nogen form for offentlig kontrol. § 268 kræver, at handlingen skal være begået »zur Täuschung im Rechtverkehr« (for at skuffe i retsforhold). Det er ikke tilstrækkeligt, at de pågældende data skal bruges i firmaets interne kontrol. 'Aufzeichnungen' er i den forbindelse kun data, som er bestemt til at tjene som bevis for en retligt relevant kendsgerning. Forskellen på dokumentfalsk og datafalsk er især, at et 'dokument' forudsætter en udstederbetegnelse og en »Gedankenerklärung« (tilkendegivelse), medens disse krav ikke stilles med hensyn til de »tekniske optegnelser«. Der stilles heller ikke krav om skriftlighed. Det er derfor muligt at anvende StGB § 268 på politiets filmoptagelser i forbindelse med gadeovervågning, på båndoptagelser med tale, på strimler fra radioaktivitetsmåleinstrumenter og selvfølgelig på de her omtalte data i edb-anlæg. Straffen er frihedsstraf op til 5 år eller bøde. Se i øvrigt i Schönke-Schröder s. 1768 ff. – Se endvidere forslaget til nye §§ 269 og 270, der for tiden behandles i forbundsdagen. § 269 skal omfatte »Fälschung gespeicherter Daten«, der skal benyttes som bevis i retsforhold. § 270 skal omfatte »Täuschung im Rechtverkehr bei Datenverarbeitung«.

3°. I *dansk ret* må man - som i tysk ret - i almindelighed afvise muligheden for at straffe efter dokumentfalskbestemmelserne. Strl. § 171, stk. 2, kræver, at der skal foreligge en »skriftlig tilkendegivelse«. Dette krav er ikke opfyldt ved lagrede data. (Smh. strl.bet. 1985 s. 60, Komm. strl. II s. 137 og Waaben: Sp. D. s. 283 f. Jfr. også finsk HRD 1983-11-10. Anderledes i norsk ret, som har en videre definition, NOU 1985:31.11 f.) Efter omstændighederne kan en ændring ses som en ødelæggelse af en sådan art, at det kan være naturligt at bruge strl. § 291 om tingsødelæggelse, jfr. ovenfor. Det ville måske være en mulighed i nedenstående eksempel.

Eksempel 37: En udenforstående person specialiserede sig i »at vaske folk rene« i et stort kreditoplysningsbureaus registre. (Los Angeles Times 1976-04-04).

Det vil være vanskeligere at finde en passende bestemmelse i de »modsatte« situationer, selv om der også her sker en slags ødelæggelse.

Eksempel 38: I årene 1968-72 fik FBI registreret falske ufordelagtige oplysninger hos kreditoplysningsbureauerne om personer, som FBI anså for radikale eller for at have kritisable politiske standpunkter. (Thomas Whiteside 1980 s. 44).

I almindelighed vil det være muligt at se indgrebet som en forberedelseshandling (eventuelt en iværksættelseshandling) til en eller anden forbrydelse. I det omfang, hvor den udskrevne tekst til sin tid vil opfylde straffelovens krav til et 'dokument', vil handlingen kunne bedømmes som et forsøg på dokumentfalsk eller dokumentsvig. (Jfr. ovenfor s. 37).

I eksempel 37 kan handlingen efter omstændighederne karakteriseres som medvirken til kreditbedrageri (strl. § 279, jfr. § 23, evt. jfr. § 21).

Endvidere kan strl. § 263 eller § 279 a eventuelt bruges, jfr. s. 38 ff. og 65 ff.

c. Kopiering

Dataanlæg yder kun et begrænset værn omkring de lagrede informationer. Det usa-nske forsvarsministerium nåede efter en undersøgelse frem til, at kun 30 af dets 17 000 datamater var »even minimally secure« mod indtrængen fra dygtige »hackers« (Time 1985-06-17). Dertil kommer risikoen for indgreb fra personalet i anlægget.

Gennem kopieringen kan der ske en tilegnelse af hemmeligheder m.m. Jfr. reglerne om industrispionage og andre fredskrænkelser, som blev behandlet ovenfor. For så vidt angår de lagrede data, rejser formuleringen af strl. § 263 et spørgsmål. Efter ordlyden skal de beskyttede data være »bestemt til at bruges«. Hvis den tilsigtede behandling for så vidt er afsluttet, men oplysningerne endnu ikke er slettet, er vi uden for det område, som efter formuleringen er beskyttet. En videre forståelse synes dog mulig. (Smh. strl.bet. 1985 s. 22 f.). Det gør ingen forskel ved de nævnte paragraffer, om der er tale om enkelte data eller om større samlinger af data.

De lagrede data kan også være beskyttet gennem ophavsretten. Det vil f.eks. gælde et magnetbånd med en ny roman i bogtrykkerens maskiner. Hvis der sker en kopiering af hele databaser, kan den særlige »katalogregel« i ophavsretslovens § 49 blive aktuel. Den relevante del af den lyder:

»Kataloger, tabeller og lignende arbejder, der sammenstiller et større antal oplysninger .... må ikke eftergøres uden samtykke af den, som har frembragt dem, før 10 år er gået efter det år, da arbejdet blev udgivet.

Er arbejder af den nævnte art eller dele deraf genstand for ophavsret eller anden beskyttelse, kan denne også gøres gældende.

...«

Se bl.a. Jon Bing 1985 s. 117 ff., Jes Anker Mikkelsen 1976, Else Mols 1985 og bet. 1064/1986 s. 19 ff.

Eksempel 39: En dansk producent af mikrodatamater skulle udforme et program, der kunne rette stavefejl til brug i et tekstbehandlingsprogrammel. En medarbejder havde kendskab til kode m.m. for en datamat på universitetet, hvor der var lagret 100 000 korrekt stavede ord. Firmaet tappede den lange liste over telefonnettet. (Jan Carlsen i Folkebladet/Erhverv (Kalundborg) 1985-05-25).

Kopieringen kan være en krænkelse af pligter, der følger med særlige ansættelsesforhold. Se således s. 47 ff. om strl. §§ 152 ff.

Eksempel 40: En politiassistent havde i privat øjemed indhentet oplysninger om personer i den ejendom, hvor han boede, fra det centrale kriminalregister. Dømt for overtrædelse af strl. § 155 om misbrug af offentlig tjenestestilling til at krænke privates eller det offentliges ret.

Han var endvidere tiltalt efter samme bestemmelse for at have indhentet oplysninger i det centrale personregister om de samme beboere og for at have videregivet oplysninger om, at to af beboerne ikke var tilmeldt adressen. For det blev han frifundet, da 4 af de 6 dommere og domsmænd ikke mente, at dette forhold havde en så alvorlig karakter, at det kunne anses for misbrug i den forstand, som ordet er brugt i strl. § 155. (U 1985.680 Ø).

I Sverige bedømmes sådant som 'dataintrång' efter datalagen. (Jan Freese 1985 s. 165).

Hvis de pågældende data på forhånd kendes af den person, som kopierer dem, vil selve kopieringen næppe i almindelighed være strafbar i sig selv. (Dog eventuelt f.eks. den nys nævnte strl. § 155). Men kopieringen vil i sådanne tilfælde (næsten) altid være en forberedelseshandling (iværksættelseshandling) til en krænkelse af tavshedspligt eller andet.

Eksempel 41: En dataoperatør i et norsk forsikringsforetagende solgte en fortegnelse over forsikringstagernes sygdomme til et lægemiddelfirma, som siden tog individuel kontakt med dem for at sælge medicin. (Thomas Whiteside 1980 s. 41). Her ville kopieringen kunne straffes efter strl. § 264 d, jfr. § 21, om forsøg på at give oplysninger om private forhold.

Eksempel 42: T kopierede lister over bankkunder med store indeståender med henblik på senere at bedrage dem. (Hälsingborgs Tingsrätt 1983. Artur Solarz 1985 s. 123.) Det ville i Danmark være forsøg på bedrageri.

Hvis kopieringen sker på et bånd, der tilhører firmaet, vil der foreligge et (forsøg på) tyveri (strl. § 276)/underslæb (strl. § 278) med hensyn til dette, jfr. ovenfor.

Eksempel 43: En tysker kopierede sit firmas adressekartotek og solgte det til en konkurrent for mere end 150 000 DM (Ulrich Sieber 1977 s. 103 ff.). Det blev bedømt som 'Vergehen der Untreue' (mandatsvig) og 'Unterschlagung' (underslæb).

For så vidt angår henførelsen under underslæb bemærker retten: »Die Zueignung ist darin zu sehen, dass er ... den wirtschaftlichen Wert, den diese Adressen darstellen, der Firma H teilweise entzog. Wird einer Sache der wirtschaftliche Wert auch nur teilweise entzogen, so liegt eine rechtwidrige Zueignung selbst dann vor, wenn die Sache dem Eigentümer später zurückgegeben wird.« (s.st.s. 105).

I Holland er der dømt for underslæb i en situation, hvor en ansat havde kopieret data og programmeller med henblik på senere brug i egen virksomhed.

Efter dansk ret vil tilegnelse eller salg af information ikke kunne bedømmes som tyveri/underslæb, medmindre informationen er fysisk knyttet til »en fremmed rørlig ting«, jfr. strl. § 276/§ 278. Det vil derimod kunne være omfattet af markedsføringslovens § 9, stk. 2, jfr. ovenfor s. 28 ff. Jeg vender tilbage til spørgsmålet om mandatsvigsbestemmelsens anvendelsesområde nedenfor i afsnit III. Der er næppe tvivl om, at nogle af disse dispositioner fra ansatte vil kunne straffes efter denne bestemmelse (strl. § 280).

3. Uddata

'Uddata' (»output«) betegner de resultater, der kommer ud af en edb-kørsel. Det kan være et enkelt tal (regneresultat), en sproglig tekst, en tabel, en grafisk fremstilling, en tegning, musik, »maskin-tale« o.s.v.

a. Hindring af udskrivning m.m.

En sådan hindring vil enten have karakter af en standsning af maskinen, jfr. ovenfor s. 23 ff., eller af en afbrydelse af datatransmissionen, jfr. nedenfor s. 57 ff.

Hvis uddata først ødelægges efter udskrivningen, vil der typisk foreligge tingsødelæggelse (strl. § 291). Efter omstændighederne kan andre bestemmelser, f.eks. strl. § 178 om undertrykkelse af bevismidler, finde anvendelse. (Strl.bet. 1985 s. 61 f.).

b. Forvanskning

De ovenfor behandlede indgreb i maskinen, programmellet eller data vil kunne resultere i en forvanskning af uddata. Efter sagens nærmere omstændigheder kan det være mest rimeligt at se indgrebet som et angreb på disse elementer eller at se det som (et forsøg på at gennemføre) en selvstændig forvanskning af uddata. Det er alene disse situationer, som behandles nedenfor. Efter gældende ret er sådanne handlinger kun selvstændigt kriminaliseret, hvis de pågældende data skal have en særlig funktion. Hvis uddata fremkommer i skriftlig form på papir eller andet underlag, kan straffe-

lovens dokumentbestemmelser blive aktuelle. Herunder kan muligvis også falde tekst på en dataskærm (billedskærm, der ligner en TV-skærm). (Se nærmere om svensk ret, Krister Malmsten 1985 s. 239). For så vidt angår forvanskninger vil det især blive reglerne om *dokumentfalsk*. Afgørende er, om betingelserne i strl. § 171, stk. 2, er opfyldt. Endvidere skal det, jfr. stk. 1, bruges til at skuffe i retsforhold.

Såfremt den skriftlige erklæring afgives til brug i retsforhold, der vedkommer det offentlige, kan *strl. § 163* anvendes. Hvis de pågældende data kommunikeres direkte fra en datamat til en anden uden mellemkommende papir, er denne bestemmelse uanvendelig, jfr. Komm. strl. II s. 120. Men § 163 kan eventuelt bruges på en medfølgende erklæring. Hvis denne datakommunikation i udpræget grad erstatter en (tidligere) skriftlig form, kan det overvejes, om der bør straffes efter bestemmelsernes analogi.

Strl. § 162 om pligtmæssige erklæringer stiller ingen formkrav. I det omfang, at f.eks. en statsinstitution accepterer, at pligtige indberetninger overføres direkte, vil det juridiske problem i praksis ofte blive afgjort gennem en fortolkning af de pågældende specialbestemmelser.

Eksempel 44: Toldvæsenet accepterer nu i et vist omfang magnetbånd. I stedet for dagligt at indsende et større antal papirformularer med bilag m.m. kan det hele nu indsendes på magnetbånd én gang om måneden, således at bilag m.m. opbevares på virksomheden (tf aktuel data/edb 1984-03-26).

Se i øvrigt strl.bet. 1985 s. 63 f.

Forvanskningen kan endvidere have som baggrund, at de pågældende uddata - skriftlige eller ikke-skriftlige - skal indgå i en maskinel eller menneskelig beslutningsproces.

Typisk vil der være tale om et *forsøg* på at hidføre en uberettiget berigelse. I disse tilfælde vil spørgsmålet være, hvilken af *berigelsesforbrydelserne,* der skal bruges. Det vender jeg tilbage til i afsnit III.

De urigtige data kan også indgå i *andre former for svig*. F.eks. kan en forvansket udskrift fra et kriminalregister måske medføre, at en uskyldig bliver sigtet (strl. § 164) eller anholdt (strl. § 261).

c. Kopiering

Kopieringer vil i de tilfælde, hvor de kan straffes, i almindelighed have karakter af fredskrænkelser (industrispionage, brud på tavshedspligt o.s.v.), jfr. ovenfor.

D. Datatransmission

Data kan transmitteres på mange forskellige måder. I denne forbindelse vil jeg alene behandle den overførsel, der foregår gennem det offentlige telefonnet eller på lignende måde. Det er i overensstemmelse med sædvanlig sprogbrug, hvorefter 'datatransmission' er betegnelse for udnyttelse af en teknik, hvor man ad elektronisk vej sender data fra et sted til et andet. Forstyrrelse af postbesørgelsen er selvstændigt kriminaliseret. Forstyrrelse af radiokommunikation er det også i nogen grad. Disse kriminalitetsformer må forbigås af pladshensyn.

Ændringer i disketter m.m., som sendes med bud eller lignende, må behandles efter reglerne om lagrede data.

Uberettiget åbning af breve eller pakker med disketter og senere afspilning antages i Norge at være strafbar efter begge sæt regler (realkonkurrence) (NOU 1985:31.32).

1. Hindringer

Datatransmission over telefonnettet kan hindres på forskellige måder. Ledninger kan klippes over, strømforsyningen kan afbrydes, forstyrrende støj kan forårsages o.s.v.

Strl. § 193 omfatter efter straffelovsændringen i 1985 den, »som på retsstridig måde fremkalder omfattende forstyrrelse i driften af ... telegraf- eller telefonanlæg ...«

I strl. 1866s tilsvarende bestemmelse var der intet krav om, at der skulle fremkaldes omfattende forstyrrelse af almindeligt benyttede telegrafer m.m. C. Goos ville ved fortolkning udelukke de »til rent privat Brug indrettede Anstalter« (1895 (I) s. 671). »Hindring af Funktionærernes Virksomhed« anså han derimod også for omfattet af bestemmelsen (s.st.s. 672). Disse to fortolkningsresultater kom direkte til udtryk i det første straffelovsudkast (strl.bet. 1912 § 394, mot. 323 f.). Angreb på private anlæg blev her forudsat straffet efter den almindelige tingsødelæggelsesbestemmelse.

I Torps udkast var særreglen om at hindre funktionærernes virksomhed udeladt. Det synes nærmest begrundet i, at Torp mente, at angreb på embedsmænd burde behandles i det særlige kapitel herom. (Strl.bet. 1917 § 176, mot. 167 ff.). Der skal næppe heri ses en afvisning af muligheden for at straffe i sammenstød.

Den 2den straffelovskommission fremhævede, at forstyrrelsen skulle være omfattende, og at man ellers måtte falde tilbage på de præventive love, som skulle bevares. (Strl.bet. 1923 § 177, mot. 295 ff.).

Det første regeringsudkast tog afstand fra dette og ville svække »omfattende« til »mere omfattende« (RT 1924/25 A.3360 om § 196). Folketingsudvalget slettede atter »mere«, men opfattede selv dette som en »[f]ormel Ændring« (RT 1928/29 B.2183). Med den netop nævnte baggrund forekommer denne kommentar noget kryptisk.

Ved straffelovsændringen i 1985 udgik ordene »almindeligt benyttede«. Der tilsigtedes ingen realitetsændring med dette. (Strl.bet. 1985 s. 41 f.).

§ 193 kan anvendes, uanset hvem der ejer anlægget, men det skal bruges eller i det mindste være til disposition for en bredere gruppe. Overklipning af en ledning, der kun fører til én virksomhed eller én kontorbygning, kan ikke straffes efter denne paragraf. Heller ikke, hvis der er nogle få ofre. Men se herved eventuelt andre led i paragraffen, jfr. ovenfor s. 23 ff. Forstyrrelsen kan også hidføres gennem tvang over for eller bestikkelse af televæsenets personale.

