Straffelovrådets betænkning
om

datakriminalitet

BETÆNKNING NR. 1032
KØBENHAVN 1985

ISBN 87-503-5436-1
Ju 00-169-bet.
Eloni tryk • København

Indholdsfortegnelse

Forord

Ved skrivelse af 19. marts 1984 anmodede justitsministeriet straffelovrådet om en udtalelse om, hvorvidt de gældende bestemmelser i straffeloven er tilfredsstilllende udformet med henblik på gerningstyper, der har forbindelse med elektronisk databehandling (datakriminalitet).

I justitsministeriets skrivelse henvistes til, at en række sager om datakriminalitet, der var under behandling hos politiet eller anklagemyndigheden, havde givet anledning til offentlig omtale og diskussion. Det oplystes, at justitsministeriet og anklagemyndigheden, navnlig statsadvokaten for særlig økonomisk kriminalitet, havde fulgt udviklingen på dette ormdåe, og at anklagemyndigheden endnu ikke havde haft sager om datakriminalitet, som ikke var omfattet af de gældende bestemmelser i straffeloven. Justitsministeriet fandt det imidlertid hensigtsmæssigt, at der blev foretaget en samlet vurdering af, om de gældende regler er tilfredsstillende udformet med henblik på sådanne forhold. Der kunne efter justitsministeriets opfattelse bl.a. være en vis tvivl om "hvorvidt gerningsbeskrivelsen i straffelovens bestemmelser navnlig om fredskrænkelser, berigelseforbrydelser, tingsødelæggelse og brugstyveri i tilstrækkeligt omfang omfatter f.eks. retsstridig tilegnelse, ødelæggelse eller brug af dataudstyr, dataprogrammer eller data, som er lagret i databehandlingsudstyr". Desuden nævntes det spørgsmål, om straffelovens bestemmelser giver mulighed for at idømme tilstrækkelig høj straf for tilfælde af særlig grov datakriminalitet, der er omfattet af loven.

Justitsministeriet anmodede om, at straffelovrådets udtalelse så vidt muligt måtte foreligge i løbet af 1984. Denne frist er senere blevet forlænget til ca. 1. marts 1985.

Straffelovrådet har modtaget værdifuld bistand fra Kommunedata I/S, Kjøbenhavns Handelsbank A/S og statsadvokaten for særlig økonomisk kriminalitet.

Rådets formand og sekretariatet har endvidere deltaget i møder med sagkyndige i de andre nordiske lande og i et af OECD afholdt møde i Paris den 10. og 11. december 1984 om "computer-related criminality". Det er i mange lande aktuelt at overveje, om datakriminalitet giver anledning til ændringer i straffelovgivningen, og opmærksomheden samler sig navnlig om de gerningstyper, der er nævnt nedenfor i kapitel 1.3.

Om aktuelle overvejelser i de nordiske lande skal kort anføres følgende. I Norge har strafffelovrådet i 1983 fået stillet en opgave, der i det væsentlige svarer til den, der foreligger i Danmark, og en norsk betænkning ventes afgivet i 1985. I Sverige er nogle sider af datakriminaliteten omtalt i betænkningen översyn av lagstiftningen om förmögenhetsbrott utom gäldenärsbrott" {SOU 1983:50). Der stilles her forslag om en ny straffebestemmelse om "datorbedrägeri". Tilsvarende foreligger der fra det finske strafflagsprojekt et forslag om en ny bedrageribestemmelse (se om det svenske og det finske forslag nedenfor i kapitel 6). Både i Sverige og Finland går man videre med drøftelser om andre sider af datakriminaliteten.

I straffelovrådets sammensætning er der i januar 1984 sket følgende ændringer. Tidligere afdelingschef i justitsministeriet Michael Lunn er udtrådt af rådet efter at være blevet udnævnt til departementschef i energiministeriet, og i hans sted er kontorchef i justitsministeriet Michael Elmer udpeget som medlem af rådet og leder af dettes sekretariat. Fængselsinspektør, lic. jur. Ole Ingstrup er udtrådt af rådet efter at have overtaget en stilling ved Correctional Service, Canada, og han er blevet efterfulgt af direktør for kriminalforsorgen Frits Hellborn som medlem af rådet. Endvidere er politimester Jørgen Langkilde blevet udpeget som medlem af rådet.

Straffelovrådet har således ved afgivelsen af denne betænkning haft følgende sammensætning: professor, dr. jur. Knud Waaben (formand), advokat Jørgen Bang, kontorchef Michael Elmer,- retspræsident Kurt Haulrig, direktør for kriminalforsorgen Frits Hellborn, politimester Jørgen Langkilde og rigsadvokat Per Lindegaard.

Hvervet som sekretær for rådet er varetaget af fuldmægtig i justitsministeriet Bent Carlsen.

København, den 4. marts 1985.

Jørgen Bang	Elmer	Kurt Haulrig
Frits Hellborn	Jørgen Langkilde	Per Lindegaard
	Knud Waaben (formand)	
		/Bent Carlsen (sekretær)

Sammenfatning

Straffelovrådet har i denne betænkning behandlet spørgsmålet om datakriminalitet. Rådet har i den forbindelse foretaget en gennemgang af straffeloven og de væsentligste særlove med henblik på at konstatere, om der er behov for at foretage lovændringer.

I betænkningens kapitel 1 har man kort beskrevet datateknikken, og hvad der forstås ved datakriminalitet. Det anføres, at den egentlige datakriminalitet er de strafbare handlinger, der rummer en anvendelse af den for databehandling særegne teknik med hensyn til registrering, opbevaring, bearbejdelse og brug af oplysnnger. Rådet har dog ikke lagt vægt på at fastholde en begrænsning til den egentlige datakriminalitet, men har også behandlet handlinger, som har forbindelse til databehandling, uden at der anvendes særlig datateknik, f.eks. beskadigelse eller ødelæggelse af dataanlæg. I samme kapitel beskrives de vigtigste typer af datakriminalitet.

I kapitel 2 findes en gennemgang af straffelovens bestemmelser om fredskrænkelser, navnlig bestemmelserne i § 263 og § 264. Det kan efter rådets opfattelse give anledning til en vis tvivl, om uberettiget indsigt i data er omfattet af bestemmelsen i § 263. For at gøre det klart, at det er strafbart at skaffe sig sådan adgang til oplysninger, som er lagret i et dataanlæg, foreslås en ny bestemmelse herom indføjet i § 263 som et nyt stk. 2. Endvidere foreslås en ny strafskærpelsesbestemmelse indføjet i § 263 for de tilfælde, hvor gerningsmanden i forbindelse med en overtrædelse af § 263, stk. 1 og 2, har haft forsæt til at skaffe sig oplysninger om en virksomheds erhvervshemmeligheder, eller hvor der i øvrigt foreligger særligt skærpende omstændigheder.