Forsætlige overtrædelser straffes efter lovændringen i 1985 med hæfte eller fængsel indtil 4 år eller under formildende omstændigheder med bøde. Begås forbrydelsen uagtsomt, er straffen bøde eller hæfte. I praksis rejses der kun tiltale i særligt grove tilfælde (Komm. strl. II s. 185). Der ses ingen danske trykte domme om afbrydelser af telefonledninger m.m.

Eksempel 45: En telefonmontør i Örebro åbnede et af telefonselskabets relæskabe og afbrød ledningen til en banks datasystem. Derpå gik han hen til banken og præsenterede en udtrækseddel på sin hustrus konto på et ikke særligt stort beløb, men dog på mere, end der stod på kontoen. Kassereren kunne ikke kontrollere, hvad der stod på kontoen, og udbetalte beløbet. Derpå ilede montøren tilbage til relæskabet og genskabte bankens dataforbindelse. Efter nogle få dage indbetalte han det overtrukne beløb til banken. Først efter at have gennemført dette 14 gange i løbet af 1½ år blev han afsløret. (Politiken 1984-02-08).

Sådan som sagen ligger oplyst, fik montøren blot nogle kortvarige og små lån, som alle blev indfriet meget hurtigt. Det er derfor lidet naturligt at se hans forhold som en berigelsesforbrydelse. I anklageskriftet siges det, at banken ikke har lidt økonomisk skade. Under lidt andre omstændigheder kunne det ellers have været naturligt at straffe for bedrageri over for banken.

Montøren blev tiltalt efter BrB 13:4 om 'sabotage'. Denne bestemmelse svarer til strl. § 193, derved at den kriminaliserer den, som »allvarligt stör eller hindrar den allmänna samfärdseln eller användningen av telegraf, telefon, radio eller dylikt allmänt hjälpmedel«. Tingsrätten frifandt montøren under henvisning til, at den pågældende ledning alene blev anvendt til bankens egen datakommunikation, selv om den blev ejet af Televerket. »Ansvar för sabotage måste ... förutsätta att ett allmänt hjälpmedel eller en anläggning för allmänhetens nyttjande angripits«.

Subsidiært var han tiltalt efter BrB 8. kap. 8. § 2. st. om 'egenmäktigt förfarande' (grovt brott). Denne bestemmelse dækker det forhold, at »någon utan tillgrepp, genom att anbringa eller bryta lås eller annorledes, olovligen rubbar annans besittning eller och med våld eller hot om våld hindrar annan i utövning av rätt att kvarhålla eller taga något«. Denne bestemmelses nærmeste modsvarighed i dansk ret er strl. § 293, stk. 2. Se i øvrigt om bestemmelsen Nils Jareborg 1978 s. 93 f. Tingsrätten fortsatte: »...s förfarande har dock inneburit att han olovligen rubbat bankens besittning till datalinjen«, og montøren blev herefter idømt en betinget dom med en tillægsbøde på 120 dagbøder à 50 kr. (Örebro Tingsrätt 1984-04-12).

I forarbejderne til straffeloven af 1930 blev det forudsat, at de præventive love på området skulle opretholdes ved siden af strl. § 193.

Den første af disse var l. 54 15.2.1895 om forholdsregler til beskyttelse af *undersøiske telegraf- og telefonledninger.* Den gælder stadig. Overtrædelser straffes nu med bøde, hæfte eller fængsel i indtil 1 år.

Den anden var l. 84 11.5.1897 om *telegrafer og telefoner.* Dens straffebestemmelse blev ophævet ved l. 119 31.3.1960.

Den tredje var l. 99 19.4.1907 om *trådløse* telegrafer (radiotelegrafer). Den tilsvarende er nu lbkg. 210 6.4.1976 om radiokommunikation. Til denne slutter sig adskillige bekendtgørelser.

De nævnte præventive love genemgås nærmere i denne bogs 1. udgave.

I det omfang, der ikke er specialbestemmelser, kan de almindelige regler om hindringer af ejerens eller brugerens rådighed (strl. § 293, stk. 2), tingsødelæggelse (strl. § 291), ulovlig tvang (strl. § 260) o.s.v. efter omstændighederne anvendes. Det må understreges, at en standsning eller forandring af de elektroniske signaler, lysimpulser m.m. ikke som sådan kan henføres under strl. § 291 om tingsødelæggelse (strl.bet. 1985 s. 38 f., smh. NOU 1985:31.10). Derimod er en overklipning af ledningen omfattet af bestemmelsen.

Hvis indgrebet ikke skal hindre al kommunikation, men kun modtagelsen af en konkret meddelelse, kan strl. § 263, stk. 1, nr. 1 (også) anvendes (strl.bet. 1985 s. 22 og 38 f.). Efter denne paragraf straffes den, som uberettiget »unddrager nogen ... anden lukket meddelelse«.

Bestemmelsen havde ingen direkte modsvarighed i strl. 1866, jfr. dennes § 222. Strl.bet. 1912 § 260, nr. 2, dækkede derimod »at tilintetgøre eller paa anden Maade unddrage nogen« en »til en anden rettet Meddelelse«. I motiverne fremhæves særligt den situation, hvor en ansat »udtager og beholder en Forretningen vedrørende Skrivelse ... uden Hensyn til, hvad Brug han vil gøre af den« (s. 238). Torp foretog kun en redaktionel ændring (strl.bet. 1917 s. 225). Den 2den straffelovskommission og det 1ste regeringsforslag så reglens område som »Krænkelse af en Persons Ret til at komme i Besiddelse af til ham bestemte lukkede Meddelelser« (strl.bet. 1923 sp. 355 og RT 1924/25 A.3389).

Der ses kun én trykt dom, U 1976.186 V. Den vedrørte en person, der på et posthus fik fat i to breve til Retsmedicinsk Institut fra politiet for at fjerne en blodprøve, der var taget af ham.

Waaben har fortolket 'unddrage' således, at ordet »muligvis også [omfatter] det forhold at bevirke at et brev kommer frem med væsentlig forsinkelse eller at fjerne det midlertidigt fra adressatens bord« (Sp. D. s. 238). I Komm. strl. antages dette resultat under forudsætning af, at fjernelsen ikke er ganske kortvarig (II s. 292). »Ganske« bør muligvis udelades her.

2. *Ændringer*

a. Televærkets personale

Det klassiske eksempel på en forvanskning er greven af Monte Christos indgreb i den optiske, semaforiske telegraf. Embedsmanden, der lod sig bestikke til at sende den »forkerte« meddelelse, kan selvfølgelig straffes for at have modtaget bestikkelsen. Desuden kan tjenestemanden straffes efter *strl. § 153, stk. 2,* om tilintetgørelse, forvanskning eller underslæb af telegram. Hvis tjenestemanden »understøtter en anden i sådan færd«, straffes han ligeledes. Derimod må »den anden« være straffri i relation til denne bestemmelse (Krabbe s. 406). Af dette synes at følge, at der er tale om et egenhændigt delikt. Straffen er hæfte eller fængsel indtil 3 år. Der kan næppe være tvivl om, at § 153 kan anvendes (eventuelt analogt) på de tilsvarende handlinger i relation til en datatransmission.

b. Udenforstående

Hvis en udenforstående på egen hånd trænger ind på ledningen, kan strl. § 153 ikke bruges.

Eksempel 46: En bankkunde indsætter et beløb på sin konto i en anden filial end den, hvor kontoen er oprettet. Beløbet overføres fra indsættelsesstedet til den kontoførende filial ved edb-transmission. Kunden »aflytter« og optager denne transmission på sit eget anlæg. Noget sådant skal være let at gøre, hvis banken og kunden bruger de samme standardanlæg. Kunden kan let identificere den meddelelse, der vedrører hans indbetaling, blandt de mange andre, eftersom han jo kender sit eget kontonummer. Når ledningen atter bliver fri, afspilles optagelsen, og dette kan gentages igen og igen. Hver gang forøges kontoens udvisende med det pågældende beløb - til sin tid på bankens bekostning. (Erik Fjord Hansen & Jan Mølgaard 1980 s. 43).

Dette hændelsesforløb kan opdeles i en række elementer. Selve »aflytningen« og tapningen af meddelelsen er strafbar efter strl. § 263 om krænkelse af datahemmeligheden. De »afsendte« oplysninger skal modtages og registreres på en eller anden måde i modtagerens anlæg. Det vil formentlig altid være mere nærliggende at bruge stk. 2 end stk. 1 på forholdet. Strafbarheden er uafhængig af, om den pågældende er så dygtig eller heldig, at han kun tapper den overførsel, der vedrører ham selv. Den senere brug af den kopierede meddelelse er databedrageri (strl. § 279 a).

3. Kopiering

Kopieringen af datatransmissioner er, som nævnt umiddelbart ovenfor, strafbar efter strl. § 263, selv om den opsnappede information ikke bruges. Forbrydelsen fuldbyrdes allerede ved selve kopieringen, og der behøver ikke at være et videregående forsæt.

Se retsplejelovens kap. 71 (som ændret i 1985) og bet. 1023/1984 s. 57 f. om kopieringer, der foretages af politiet under efterforskning.

Det antages, at den almindelige bestemmelse om krænkelse af brevhemmeligheden ikke beskytter mod fremskaffelse af viden om afsender- og modtageradresser. Brugen af denne viden kan derimod efter omstændighederne være en overtrædelse af strl. § 264 d om krænkelse af privatlivet. (Komm. strl. II s. 292). Tilsvarende må formentlig antages her. Det betyder, at hotellers automatiske registrering af, hvem gæsterne ringer til, ikke er strafbar i sig selv efter denne bestemmelse. (Smh. Artur Solarz 1985 s. 163). Efter omstændighederne kan der derimod være tale om et brud på registerlovgivningen. (Jfr. Registertilsynets Årsberetning 1984.52 f.).

Bestemmelsen kræver forsæt. Overtrædelse straffes med bøde, hæfte eller fængsel indtil 6 måneder. Visse former for efterfølgende medvirken straffes efter strl. § 264 c med tilsvarende straf.

III. Kriminalitet ved hjælp af edb

Under afsnit II behandlede jeg de tilfælde, hvor beskyttelsesinteressen (og angrebsobjektet) i det væsentlige var knyttet til edb-systemet som sådant eller til en del af dette. I nærværende afsnit III er det kun angrebsobjektet eller midlet, som er et edb-anlæg. Der er ingen skarp grænse mellem afsnit II og afsnit III. Opdelingen er kun i ringe grad begrundet i systematiske betragtninger, snarere i fremstillingshensyn.

A. Utilladt brug af edb

1. Registerlovgivningen

Olivetti havde i 1984 en annoncekampagne, hvori det blev sagt: »Orwell was wrong. According to Orwell, in 1984 man and computer would have become enemies«. IBM er lige så beroligende i deres reklamer, »The computer didn't do it«. Dansk lovgivning har med god føje indtaget et mindre sangvinsk standpunkt. Datamaten har klart skabt nye muligheder for misbrug med mulighederne for brug. (Smh. f.eks. Erik Samuelsen 1972 og David H. Flaherty 1984.) Nogle eksempler på »pæn« brug kan let ved fantasiens hjælp ændres til ubehagelige eksempler på overvågningssamfund. I forbindelse med efterforskningen af Watergate kortlagde FBI en persons liv gennem mere end ½ år – hvilke hoteller han havde boet på, hvor han havde spist, hvilke transportmidler han havde brugt. Alle oplysninger lå hos credit card-firmaet. I et andet tilfælde manglede New Yorks politi vidner til et drab, der var sket uden for en restaurant. American Express forsynede det med navne på 20 personer, som havde spist dér på det relevante tidspunkt. (Adrian R.D. Norman 1983 s. 112 og 130). Det svenske politi fandt ud af, hvilke personer der var i nærheden af Palmes drabssted ved at undersøge, hvem der havde brugt to bankomater. (Expressen 1986-04-07). De nærliggende muligheder for ubehagelig brug af datamaternes mange anvendelsesmuligheder har ført til, at der er blevet gennemført nogle begrænsninger i den frie anvendelse af edb-anlæg. Det ville føre for vidt, om jeg i denne sammenhæng skulle redegøre for detaljerne. Det følgende er blot en omtale af visse hovedpunkter. De vigtigste love er l. 293 8.6.1978 om private registre m.v. (privatregisterloven) og l. 294 8.6.1978 om offentlige myndigheders registre (offentligregisterloven). De er baserede på registerudvalgets delbetænkninger nr. 687/1973 om private registre og nr. 767/1976 om offentlige registre. Af speciallove fremhæves l. 284 6.6.1984 om betalingskort.

Privatregisterlovens formål er at sikre, at oplysninger om private og økonomiske forhold kun registreres af private i det omfang, registreringen tjener anerkendelsesværdige interesser, og at de registrerede oplysninger opbevares på betryggende måde.

Offentligregisterloven skal sikre, at det offentliges oprettelse og brug af edb-registre med personoplysninger sker på en sådan måde, at den enkelte borgers retsbeskyttelse og integritet ikke krænkes. Grundtanken er, at registrering og sågar blot muligheden for registrering påvirker borgernes muligheder for at leve et liv i frihed. Lovens betydning illustreres af, at der er mere end 700 offentlige registre i Danmark (Flemming Sørensen 1984). I denne forbindelse må det dog fremhæves, at det farligste er mulighederne for at samle oplysningerne på et sted, eventuelt gennem en samkøring af registrene. Det store antal registre kan således ses som et positivt tegn.

For at sikre lovenes overholdelse og gennemførelse er der oprettet et særligt Registertilsyn.

Afgørende for, om det er *den ene eller den anden lov,* der gælder, er, hvem registeret føres *for,* ikke hvem det føres *af,* jfr. lovenes kap. 1. Begge love kan ikke anvendes på samme register (jfr. privatregisterlovens § 2). Der må foretages et valg mellem dem.

Spørgsmålet om, hvad et register er, forbigås her. Se i denne forbindelse Registertilsynets årsberetninger 1983.18 ff. og 1984.21 ff. om problemer i forbindelse med automatiske kontormaskiner.

Begge love har begrænsninger i *hvilke data,* der må registreres. Hovedreglen i privatregisterloven er, at registreringen skal være et naturligt led i den normale drift af erhvervsvirksomheder af den pågældende art. (§ 3, stk. 1, jfr. også § 9, stk. 1, og § 17). I de offentlige registre må der kun registreres oplysninger, der klart er af betydning for varetagelsen af vedkommende myndigheds opgaver (§ 9, stk. 1).

Formålet med lovene er at beskytte privatlivet i ordets vide forstand. Det finder udtryk i privatregisterlovens § 1, stk. 1, hvor det siges, at registrering, der omfatter personoplysninger, og hvor der gøres brug af elektronisk databehandling, og systematisk registrering, der omfatter oplysninger om personers, institutioners, foreningers eller virksomheders private og økonomiske forhold, eller i øvrigt oplysninger om personlige forhold, som med rimelighed kan forlanges unddraget offentligheden, kun må finde sted efter reglerne i lovens kapitler 2 og 3.

I kapitel 2 om erhvervsvirksomheder m.m. uddybes dette i § 3, stk. 2, 1. pkt., hvorefter oplysninger om race, religion og hudfarve, om politiske, seksuelle og strafbare forhold, om helbredsforhold, misbrug af nydelsesmidler og lignende som udgangspunkt kun må registreres, når det følger af anden lovgivning. Se endvidere § 4, stk. 1, om videregivelse. Under de nævnte op-

lysninger falder f.eks., at den pågældende har deltaget i en demonstration om et samfundsanliggende (smh. Registertilsynets årsberetning 1983.36), og at den registrerede person modtager invalidepension (s.st. 1980.72). Se om dødsårsager s.st. 1981.82 f., om medlemskab af frimurerordenen s.st. 1981.90 f. og om en kirkes registrering af medlemmernes psykiatriske behandling og narkotikamisbrug s.st. 1983.54 og 1984.49. I praksis har spørgsmålet om forretningers og vagtværns registreringer af butikstyve m.fl. givet anledning til megen debat, se s.st. 1979.209 ff., 1980.72 f., 1981.83 f. og 1982.54 f. (politianmeldelse).

Begrænsningerne i privatregisterloven har fået en formulering, der minder om, men ikke ganske svarer til ordlyden af strl. § 264 d om videregivelse af meddelelser vedrørende en andens private forhold. Registerudvalget synes at have forudsat, at bestemmelserne skulle have samme reelle indhold (bet. 687/1973 s. 60). Hvis man på trods af denne forudsætning i forarbejderne måtte komme til, at strl. § 264 d sætter snævrere grænser for den pågældendes udfoldelsesmuligheder i en eller anden henseende, må strl. § 264 d antages at gælde uanset registerlovens karakter af specialbestemmelse. For dette taler - udover den nævnte udtalelse i forarbejderne - at formålet med registerlovgivningen var at skabe en videre beskyttelse end den, der eksisterede i de almindelige regler. En vis formel støtte for dette kan hentes i formuleringen af straffebestemmelsen i privatregisterlovens § 27.