Kapitel 3 indeholder en gennemgang af straffelovens bestemmelser om tyveri (§ 276) og brugstyveri (§ 293). Det konstateres, at tyveribestemmelsens krav om borttagelse af en fremmed rørlig ting giver den et meget begrænset anvendelsesområde i datafor-

hold, men at der på den anden side ikke er noget behov for at udvide bestemmelsen. Endvidere konkluderes det, at bestemmelsen om brugstyveri i vidt omfang vil kunne finde anvendelse på uberettiget brug af dataanlæg, programmer og oplysninger, der er lagret på fysiske genstande.

Kapitel 4 indeholder en gennemgang af straffelovens bestemmelse i § 291 om tingsbeskadigelse og tingsødelæggelse med hensyn til dataforhold. Rådet antager, at bestemmelsen vil kunne finde anvendelse ikke alene på tilfælde, hvor et dataanlæg beskadiges, men også på en række tilfælde, hvor datalagrede oplysninger eller programmer ændres eller slettes. Der foreslås derfor ikke ændringer af denne bestemmelse.

I kapitel 5 har man foretaget en gennemgang af straffelovens kapitel 20 og 21 om almenfarlige og almenskadelige forbrydelser. Rådet finder, at det bør være strafbart at fremkalde omfattende forstyrrelse i driften af dataanlæg, og foreslår en tilføjelse herom til straffelovens § 193 samt en forhøjelse af denne bestemmelses strafmaksimum til 6 års fængsel.

I kapitel 6 gennemgås straffelovens § 279 om bedrageri med henblik på dataforhold. Efter rådets opfattelse vil bestemmelsen ikke være anvendelig i de bedragerilignende situationer, hvor det ikke er et menneske, der besviges, men en datamaskine, som modtager urigtige oplysninger fra gerningsmanden, og som derfor leverer et urigtigt resultat med økonomiske følger. En del af disse forhold vil i dag kunne straffes efter straffelovens bestemmelser om underslæb og mandatsvig. Men straffelovrådet har fundet det hensigtsmæssigt at udforme en ny bestemmelse i § 279 a om databedrageri, som gør det klart, at det er strafbart retsstridigt at påvirke resultatet af en databehandling for at skaffe sig eller andre en uberettiget vinding.

I kapitel 7 beskrives straffelovens bestemmelser om pengeunderslæb (§ 278) og mandatsvig (§ 280). Navnlig den sidstnævnte har i praksis fundet anvendelse på datakriminalitet. Bl.a. under hensyn til det foran nævnte forslag om en bestemmelse om databedrageri finder rådet ikke behov for ændringer af de to bestem-

melser.

Kapitel 8 indeholder en gennemgang af straffelovens bestemmelser i kapitel 19 om bevisforbrydelser, navnlig § 171 om dokumentfalsk og § 178 om bevisødelæggelse. Det konstateres, at bestemmelserne i kapitel 19 kun har et begrænset anvendelsesområde med hensyn til dataforhold. Efter rådets opfattelse er der ikke på nuværende tidspunkt tilstrækkeligt grundlag for at foreslå en ny bestemmelse i kapitel 19 om dataindgreb eller lignende. Samme konklusion er rådet nået til med hensyn til straffelovens bestemmelser i kapitel 17 om urigtige erklæringer .

I kapitel 9 omtales de vigtigste af de særlove, som har tilknytning til spørgsmålet om datakriminalitet: registerlovene, lov om betalingskort, markedsføringsloven og ophavsretsloven.

Kapitel 1

Indledning

1.1. Datateknikken

Den centrale enhed i et dataanlæg er den, som styrer og udfører de elektroniske operationer. Det udefra kommende materiale af oplysninger formuleres i maskinkode, d.v.s tegn, der kan omsættes til impulser i de elektroniske komponenter - chips eller integrerede kredsløb -, som indeholdes i centralenheden. Hvis oplysninger skal bevares, sker dette i computerens "ydre lager", typisk et magnetbånd eller en pladeformet diskette,- der har en partikeibelægning, som kan magnetiseres. De registrerede oplysninger eller et ordnet udvalg af dem gøres tilgængelige ved aktivering af de elektroniske impulser. Alle operationer bestemmes af programmer, d.v.s. forud fastlagte instruktioner for ordning, udvælgelse og anden bearbejdelse af data fra computerens lager. Centralenheden rummer en regneenhed, der udfører alle regneoperationer, samt en styreenhed, der sørger for, at kørsel sker efter de i programmet angivne retningslinier. Det beror på brugerens behov, om oplysninger og programmer på magnetbånd og disketter skal være direkte knyttet til computeren, det vil sige umiddelbart disponible til brug for operationer, eller de skal adskilles fra computeren og arkiveres, indtil de igen forbindes med computeren. Et typisk objekt for arkivering er sikkerhedskopier af materiale.

Det må fremhæves, at programmer ikke er en del af beholdningen af oplysninger, selvom de datateknisk foreligger og virker på samme måde som disse. Programmer er selvstændige redskaber til strukturering af datamassen. De spænder fra det meget enkle til det stærkt komplicerede, fra standardiserede programmer med et bredt anvendelsesområde til de mest specialiserede. Datakriminalitet kan derfor ikke blot bestå i uberettiget indblik i eller ændring af lagrede oplysninger, men også f.eks. i ulovlig tilegnelse af et program gennem misbrug af et dataanlæg.

Ved indlæsning og udlæsning af data benyttes oftest terminaler, der består af et tastatur og en dataskærm, eventuelt også en printer der kan udskrive det ønskede på papir. I sin oprindelige form var computeren indrettet således, at alle operationer fra modtagelsen af inddata til afslutningen af databehandling foregik på samme sted. Det er karakteristisk for den senere udvikling, at terminaler kan befinde sig langt fra den centrale enhed, således at der ved terminalen kan afsendes og modtages data til og fra et hovedkontor o.l. Der kan desuden til en terminal være knyttet en mindre computer med mulighed for brug af terminalens egne disketter.

Transmissionen mellem centralenheden og terminalen eller mellem flere terminaler indbyrdes kan foregå på forskellige måder, f.eks. gennem interne ledninger eller kabler, gennem telexnettet, det offentlige datanet, det almindelige telefonnet (herunder lejede telefonkredsløb) eller bredbånd. Ved brug af telefonnettet anvendes apparater ("modemer"), der omsætter datamaskinens signaler til signaler, der kan transmitteres via telefonnettet.

De vigtigste elementer i et datasytem er således: den centrale enhed, terminalen, transmissionsforbindelsen, de lagrede data og programmet. På hvert af disse punkter kræves der sikkerhedsforanstaltninger, dels for at sikre korrektheden af datamassen og dens behandling, dels for at værne systemets indhold og funktioner mod uberettiget indsigt og brug. De foran nævnte elementer er samtidig dem, der udgør mulige angrebspunkter for datakriminalitet.Sikkerhedsforanstaltningerne er af mange forskellige slags: aflåsning af døre, nøglekontrol, tyverialarm, hemmeligt telefonnummer til modemforbindelser, kopiering af data og programmer, kontrolkørsel af materiale, logiske prøver på databehandlingens korrekthed, efterfølgende revision o.s.v.

En særlig form for sikring er den, der er indlagt i systemet med henblik på adgangsbegrænsning og anvendelseskontrol. Som eksempler på sådan sikring kan nævnes navne- og initialidentificering (hvor kun indtastning af legale brugeres navne eller initialer åbner forbindelsen), anvendelse af passwords eller

kodeord, der bestemmer, hvilke dele af systemet den pågældende har adgang til, samt anvendelse af protektionskoder, der bestemmer, hvad den pågældende må foretage sig (læse, skrive, slette) i den del af systemet, som han har legal adgang til.

I mange større systemer vil der endvidere ske en særskilt registrering af illegale adgangsforsøg, og i de fleste større systemer sker der en logregistrering af, hvem der har været inde i systemet og i hvilket tidsrum m.v.

Værdien af sikringer afhænger naturligvis af, i hvilket omfang de fungerer i praksis. F.eks. er initialidentificering ikke meget værd, hvis en terminal efterlades åbnet i frokostpausen, og passwords er ikke meget værd, hvis andre er bekendt med dem. Dertil kommer, at i stort set alle systemer vil programmører, der kender systemerne, kunne læse alle aktuelle initialer, passwords o.l.

Logregistrering og registrering af illegale adgangsforsøg øger muligheden for at opdage angreb på systemet i tide og forbedrer politiets efterforskningsmuligheder.

En særlig form for sikring er knyttet til arbejdsdeling. Det øger mulighederne for kriminalitet i ansættelsesforhold, at samme person er beskæftiget med den forudgående ekspedition af grundmateriale (arbejdssedler, fakturaer o.l), indlæsning eller forberedelse hertil og den efterfølgende ekspedition på grundlag af databehandlingen (udsendelse af lønsedler, regninger o.l.) samt kontrol med overensstemmelsen med grundmaterialet. Risikoen for, at flere ansatte medvirker om en forbrydelse, er gennemgående mindre end risikoen for, at en person, der sidder på alle funktioner, begår kriminalitet.

1.2. Datakriminalitet.

Udtryk som "data", "databehandling" o.l. omfatter sprogligt alle oplysninger og enhver form for behandling - herunder manuel behandling - af oplysninger. Når udtryk som disse anvendes i det følgende, sigtes der imidlertid til forhold, der har

tilknytning til den elektroniske databehandling. Udtrykket "elektronisk databehandling" er anvendt i to af de udkast til lovændringer, som straffelovrådet fremlægger. Efter det for rådet oplyste er der ikke behov for at foretrække det i dansk sprogbrug mindre indarbejdede udtryk "automatisk databehandling" (på svensk: ADB) frem for udtrykket "elektronisk databehandling" (EDB).

Datakriminalitet eller EDB-kriminalitet ("computer crime") kan defineres på forskellige måder. Enkelte sider af definitionsspørgsmålet skal her kort omtales, særlig med henblik på en foreløbig præsentation af forskellige gerningstyper.

Det kan være praktisk først at fremhæve, at udtrykket "datakriminalitet" ikke her begrænses til handlinger, der allerede nu er strafbare i dansk ret. Ordet omfatter handlinger, der enten er eller muligvis bør være strafbare. I almindelighed er det ikke hensigtsmæssigt at bruge udtrykket "kriminalitet" om andre forhold end dem, der er kriminaliserede, d.v.s. strafbare. Men formålet med de følgende afsnit er at undersøge, om de gældende regler er vide nok til at ramme de dataforhold med straf, som bør kunne rammes. I denne sammenhæng er det formentlig hensigtsmæssigt, at de handlinger, som kommer i søgelyset, kan kaldes "datakriminalitet", før man ved, om de er strafbare. Ville man undgå denne terminologiske inkonsekvens, måtte man formentlig begynde med at tale om "datamisbrug" el.lign. og reservere ordet "datakriminalitet" for de forhold, om hvilke det tillige kan fastslås, at de er strafbare.

Når det gælder den nærmere forståelse af udtrykket "datakriminalitet", bør man formentlig lægge til grund, at den egentlige datakriminalitet er de strafbare handlinger, der rummer en anvendelse af den for databehandling særegne teknik med hensyn til registrering, opbevaring, bearbejdelse og brug af oplysninger. Hertil hører ikke blot uberettiget tilføjelse, ændring eller slettelse af oplysninger, indgreb i datanlæggets programmering etc., men også det forhold, at en person uden at ændre noget skaffer sig kendskab til oplysninger eller programmer ved uberettiget brug af dataanlægget.

Datakriminalitet i vid forstand omfatter også andre handlinger end de her nævnte: forfalskning af det grundmateriale, der foreligger før dataregistreringens påbegyndelse, eller af udskrifter af en afsluttet databehandling, undladelse af at gøre opmærksom på fejl ved en databehandling, modtagelse af penge efter fuldbyrdelsen af en hovedforbrydelse, der er realiseret ved brug af datateknik, tyveri af et dataanlæg eller dele heraf, beskadigelse og ødelæggelse af et anlæg eller dele heraf ved traditionelle fysiske midler som slag eller overrivning af ledninger etc. I forbindelse med de sidstnævnte eksempler kan anføres, at der foreligger egentlig datakriminalitet i den ovenfor fremhævede betydning, såfremt beskadigelse eller ødelæggelse forvoldes ved indtastning af ordrer om ændring eller sletteIse af oplysninger.

Straffelovrådet har ikke i det følgende lagt vægt på at fastholde en begrænsning til datakriminalitet i egentlig forstand. De centrale problemer er dog givetvis dem, der knytter sig til registrering, ændring, bearbejdelse, transmission og brug af oplysninger inden for rammerne af et dataanlæg. Nogle hovedtyper af datakriminalitet vil blive fremhævet nedenfor i kapitel 1.3.

Oplysninger fra mange lande tyder på, at datakriminaliteten har fået et meget stort omfang. Der udfoldes derfor mange bestræbelser for at indbygge sikkerhedsforanstaltninger i brugen af dataanlæg. De mest omfattende og indgående undersøgelser og rapporter vedrører forholdene i USA, og herfra stammer den største del af det materiale, der belyser variationer i de faktisk anvendte kriminelle metoder, herunder eksempler på økonomiske besvigelser i stor stil. Samtidig kan det dog konstateres, at en række gerningstyper går igen i flere lande, hvilket ikke kan overraske, eftersom datateknikken og dens anvendelse i forretningslivet og i offentlig administration stort set er den samme alle steder og frembyder de samme muligheder for at udnytte systemets svage punkter. Straffelovrådet har ikke fundet det nødvendigt at gå ind på en nærmere redegørelse for forholdene i andre lande, men har i hovedsagen begrænset sig til

at behandle de erfaringer og problemer, der er af størst betydning med henblik på en vurdering af de gældende danske regler. Der er dog på en række punkter anledning til at benytte eksempler, der ikke støtter sig på erfaringer fra dansk praksis, men i mere hypotetisk form belyser områder, der enten er eller ikke er dækket af de gældende regler.