Jfr. også privatregisterlovens § 9, stk. 2, og § 17, stk. 2, samt offentligregisterlovens § 9, stk. 2.

Sensitive oplysninger, der må registreres, må også bruges, men af dette følger ikke nødvendigvis, at de må videregives, jfr. privatregisterlovens § 4, stk. 2.

Indehaveren af registeret skal føre *kontrol* med, at der ikke indføres urigtige eller vildledende oplysninger i registeret, jfr. privatregisterlovens § 6, stk. 3, og offentligregisterlovens § 11. (Se eksempler i Flemming Sørensen 1984 s. 97 ff.) Hvis det alligevel sker, skal de pågældende oplysninger slettes, jfr. privatregisterlovens § 6, stk. 3, og § 13, samt offentligregisterlovens § 11. Tilsvarende gælder om gamle og forældede oplysninger, jfr. privateregisterlovens § 4, § 6, stk. 1, og § 9, stk. 3, samt offentligregisterlovens § 9, stk. 3. Endelig skal der træffes sikkerhedsforanstaltninger m.m., så oplysninger ikke kan komme til uvedkommendes kundskab, jfr. privatregisterlovens § 6, stk. 4, § 12, § 16 og § 20, stk. 2 og 3, samt offentligregisterlovens § 12. Efter omstændighederne kan en passivitet med hensyn til sikkerhedsforanstaltningerne være så grov, at reglerne om videregivelse kan bruges i stedet.

Oprettelse af registre med henblik på at advare andre mod forretningsforbindelse m.m. må kun finde sted efter forudgående tilladelse fra Registertilsynet, jfr. privatregisterlovens § 3, stk. 3. Virksomhed med kreditoplysning og elektronisk databehandling for tredjeperson kræver en forudgående anmeldelse til Registertilsynet, jfr. privatregisterlovens §§ 8 og 20.

Strafferammen er bøde eller hæfte, medmindre højere straf er forskyldt

efter den øvrige lovgivning. Nogle af de nævnte lovovertrædelser bliver først strafbare, når Registertilsynets påbud om lovliggørelse ikke efterleves (FT 1977/78 A.651). Uagtsomt forhold straffes også, jfr. strl. § 19. Aktieselskaber, andelsselskaber og lignende kan ifalde bødeansvar. I forskrifter, der udstedes i medfør af privatregisterloven, kan der fastsættes straf af bøde eller af bøde eller hæfte. I den tilsvarende bestemmelse i offentligregisterloven er der kun hjemmel til at fastsætte bøde. Jfr. i øvrigt privatregisterlovens § 27 og offentligregisterlovens § 29.

Registerudvalget overvejede, om der burde være adgang til administrativ *fratagelse af retten* til at udøve kreditoplysningsvirksomhed, men tog afstand herfra ud fra de almindelige strafferetlige principper. Derimod ønskede udvalget en skærpelse af de regler, der ellers ville gælde, således at det i stedet blev reglerne i strl. § 79, stk. 1, 1. pkt., der skulle bruges. (Jfr. bet. 687/1973 s. 76 f. og Komm. strl. I s. 307 ff.) Det gennemførtes ved privatregisterlovens § 28, der yderligere kom til at gælde for de to andre særlige virksomhedsformer (§ 3, stk. 3, og § 20). Herefter kan de tre former for virksomhed frakendes ved dom, såfremt det udviste forhold begrunder en nærliggende fare for misbrug i fremtiden. (Smh. også l. 284 6.6.1984 om betalingskort m.v. § 32.)

Danmark har underskrevet, men ikke ratificeret *Europarådets konvention* af 28. januar 1981 *om beskyttelse af personoplysninger*. Den manglende ratifikation skyldes især, at vor lovgivning ikke kan leve op til konventionens krav om adgang til registeroplysningerne for den registrerede (»access«). Den 1. oktober 1985 trådte den i kraft efter at være blevet ratificeret af BRD, Frankrig, Norge, Spanien og Sverige.

Se nærmere om konventionen Måns Jacobsson 1981.

Se endvidere folketingsdebatten FT 1984/85.3854 ff. og 4576.

Se også strl.bet. 1985 s. 65 ff., spec. s. 67.

2. Miljølovgivningen

Brugen af datamaten kan være ulovlig på grund af dens indvirkninger på omgivelserne. I denne forbindelse har den eventuelle sundhedsfare ved *skærmarbejde* påkaldt sig mest opmærksomhed. Den japanske fagbevægelse mener at have konstateret, at mere end én tredjedel af de kvinder, der arbejder ved dataskærme, har problemer under graviditet eller fødsel. (Information 1985-06-05). En svensk undersøgelse, der blev lagt frem af Socialstyrelsen, viste en lille forøgelse af antallet af fosterskader hos kvinder, der arbejder ved billedskærme (Göteborgs-Posten 1985-05-02). Efter 4 aborter ud af 6 graviditeter blev gravide fritaget for skærmarbejde på Århus kommunes edb-central (Printeren 1984:6-8). Der er iværksat en større dansk »skærmabortundersøgelse« (Information 1985-07-27). Se også arbejdsministerens redegørelse FT 1984/85.9652 ff.

Indtil videre er det kun andre og mindre sundhedsmæssige gener, som har medført regulering i Danmark, jfr. Arbejdstilsynets vejledning om arbejde ved skærmterminaler af januar 1985.

Datamaterne kan også påvirke omgivelserne på anden måde, f.eks. forstyrre fjernsynsmodtagningen. (Politiken 1984-12-14).

B. Berigelseskriminalitet

I det følgende behandles først det særlige databedrageri (strl. § 279 a) i almindelighed (1). Derefter ses der på nogle kriminelle situationer: den edb-disponerendes berigelseskriminalitet over for en udenforstående (2), en udenforstående over for edb-brugeren (3), en intern over for ansættelsesstedet (4), og en udenforstående over for en anden udenforstående (5).

1. Databedrageri

Ved en ændring af straffeloven i 1985 (l. 229 6.6.1985) blev der indsat en § *279 a* om databedrageri. Den har følgende ordlyd:

»For databedrageri straffes den, som for derigennem at skaffe sig eller andre uberettiget vinding retsstridigt ændrer, tilføjer eller sletter oplysninger eller programmer til elektronisk databehandling eller i øvrigt retsstridigt søger at påvirke resultatet af sådan databehandling.«

Begrundelsen for lovændringen var, at den almindelige bedrageribestemmelse i strl. § 279 næppe er direkte anvendelig, når det ikke er et menneske, men en datamat, der besviges. (Se herom blandt andet denne bogs 1. udgave s. 87 ff., Leo Lemvig 1985 og strl.bet. 1985 s. 9, 44 ff. og 80 ff.). Den nye bestemmelse skal imidlertid ikke blot supplere bedrageriparagraffen (§ 279), men også dække visse forhold, som ellers ville være strafbare som underslæb (§ 278) eller mandatsvig (§ 280) (strl.bet. 1985 s. 9 f. og 51 ff.).

§ 279 a er anbragt i straffelovens kap. 28 om *berigelsesforbrydelser*. De er karakteriserede ved, at en uberettiget vinding opnås direkte gennem en retstridig tilføjelse af et tilsvarende formuetab hos den forurettigede. Dette gerningsmoment er formuleret på forskellig måde i de enkelte paragraffer, og retspraksis har yderligere nuanceret billedet (Komm. strl. II s. 342 ff. med henvisninger). I § 279 a siges det, at handlingen skal udføres »for derigennem at skaffe sig eller andre uberettiget vinding«.

I ordet »derigennem« ligger, at vinding skal opnås direkte ved den retstridige handling. Hvis en person modtager et honorar for at destruere oplysninger, der ligger i et edb-lager (jfr. f.eks. eksempel 37), kan § 279 a ikke bruges. Det ville være en vindingsforbrydelse, men ikke en berigelsesforbrydelse.

Det er ligegyldigt, hvem der får vindingen. Der behøver ikke at være anden forbindelse mellem den handlende og den begunstigede.

Vindingen skal bestå i penge eller andre goder med økonomisk værdi. Disse goder behøver ikke at være 'ting'.

I modsætning til den almindelige bedrageriparagraf (§ 279) er der intet udtrykkeligt krav om, at offeret skal lide et tab. Det fremgår imidlertid af

bestemmelsens placering i straffeloven og af forarbejdernes beskrivelse af dens område, at § 279 ikke blot er en vindingsforbrydelse, men at den også er en berigelsesforbrydelse. Når »tab« er udeladt af ordlyden, skyldes det, at man ønskede et andet fuldbyrdelsesmoment end i § 279. Tabselementet kommer således kun ind i forsætskravet. Men dér er det lige fuldt. Det almindelige 'berigelsesforsæt' skal være til stede. (Strl.bet. 1985 s. 20 og 81).

Handlingen skal være *retstridig*. Heri ligger et almindeligt forbehold om, at alskens momenter kan gøre en sletning af data o.s.v. lovlig eller i hvert fald straffri. Det kan f.eks. følge direkte eller forudsætningsvis af en leasingaftale, at lageret i et tilbageleveret edb-anlæg kan slettes. Det kan være lovlig nødret (strl. § 14), at indehaveren af ophavsretten til et programmel udsletter det hos en pirat (men det kan også være ulovlig selvtægt (strl. § 294)). Tro på berettigelsen udelukker forsæt. (Smh. URD Frederiksberg 1985-08-09 (anket)).

Den kriminaliserede handling i bestemmelsens 1ste led er at *ændre, tilføje eller slette* oplysninger eller programmer. Der kan manipuleres med enkelte oplysninger eller med dele af programmellet. Der kan foretages ombytninger og suppleringer. Der kan også foregå en total sletning. Paragraffen har i så henseende skullet dække alt tænkeligt. Der stilles ikke krav om, at gerningspersonen skal bruge bestemte metoder. Det vil også kunne være strafbart efter bestemmelsen at slukke for klimaanlægget, så datamaten kører varm. (Jfr. strl.bet. 1985 s. 80 f.).

Det er tvivlsomt, om § 279 a kan bruges på en person, som med berigelsesforsæt udnytter sit kendskab til, at andre har foretaget manipulationer. Formuleringen af bestemmelsen gør dette mindre nærliggende end ved andre berigelsesforbrydelser. Hæleribestemmelsen (§ 284) kan slet ikke bruges på sådanne tilfælde.

De nævnte handlinger skal rettes mod *oplysninger eller programmer* til elektronisk databehandling. Formuleringen adskiller sig lidt fra den tilsvarende i § 263, stk. 2. I denne står der i stedet for »til« », der er bestemt til at bruges i et anlæg til«. Straffelovrådet ses ikke at begrunde forskellen på de to formuleringer, og der er næppe grund til at tro, at der har været tilsigtet en forskel i realiteten. § 279 a's formulering gør det dog lettere at acceptere, at færdigbehandlede oplysninger og udgået programmel er omfattet af bestemmelsen. I forbindelse med gennemgangen af § 263 blev det kritiseret, at formuleringen inddrog et urimeligt stort antal oplysninger under bestemmelsens område. En tilsvarende kritik kan rettes mod § 279 a's formulering. I motiverne til bestemmelsen synes Straffelovrådet dog at give støtte for,

at bestemmelsen skal fortolkes indskrænkende. Det siges (strl.bet. 1985 s. 81), at det er »uden betydning, hvorledes disse oplysninger ... er lagret, eller om de er under transmission«. Det synes her forudsat, at bestemmelserne ikke kan bruges på enhver oplysning, som på et eller andet tidspunkt i sin senere eksistens vil få karakter af inddata. Der må være en vis tidsmæssig og(?) rumlig nærhed til databehandlingen i så henseende.

En sådan begrænsning må også læses ud af Straffelovrådets motiver til bestemmelsens 2det led (s.st.). Det skal blandt andet omfatte ændringer af oplysninger, som senere skal indtastes af en person.

Elektronisk databehandling defineres ikke. Se om forståelsen af dette begreb ovenfor s. 16 f.

§ 279 a, *2det led,* indeholder en generel og temmelig ubestemt udvidelse af 1ste led. Det omfatter personer, som *i øvrigt søger at påvirke resultatet af sådan databehandling.*

Nogle situationer med udnyttelse af uvidende mellemled omfattes af 1ste led. Det gælder, f.eks. hvis edb-chefen i et firma afleverer nogle uigennemskuelige bilag til indtastning hos nogle assistenter. Hvis tilsvarende afleveres af udenforstående, ville den nævnte konstruktion være mindre nærliggende. De pågældende assistenter kan ikke naturligt ses som uansvarlig medhjælp for den forbryderske udenforstående. Disse situationer er derimod omfattet af § 279 a, 2det led. I begge de nævnte tilfælde har jeg forudsat, at assistenterne var i god tro. Hvis assistenterne har det fornødne forsæt skal § 279 a bruges i begge tilfælde sammen med den almindelige regel om medvirken i strl. § 23.

Medens det ovenfor blev antaget - med støtte i strl.bet. 1985 s. 80 f. - at 1ste led også omfatter en handling, der sletter alt det lagrede, er dette mere tvivlsomt ved 2det led. Straffelovrådet siger her (s.st. s. 81 f.), at dette led »ikke i almindelighed« kan anvendes på en fuldstændig hindring af databehandlingen »f.eks. ... ved ødelæggelse af anlægget«. Noget sådant ville også stemme mindre godt med ordlyden, jfr. »påvirke resultatet«.

»Påvirkningen« af resultatet kan efter omstændighederne ske gennem passivitet, f.eks. hos en terminaloperatør. Passiviteten skal dog have en sådan karakter, at det er rimeligt at ligestille den med en aktiv handling. (Strl.bet. 1985 s. 82 og Hurwitz: Alm. D. s. 21 ff.).

En operatør kan også få en uberettiget berigelse i visse tilfælde, selv om databehandlingen sker på grundlag af rigtige oplysninger. Der sker ingen besvigelse af maskinen, men der begås et tillidsbrud. Sådanne tilfælde har ikke meget med bedrageri at gøre. Formålet med § 279 a var imidlertid, at

den også skulle dække nogle af de tillidsbrudssituationer, som ellers skulle have været henført under underslæb (§ 278) eller mandatsvig (§ 280).

§ 279 a kræver *forsæt*, jfr. strl. § 19. Der findes et supplement til den almindelige bedrageribestemmelse i strl. § 300 a, som kun kræver grov uagtsomhed. Den vil kun have ringe betydning i databedrageritilfælde.

Alle de almindelige forsætsformer kan føre til domfældelse. Der kan ikke indlægges et krav om skærpet forsæt i 2det leds »søger at«.

Som nævnt ovenfor skal der være 'berigelsesforsæt'.

Databedrageri efter 1ste led *fuldbyrdes*, når gerningspersonen har påvirket oplysningerne eller programmellet. 2det led fuldbyrdes, når gerningspersonen har foretaget sin handling, f.eks. foretaget en indtastning af nye data.

Jfr. strl.bet. 1985 s. 82.

De almindelige *forsøg*sregler i strl. §§ 21, 22 og 24 kan bruges.

Bistand til gerningspersonen kan henføres under *medvirkens*reglerne i strl. §§ 23 og 24 indtil den retstridige berigelse er overført fra offeret til personen, som skal have vindingen, jfr. Komm. strl. I s. 204. Efterfølgende modtagelse af beløbet m.m. kan efter omstændighederne straffes som hæleri, jfr. strl. § 284, som ændret i 1985.

Strafferammerne findes i strl. §§ 285-287. Straffen kan blive fra én dagbod i § 287 (om forbrydelser af mindre strafværdighed) til fængsel i 8 år i § 286 (om forbrydelser af særlig grov beskaffenhed).

I andre lande overvejes indførelsen af tilsvarende regler.

Det *norske* straffelovråd har foreslået, at n.strl. § 270, nr. 2, skal formuleres således: »... ved bruk av uriktig eller ufullstendig opplysning, ved endring i dataprogram eller på annen måte rettsstridig påvirker resultatet av en automatisk databehandling, og derved volder tap eller fare for tap ...« (NOU 1985:31.35).

Den *svenske* regering har foreslået en tilføjelse til den almindelige bedrageribestemmelse i 9. kap. i BrB. »För bedrägeri döms också den som genom att lämna oriktig eller ofullständig uppgift, ändra i program eller upptagning eller på annat sätt olovligen påverkar resultatet av en automatisk informationsbehandling eller någon annan automatisk eller mekanisk hantering, så att förfarandet innebär vinning för gärningsmannen och skada för någon annan.« Til forskel fra den danske strl. § 279 a, men ligesom det norske forslag, er den svenske bestemmelse ikke begrænset til elektronisk databehandling. Det skyldes, at man mener, at den tekniske udvikling løber så hurtigt, at det er uhensigtsmæssigt at begrænse bestemmelsen til en enkelt form for apparatur. (Lagrådsremiss 1985-09-19, jfr. også SOU 1983:50 s. 28, 186 ff. og 274 f., samt strl.bet. 1985 s. 48 f.)