Hvis man ville slutte noget om datakriminalitetens omfang i Danmark på grundlag af de sager, der har foreligget for politiet og anklagemyndigheden, måtte man komme til det resultat, at denne kriminalitet spiller en ret ringe rolle. Straffelovrådet har haft lejlighed til at gøre sig bekendt med de fleste af de sager, der har været behandlet af statsadvokaten for særlig økonomisk kriminalitet. I forhold til samtlige sager om forbrydelser som underslæb, bedrageri, mandatsvig o.l. udgør sagerne om datakriminalitet en meget lille gruppe. Der er dog grund til at antage, at datakriminaliteten faktisk har et noget større omfang, men det lader sig næppe gøre at anstille blot nogenlunde realistiske skøn over, hvilken størrelsesorden det drejer sig om. Mange forhold bliver ikke opdaget, bl.a. fordi der er mangelfuld kontrol med de ansattes adgang til at betjene et dataanlæg eller mangelfuld revision eller anden efterfølgende kontrol med de forhold, som er genstand for databehandling. Men en væsentlig rolle spiller det formentlig også, at der i mange tilfælde ikke sker anmeldelse til politiet af forhold, der er blevet opdaget. Det kan bl.a. skyldes det også fra underslæbssager kendte forhold, at et firma ønsker at undgå publicitet omkring interne fremgangsmåder, der med rette eller urette kan give indtryk af manglende sikkerhed og kontrol, og at firmaet desuden finder, at en afskedigelse - eventuelt i forbindelse med en aftale om tilbagebetaling - og en ændret intern praksis er en tilstrækkelig reaktion. Ligesom det er vanskeligt at skønne over datakriminalitetens reelle omfang, savnes der holdepunkter for at sige noget generelt om, i hvilken grad eller på hvilke områder man har forsømt at følge den øgede brug af datateknik op med nærliggende og let praktikable sikkerhedsforanstaltninger.

Der kan dog næppe være tvivl om, at virksomheder og myndigheder

i betydeligt omfang udfolder bestræbelser for at øge sikkerheden mod, at dataanlæg kan misbruges af ansatte eller udefra kommende personer. I forbindelse med den opgave, der foreligger for straffelovrådet, bør det understreges, at brugen af sikkerhedsforanstaltninger utvivlsomt har en langt større præventiv betydning end nogle ændringer i straffelovens afgrænsning af det strafbare område.

1.3. Gerningstyper og lovregler

I straffeloven findes der kun en enkelt bestemmelse, der ved selve sin formulering viser, at den har noget at gøre med elektronisk databehandling. Det er § 152, stk. 4, om brud på tavshedspligt, begået af en person, der har fået en vis viden "under arbejde for en virksomhed, der maskinelt behandler eller opbevarer oplysninger for det offentlige". Men i øvrigt beror dataforholds strafbarhed på, om de er dækkede af gerningsbeskrivelsen i en bestemmelse, der kan overtrædes på mange forskellige måder, f.eks. § 263 om fredskrænkelser eller § 279 om bedrageri. Mange bestemmelser i straffeloven - bl.a. i kap. 28 om berigelsesforbrydelser - har ikke været ændrede siden lovens vedtagelse i 1930, da ingen tænkte på datateknik, men alligevel vil mange dataforhold være omfattet af ordvalget i sådanne bestemmelser. Når man opdeler angreb på eller misbrug af dataanlæg i en række forskellige typer, er det for de fleste forholds vedkommende relativt let at afgøre, om de falder indenfor eller udenfor en straffebestemmelses område, medens spørgsmålet på nogle punkter frembyder tvivl.

Straffelovrådet har i de følgende afsnit anvendt den systematik, at udgangspunktet tages i de straffebestemmelser, som må antages at finde anvendelse på forskellige former for datakriminalitet. Inden for hver bestemmelse søges det belyst, hvilke forhold der må antages at være strafbare, og det drøftes, om der må antages at være behov for lovændringer.

De vigtigste af de typer af datakriminalitet, som skal tages i betragtning, kan skematisk opstilles således:

1) Ulovligt indblik i andres data.

En række datamisbrug består i at skaffe sig uberettiget adgang til andres dataoplysninger uden herved at ændre oplysningernes indhold eller i øvrigt påvirke den fremtidige retmæssige brug af dataanlægget. Sådanne handlinger må opfattes som fredskrænkelser på linie med de i straffelovens §§ 263 ff. beskrevne krænkelser af andres ret til at have deres gemmer, brevveksling, samtaler, privatliv m.v. uforstyrret for sig selv.

2) Videregivelse af data.

Den, som i medfør af et ansættelsesforhold o.l. lovligt har fået kendskab til oplysninger, kan misbruge sin viden ved at videregive oplysninger til andre.

Datateknik som middel til berigelsesforbrydelser.

Misbrug af et dataanlæg kan på forskellige måder være et middel til at begå en af straffelovens kap. 28 omfattet berigelsesforbrydelse. De forbrydelser, som især kommer i betragtning, er bedrageri (§ 279), pengeunderslæb (§ 278, stk. 1, nr. 3) og mandatsvig (§ 280). Derimod vil datateknik formentlig sjældnere være et middel til at begå tyveri (§ 276) eller tingsunderslæb (§ 278, stk. 1, nr. 1), men et dataanlæg eller dele heraf kan i sig selv være genstand for en sådan forbrydelse.

4) Beskadigelse og ødelæggelse af dataanlæg og data.

Uden at have forsæt til at skaffe sig selv eller andre uberettiget økonomisk vinding kan en person angribe en andens dataanlæg ved handlinger, der medfører en beskadigelse eller ødelæggelse af selve anlægget eller dele heraf eller af lagrede oplysninger. Foruden ting'sbeskadigelse og -ødelæggelse efter § 291 omtales senere de forhold af særlig grovhed eller farlighed, der kan forvoldes ved brandstiftelse eller sprængning eller medføre omfattende forstyrrelse af kommunikationsmidler o.l.

5) Ulovlig brug af et datanlæg.

Den uberettigede brug af en andens dataanlæg eller af tilbehør hertil kan straffes efter straffelovens § 293 om brugstyveri. Da denne bestemmelse ligesom § 291 indeholder udtrykket "ting", må det overvejes, om der kan forekomme en uberettiget brug af andres dataoplysninger, der ikke er omfattet af dette udtryk.

6) Forfalskning af bevismidler.

Et uberettiget indgreb i dataregistrerede oplysninger kan have lighed med dokumentfalsk og andre bevisforbrydelser, når gerningsmanden handler med forsæt til at forvanske de beviser, som senere kan tænkes støttet på et dataanlægs udvisende. Eksempler herpå kan foreligge, hvor forvanskning af dataoplysninger sker for at skjule en allerede begået berigelsesforbrydelse, eller hvor forvanskningen angår retsforhold, der ikke har noget at gøre med økonomiske forhold.

7) Modtagelse af penge eller oplysninger efte en forudgående dataforbrydelse.

Til datakriminalitet i vid forstand kan bl.a. henregnes nogle tilfælde, hvor en person begår hæleri eller et hermed beslægtet forhold ved at modtage penge eller oplysninger, der er fremkommet ved en egentlig dataforbrydelse, f.eks. underslæb ved dataoverførsel af penge eller ulovlig tapning af beskyttede oplysninger om forretningsforhold.

8) Tilegnelse eller brug af ophavsretligt beskyttede programmer for databehandling.

Udenfor tilfælde, hvor tilegnelse af dataprogrammer kan bedømmes som tyveri eller tingsunderslæb, kan der tænkes tilfælde, hvor sådan tilegnelse af beskyttede programmer er eller bør være en krænkelse af ophavsretten til programmer.

De gældende straffelovsbestemmelser - eventuelt med visse udvidelser - finder anvendelse på ret forskelligartede gerningsty-

per. Bestemmelser om edskrænkelser angår typisk det blotte indblik i andres dataoplysninger uden indgreb i deres indhold eller behandling. Nogle bestemmelser om formueforbrydelser retter sig alene eller fortrinsvis mod dataanlæg eller dele heraf som fysiske genstande, medens andre angår et dataanlægs informationer og deres behandling. Fælles for alle berigelsesforbrydelser (modsat f.eks. tingsødelæggelse og brugstyveri) er et krav om, at der skal være handlet med berigelsesforsæt. Dette gør det nødvendigt at overveje, om der er fornøden strafhjemmel i tilfælde, hvor datakriminalitet ikke er forbundet med (beviseligt) berigelsesforsæt. Af berigelsesforbrydelserne vil pengeunderslæb og mandatsvig være begrænsede til personer, der i kraft af et ansættelsesforhold eller lignende har en særlig tilknytning til den person eller virksomhed, hvor forbrydelsen begås, medens bedrageri o.l. kan begås såvel af ansatte som af udefra kommende personer, der skaffer sig adgang til at betjene et dataanlæg.

De fleste af de straffelovsbestemmelser, der kommer i betragtning, forudsætter, at der er handlet med forsæt, jfr. straffelovens § 19. Der er dog enkelte bestemmelser om uagtsomhed, bl.a. § 291, stk. 3, om tingsbeskadigelse eller -ødelæggelse af betydeligt omfang, ligesom uagtsomhed som hovedregel er omfattet af straffebestemmelser i særlovgivningen, bl.a. markedsføringsloven. Straffelovrådet har overvejet, om der er behov for at ramme uagtsomme (eventuelt blot groft uagtsomme) datamisbrug, som ikke i dag er strafbare. Man er nået til den konklusion, at der ikke bør stilles forslag om nykriminalisering af forhold, der ikke er begået med forsæt, se dog kapitel 5 om § 193.

Spørgsmålet om fastsættelse af strafferammer omtales i forbindelse med de enkelte forbrydelsestyper.

Straffelovrådet har ikke i det følgende anført detailhenvisninger til litteraturen om de omtalte strafbare gerningstyper. For så vidt angår litteratur på dansk om EDB-kriminalitet skal navnlig fremhæves Ulla Høgs artikel "EDB og EDB-kriminalitet" i Anklagemyndighedens årsberetning 1981, side 58-73, og Vagn Greves bog "EDB-strafferet" (1984).

Kapitel 2

Fredskrænkelser

2.1. Straffelovens bestemmelser om fredskrænkelser, navnlig §§ 263-264 d, handler om forskellige former for uberettiget indtrængen på områder eller indblik i forhold, som private, virksomheder, myndigheder m.v. har et rimeligt krav på at have uforstyrret for sig selv. Hovedtyper af fredskrænkelser er krænkelse af brevhemmeligheden, husfredskrænkelse, ulovlig aflytning og fotografering samt videregivelse af meddelelser eller billeder vedrørende private forhold, se nærmere nedenfor.

Bestemmelserne om fredskrænkelser blev revideret ved lov nr. 89 af 29. marts 1972 på grundlag af straffelovrådets betænkning om privatlivets fred (Bet. nr. 601, 1971). Om lovforslaget henvises til FT 1971-72, tillæg A, sp. 551 ff. Et af formålene med denne revision var at indføje bestemmelser om fredskrænkelser begået med de i den nyeste tid udviklede tekniske midler til aflytning, lydoptagelse, iagttagelse og fotografering.

Den elektroniske databehandling havde i 1971-72 endnu ikke nået en sådan udvikling og fået en sådan udbredelse, at der var anledning til at foreslå bestemmelser herom i forbindelse med en revision af §§ 263 ff. Databehandlingen var dog ikke ukendt, og på et enkelt punkt blev loven af 1972 om ændring af straffeloven udformet med databehandling for øje. Som det allerede er nævnt, findes der i § 152, stk. 4, en bestemmelse om krænkelse af tavshedspligt, begået af den, der har fået en vis viden "under arbejde for en virksomhed, der maskinelt behandler eller opbevarer oplysninger for det offentlige". Bestemmelsen blev i 1971 efter afgivelsen af straffelovrådets betænkning foreslået af justitsministeriets registerudvalg, der havde til opgave at overveje problemer i forbindelse med brugen af offentlige og private registre. I sin udtalelse af juli 1971 omtalte registerudvalget den EDB-behandling og anden maskinelle behandling, som private servicevirksomheder på den tid udførte

med hensyn til offentlige myndigheders materialer. Og man fandt, at de ansatte burde være undergivet en tavshedspligt, der svarede til den, der efter § 152 gjaldt for offentligt ansatte. Se til det anførte FT 1971-72, tillæg A, sp. 579 ff, hvor registerudvalget også kort berørte forholdet til de af straffelovrådet foreslåede bestemmelser om edskrænkelser.

I det følgende omtales nogle hovedtræk af fortolkningen af §§ 263 ff. om fredskrænkelser. Af disse bemærkninger og den konklusion, som følger derefter, fremgår det, at de gældende bestemmelser efter straffelovrådets opfattelse ikke i tilstrækkeligt omfang hjemler strafansvar for misbrug af dataanlæg og data.