I det nye *finske* udkast til straffelov af 31. maj 1984 foreslås det kriminaliseret som bedrageri »att mata in felaktiga uppgifter i dator eller på annat sätt ingripa i databehandling ... eller utnyttjar fel som han observerat i databehandling ...« (36. kap. 1.§) (strl.bet. 1985 s. 49).

Se endvidere *br-tysk* forslag til StGB §§ 263 a, 269 og 270, som for tiden er til behandling i forbundsdagen. Efter § 263 a bliver 'Computerbetrug' selvstændigt kriminaliseret, når en person »eines Datenverarbeitungsvorgangenes durch unrichtige Gestaltung des Programms oder Einwirkung auf seinen Ablauf oder durch Verwendung unrichtiger oder unvollständiger Daten beeinflusst ...«

Se om *engelsk* ret Christopher J. Millard 1985 s. 156 ff.

I *Alaska* har lovgivningsmagten bestemt, at det ikke i relation til lovregler, der kræver en vildfarelse, er »a defense that the defendant deceived or attempted to deceive a machine«, herunder »a vending machine, computer, turnstile or automatic teller machine«.

2. Den edb-disponerende over for en udenforstående

I disse tilfælde udnyttes edb-systemets uigennemskuelighed og tilsyneladende troværdighed til at opnå en uberettiget berigelse fra en udenforstående tredjeperson. I de typiske tilfælde foreligger der bedrageri (strl. § 279) (strl.bet. 1985 s. 45). Det gælder, hvad enten operatøren lader pengene gå i firmaets kasse eller i egen lomme. Det kan også være f.eks. åger (strl. § 282), skyldnersvig (strl. § 283) eller vildledende angivelser i selskabsforhold (strl. § 296). Se nærmere i Komm. strl. II om disse lovovertrædelser.

I nogle af disse bedrageritilfælde vil der fortsat skulle straffes efter den almindelige bedrageribestemmelse. I andre kan det elektroniske element få en sådan plads, at det kan blive aktuelt at overveje databedrageri. Som eksempel på dette kan måske bruges det følgende eksempel 48.

Eksempel 47: T var fuldmægtig i en bank. Når kunder havde optaget lån, opførte han rentebeløb, stiftelsesprovision og indskud med for store beløb. Det var vanskeligt for kunderne at kontrollere de enkelte beløbs rigtighed. Derefter tilegnede han sig det beløb, hvormed indbetalingerne oversteg gælden. (U 1977.86 H. Det fremgår ikke, at der var edb indblandet, men dette betyder intet for illustrationen af problemet.)

Eksempel 48: Et stort usa-nsk benzinselskab ændrede tankenes måleapparater, så bilisterne kom til at betale for mere benzin, end de i virkeligheden fik. (Time 1983-08-22).

3. En udenforstående over for edb-brugeren

a. Overførslen sker uafhængigt af edb-systemet

Hvis overførslen af berigelsen fra offeret til gerningspersonen sker selvstændigt og i princippet uafhængigt af edb-anlægget, gælder de almindelige regler om tyveri, underslæb o.s.v. Edb-systemet bruges til at skjule sporene, men der er ikke tale om, at forbrydelsen som sådan ændrer karakter.

Eksempel 49: Et amerikansk jernbaneselskab mistede et stort antal meget dyre jernbanevogne, der var blevet kørt ud på et sidespor og malet om til et konkurrerende selskabs farver. Der gik lang tid, før det blev opdaget, fordi en person, der var ansat i det bestjålne selskab, sørgede for, at de pågældende vogne blev slettet af registeret over selskabets vogne.

I dette tilfælde var der tale om tyveri - både efter usa-nsk og dansk ret. Den interne, som i overensstemmelse med aftalen efterhånden skjuler forbrydelserne, skal dømmes for medvirken til tyveri, jfr. strl. § 23.

b. Overførslen sker rent maskinelt

1°. Ved århundredskiftet blev det diskuteret, om det var bedrageri eller tyveri at tømme automater for varer ved hjælp af indkastede blyknapper, metalskiver o.s.v. I dansk praksis blev det med god føje, som i andre lande, slået fast, at det er ligegyldigt for den juridiske bedømmelse, om automaten åbnes ved hjælp af et brækjern eller af en værdiløs metalskive. I begge situationer er der tale om egenmægtige tilegnelser. Hvis en person, som er brudt ind i en bank, åbner og tømmer pengeskabet, fordi han gætter kombinationen, eller fordi han er så heldig at finde den i en skrivebordsskuffe i nærheden af pengeskabet, er det klart, at der skal straffes for tyveri. Det gør ingen forskel heri, at låsen til pengeskabet er elektronisk. Det gør næppe heller forskel, at der ikke har været noget indbrud, men at T f.eks. står ude på fortovet og får penge til at strømme ud af en pengeautomat. (Smh. strl.bet. 1985 s. 32).

Eksempel 50: T tilegnede sig som hittegods en taske med et købekort til BP. Ved hjælp af købekortet *stjal* han ad to gange 830 l benzin gennem automaten. (VLD. Meddelelser 34/1984.)

Det kræves, at tyveriets øvrige krav er opfyldt. Hvis personen, som hæver på sit kort, ikke har berigelsesforsæt, kan han ikke straffes. Det kan f.eks. være tilfældet, hvis han en aften har glemt at få kontanter med i byen, men indsætter beløbet næste dag.

Dansk ret svarer her ganske til norsk, svensk og finsk ret, jfr. Johs. Andenæs 1984 s. 365 om NRT 1982.1816 H, Nils Jareborg 1975 s. 261 og 1978 s. 182, Krister Malmsten 1979 s. 254 ff., SVJT 1977 rf. s. 45 (fremmed kort), NJA 1980.224 H (eget kort), Per-Edwin Wallén 1980, Anders Hedström 1981, SOU 1983:50.179 og Lauri Lehtimaja 1979 s. 670 f.

Eksempel 51: T havde ved 23 lejligheder brugt sit minibankkort til at hæve i alt 5900 norske kr., selv om der ikke var dækning på hans konto. Tiltalt for tyveri, men frifundet ved byretten. Højesteret fandt derimod bestemmelsen anvendelig. Førstvoterende udtalte: »At borttagelsen skjer ved hjelp av et middel - minibankkortet - som banken har udstyrt ham med ... kan ikke lede til at han går klar av tyveribestemmelsen ...« I Norge (og Sverige) er overtræk af checkkonti kriminaliseret i checkloven. Byretten havde henvist til denne bestemmelse, men førstvoterende i Højesteret afviste, at det skulle være en »nærliggende parallell«. (NRT 1982.1816 H).

Hvis det ovennævnte svenske forslag til en ny databedrageribestemmelse gennemføres, vil det betyde, at automattyverierne i fremtiden skal bedømmes efter denne. (Lagrådsremiss 1985-09-19).

Derimod antager det norske straffelovråd, at der fortsat skal straffes efter tyveribestemmelsen dér (NOU 1985:31.33).

I fremmed ret ses der i øvrigt noget forskellige løsninger. Efter schweizisk ret skal sådant også bedømmes som tyveri (Ulrich Sieber 1977 s. 129 n. 123). Hvis man anvender hævekortet sammen med en »hemmelig« kode, som måske lå sammen med hævekortet, skal det efter fransk ret bedømmes som bedrageri, selv om det hele foregår rent maskinelt (Ulrich Sieber 1977 s. 128 f.). Derimod er overtræk på egen konto ikke kriminaliseret. I br-tysk ret er der en særbestemmelse om automatmisbrug i StGB § 265 a; i den her behandlede situation er det

imidlertid ikke § 265 a, men den almindelige tyveribestemmelse, som skal anvendes (Schönke-Schröder s. 1718).

2°. I de nævnte tilfælde flyttes tingene (pengene) direkte og umiddelbart fra offeret (pengeinstituttet) til gerningspersonen. Hvis eksemplet ændres lidt, så gerningspersonen i stedet maskinelt *foranlediger penge* - eller snarere en »fordring« på pengene - *overført fra offer-banken til en anden bank,* hvor gerningspersonen senere hæver pengene, er situationen en anden.

Disse situationer er praktisk vigtige, fordi der foretages fantastisk mange pengeoverførsler af denne art. Som eksempel kan nævnes SWIFT (Society for Worldwide Interbank Financial Telecommunication), der omfatter godt 1000 banker i 35 lande. Ved hjælp af dette system sender bankerne kundebetalinger til udlændinge, betaler valuta og afregner andet. Alene i dette system behandles mere end 300 000 betalinger om dagen. (Artur Solarz 1985 s. 185 f.). Der er virkelig noget at gemme sig blandt for en svindler.

Eksempel 52: En fransk bank modtog som sædvanlig et magnetbånd med instruktioner om betalinger fra en storkunde. Det samlede beløb var 24 mio. fr. Ved et tilfælde blev det opdaget, at de konti, der var angivet på magnetbåndet, var blevet åbnede i falske navne. Ved en undersøgelse blev det så konstateret, at magnetbåndet ikke kom fra den angivne storkunde. Sagen er uopklaret. (Polisens åtgärder mot datakriminalitet s. 52).

Det er ikke et tyveri. Der sker ingen borttagelse af en fremmed rørlig ting. Det er heller ikke et bedrageri over for pengeinstitut nr. 2. Pengeinstitut nr. 1 vil antagelig komme til at bære tabet i den interne opgørelse, og T har fået sin uberettigede berigelse i samme øjeblik, som hans konto i pengeinstitut nr. 2 godskrives for beløbet. Efter tidligere ret var det tvivlsomt, om dette var omfattet af den almindelige bedrageribestemmelse (§ 279). (Se nærmere denne bogs 1. udgave s. 87 ff.). Forholdet er klart omfattet af den nye bestemmelse om databedrageri (§ 279 a).

c. Overførslen sker kun delvis maskinelt

Efter strl. § 279 foreligger der et bedrageri, når en person retstridigt fremkalder, bestyrker eller udnytter en vildfarelse og derved bestemmer en anden til en handling eller undladelse, hvorved der påføres et formuetab. En sådan situation ville f.eks. foreligge, hvis man ændrede eksempel 51 en smule: Bankkortet bruges ikke i en automat, men vises frem til en kasserer, som - i den tro at der er dækning på kontoen - udbetaler et beløb. Tilsvarende i eksempel 50, hvis kortet vises til betjeningen på tankstationen og bruges til afstempling af en særlig bon. (Jfr. f.eks. U 1981.21 H.) (I praksis kræves desuden en underskrift på bonen. Hvis det er et fremmed kort, absorberes ansvaret efter bedrageribestemmelsen i så fald af dokumentfalskforbrydelsen, men det ændrer intet i det principielle.)

Eksempel 53: Ved hjælp af et falsk Dankort fik et ungt par i løbet af et par måneder ad 100 gange tilsvindlet sig for i alt 60 000 kr. Sigtet for dokumentfalsk. (Politiken 1984-03-14.)

I det nye finske udkast til straffelov af 31. maj 1984 er der en særbestemmelse om 'betalingsmedelsbedrageri' (37. kap.), der blandt andet skal ramme misbrug af 'betalkort', herunder såvel bankkort som købekort.

Efter § 279 (bedrageri) skal den vildledte bestemmes til en handling eller undladelse, »hvorved der påføres denne eller nogen, for hvem handlingen eller undladelsen bliver afgørende, et formuetab«. Med denne formulering gjorde man det blandt andet strafbart at vildlede personer, der handler som fuldmægtige for en anden (den tablidende). I praksis anvendes bestemmelsen også i tilfælde, hvor den handlende ikke har en sådan stilling i forhold til den tablidende, at der efter almindelig sprogbrug ville foreligge et repræsentationsforhold (stillingsfuldmagt eller andet).

Eksempel 54: T fik læsset sin lastvogn med brunkul i et brunkulsleje. I stedet for at køre hen til vægten, hvor brunkullene skulle vejes og betales, kørte han bort med dem. Straffet for bedrageri. (VLT 1950.96).

Med Hurwitz formulering (Sp. D. s. 449) omfatter bedrageribestemmelsen »enhver, der har magt til at træffe en for den interesserede person bindende afgørelse«. Hans formulering må - til trods for bestemmelsens forhistorie - forstås på den måde, at magten ikke behøver at følge af aftaleretlige og procesretlige regler, men blot kan være en faktisk magt. (Smh. også Peter Rørdam 1960 s. 50 f., Erik Christensen 1960 s. 83 og Peter Rørdam 1960 s. 166 f. I denne sammenhæng betyder det, at den almindelige bedrageribestemmelse (§ 279) er anvendelig, hvis gerningspersonen får en godtroende person i offerfirmaet til at sætte en eller anden procedure i værk, så firmaet kommer til at lide et tab.

Hvis den pågældende procedure i udpræget grad har karakter af en elektronisk databehandling, fortrænges den almindelige bedrageribestemmelse af databedrageriets 2det led, »eller i øvrigt retsstridigt søger at påvirke resultatet af sådan databehandling«. (Jfr. strl.bet. 1985 s. 47 f. og 81).

Den menneskelige handling kan forekomme som et senere led i processen. Gerningspersonen kan egenmægtigt starte edb-proceduren, men på et senere tidspunkt forekommer der en overvågning, eventuelt en stikprøvekontrol. Disse forbrydelser skal normalt straffes som databedragerier (§ 279 a). Det kan næppe ganske udelukkes, at det menneskelige islæt kan have en så stor betydning for vurderingen af hændelsesforløbet, at det bliver mere naturligt at bruge den almindelige bedrageribestemmelse. Det kan dog kun være i undtagelsessituationer.

Eksempel 55: En ingeniør (T) havde ved gennemrodning af skraldespande m.m. fundet edb-udskrifter, der gjorde det muligt for ham at bryde et telefonselskabs sikkerhedskode. Han afgav derpå jævnligt gennem en længere periode over edb bestillinger på forskellige former for telefonmateriel. Ordren indgik til firmaets hovedsæde, men fremtrådte som afsendt fra en af filialerne. Det bestilte materiel blev uden fakturering leveret til filialen om natten og læsset af på dens gårdsplads. Her hentede T det, så snart den leverende lastbil var kørt. Han bragte det hjem til sin egen virksomhed, hvorfra han solgte det. Han blev dømt for »grand theft« (groft tyveri). (Ulrich Sieber 1977 s. 52 f.) (Se nærmere om T i Donn B. Parker 1983 s. 104.)

I dette tilfælde kan det være blevet tillagt vægt, at T selv fjernede tingene fra firmaets (filialens) område. Hvis de i stedet var blevet sendt direkte til ham med post eller fragtmand, ville det efter dansk ret være mindre nærliggende at bedømme forholdet som tyveri. Derimod kan § 279 a bruges (strl.bet. 1985 s. 32).

Det menneskelige islæt kan også indgå som sidste led i forløbet. Hvis T ved hjælp af sin hjemmedatamat har ændret udseendet på sin bankkonto og derefter ved bankens kasse får udbetalt et beløb uberettiget, foreligger der givet bedrageri eller databedrageri. Hvis vægten lægges på manipulationen med kontoen, er det det sidstnævnte; hvis vægten lægges på udbetalingen hos kassereren, det førstnævnte. Begge paragraffer kan ikke bruges samtidig. Normalt må det være mest rimeligt at straffe for databedrageri.

4. En intern over for ansættelsesstedet

I disse tilfælde udnytter en ansat sin adgang til at bruge firmaets edb-system til at overføre penge eller andre økonomiske goder fra firmaet til sig selv eller andre.

a. Overførslen sker uafhængigt af edb-proceduren

Eksempel 56: I en amerikansk bank udnyttede hovedkassereren anlæggets korrektionssystem. Når en kunde f.eks. indbetalte $ 5000, indkodede T det rigtige beløb og gav kunden kvittering herfor. Når kunden havde forladt kassen, markerede T den tidligere indførsel som en fejlkodning, rettede beløbet til $ 500, og stak de $ 4500 i lommen.

Smh. VLD 1979 refereret af Ulla Høg 1981 s. 61 f.

Eksempel 57: T var kasserer i en bank. Når hun tømte kassetten, som et benzinselskab havde lagt i døgnboksen, indsatte hun hovedparten af beløbet på benzinselskabets konto og en mindre del på sin ægtefælles. Benzinselskabet havde en gang for alle meddelt banken, at det lagde bankens sammentælling af beløbet til grund. (Stockholms tingsrätt 1983. Artur Solarz 1985 s. 114).

Disse situationer må bedømmes som underslæb (strl. § 278). (Jfr. eksempel 58. Smh. også U 1982.1187 V om en afløser ved et supermarkeds kasse). Edb-rettelsen i eksempel 56 adskiller sig ikke fra en rettelse med radérvand i de gode gamle dage. I begge situationer putter kassereren fremmede penge i lommen i stedet for i bankens kælder, og rettelsen henholdsvis indkodningen af benzinselskabets penge tjener alene til at skjule et allerede begået underslæb. Det er derfor ikke databedrageri. Vindingen opnås helt uafhængigt af datafusket. (Jfr. § 279 a's »derigennem« og strl.bet. 1985 s. 52).