2.2. Straffelovens § 263, nr. 1, handler om den, som uberettiget "bryder eller unddrager nogen et brev, telegram eller anden lukket meddelelse eller optegnelse eller gør sig bekendt med indholdet". Spørgsmålet om anvendelse af denne bestemmelse på dataforhold kan ikke anses for afgjort i retspraksis. De følgende bemærkninger tager udgangspunkt i bestemmelsens ordvalg og forarbejderne til den.

Mindst problematisk er formentlig udtrykket "lukket meddelelse". Det er rimeligt at anlægge den betragtning, at der fra et dataanlæg kan udgå en "lukket meddelelse", såfremt anlægget er aktiveret med henblik på at bringe informationer til en modtager, og den, som uberettiget kobler sig ind på en sådan transmission, kan da siges at gøre sig bekendt med en lukket meddelelse. Man kan også forhindre, at meddelelser når frem, f.eks. ved at sætte et modtagerapparat ud af funktion, og derved "unddrage nogen" lukkede meddelelser. Det er i forarbejderne forudsat, at en meddelelse kan være "lukket" på anden måde end ved at være fysisk emballeret i kuvert, indpakning, kassette el.lign., og at § 263, nr. 1, f.eks. omfatter den, der opsnapper en telekommunikation. Der er ikke grund til at se anderledes på forholdet, hvor kommunikationen udgår fra datalagrede informationer.

For så vidt angår dataanlæggets "hvilende" informationer - dem der ikke på indgrebets tid er genstand for transmission

- falder det ikke sprogligt naturligt at betegne dem som "lukkede optegnelser". Et tilsvarende spørgsmål foreligger i Norge vedrørende et udtryk i den norske straffelovs § 145, der er indføjet i 1979. Bestemmelsen handler om "den, som uberettiget skaffer seg adgang til innholdet av en lukket meddelelse eller opptegnelse når dette regulært bare er tilgjengelig ved hjelp av særskilt utstyr for tilkopling, avspilling, gjennomlysing, aflesing eller liknende". Bestemmelsen peger dog tydeligere end den danske hen på tekniske midler til opbevaring og brug af informationer., 1 bestemmelsens forarbejder er det forudsat, at datalagrede oplysninger i sig selv er "en optegnelse", og at strafansvaret omfatter den, der ved hjælp af teknisk udstyr gør sig bekendt med oplysningerne. Det er sandsynligt, at danske domstole ville nå til samme resultat ved en vid fortolkning af udtrykket "lukket optegnelse", bl.a. under hensyn til, at registerudvalget synes at være gået ud fra denne opfattelse i en udtalelse forud for vedtagelsen af § 263, jfr. FT 1971-72, tillæg A, sp. 588. Straffelovrådet finder imidlertid, at man ved en lovændring bør gøre det klart, at det er strafbart at skaffe sig adgang til et dataanlægs informationer.

2.3. § 263, nr. 2, nævner den, som uberettiget "skaffer sig adgang til andres gemmer". Det er klart, at denne bestemmelse omfatter tilfælde, hvor en person skaffer sig adgang til en skuffe, et pengeskab, en boks el.lign., der er et opbevaringssted for magnetbånd, programmer m.v. Det kan derimod diskuteres, om det ligger inden for den sprogligt naturlige forståelse af ordet "gemme" at anse et dataanlæg som et "gemme" for de deri lagrede informationer. Dette fortolkningsspørgsmål vil være uden praktisk betydning, såfremt der som ovenfor nævnt foretages en tilføjelse bl § 263 om dataoplysninger.

2.4. De i 1972 indførte bestemmelser om redskrænkelser begået ved tekniske midler er ikke affattet således, at de vil kunne få nogen væsentlig anvendelse på dataforhold. § 263, nr. 3, omfatter hemmelig aflytning eller optagelse ved hjælp af et apparat af samtaler, forhandlinger eller udtalelser fremsat i enrum. Bestemmelsen er således begrænset til at angå lydmæssig tilegnelse af den menneskelige stemme. Og § 264 a angår

alene uberettiget fotografering eller iagttagelse af personer og f.eks. ikke affotografering af datamateriale.

2.5. Husfredskrænkelse beskrives i § 264 således, at en person uberettiget "skaffer sig adgang til fremmed hus eller andet ikke frit tilgængeligt sted" eller "undlader at forlade fremmed grund efter at være opfordret dertil". Husfredskrænkelse kan begås af den, der uberettiget skaffer sig adgang til en bygning eller en del af en bygning, hvor dataanlæg eller -tilbehør er installeret eller opbevares. Herunder falder ikke blot den helt uvedkommende person, men efter omstændighederne også den, der er ansat i en større virksomhed uden at have med dataenheden at gøre, når det efter forholdene på stedet er klart markeret eller tilkendegivet, at han ikke har noget at gøre på det pågældende sted.

Kriminaliseringen er ikke knyttet til det, som en person foretager sig eller agter at foretage sig på et fremmed sted. Hvad enten en person vil finde frem til et dataanlæg eller orientere sig om mulighederne for at begå tyveri, er hans strafbare handling selve dette at skaffe sig uberettiget adgang til den pågældende lokalitet.

§ 264, stk. 2, fremhæver som en strafforhøjende omstændighed, at en person begår husfredskrænkelse "med forsæt til at skaffe sig eller gøre sig bekendt med oplysninger om forretnings- eller fabrikationsforhold eller med dokumenter eller optegnelser". I disse tilfælde forhøjes strafmaksimum for husfredskrænkelse fra 6 måneders til 4 års fængsel. § 264, stk. 2, vil omfatte de fleste af de tilfælde, hvor nogen uberettiget skaffer sig adgang til fremmed område for at skaffe sig indsigt i en erhvervsvirksomheds dataoplysninger, idet praktisk talt alt, hvad der rummes i en sådan virksomheds dataanlæg, vil være "oplysninger om forretningsforhold". Derimod omfatter bestemmelsen ikke med tilstrækkelig klarhed tilfælde, hvor nogen skaffer sig adgang for at gøre sig bekendt med f.eks. foreningers eller offentlige myndigheders dataoplysninger, når disse ikke kan betegnes som "oplysninger om forretnings- eller fabrikationsforhold". Vedrørende tilføjelsen i § 264, stk. 2: "eller

(gøre sig bekendt) med dokumenter eller optegnelser" henvises til bemærkningerne ovenfor om udtrykket "optegnelser" og nedenfor i kapitel 8 om dokumenter.

I relation til datakriminalitet må man således navnlig pege på følgende begrænsninger i anvendelsen af § 264:

1. Bestemmelsen handler kun om adgang til stedet, ikke om det, som en person foretager sig på stedet.

2. Bestemmelsen omfatter ikke den, der f.eks. som ansat, kunde eller håndværker lovligt kan indfinde sig eller opholde sig på stedet.

3. Det i § 264, stk. 2, nævnte forsæt er beskrevet således, at ordene "forretnings- eller fabrikationsforhold" samt ordene "dokumenter eller optegnelser" begrænser arten af de dataoplysninger, som kommer i betragtning.

2.6. Straffelovrådet foreslår, at der i § 263 som nyt stk. 2 indføjes følgende bestemmelse:

> "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."

I lighed med flere af de andre fredskrænkelser vil overtrædelser af den foreslåede bestemmelse bestå i, at en person skaffer sig adgang til noget, der i forhold til ham med rimelighed kan ventes at være et lukket område, det vil sige utilgængeligt. Bestemmelsen omfatter dels den, der som helt udenforstående benytter anlægget (f.eks. ved at tilkoble egen terminal), dels den, der i kraft af et ansættelseforhold eller som reparatør har lovlige opgaver med hensyn til betjening af anlægget, men går ud over det, som han er bemyndiget til at foretage sig. Hvis den pågældende har tilføjet, ændret eller slettet data eller på anden måde påvirket resultatet af en aktuel eller fremtidig retmæssig betjening af anlægget, kan dette væ-

re en overtrædelse af en af de senere omtalte bestemmelser, f.eks. om tingsbeskadigelse eller bedrageri.

Udtrykket "en andens" er efter udkastets formulering knyttet til "oplysninger eller programmer", ikke til "anlæg", idet man herved kan gøre det klart, at der kan foreligge en strafbar krænkelse af andres interesse ved uberettiget brug af eget dataanlæg, f.eks. hvis udlejeren af et dataanlæg uberettiget skaffer sig adgang til lejerens oplysninger eller programmer, som er indkodet i dataanlægget.

Ligesom med hensyn til en række andre fredskrænkelser må det anses for nødvendigt at indføje ordet "uberettiget" som led i gerningsbeskrivelsen. Det antydes herved, at der kan forekomme tilfælde, hvor man kun ved et konkret skøn kan afgøre, om en handling, der formelt falder under bestemmelsens ordlyd, skal anses som strafbar. Det nævnte forbehold får næppe nogen praktisk betydning, når det drejer sig om handlinger foretaget af personer, der mangler enhver adkomst til at beskæftige sig med det pågældende dataanlæg. For så vidt angår ansatte, vil resultatet være det samme, såfremt den pågældende har benyttet en personlig kode, der ikke tilkommer ham, og på den måde har skaffet sig adgang til oplysninger, der ligger udenfor hans bemyndigelse .Men der kan tænkes grænsetilfælde, hvor den ansatte vel må siges at være gået udenfor sine arbejdsopgaver, men dog ikke på en sådan måde, at han bør straffes. Med henblik på sådanne tilfælde vil ordet "uberettiget" indicere, at der skal anlægges en konkret vurdering af den pågældendes forhold.

Med hensyn til forbrydelsens fuldbyrdelsesmoment bemærkes følgende:

Efter straffelovrådets lovudkast består den beskrevne dataforbrydelse i, at en person uberettiget "skaffer sig adgang til en andens oplysninger eller programmer etc." Heri ligger, at den pågældende ved tilkobling og betjening af dataanlægget skal have opnået forbindelse til dettes indhold, medens det på den anden side ikke kræves, at han beviseligt har fået kendskab

til noget. Det har næppe den største betydning at fastlægge en præcis grænse mellem forsøg og fuldbyrdet forbrydelse. Til strafbart forsøg må henregnes tilfælde, hvor en person, der har forsæt til at skaffe sig oplysninger, men er ubekendt med en indgangskode, ved sin betjening af dataanlægget kun har opnået at konstatere, at et skærmbillede viser en blokering af tilgang til anlæggets indhold. Det er på den anden side en fuldbyrdet overtrædelse, at den pågældende har opnået adgang til andre oplysninger end dem, han er interesseret i.

Ligesom de øvrige bestemmelser om fredskrænkelser kræver den foreslåede bestememlse, at der er handlet med forsæt, jfr. straffelovens § 19.

Såfremt den nye bestemmelse, som her foreslået føjes til § 263, vil § 264 c uden særskilt ændring gælde også i forhold til den nye bestemmelse. Det betyder, at § 263, stk. 2, med det heri fastsatte strafmaksimum "finder tilsvarende anvendelse på den, der uden at have medvirket til gerningen skaffer sig eller uberettiget udnytter oplysninger, som er fremkommet ved overtrædelsen".

2.7. Om fastsættelsen af strafferamme for den nye bestemmelse bemærkes følgende:

Ved revisionen af bestemmelserne om fredskrænkelser i 1972 blev der i §§ 263-264 d fastsat en strafferamme af bøde, hæfte eller fængsel indtil 6 måneder. Herfra er dog gjort to undtagelser i skærpende retning. For det første gælder der som foran omtalt et strafmaksimum af 4 års fængsel i tilfælde, hvor husfredskrænkelse efter § 264, stk. 1, nr. 1, er begået med forsæt til at skaffe sig eller gøre sig bekendt med nærmere angivne forretningsoplysninger m.v. (stk. 2). For det andet finder dette maksimum af 4 års fængsel også anvendelse på den, der efterfølgende skaffer sig eller udnytter oplysninger, der er fremkommet ved den nævnte kvalificerede husfredskrænkelse (§ 264 c, jfr. § 264).

Det forekommer velbegrundet, at der gælder et forhøjet straf-

maksimum for de i § 264, stk. 2, nævnte tilfælde af husfredskrænkelse. Det kan her dreje sig om indbrud under omstændigheder, hvor betingelserne for at anse forholdet som tyveri eller forsøg herpå ikke er opfyldt, men hvor det med husfredskrænkelsen forbundne forsæt til at skaffe sig forretningsoplysninger m.v. kan angå så betydelige værdier, at forholdet må sættes i klasse med tyveri. Ud fra dette synspunkt vil det utvivlsomt også være rimeligt at give mulighed for højere straf end 6 måneders fængsel - fredskrænkelsernes normale maksimum - i tilfælde, hvor en dataforbrydelse efter den nu foreslåede bestemmelse er begået med et tilsvarendelse forsæt.

Det er vanskeligt at tage stilling til dataforbrydelsens strafferamme uden at overveje to andre spørgsmål, der rækker ud over den opgave, som umiddelbart foreligger for straffelovrådet. Det ene er, om der ikke også bør gælde et forhøjet strafmaksimum, når andre fredskrænkelser end husfredskrænkelsen og dataforbrydelsen er begået med det i § 264, stk. 2, nævnte forsæt. Det andet spørgsmål er, om ikke det gældende strafmaksimum i § 264, stk. 2, på 4 års fængsel er for højt. Dette maksimum er mere end dobbelt så højt som normalmaksimum for tyveri i § 285 (der er blevet nedsat to gange siden 1972) og svarer til det skærpede maksimum for tyveri i § 286, stk. 1, der både efter bestemmelsens affattelse og efter retspraksis er knyttet til forudsætningen om en kriminalitet af betydelig grovhed.