Sagerne viser også, hvorledes man meget let kan komme i en situation, hvor det vil afhænge af ret så uigennemtrængelige beviser, om det bliver den ene eller den anden, som faktisk kommer til at lide tabet. Kunden kan til tider få svært ved at overbevise banken om, at den skal udbetale et større beløb, end der synes at stå på kontoen.

Se også eksempel 49 ovenfor om internes medvirken til eksternes tyverier.

b. Ved edb-fusk overført penge til egen kasse

Såfremt kassereren i et firma ved hjælp af falske bilag m.m. får flere kontanter i sin kasse, end han rettelig skulle have, og han derefter tilegner sig det overskydende beløb, kan hans forhold ses som bedrageri over for den del af firmaet, der står for disse pengetransaktioner, som mandatsvig gennem misbruget af stillingen eller som underslæb med hensyn til kontanterne. Valget mellem disse vil afhænge af omstændighederne. Eftersom den reelle krænkelse først sker, når pengene vandrer fra kassen over i kassererens tegnebog, ville det tidligere hyppigt have været mest nærliggende at bruge underslæbsbestemmelsen (strl. § 278).

Eksempel 58: En sagfører var tiltalt for bedrageri. Under sin administration af en ejendom havde han tilegnet sig 8000 kr. ved i de til ejeren afgivne regnskaber at have angivet forskellige poster som betalte. Han blev straffet for underslæb, idet de urigtige regnskaber ikke var benyttet som grundlag for tilegnelsen af de besvegne beløb, men alene havde tjent til at skjule besvigelserne. (HRT 1940.391).

Eksempel 59: En assistent skulle beregne de ansattes lønninger ved hjælp af firmaets edb-system og derefter udbetale lønnen kontant til de ansatte. Efter en tid satte hun syge, tidligere ansatte, ferierende o.s.v. på lønningslisten. Efter skattefradraget m.m. puttede hun de tilsvarende beløb i lønningsposer, men beholdt selv poserne. En række klager over lønberegning m.m. indkom, men blev behandlet af hende selv. Først da nogle tomme lønposer blev fundet ved et tilfælde, blev sagen opklaret. Hun havde da tilegnet sig 350 000 n.kr. Dømt for groft bedrageri efter den norske straffelov. Medvirkende til denne bedømmelse synes at have været, at hun ved hjælp af sine falske lønberegninger fik firmaets kasserer til at udbetale de beløb, som hun senere puttede i lønposerne. (Stein Schjølberg 1980 s. 462).

Eksempel 60: Et tysk selskab havde den regel, at pensionister skulle dokumentere deres eksistens gennem personligt fremmøde hvert år i marts måned. Et revisionsfirma syntes, at det var mærkeligt, at næsten alle pensionister døde i januar og februar. Det viste sig, at en af de ansatte lod checken gå på egen bankkonto fra dødsfaldet til efter det følgende nytår. (Adrian R.D. Norman 1983 s. 102).

Transaktioner som i eksemplerne 59 og 60 må nu som udgangspunkt straffes som databedrageri (§ 279 a).

c. Ved edb-fusk overført et beløb til sin egen konto i firmaet

1°. Der findes en række eksempler på, at ansatte har udnyttet deres adgang til firmaets edb-anlæg til at overføre beløb eller andre økonomiske goder til deres egne eller medskyldiges konti inden for firmaet. De fleste kendte

eksempler stammer fra bankverdenen, men der har været lignende manipulationer med lønkonti i andre virksomheder. Udgangspunktet ved bedømmelsen er også her straf for databedrageri (§ 279 a).

Eksempel 61: En ansat i en amerikansk bank skulle lave et renteberegningsprogrammel. Han gjorde det sådan, at der blev overført én dollar til hans egen konto, hver gang datamaten havde foretaget en renteberegning, som resulterede i et beløb af en vis størrelse. Han gik ud fra, at en så lille forskel ikke ville blive bemærket af kunderne. - Til tider kaldet »salami-teknikken«.

Eksempel 62: En programmør lod de brøkdele af centimer, som ikke blev udbetalt på grund af afrundinger ved rente- og kursberegninger, overføre til sin egen konto ud fra den filosofi, at selv de mindste bække kan blive til en stor å, når der blot er nok af dem. Kunden venter kun at få udbetalt det afrundede beløb, og banken savner ikke det beløb, som den strengt taget skulle udbetale. Alligevel er der klart tale om en uberettiget berigelse og om berigelsesforsæt hos programmøren.

Eksemplet optræder tit i litteraturen. Til tider placeres det i Frankrig (som her), til tider i U.S.A. eller BRD. John K. Taber (1980 s. 280) har imidlertid oplyst, at det er en myte; det er aldrig sket i virkeligheden; i et tillæg gør han endvidere overbevisende rede for, at det heller ikke vil komme til at forekomme. Det ændrer ikke dets værdi som retspædagogisk eksempel.

Den senere udbetaling af beløbet får ingen betydning for den strafferetlige bedømmelse. Den vil have karakter af et straffrit accessorium.

Hvis overførslen forudsætter en attestation eller en anden godkendelse fra en person, der har til opgave at kontrollere anvisningerne, evt. blot udtage stikprøver til kontrol, kan svigen efter omstændighederne anses for mest rettet mod kontrollanten. I så fald skal den almindelige bedrageribestemmelse (§ 279) bruges. (Smh. U 1984.334 H).

Eksempel 63: T fik en dertil bemyndiget til at attestere forskudsbilag. Dømt for bedrageri. (URD. Ulla Høg 1981 s. 68 f.).

Hvis kontrollen derimod er efterfølgende (revision), er vi uden for den almindelige bedrageribestemmelse og tilbage i databedrageriet.

Fremgangsmåden kan ændres, og udbyttet kan være ting i stedet for penge, men det vil stadig være databedrageri (§ 279 a).

Eksempel 64: T var ansat i et usa-nsk stormagasins bogholderi og tastede her en fiktiv kundekonto ind på anlægget. Ved hjælp af det udstedte kontokort købte en medskyldig varer for 2,5 mio. kr. Derpå slettede T alt om kontoen i datamatens hukommelse. (Printeren 1985:4.8).

Det gør næppe nogen forskel, at beløbet »udbetales« uden at tage omvejen over den særlige lønkonto. I visse tilfælde kan man dog komme i situationer, der er eller nærmer sig tyveri/underslæb.

Eksempel 65: T holdt øje med, hvornår edb-anlægget udskrev hans løncheck. Medens den gjorde det, trykkede han på en repetérknap, så checken blev mangfoldiggjort. (Edward H. Coughran 1976 s. 7).

Databedrageri er stadig mest nærliggende, men ligheden med den situation, hvor han tilegner sig de andre ansattes lønchecks er dog ganske stor. I disse tilfælde skulle han dømmes for tyveri/underslæb afhængig af hans plads i firmaet.

Eksempel 66: En vikar i et dansk forsikringsselskab udfyldte skemaer med opsagte policers numre. Den følgende dag fik han maskinudskrevne checks på ristornoen. Derefter forsynede han checkene med falsk endossement. Blandt andet dømt for mandatsvig med hensyn til udfærdigelse af falske hulleskemaer. (ØLD. Ulla Høg 1981 s. 69 f. Strl.bet. 1985 s. 56.) I dag skulle han formentlig have været straffet for databedrageri.

2°. Det gør ingen forskel i det her sagte, at pengene er »øremærkede« på en eller anden måde inden for det pågældende firma. I en række sager har bankfunktionærer »angrebet« kunders konti i banken. Det kan medføre bevisvanskeligheder og dermed en risiko for formuetab for kunderne. I de fleste tilfælde vil tabet dog ramme banken. Den frigøres ikke for sine forpligtelser over for kunderne, fordi en ansat laver fusk. (Smh. U 1984.1053 H). Og der vil næppe være grund til at behandle de situationer, hvor kundens krav reelt forspildes, anderledes end de situationer, hvor kundens krav fortsat eksisterer og opfyldes.

Eksempel 67: T var kasserer i en bank. Gennem to år tilegnede hun sig 280 000 kr. ved at hæve på sjældent brugte konti. Straffet for underslæb (§ 278). (Hillerød Kriminalret 1983. Strl.bet. 1985 s. 54.) Nu ville det være databedrageri (§ 279 a).

Tabet/vindingen kan ligge i tilskrivningen og udbetalingen af renter. (Smh. Komm. strl. II s. 343). Sådant rentefusk kan ramme pengeinstituttet.

Eksempel 68: Kassereren i en bank satte fiktive beløb ind på sin konto og hævede dem siden lige så fiktivt. Derved opnåede han en reel forrentning af sit indestående på ca. 150%. (Malmö tingsrätt 1981. Artur Solarz 1985 s. 117).

Sådant rentefusk kan også være rettet mod en eller flere af bankens kunder.

Eksempel 69: En kasserer i en usa-nsk bank overførte meget store beløb fra forskellige kunders konti til sin egen, men kun for ganske korte perioder. Kunderne kunne selvfølgelig se på deres kontoudtog, at der havde været bevægelser, men også at den tilsyneladende »fejl« var blevet korrigeret kort efter. Ts gevinst var alene de meget store rentebeløb, som maskinelt blev tilskrevet ham.

I begge typer tilfælde er databedrageri den nærmestliggende subsumption.

d. Ved edb-fusk overført penge til egen konto i et udenforstående pengeinstitut

Hvis en ansat overfører nogle af firmaets penge til sin egen konto i et (andet) pengeinstitut, må firmaets formuetab anses for at være sket i samme øjeblik, transporten er foretaget. Den senere udbetaling i det andet pengeinstitut har næppe selvstændig strafferetlig betydning. Hvis den pågældende sender pengene ud af firmaet med postvæsenet til sig selv, vil firmaets formuetab realiseres i og med, at postvæsenet modtager pengene. Der er næppe nogen forskel på de to situationer i strafferetlig henseende i denne sammen-

hæng (i modsætning til nedenfor s. 84 ff.). I begge tilfælde bruger den ansatte sin adgang til at disponere over edb-anlæg m.m. til at skaffe sig en uberettiget økonomisk gevinst. Tidligere skulle sådant som regel bedømmes som underslæb (§ 278), hvis gerningspersonen i kraft af sin stilling som direktør, kasserer eller regnskabschef var ansvarlig for pengenes tilstedeværelse (strl.bet. 1985 s. 53 f.). Andre ansatte kunne som udgangspunkt straffes for mandatsvig (§ 280) (strl.bet. 1985 s. 54 ff.). Hvis sådanne overførsler nu sker gennem anvendelsen af datateknik, skal forholdet straffes som databedrageri (§ 279 a).

I de følgende sager blev T dømt for mandatsvig. I dag skulle der i stedet have været dømt for databedrageri.

Eksempel 70: T havde ansvaret for et lønningsområde. Han opfandt en lønmodtager med et navn, der lignede hans eget og med en tidligere ansats CPR-nummer. I en bank åbnede han en lønkonto på navnet, men knyttet til sit eget CPR-nummer. Ved lønoverførsler fra firmaet anvendtes et internt lønnummer, men ikke CPR-nummeret. Han overførte løn 7 gange (70 000 kr.) og angav, at der var frikort fra skattevæsenet. Derpå slettede han den relevante del af båndet, så overførslen ikke kom til at fremgå af årsopgørelsen, og destruerede det øvrige materiale. Da han meldte sig til politiet, havde ingen opdaget noget. (VLD. Ulla Høg 1981 s. 70 f.).

Eksempel 71: T var ansat i en virksomhed, hvor han modtog timesedler fra de ansatte, lavede hullebilag o.s.v. T overførte de ansattes løn og lidt mere til sin egen konto i et pengeinstitut. (URD. Ulla Høg 1981 s. 68 f.).
Jfr. også ØLD. Meddelelse 61/1984.

Eksempel 72: T var assistent på et offentligt personalekontor. Når lønmodtagere fratrådte, ændrede han deres lønkontonummer til sit eget. Derefter udfærdigede han fiktive lønsedler vedrørende skattefri ydelser, f.eks. kørselsgodtgørelse. Efter 5½ år blev kontorets leder opmærksom på en af de fiktive udbetalinger. Dømt for 300 000 kr. (URD. Ulla Høg 1981 s. 69).

Hvis svindleren bruger nogle godtroende kolleger, kan forholdet ændre karakter, så det bliver mere naturligt at bedømme det som *bedrageri.*

Eksempel 73: En ansat i et norsk finansieringsselskab lavede falske kontrakter mellem fiktive firmaer og fiktive kunder. På det grundlag fik hun andre af de ansatte til at udstede checks m.m. Disse blev ved nye fiksfakserier, der også blev udført ved hjælp af hulkort, overført til hendes bankkonto. I løbet af mindre end 4 år havde hun besveget firmaet for næsten 1 mio. n.kr. Dømt for groft bedrageri. (Stein Schjølberg 1980 s. 460).

I princippet havde det været muligt at lave ganske tilsvarende-former for svindel, som i de ovennævnte eksempler, før edb-alderen. (Se f.eks. VLD, Domme 1968-1972 s. 207, om en kommuneassistents falske lønopgørelser. Dømt for bedrageri). Der er dog den væsentlige forskel på de praktiske muligheder, at det ikke længere er nødvendigt at producere bilag og lignende, som må vandre gennem mange hænder. I dag kan det hele gøres fra svindlerens egen arbejdsplads og uden at nogen får mulighed for at studse. Dette i forbindelse med mulighederne for senere at slette bånd m.m. kan yderligere

gøre det særdeles vanskeligt at konstatere svindelen ved en revision. Det er ganske illustrerende for transaktionernes uigennemskuelighed, at en af de største svindler over for en bank ($ 1,4 mio. over 3½ år) blev opdaget ved et rent tilfælde. Politiet ransagede en book-makers kontor i New York og fandt bilag, der viste, at en bestemt person dagligt spillede for $ 30 000. Da politiet fandt ud af, at den pågældende var hovedkasserer i en bank, orienterede det banken, der først nu opdagede, at der var noget galt. (Se om hans videre skæbne Donn B. Parker 1983 s. 105).

Der er imidlertid også en anden forskel. I dag har ganske underordnede funktionærer muligheder for at begå kriminalitet af et omfang, som tidligere kun kunne begås af højt betroede medarbejdere.

De danske domstoles anvendelse af mandatsvigsbestemmelser på underordnede funktionærer, gav den et område, som lovens fædre næppe ville have accepteret. Eftersom de nævnte tilfælde nu skal bedømmes som databedrageri, skulle der være mulighed for at vende tilbage til en snævrere personkreds. Dette ville være i overensstemmelse med retstilstanden i f.eks. Norge, Sverige, Schweiz, BRD og Østrig. Det nye svenske regeringsforslag (lagrådsremiss 1985-09-19) vil ganske vist betyde, at flere vil blive omfattet af straffebestemmelsen om 'trolöshet mot huvudman', men det er fortsat kun personer i særlig ansvarsfulde stillinger. (Jfr. også SOU 1983:52 og NOU 1985:31.11).

e. Ikke registrering af gæld eller lignende

I de ovenfor behandlede situationer sker der tilsyneladende først en indbetaling på den ansattes konto, og derefter hæves beløbet af kontohaveren. Et tilsvarende resultat kan opnås ad anden vej. Der kan egenmægtigt skabes en gæld, som enten slet ikke registreres som gæld, eller som vel registreres, men på en måde, så den går uden om den sædvanlige procedure mod debitorer.

Eksempel 74: I en af de ældste usa-nske edb-sager havde en ansat i et pengeinstitut ændret programmellet, så datamaten ignorerede overtræk på hans egen check-konto.

Han blev dømt for 'alteration of bank records' (Edward H. Coughran 1976 s. 7 og 16). Vi har ingen tilsvarende bestemmelse.

Det reelle er, at pengene vandrer fra bankens kældre over i hans lommer, uden at banken så at sige kan »hente dem igen« på hans konto. Situationen minder i meget høj grad om de ovennævnte, og den bør behandles på samme måde, d.v.s. som databedrageri (§ 279 a).

Det er ikke muligt at bedømme forholdet som fragåelsesunderslæb (strl. § 278, stk. 1, nr. 2).

f. »Udslettelse« af gæld

Udslettelse af gæld er i og for sig en dårlig betegnelse. Det er klart, at der ikke gennem en persons retstridige destruktion af regnskaber m.m. kan ske en civilretligt gyldig udslettelse af gælden. Det, der tænkes på, er de situa-

tioner, hvor resultatet bliver (eller tilsigtes at blive), at fordringshaveren tror (skal tro), at gælden med rette er udslettet som betalt, eller at registreringen af gælden ganske fjernes, så fordringshaverens muligheder for at blive opmærksom på sit krav ødelægges eller mindskes.

Eksempel 75: Et schweizisk skattevæsen havde et system, hvor gælden blev registreret på hulkort. Når en person betalte sin gæld, blev det tilsvarende hulkort udskilt. En ansat fjernede de hulkort, der vedrørte ham selv og nogle af hans bekendte. Når skattevæsenet herefter producerede lister over restanter, fremgik det ikke af disse, at han og hans venner ikke havde betalt.

I dette tilfælde blev der dømt for 'Betrug' (bedrageri). T indbragte sagen for kassationsretten, idet han gjorde gældende, at der ikke var tale om bedrageri, fordi der ikke var sket en formueoverførsel, og fordi han ikke havde besveget en fysisk person.

Ulrich Sieber sammenfatter kassationsrettens stilling til det sidste punkt således: »Zum einen setze eine DVA bei der Programmerstellung, Datenanlieferung und Datenauswertung eine Zusammenarbeit mit *Menschen* voraus. Zum anderen habe S die *Organe* des EDV-Zentrums und der kantonalen Steuerbehörde getäuscht, die von dem Computer erwartet hätten, dass er vertrauenswürdige Informationen liefern würde, und dass das erlangte Resultat komplett und materiell richtig sei. Weiterhin habe S die Operatoren des EDV-Zentrums, welche die Debitoren- und Zahlungslochkarten in den Computer eingegeben hätten, getäuscht. Diese seien nämlich der Überzeugung gewesen, dass kein anormales Element, insbesondere keine fiktiven Karten, vorhanden gewesen seien.« (1977 s. 51. Dommen er trykt i Louis Rohner 1976).

Sieber erklærer, at argumentationen efter tysk retsopfattelse er »zweifellos unzulässig«, for så vidt angår påstanden om, at regnecentralens organer og operatører er blevet »getäuscht« (besveget). (S. 205).

Efter dansk ret ville det formentlig være mest nærliggende at straffe for databedrageri (§ 279 a).

2. *En udenforstående over for en anden udenforstående*

Eksempel 76: En usa-nsk bank udleverede blanke, men forkodede indbetalingskort til sine kunder. Tilsvarende, men ikke forkodede, stod i bankens ekspeditionslokale. T blandede de kort, som han som kunde havde fået udleveret, med de kort, der lå til almindelig brug på skrivepultene. Resultatet blev, at folk, der kom ind fra gaden og brugte kortene på skrivepultene, ikke fik beløbene godskrevet på deres egne konti, men at de i stedet blev registreret på Ts. (Adrian R.D. Norman 1983 s. 70. Se også diskussionen hos Ernst-Joachim Lampe 1975 s. 10 ff.).

Eksempel 77: I U.S.A. har der været en række tilfælde, hvor betaling for brug af telefoner er blevet overvæltet på andre. Mere end 50 mio. usa-nere har særlige telefon credit cards. For at beskytte mod misbrug af eftergjorte, stjålne og tabte kort skal der i forbindelse med opringningen benyttes et firecifret tal eller en anden kode. Til trods for dette er der eksempler på, at »card sharks« (korthajer) har overvæltet enorme regninger på sagesløse private. En 71-årig mand i New York fik en regning på $ 176 983. Misbrugernes effektivitet viste sig, da et credit card firma fik telefonregninger på over $ 300 000, *før* dets credit card var blevet sat i omløb (Time 1984-03-26). Jfr. også Marcel Giroux 1986.

Eksempel 78: Beboerne i et almennyttigt boligbyggeri i Rødovre har fået en pengeløs vaskekælder. Hver lejer får et plastmagnetkort, som kan starte vaskemaskinen, sæbeautomaten o.s.v. Oplysning om brugen af kortet sendes automatisk over telefonnettet til boligselskabet, der opkræver betalingen sammen med huslejen. (Morgenavisen Jyllandsposten 1984-07-10).

Hvor der indskydes en person som mellemled, f.eks. en telefondame i eksempel 77, foreligger der givet bedrageri i sådanne situationer. Hvor det hele går maskinelt, må det efter dansk ret være databedrageri (§ 279 a).

C. Anden kriminalitet

I princippet er der *ingen grænser* for hvilke forbrydelser, der kan tænkes begået ved hjælp af edb. En overbringelse af en oplysning til en drabsmand kan være medvirken til drab. I et tilfælde er der uforsætligt blevet foretaget indgreb og ændringer i en us-amerikansk kræftkliniks journaler, så patienterne fik forkerte strålingsbehandlinger (Report on Computer Crime 1984 s. 49). Sådant ville efter dansk ret meget vel kunne medføre ansvar efter straffelovens bestemmelser om uagtsomt drab og uagtsom legemsbeskadigelse. En kommunikation af en trussel kan være en forberedelseshandling til voldtægt. O.s.v. (Strl.bet. 1985 s. 40). Stein Schjølberg har en sag fra Interpol (!) om en soldat, der fik indføjet injurier på en overordnets lønseddel (1983 s. 314). I praksis vil den kriminalitet, der må ventes begået ved hjælp af edb, som regel være berigelsesforbrydelser eller fredskrænkelser. Hovedvægten er derfor ovenfor lagt på disse. I forbindelse med fredskrænkelserne må særligt fremhæves spionagereglerne. Der vil næppe komme særlige subsumptionsproblemer her. Når gerningspersonen arbejder for en totalitær stat, kan det dog til tider være vanskeligt at finde ud af, om der er tale om civil industrispionage eller militær efterretningsvirksomhed.

I forbindelse med de forskellige forbrydelser kan der opstå et særegent problem. Datamater kan ødelægge (slette) data med stor hast og effektivitet og derved gøre det praktisk umuligt at skaffe de nødvendige *beviser for en straffesag*. Hvis dette gøres for at skjule sporene efter den egne forbrydelse (eller ens nærmestes forbrydelse), er det straffrit efter strl. § 125, stk. 2. Hvis det gøres for at hindre efterforskning m.m. af andres forbrydelser, er det strafbart efter strl. § 125, stk. 1.

Sletningen kan også være strafbar i sig selv efter *bogføringslovgivningen m.m.* I denne er der fastsat regler om opbevaring af regnskabsmateriale m.m. Såfremt dette opbevares på et edb-anlæg, må ejeren ved udskiftning af dette eller ved salg af virksomheden sikre sig, at regnskaberne m.m. stadig kan stilles til disposition for myndighederne.

D. International strafferet

Edb-forbrydelser begås tit ved hjælp af det almindelige telekommunikationsnet. Det gør det let at udføre kriminalitet over landegrænserne.

Eksempel 79: En 19-årig brød fra sin hjemby - Los Angeles - ind i Det norske Televerkets forskningsinstitut uden for Oslo. (Jan Carlsen 1984).

Udgangspunktet efter dansk international strafferet er, at straffemyndigheden afgøres af, hvor handlingen foretages, jfr. strl. §§ 6 ff. Ved edb-forbrydelser vil det typisk være ensbetydende med stedet, hvor der »trykkes på knapperne«. Smh. hermed den engelsk Data Protection Act 1984, der i s. 39 udtaler, at »data shall be treated as held where the data user exercises the control ... in relation to the data ... «. I eksempel 79 bliver det Los Angeles.

Strl. § 9 udvider den almindelige regel, således at handlingen tillige betragtes som foretaget dér, hvor virkningen er indtrådt eller tilsigtedes at skulle indtræde, hvis handlingens strafbarhed afhænger af eller påvirkes af en indtrådt eller tilsigtet følge (»ubiquitetsteorien«). Ved edb-forbrydelserne mod edb-anlægget, f.eks. tingsødelæggelse af de lagrede programmer m.m. eller tilegnelse af information, vil virkningen indtræde på datamatens »bopæl«. Derimod har det ingen betydning, at signalet passerer et tredje land. Hvis en datamat i Sverige betjenes fra Tyskland gennem det danske telefonnet, har dette ingen strafferetlig betydning i Danmark. (Jfr. Dietrich Oehler 1983 s. 215 om »transitforbrydelser«.)

Når det i stedet drejer sig om berigelsesforbrydelser m.m. ved hjælp af edb, er det vanskeligere at fastlægge, hvor virkningen indtræder. En vis vejledning kan findes i, hvor regnskabet over den angrebne formue føres. Jfr. også eksempel 80 nedenfor. (Hvorved det dog må erindres, at engelsk international strafferet adskiller sig en del fra dansk.)

Eksempel 80: T var programmør i en bank i Kuwait. Han åbnede nogle konti for sig selv i banken og programmerede datamaten til at overføre penge fra andre konti til hans. Tilbage i England bad han banken overføre det, der stod på hans konti dér til konti i England. Dømt for 'obtaining property by deception' (bedrageri).

T gjorde gældende, at den relevante »obtaining« var sket i Kuwait, således at engelske domstole ikke havde jurisdiktion. Dette blev afvist af Court of Appeal »on the undisputed facts the »obtaining« occurred when the relevant sum of money were received by the appellant's banks in England as a result of the letters the appellant wrote«.

Afgørelsen kritiseres af J.C. Smith. Han gør gældende, at hvis handlingen var begået i England, ville der ikke have været nogen »deception«, eftersom der ikke var nogen »intervention of any human mind«. T skulle derfor i stedet have været dømt for »false accounting« (urigtig bogføring). Desuden gør J.C. Smith gældende, at pengeoverførslen ikke vedrørte »property belonging to another«. (The Criminal Law Review 1984.427.)

Efter hollandsk ret tillægges stedet, hvor personen besviges ved bedrageri, betydning (Dietrich Oehler 1983 s. 227). Overført til dette område skulle det formentlig betyde, at databedrageri fuldbyrdes, hvor datamatens centrale dele (regneenheden) er anbragt.

Der er nedsat en arbejdsgruppe under Europarådet til at undersøge de internationale strafferetlige spørgsmål.

IV. Kriminalitet på grund af edb

Dagens undskyldning er som bekendt: »Vi er gået over til edb!« Al erfaring viser, at årsagen til masser af fejl ligger her. Der kan være tale om relativt uskyldige fejl, som når personer efter at være fyldt 100 år bliver behandlet som spædbørn i de offentlige registre, får tilsendt oplysninger om vuggestuer m.m., fordi datamaten kun er programmeret til at læse de to sidste cifre ved alder og fødselsdato. Fejlene kan også være meget kostbare. Et manglende semicolon i et programmel betød engang, at en usa-nsk satellit røg ind i Solen i stedet for at flyve mod Mars. Det kostede den usa-nske stat $ 80 mio. (Robert W. Bailey 1983 s. 7). Uigennemtænkte programmeringer har også kostet menneskeliv. Datamaten på det engelske krigsskib »Sheffield« var programmeret til at betragte de fransk-fremstillede Exocet-missiler som venligsindede. Det gjorde den følgelig også under Falklandskrigen, hvor denne type missiler blev brugt af Argentina. Resultatet blev, at skibet blev sænket med 20 mand. (Flemming Madsen Poulsen, Politiken 1985-08-14).

Fra en strafferetlig synsvinkel bliver de relevante spørgsmål for det første, om en manglende opfyldelse af retlige forpligtelser kan blive straffri, når årsagen skal søges i datamatfejl af en eller anden art, og for det andet, hvordan »medkontrahentens« stilling skal bedømmes.

A. Ansvaret for edb-besidderen

I denne sammenhæng forudsættes det, at der er en forpligtelse til at handle, afgive oplysninger, overføre beløb o.s.v., som ikke bliver opfyldt, fordi edb-besidderen på grund af fejlprogrammeringer eller lignende ikke bliver opmærksom på forpligtelsen eller undlader at opfylde forpligtelsen (fuldt ud). Det afgørende vil her ikke være pligtens eksistens, men tilregnelsen. Hvad der kræves i så henseende afhænger af, hvilken bestemmelse der er tale om. Særligt må det mærkes, at strafbar uagtsomhed ikke blot kan forekomme i forbindelse med den aktuelle brug af anlægget, men også kan tænkes opfyldt, når der foreligger sjusk, udygtighed m.m. i forbindelse med opbygningen af anlægget, ansættelsen af personale, programmeringen o.s.v.

B. Ansvaret for modtageren

Ansvaret for modtageren vil i praksis især kunne blive aktuelt, når der ved en fejl overføres et pengebeløb eller lignende til denne.

1. Gæld udslettet

Ved en fejl kan en gæld blive reduceret eller slettet i en fordringshavers regnskaber. Det behøver ikke at vise sig for omverdenen, men i forretningsforhold vil det ofte kunne ses af de månedlige kontoudtog m.m. Spørgsmålet er her, om passivitet hos skyldneren kan pådrage et strafferetligt ansvar. Udgangspunktet i dansk ret er, at det ikke er strafbart at undlade at betale sin gæld, og at det heller ikke er strafbart at undlade at gøre en fordringshaver opmærksom på, at der eksisterer et krav.

Eksempel 81: En programmør i et us-amerikansk firma blev vred og slettede alle firmaets magnetbånd. Derefter vidste firmaet ikke, hvad det havde af debitorer. Et forsøg på at få debitorerne til at betale gennem et opråb i aviserne hjalp ikke. Og konkursen fulgte straks efter.

Eksempel 82: Datamaten i en forretning var programmeret til at sende kunden en saldokvittering, når sidste rate i afbetalingshandlerne indgik. En kunde brugte ved sin første indbetaling - tilsigtet? - det girokort, som lå nederst, og som efter nummereringen skulle have være brugt sidst. Maskinen afsendte derpå saldokvittering. (Thomas Whiteside 1980 s. 25).

Eksempel 83: I lovgivningen om afgift af fjerkræ er det foreskrevet, at slagterierne skal indberette salg til fjerkræeksportudvalget. Ejeren af et slagteri undlod at indberette sit salg, hvorved han unddrog sig fra at betale over 30 000 kr. Frifundet for tiltale for bedrageri, eftersom det »beskrevne forhold, der fra tiltaltes side er rent passivt, findes ikke at kunne henføres under straffelovens § 279 som bedrageri«. (U 1966.882 V).

Til trods for at der i eksempel 83 var en særlig pligt til at oplyse om sin gældsforpligtelse, blev der altså frifundet for bedrageri. (Dommen indeholder nogle bemærkninger om en mulighed for et strafansvar for underslæb, der normalt ikke vil være til stede i de her behandlede tilfælde.) Når der frifindes i en sådan situation, må der des mere frifindes i eksempel 82. (Medmindre der var tale om en bevidst manipulation, som ville være databedrageri).

Et ansvar efter den almindelige bedrageribestemmelse kan blive aktuelt, hvis der er en forhåndsaftale mellem parterne om oplysningspligt (Johs. Andenæs 1975 s. 84 f., Waaben: Sp. D. s. 158 og Komm. strl. II s. 367).

Eksempel 84: En kvinde fik bevilget boligtilskud og underskrev samtidig en erklæring, hvorefter hun havde pligt til straks at give oplysninger om ændringer i antallet af beboere m.m. Senere flyttede en mand ind hos hende, men hun undlod at indberette det til socialforvaltningen, og fik derfor stadig udbetalt boligtilskud. Dømt for bedrageri (strl. § 279). (U 1973.1006 Ø).

Jfr. også U 1973.221 Ø, hvor manden i en tilsvarende situation blev dømt for medvirken, skønt han havde forholdt sig passiv.

2. Modtagelse af penge m.m. i ond tro

Hvis en person modtager penge eller andre økonomiske goder og tilegner sig dem, skønt han på modtagelsestidspunktet ved, at overladelsen er begrundet i en fejl, begår han en berigelsesforbrydelse, typisk et bedrageri (§ 279). Situationen er særlig klar, når der ved en fejl udleveres to lønningsposer (U 1949.509 Ø), en for stor pengeseddel (JD 1936.42 U), eller hvis en ekspedient ved en misforståelse giver penge tilbage som for en 500 kr. seddel, skønt der er betalt med en 50 kr. seddel. Tilsvarende gælder, hvis postbudet forveksler to personer og giver den forkerte pengene. Det vil også kunne være et bedrageri, hvis modtageren ved, at tilsendelsen er begrundet i en vildfarelse hos afsenderen.

Eksempel 85: En fraskilt kvinde indgik nyt ægteskab. Hun blev ved med at modtage bidrag fra sin tidligere ægtefælle, skønt hun vidste, at hun ikke var berettiget dertil. (JD 1958.222 U.)

På edb-området optræder især to former for fejl. Den ene er, at en person, som ikke længere opfylder betingelserne for at få en vis ydelse, ikke bliver slettet af udsendelsesregisteret, så beløbet fortsat tilsendes.

Eksempel 86: I mere end to år efter sin fratræden fik en scenefunktionær udbetalt sin løn, i alt ca. 250 000 kr. Tiltalt for bedrageri. (Politiken 1984-03-17.)

Den anden er, at et beløb (pludseligt) bliver forkert. Der har f.eks. været tilfælde, hvor en assistent har skullet indkode f.eks. 1267 kr. Medens han er i gang med at gøre dette, bliver han forstyrret og glemmer, at han allerede har indtastet de første tal. Han begynder derfor forfra igen. Beløbet kan så komme til at være 1 261 267 kr. Sådanne fejl ville næppe have forladt huset i gamle dage. (Cfr. Colin Tapper 1973 s. 42.)

Der har også været tilfælde, hvor edb-maskinen har »sat sig fast«, så den samme løncheck er blevet udskrevet en mængde gange.

Afgørende for den strafferetlige bedømmelse er det svigagtige forsæt til tilegnelse på modtagelsestidspunktet. Det er overleveringstidspunktet, hvis beløbet udbetales i kontanter fra betaleren til modtageren. Hvis det sendes med postanvisning, check eller lignende, er det afgørende posthusets eller pengeinstituttet udbetaling af kontanterne. (Cfr. eksempel 87 nedenfor).

En del af disse tilfælde er blevet foreslået udtrykkeligt kriminaliseret som bedrageri af den svenske förmögenhetsbrottsutredning. (SOU 1983:50. 9. kap. 1. § st. 3).

3. Modtagelse af penge m.m. i god tro

Det er forekommet, at der ved en fejl indbetales et eller flere beløb til en persons konto i et pengeinstitut eller til hans postgirokonto. Hvis det gøres af

andre end det pågældende pengeinstitut, henholdsvis postvæsenet, har beløbet »forladt« betaleren og er kommet indenfor kontohaverens rådighedssfære. Det viser sig hyppigt at være en uimodståelig fristelse, så kontohaveren hæver og bruger beløbet. En lidt anden situation kan være, at man to gange får udbetalt et beløb gennem postvæsenet og først efter, at man er kommet hjem, opdager, at det er betaling for det samme arbejde.

Situationen kan opfattes som et bedrageri (udnyttelse af bankens vildfarelse), som et underslæb (forbrug af betroede midler) eller som ulovlig omgang med hittegods.

Ud fra straffelovens formulering (ordlyd) er den nærmest liggende bestemmelse utvivlsomt den sidste (d.v.s. § 277, 2. led). Efter denne bestemmelse skal der straffes, når en person tilegner sig en fremmed rørlig ting (herunder penge), som ved ejerens forglemmelse eller på lignende tilfældig måde er kommet i gerningspersonens varetægt.

Bestemmelsen stammer fra strl. 1866 § 248. C. Goos skrev om den situation, hvor der er sket en overlevering, og hvor begge på det tidspunkt var in bona fide (i god tro), at § 248 vistnok burde anvendes på den senere tilegnelse. »Men om dette vil blive almindeligt fulgt, er vistnok tvivlsomt i Betragtning af Tilbøjeligheden til ikke at blive staaende ved § 248, naar Fejltagelsen alene er paa Overleverernes Side, da det ikke her kan gjøre nogen væsentlig Forskjel, om der er *mala fides ab initio* [ond tro fra begyndelsen] eller blot *superveniens* [efterfølgende ond tro].« (1895 II s. 446). Rigtigheden af dette argument er bestemt ikke indlysende.

I straffelovens forarbejder blev der givet udtryk for, at dette led i hittegodsbestemmelsen som regel ikke skulle bruges, hvor »Genstanden er overleveret den paagældende uden at være betroet ham« (strl.bet. 1923 mot 367, jfr. også strl.bet. 1917 mot. 246). Disse forhold synes i stedet henført under underslæb (strl.bet. 1923 mot. 368).

Krabbe fremhæver, at § 277 er uanvendelig i tilfælde, hvor varetægtsforholdet er stiftet gennem overleverelse, der skyldes en fejl fra overleverernes side; som eksempel nævnes postbudets aflevering af en pakke til en forkert modtager; disse forhold skal i stedet bedømmes som underslæb (strl. § 278) (s. 663 f.). Hurwitz tager afstand fra Krabbes synspunkt: »Har modtageren derimod været i god tro ... burde hans tilegnelse i efterfølgende ond tro derimod nok kunne henføres under § 277 fremfor at opfattes som underslæb.« (Sp. D. s. 406). Men heroverfor Waaben: »En »tilfældighed« ligestillet med ejerens forglemmelse foreligger endnu mindre hvor en person har fået en ting overleveret ved en fejltagelse ...« (Sp. D. s. 138 f.).

Eksempel 87: T skulle tjære et tag for 275 kr. og fik et forskud på 150 kr. Ved en fejltagelse gav kassereren ham en check på 275 kr., som han brugte. Dømt for underslæb. (U 1951.661 Ø.) (Hvis han havde været klar over fejlen, da han fik checken af kassereren, skulle forholdet i stedet straffes som bedrageri).

Konklusionen synes nærmest at være, at der efter gældende ret skal straffes for underslæb (§ 278) til trods for formuleringen af § 277, 2. led, i disse tilfælde. Det er væsentligt at fastholde, at straf efter underslæbsbestemmelsen (§ 278) forudsætter, at gerningspersonen skal forbruge de betroede penge. I lighed med svensk ret kan det derfor være nærliggende at antage, at det ikke er strafbart at forholde sig ganske passiv i en sådan situation. Og at dette ikke påvirkes af, at kontohaverens hensigt er, at beløbet med påløbne renter skal fordeles mellem hans godtroende arvinger. Eftersom beløbet og renterne ikke tilhører kontohaveren, er der selvfølgelig ingen pligt til at selv-

angive dem til skattevæsenet. (Jfr. Krister Malmsten 1985 s. 240). Der må også kunne opnås ejendomsret (og skattepligt) ved hævd. På den anden side ville det nævnte resultat være vanskeligt at forene med fortolkningen af hittegodsbestemmelsen (§ 277). Denne fuldbyrdes ved beslutningen om at beholde den fundne ting. (Komm. strl. II s. 355 f.)

Eksempel 88: En svensk folkepensionist fik anvist 983 000 kr. for meget på sin postgirokonto. Han tog til Barbados på ferie med hele sin familie. Efter hjemkomsten dømt for 'olovligt förfogande'. (Artur Solarz 1982 s. 17). 'Olovligt förfogande' er en slags underslæb. Nils Jareborg 1978 s. 77 f. og Krister Malmsten 1985 s. 239 f. sætter spørgsmålstegn ved denne subsumptions rigtighed.

En mand henvendte sig i Bikuben og bad om de 250 kr., der stod på hans konto. Kassereren oplyste, at saldoen var 217 131 kr. Derpå hævede han 125 000 kr. (Politiken 1986-05-03).

Uanset hvilken af de nævnte bestemmelser, der skal anvendes, kræves der forsæt hos brugeren af pengene. I mange tilfælde ledsages udbetalinger i dag af uigennemskuelige edb-udskrifter. Ved mindre åbenbare fejl må der gives borgerne en rimelig margin, før der statueres forsæt.

V. Behovet for lovændringer

I indledningen konkluderede jeg, at edb-kriminalitet efter al sandsynlighed har en forbavsende ringe betydning i virkeligheden. Det gør det imidlertid ikke overflødigt at sikre sig, at lovgivningen er i stand til at give et rimeligt værn mod misbrug. I afsnittene II-IV har jeg gennemgået de forskellige former for misbrug og gjort rede for, hvordan de eventuelt skal bedømmes efter dansk strafferet. Disse afsnit prætenderer på ingen måde at være en udtømmende edb-strafferet, men jeg tror, at alle de væsentligste muligheder for misbrug er behandlet.

Gennemgangen har vist, at der næppe er huller i den strafferetlige beskyttelse, hvis man ved huller forstår, at der vil kunne forekomme grove misbrug, som ikke vil kunne rammes strafferetligt. Vi har traditionelt udformet straffebestemmelserne generelt og bredt, og det har i denne forbindelse haft den fordel, at vi uden vanskelighed har kunnet medinddrage nye former for svindel m.m. under de eksisterende straffebud. De nye specialregler om registre, databedrageri m.m. har dækket de vigtigste lakuner. Når der er blevet henvist til, at flere stater i U.S.A. har »vedtaget love, der gør selve det at bruge edb-værktøjet til forsøg på noget kriminelt til noget ulovligt«, må det siges, at den regel har vi haft i mangfoldige år (strl. § 21). (Politiken 1984-01-30). Der er næppe noget land i verden, der har større muligheder for at straffe forsøgshandlinger end Danmark.

Det er imidlertid ikke ensbetydende med, at det ikke kan være rimeligt at overveje visse lovgivningsinitiativer, men det bør understreges, at det ikke i særlig høj grad er for at skaffe mulighed for at straffe på et område, som nu er straffrit, men snarere for at gøre det juridiske system klarere og mere overskueligt, og for at få en rimelig overensstemmelse mellem de ligeartede forbrydelser i systemet.

I denne forbindelse er der særlig grund til at overveje

1) en særlig kriminalisering af datafalsk, jfr. s. 52, cfr. strl.bet. 1985 s. 10.
2) justeringer af strafferammerne for
   a) industrispionage, jfr. s. 27
   b) hindring af ejeres råden, jfr. s. 25
   c) enerettighedslovgivningen, jfr. s. 33.

Forkortelser

.	Side eller spalte
A	Afdeling A eller tillæg A
B	Afdeling B eller tillæg B
bet.	Betænkning
bkg.	Bekendtgørelse
BrB	Brottsbalken (den svenske straffelov)
BRÅ	Brottsförebyggande rådet
cfr.	I modsætning til
Domme 1968-1972	BJARNE FRANDSEN, MOGENS BEIER & UNO VALBAK: *Systematisk oversigt over domme i kriminelle sager 1968-72.* København 1974
Domme 1973-1977	BJARNE FRANDSEN, MOGENS BEIER & UNO VALBAK: *Systematisk oversigt over domme i kriminelle sager 1973-1977.* København 1978
Domme 1978-1982	MOGENS BEIER, JØRN HOLMANN HANSEN, ERIK RIIS & UNO VALBAK; *Systematisk oversigt over domme i kriminelle sager 1978-1982.* København 1984
FT	*Folketingstidende*
H	Højesteretsdom
HRT	*Højesteretstidende*
Hurwitz: Alm. D.	STEPHAN HURWITZ: *Den danske kriminalret. Almindelig del.* 4. udg. ved KNUD WAABEN. København 1971
Hurwitz: Sp. D.	STEPHAN HURWITZ: *Den danske kriminalret. Speciel del.* København 1955
i.f.	in fine (i slutningen)
J	*Juristen* eller *Juristen og Økonomen*
JD	*Juristens Domssamling*
Karnov	W.E. von EYBEN & HENNING SKOVGAARD: *Karnovs lovsamling.* 10. udg. København 1983
Komm. strl. I	VAGN GREVE, BENT UNMACK LARSEN & PER LINDEGAARD: *Kommenteret straffelov. Almindelig del.* 3. udg. København 1984
Komm. strl. II	VAGN GREVE, BENT UNMACK LARSEN & PER LINDEGAARD: *Kommenteret straffelov. Speciel del.* 3. udg. København 1983
Krabbe	OLUF H. KRABBE: *Borgerlig Straffelov.* 4. udg. København 1947
l.	Lov
lbkg.	Lovbekendtgørelse
markedsføringsloven	Lovbekendtgørelse nr. 142 af 19. marts 1986 af loven om markedsføring
Meddelelser	*Meddelelser fra Landsforeningen af advokater antaget til udførelse af offentlige og beneficerede sager*
mia.	Milliarder
mio.	Millioner

NJA	*Nytt juridiskt arkiv*
NOU	Norges offentlige utredninger (norsk betænkning)
NRT	*Norsk Rettstidende*
ODS	*Ordbog over det danske Sprog*
offentligregisterloven	Lov nr. 294 af 8. juni 1978 om offentlige myndigheders registre
ophavsretsloven	Lovbekendtgørelse nr. 130 af 15. april 1975 om ophavsretten til litterære og kunstneriske værker med senere ændringer
patentloven	Lovbekendtgørelse nr. 546 af 25. oktober 1978. Patentlov
privatregisterloven	Lov nr. 293 af 8. juni 1978 om private registre m.v.
rf.	Rättsfallsavdelingen
RT	*Rigsdagstidende*
Schönke-Schröder	SCHÖNKE/SCHRÖDER: *Strafgesetzbuch. Kommentar.* 20. Auflage. München 1980
SOU	Statens offentliga utredningar (svensk betænkning)
StGB	Strafgesetzbuch (straffelov; hvis ikke andet fremgår fra BRD)
strl.	Lovbekendtgørelse nr. 527 af 1. november 1981 af borgerlig straffelov med senere ændringer
strl. 1866	Almindelig borgerlig straffelov af 10. februar 1866 (den nugældende straffelovs forgænger)
strl.bet. 1912	*Betænkning afgiven af Kommissionen nedsat til at foretage et Gennemsyn af den almindelige borgerlige Straffelovgivning.* København 1912
strl.bet. 1917	CARL TORP: *Betænkning angaaende de af den under 11. August 1905 nedsatte Straffelovskommission udarbejdede Forslag indeholdende Udkast til Love vedrørende den borgerlige Straffelovgivning med Motiver.* København 1917
strl.bet. 1923	*Betænkning afgiven af Straffelovskommissionen af 9. November 1917.* København 1923
strl.bet. 1985	*Straffelovrådets betænkning om datakriminalitet.* Nr. 1032. København 1985
SVJT	*Svensk Juristtidning*
U	Underretsdom eller byretsdom eller *Ugeskrift for Retsvæsen*
URD	Underretsdom eller byretsdom
V	Vestre Landsrets dom eller Viborg Landsoverrets dom
VLD	Vestre Landsrets dom
VLT	Vestre Landsret Tidende
Waaben: Sp. D.	KNUD WAABEN: *Strafferettens specielle del.* København 1981
Ø	Østre Landsrets dom
ØLD	Østre Landsrets dom

Litteraturliste

(Se også forkortelseslisten ovenfor.)

SAL ALFANO: The ethic of hacking. *Psychology Today* 1984, december, s. 66 f.

BRANDT ALLEN: De største EDB-bedragerier - stof til eftertanke for revisor. *Revision og Regnskabsvæsen* 1977. 447 ff. (Oversat fra The biggest computer frauds: lessons for CPAS. *The Journal of Accountancy* May 1977 s. 52 ff.).

JOHS. ANDENÆS: *Formuesforbrytelsene.* 3. utg. Oslo 1975.

JOHS. ANDENÆS: Norsk rettspraksis 1982-1983. *Nordisk Tidsskrift for Kriminalvidenskab* 1984 s. 353 ff.

ROBERT W. BAILEY: *Human Error in Computer Systems* N.J. 1983.

ANNE-LISE BAKKEN: Edb og kriminalitet som rettspolitisk utfordring. *Lov og Rett* 1983.488 ff.

STRANGE BECK & OLE BRUUN NIELSEN (red.): *Edb-retlige afgørelser 1.* Kbh. 1984.

STRANGE BECK: Retsbeskyttelse af EDB-programmer. *Datatid* 1985 (5). 36 ff.

JAY BECKER: Anmeldelse af ROBERT FARR: *The Electronic Criminals. Crime & Delinquency* 1977.86 ff.

KRISTIAN BECKMAN: *Läckande datorer - en information om RöS.* Stockholm 1984.

AUGUST BEQUAI: *Computer Crime.* Massachusetts 1978.

AUGUST BEQUAI: *How to Prevent Computer Crime. A Guide for Managers.* New York 1983.

AUGUST BEQUAI: The politics of computer crime. *Security Management* 1984.31 ff. (Her efter *Criminal Justice Abstracts* 1984.238).

FLEMMING BERG: Computer-kriminalitet. *Printeren* 1984:3.3 ff.

Betænkning. Se også Delbetænkning.

Betænkning angående en ny konkurrencelov. Nr. 416. Kbh. 1966.

Betænkning nr. 601. *Privatlivets fred.* Kbh. 1971.

Betænkning nr. 681. *Markedsføring. Forbrugerombudsmand. Forbrugerklagenævn.* Kbh. 1973.

Betænkning om tavshedspligt. Nr. 998. Kbh. 1984.

Betænkning nr. 1023. *Politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter.* Kbh. 1984.

Betænkning nr. 1064. *Ophavsret og edb.* Kbh. 1986.

JON BING: Transnational Data Flows and the Scandinavian Data Protection Legislation. *Scandinavian Studies in Law XXIV* 1980 s. 65 ff.

JON BING: *Opphavsrett og edb. Teresa* (35). Oslo 1985.

JON BING & KNUT S. SELMER (ed.): *A Decade of Computers and Law.* Oslo 1980.

JØRGEN BLOMQVIST: Programmørers ophavsret. *Datatid* 1985(6).41.

PETER BLUME: Edb-kriminalitet. *Årsberetning 1985.* Retsvidenskabeligt institut B. Kbh. 1986.

H.J. BONNICHSEN: Edb-forbrydelser - en databehandling. *Tidsskrift for Dansk Politi* 1977 s. 405 ff.

H.J. BONNICHSEN: Systemhacking - datadidling - cracking og straffeloven. *Tidsskrift for Dansk Politi* 1985.534 ff.

BRÅ-S 1982:7. *Datorteknik. Brottslighet. ADB-säkerhet. Dokumentation från en konferens.* Stockholm.

JØRGEN BULL: *Rettslig beskyttelse av dataprogrammer. En oversikt og en nærmere redegjørelse for beskyttelse etter åndsverkloven § 43 og lov om markedsføring § 1.* Oslo 1973.

JØRGEN BULL: Legal Protection of Computer Programs, i JON BING & KNUT S. SELMER (ed.): *A Decade of Computers and Law.* Oslo 1980 s. 410 ff.

JAN CARLSEN: Sådan kan du beskytte dig imod Datatyveri. *Kontor-Bladet* april 1984 s. 22 ff.

ERIK CHRISTENSEN: Om bedrageri, mandatsvig og skyldnersvig. *Ugeskrift for Retsvæsen* 1960 B.82 ff.

BIRGIT CLAUSEN & HELGE CLAUSEN: *Dansk edb-bibliografi.* Mørke.

Computer Crime. Legislative Resource Manual. Washington, D.C. 1980.

Computer crime needs international countermeasures. Oxford 1983.

EDWARD H. COUGHRAN: *Computer Abuse and Criminal Law.* San Diego 1976.

Delbetænkning om private registre. Nr. 687. Kbh. 1973.

Delbetænkning om offentlige registre. Nr. 767. Kbh. 1976.

Delbetænkning nr. 944. *Båndafgifter. Sanktioner. Påtale.* Kbh. 1982.

Edb og beskyttelsesforanstaltninger. Kbh. 1981.

Edb ordbog. 3. udg. Risskov 1982.

Elektroniske betalingssystemer i Norden. Oslo 1983.

KEN ENGLADE: Can You Keep a Secret? *Savoy* 1984:1.65 ff.

ROBERT FARR: *The Electronic Criminals.* New York 1975.

DAVID H. FLAHERTY: *Privacy and Data Protection - An International Bibliography.* London 1984.

LARS FRANK: *Edb-ordbogen.* Kbh. 1984.

JAN FREESE: *Kommentar till datalagen.* Hälsingborg 1983.

JAN FREESE: Kan man göra husrannsakan i en dator? *Advokaten. Tidskrift för Sveriges Advokatsamfund* 1984.233 ff.

B.J. GEORGE: Contemporary Legislation Governing Computer Crimes. *Criminal Law Bulletin* 1985.389 ff.

MARCEL GIROUX: Intercity Telephone Fraud in the electronic age. *International Criminal Police Review* 1986.23 ff.

BRUCE GOLDSTEIN: Electronic fraud: The crime of the future. *International Criminal Police Review* 1985.214 ff.

C. GOOS: *Forelæsninger over den danske Strafferets specielle Del.* Kbh. 1887.

C. GOOS; *Den danske Strafferets specielle Del* I Kbh. 1895, II Kbh. 1895, III Kbh. 1896.

VAGN GREVE: *Studier i færdselsstrafferet.* Kbh. 1979.

VAGN GREVE, OLE INGSTRUP & MINNA BLOCH: *Afsnit af Den danske Strafferet.* 3. udg. Kbh. 1977.

TOR HAFLI: Transborder Data Flows - The Scandinavian Solution, i JON BING & KNUT S. SELMER (ed.): *A Decade of Computers and Law.* Oslo 1980 s. 59 ff.

ERIK FJORD HANSEN & JAN MØLGAARD: *Databeskyttelse i datamatiske systemer.* Kbh. 1980.

I. TROTTER HARDY, JR.: Transborder data flow: An overview and critique of recent concerns. *Rutgers Computer and Technology Law Journal* 1983.247 ff.

ANDERS HEDSTRÖM: Tillrättaläggande angående bankomatmissbruk. *Svensk Juristidning* 1981.558 f.

LANCE J. HOFFMAN: *Modern Methods for Computer Security and Privacy.* New Jersey 1977.

LANCE J. HOFFMAN (Ed.): *Computers and Privacy in the Next Dacade.* New York 1980.

MICHAEL HOPPE: *Straf- und zivilrechtliche Würdigung von Missbrauchsfällen im EDV-Bereich nichtöffentlicher Unternehmungen, technischorganisatorische Datensicherungsmöglichkeiten und Entscheidungshilfen zur Auswahl von Sicherungsmassnahmen.* Hamburg 1978.

LUCY A. HUMMER: International Law, i *Computer crime needs international countermeasures.* Oxford 1983.

ULLA HØG: EDB og EDB-kriminalitet. *Anklagemyndighedens årsberetning* 1981.58 ff.

FINN BERG JACOBSEN: EDB-svindel. *Revision og Regnskabsvæsen* 1977.345 ff.

MÅNS JACOBSSON: Europarådskonvention om skydd för enskilda vid automatisk databehandling av personuppgifter. *Svensk Juristtidning* 1981.155 ff.

NILS JAREBORG: *Förmögenhetsbrotten.* Stockholm 1975.

NILS JAREBORG: *Brotten II.* Stockholm 1978.

NILS JAREBORG: *Brotten I.* 2. uppl. Stockholm 1984.

TORKIL C. JOHNSEN: *Opfinderretlig beskyttelse af edb-programmer med fortryk til egnede patentkrav for samme.* Kbh. 1980.

GUNNAR KARNELL: Upphovsrätt till datorprogram. *Nordiskt Immateriellt Rättsskydd* 1984.133 ff.

ALISTAIR KELMAN & RICHARD SIZER: *The Computer in Court. A Guide to Computer Evidence for Lawyers and Computing Professionals.* Aldershot 1982.

KJ-H (J. KJÆR-HANSEN): Data-tyveri kan stoppes. *Nyt fra Odense Universitet* 1984.57 f.

MOGENS KOKTVEDGAARD: *Immmaterialretspositioner.* Kbh. 1965.

MOGENS KOKTVEDGAARD: Det ophavsretlige sanktionssystem. *Juristen* 1966.49 ff.

MOGENS KOKTVEDGAARD: Bidrag til elektronrettens almindelige del. (Elektronisk databehandling). *Juristen* 1968.157 ff.

MOGENS KOKTVEDGAARD: Elektronisk databehandling. Immaterialretlige aspekter. *Nordiskt Immateriellt Rätsskydd* 1968.139 ff. med diskussion 1969.18 ff.

MOGENS KOKTVEDGAARD: Retlige problemer i forbindelse med adgang til datalagre. *Juristen* 1970.221 ff.

MOGENS KOKTVEDGAARD: Retsbeskyttelse af EDB-programmer. *Ugeskrift for Retsvæsen* 1983 B.317 ff.

MOGENS KOKTVEDGAARD: Lovgivning, i HENRIK JUHL & OLE ENGBERG (red.): *Politikens edb-bog.* Kbh. 1985. s. 204 ff.

Kriminalstatistik 1979 og 1980. Kbh. 1984.

ERNST-JOACHIM LAMPE: Die strafrechtliche Behandling der sog. Computer-Kriminalität. *Goltdammer's Archiv für Strafrecht* 1975.1 ff.

BILL LANDRETH: *Datorernas »häxmästare«. En fd hackers guide till informationssäkerhet.* Malmö 1985.

LAURI LEHTIMAJA: Om databrott ur finländsk synvinkel. *JFT Tidskrift utgiven av Juridiska Föreningen i Finland* 1979.668 ff.

LEO LEMVIG: Anmeldelse af VAGN GREVE: *Edb-strafferet. Fuldmægtigen* 1985.64 f.

JAN LINDER: Svenska företag tystar ner databrott. *Affärs Nyheterna* sept. 1979.

CARL MAGNELL: Databrott i Sverige, i THOMAS WHITESIDE: *Databrott.* Malmö 1980. S. 99 ff.

SIGURDUR TOMAS MAGNUSSON: *Tölvubrot.* Reykjavik 1985.

KRISTER MALMSTEN: Datorrelaterade gärningar. *Svensk Juristtidning* 1979.249 ff.

KRISTER MALMSTEN: Anmeldelse af VAGN GREVE: *Edb-strafferet. Nordisk Tidsskrift for Kriminalvidenskab* 1985.238 ff.

MANFRED MAIWALD: Anmeldelse af ULRICH SIEBER: *Computerkriminalität und Strafrecht.* 2. Auflage. *Zeitschrift für die gesamte Strafrechtswissenschaft* 1984.99 ff.

GERALD McKNIGHT: *Computer Crime.* London 1973.

J.N. MEETARBHAN: Prosecuting Computer Criminals. *International Criminal Police Review* 1983.189 ff.

JES ANKER MIKKELSEN: Katalogreglen i ophavsretsloven § 49. *Ugeskrift for Retsvæsen* 1976 B.257 ff.

CHRISTOPHER J. MILLARD: *Legal protection of computer programs and data.* London 1985.

Miscellaneous Acts. Annotated Legislation Service 299. Butterworths, London 1984.

MOHR. Mundtlig redegørelse til retsudvalget i Deutscher Bundestag 1984-06-06.

ELSE MOLS: Om ophavsretslovens beskyttelsesregler, særligt § 49 - den såkaldte »katalogregel«. *Ugeskrift for Retsvæsen* 1985 B.253 ff.

C.M.B. NAUDÉ: Reekenaarmisdaad: 'n Skewe beeld? *SA Journal of Criminal Law and Criminology* 1983.165 ff.

RUTH NIELSEN: *Kompendium i Edb-ret.* Stencil. Kbh. 1984.

CHARLIE NORDBLOM: *Industrispionage.* Täby 1984.

ADRIAN R.D. NORMAN: *Computer Insecurity.* Bristol 1983.

NOU 1985:31. *Datakriminalitet.*

ERIC J. NOVOTNY: Transborder Data Flows and International Law. A Framework for Policy-Oriented Inquiry. *Stanford Journal of International Law* 1980.141 ff.

SUSAN HUBBELL NYCUM: The criminal aspects of computer abuse. *Rutgers Journal of Computers and the Law* 1976.271 ff.

DIETRICH OEHLER: *Internationales Strafrecht.* Limburg 1973. 2. Auflage München 1983.

HERMANN OERTEL: Mundtlig redegørelse til retsudvalget i Deutscher Bundestag 1984-06-06.

AGNE HENRY OLSSON: Amerikansk lagstiftning om rättsskyddet för »chips«. *Nordiskt Immateriellt Rättsskydd* 1985.105 ff.

HARALD A. OMDAL: Elektronisk betalingsformidling: Skaper det risiko for en ny form for økonomisk kriminalitet? *Lov og Rett* 1983.577 ff.

Oxford Dictionary of Computing. Oxford 1983.

DONN B. PARKER: *Crime by Computer.* New York 1976.

DONN B. PARKER: *Fighting Computer Crime.* New York 1983.

PETER POERTING & ERNST G. POTT: *Computerkriminalität.* Wiesbaden 1986.

Polisens åtgärder mot datakriminalitet. Rikspolisstyrelsens rapport 1984:5. Stockholm.

RAGNAR PÅLSSON: Datorn i polisens och brottlingens tjänst. *Nordisk Kriminalpolis* 1985. 19 ff.

Regeringens proposition 1981/82:189. *Ändring i datalagen (1973:289) m.m*

Registertilsynets Årsberetninger til 1984.

Report on computer crime. American Bar Association 1984.

LOUIS ROHNER: *Computerkriminalität. Strafrechtliche Probleme bei »Zeitdiebstahl« und Manipulationen.* Zürich 1976.

PETER RØRDAM: Nogle spørgsmål om forholdet mellem straffelovens bestemmelser om bedrageri, mandatsvig og skyldnersvig. *Ugeskrift for Retsvæsen* 1960 B.49 ff.

PETER RØRDAM: Mere om bedrageri, mandatsvig og skyldnersvig. *Ugeskrift for Retsvæsen* 1960 B.166 ff.

PETER RØRDAM: Vildfarelseskravet i straffelovens bedrageribestemmelse. *Juristen* 1960.301 ff.

ERIK SAMUELSEN: *Statlige databanker og personlighetsvern.* Oslo 1972.

STEIN SCHJØLBERG: Computer-Assisted Crime in Scandinavia. *The Computer/Law Journal* 1980.457 ff.

STEIN SCHJØLBERG: Computer Crime in Norway, i JON BING & KNUT S. SELMER (ed.): *A Decade of Computers and Law.* Oslo 1980 s. 440 ff.

STEIN SCHJØLBERG: *Computers and penal legislation. A study of the legal politics of a new technology.* Oslo 1983.

STEIN SCHJØLBERG: EDB og kriminalitet - oversikt og kategorier. *Lov og Rett* 1983.467 ff.

STEIN SCHJØLBERG: Er det behov for en ny lovgivning om EDB og kriminalitet. *Lov og Rett* 1983.479 ff.

STEIN SCHJØLBERG: »System hackers« - handlingenes art og juridiske konsekvenser. *Nordisk Datanytt* 1984(7).53 ff.

STEIN SCHJØLBERG: Anmeldelse af VAGN GREVE: *Edb-strafferet. Tidsskrift for Rettsvitenskap* 1985.623 ff.

PETER SEIPEL: Datorprogrammens rättsskydd. *Nordiskt Immateriellt Rättskydd* 1973.121 ff.

PETER SEIPEL: Skydda datorerne! *Dagens Nyheter* 1984-09-17.

KNUT S. SELMER: Elektronisk databehandling og rettssamfunnet. I CECILIA MAGNUSSON & OLAV TORVUND (red.): *Juristen och datasäkerheten.* Stockholm 1985. S. 171 ff.

M. SENDROW: *Impact of rapidly changing computer technology.* Virginia 1985.

PETER SIDLER: *Der Schutz von Computerprogrammen im Urheber- und Wettbewerbsrecht.* Basel 1968.

ULRICH SIEBER: *Computerkriminalität und Strafrecht.* Köln 1977. 2. Aufl. 1980.

ULRICH SIEBER: Computerkriminalität. Mundtlig redegørelse til retsudvalget i Deutscher Bundestag 1984-06-06 med bilag.

STANLEY L. SOKOLIK: Computer Crime - The Need for Deterrent Legislation. *Computer/Law Journal* 1980.353 ff.

ARTHUR SOLARZ: Datorbrott - begrepp och definition. I CECILIA MAGNUSSON & OLAV TORVUND (red.): *Juristen och datasäkerheten.* Stockholm 1985. S. 79 ff.

ARTUR SOLARZ: *Datorteknik och brottslighet.* Stockholm 1985.

ARTUR SOLARZ: Datorbedrägeri i lagstiftningen. *BRÅ apropå* 1986:1.32 ff.

ARTUR SOLARZ. Se også ovenfor under BRÅ-S 1982-7.

SOU 1972:47. *Data och integritet.*

SOU 1983:50. *Översyn av lagstiftningen om förmögenhetsbrott utom gäldenärsbrott.*

SOU 1983:52. *Företagshemligheter.*

SOU 1985:51. *Upphovsrätt och datorteknik.*

SOU 1986:24. *Integritetsskyddet i informationssamhället 1.*

GÜNTER STRATENWERTH: Computerbetrug. *Schweizerische Zeitschrift für Strafrecht* 1981.229 ff.

FRITZ SÖLDNER: Neue kriminologische Erscheinungsformen der Betriebskriminalität. *Kriminalistik* 1973.1 ff.

FLEMMING SØRENSEN: *Registersamfundet.* København 1984.

JOHN K. TABER: A Survey of Computer Crime Studies. *Computer/Law Journal* 1980.275 ff.

COLIN TAPPER: *Computers and the Law.* London 1973.

HANS B. THOMSEN: Papirløse systemer i internasjonal handel - økt risiko for manipulasjon? *Lov og Rett* 1983.568 ff.

JAN VILGEUS: Automatmissbruk. Bedrägeri, bedrägligt beteende eller stöld. *Nordisk Tidsskrift for Kriminalvidenskab* 1965.60 ff.

PER-EDWIN WALLÉN: Om bankomatmissbruk. *Svensk Juristtidning* 1980.707 ff.

PER-EDWIN WALLÉN: Om bedrägeri genom utnyttjande av annans villfarelse - en jämförelse mellan dansk, norsk och svensk rätt. *Lov og frihet. Festskrift til Johs. Andenæs.* Oslo 1982 s. 385 ff.

JOHN C. WATKINS: Anmeldelse af STEPHEN W. LIEBHOLZ & LOUIS D. WILSON: *User's Guide to Computer Crime: Its Commission, Detection and Prevention. Crime & Delinquency* 1977 s. 88 ff.

THOMAS WHITESIDE: *Databrott.* Malmö 1980. (Oversættelse af *Computer Capers.* New York 1978).

HANS WRANGHULT: ADB: Sårbarhet, säkerhet, kriminalitet. *Lov og Rett* 1983.560 ff.

E. ZIMMERLI: Computerkriminalität und Strafrecht. *Neue Zürcher Zeitung* 1986-02-26.

Lovregister

Domsregister (danske domme)