Det er straffelovrådets opfattelse, at strafmaksimum i § 264, stk. 2, kan nedsættes fra 4 til 2 års fængsel, at normalmaksimum for den foreslåede dataforbrydelse kan sættes til fængsel i 6 måneder (svarende til den iøvrigt gældende normalramme for fredskrænkelserne i §§ 263-264 d), og at der som stk. 3 i § 263 bør indsættes en bestemmelse om mulighed for fængsel indtil 2 år i tilfælde, hvor en overtrædelse af § 263, stk. 1 eller stk. 2, er begået under omstændigheder, der svarer til § 264, stk. 2. I stedet for udtrykket "oplysninger om forretnings- eller fabrikationsforhold" har man i udkastet anvendt udtrykket "en virksomheds erhvervshemmeligheder", der findes i markedsføringslovens § 9. Om enkeltheder vedrørende de her omtalte forslag henvises til de specielle bemærkninger til rådets lov-

udkast.

Straffelovrådet stiller følgende forslag om affattelse af § 263, stk. 2 og 3, og § 264, stk. 2:

§ 263.

Stk. 2. 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.

Stk. 3. Begås de i stk. 1 eller 2 nævnte forhold med forsæt til at skaffe sig eller gøre sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder eller under andre særligt skærpende omstændigheder, kan straffen stige til fængsel indtil 2 år.

§ 264.

Stk. 2. Begås det i stk. 1, nr. 1, nævnte forhold med forsæt til at skaffe sig eller gøre sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder eller under andre særligt skærpende omstændigheder, kan straffen stige til fængsel indtil 2 år.

2.8. Foran i kapitel 1.3. er det omtalt, at der i straffelovens § 152, stk. 4, findes en bestemmelse om brud på tavshedspligt begået af en person, der har fået eller skaffet sig oplysninger hidrørende fra det offentlige under arbejde for en virksomhed, der maskinelt behandler eller opbevarer oplysninger for det offentlige. Bestemmelsen henhører således under reglerne om tavshedspligt, om hvilke straffelovrådet ved justitsministeriets skrivelse af 3. oktober 1984 er blevet anmodet om en udtalelse.

Ved afgivelsen af denne betænkning om datakriminalitet har straffelovrådet endnu ikke færdigbehandlet spørgsmålet om tavshedspligt. Der kan formentlig i overensstemmelse med et forslag i betænkning nr. 998/1984 blive tale om en ændret formulering og en vis udvidelse af bestemmelsen i § 152, stk. 4, til at omfatte andre former for virksomhed, som udføres efter aftale med det offentlige. Straffelovrådet overvejer ikke at stille forslag om begrænsninger i bestemmelsens anvendelsesområde i dataforhold.

Kapitel 3

Tyveri og brugstyveri

3.1. Nogle af de bestemmelser i straffeloven, som skal omtales i det følgende, indeholder det fælles krav, at forbrydelsens genstand skal være en ting, der tilhører en anden. Efter § 276 består et tyveri i, at nogen med forsæt til tilegnelse og berigelse borttager: "en fremmed rørlig ting", d.v.s. en ting, der tilhører en anden. Det samme udtryk anvendes i § 277 om ulovlig omgang med hittegods, i § 278, stk. 1, nr. 1, om tingsunderslæb og i § 288, stk. 1, nr. 1, om røveri. En "rørlig ting" er en fysisk genstand, der kan flyttes. Udenfor §§ 276-278 og 288 falder forbrydelser med hensyn til fast ejendom. Denne fra et praktisk synspunkt uvæsentlige begrænsning gælder ikke med hensyn til tingsbeskadigelse og brugstyveri, idet § 291 og § 293 anvender udtrykket "ting, der tilhører en anden". Også i disse bestemmelser betyder "ting" en fysisk genstand, d.v.s. en genstand man kan tage og føle på, modsat en mundtlig fordring, en panteret, en brugsret, en ophavsret o.l.

Med ting sidestilles visse energimængder, der ikke kan betegnes som "ting". Det fremgår af § 276, 2. pkt., der indeholder følgende bestemmelse: "Med rørlig ting sidestilles her i det følgende en energimængde, der er fremstillet, opbevaret eller taget i brug til frembringelse af lys, varme, kraft eller bevægelse eller i andet økonomisk øjemed". Denne udvidelse gælder ikke blot §§ 276-278 og 288 om "rørlige ting", men også § 291 om tingsbeskadigelse og -ødelæggelse og § 293 om brugstyveri. Der foreligger nogle domme om tyveri med hensyn til elektricitet og gas, men den praktiske betydning af bestemmelsen om energimængder er dog forholdsvis lille. Det er en selvfølge, at bestemmelsen om "(rørlig) ting" anvendes i tilfælde, hvor handlingen retter sig mod den fysiske genstand, der indeholder energimængden, f.eks. tyveri af en akkumulator eller en flaske med flaskegas. Spørgsmålet om, hvorvidt der kan tales om energimængder i forbindelse med dataforbrydelser, vil blive berørt, senere.

De følgende bemærkninger angår navnlig tyveri og brugstyveri med hensyn til ting. Tingsbeskadigelse og -ødelæggelse omtales særskilt i kapitel 4.

3.2. Til tyveri hører ud over det foran anførte, at tingen borttages fra fremmed varetægt uden besidderens samtykke, at dette sker med forsæt til tilegnelse af tingen (modsat den blotte brug), og at gerningsmanden desuden har forsæt til at skaffe sig selv eller andre uberettiget vinding ved tilegnelsen af tingen. Af disse krav kan man desuden udlede, at tingen skal have en vis økonomisk værdi, idet værdiløse ting hverken kan bringe vinding eller tab.

En datamaskine, en del heraf, et datalagringsmiddel og et program, der foreligger i form af en fysisk genstand, kan som andre ting være objekt for tyveri. Dette gælder, hvad enten borttageisen sker fra selve anlægget eller fra et lager for reservedele, programmer m.v.

Hvis en person i stedet for at stjæle et magnetbånd kopierer det ved brug af datateknik eller foretager afskrift fra en dataskærm eller fra en udskrift af båndet, falder forholdet udenfor § 276 om tyveri, fordi der ikke er sket borttagelse af en fysisk genstand. Fremgangsmåden svarer til den, der kendes udenfor dataforhold, når en person foretager afskrift af en virksomheds formler, konstruktionstegninger eller andet fortroligt materiale. Tilføjelsen om energimængder i § 276, 2. pkt., kan ikke føre til et andet resultat, men kan højst bevirke, at der opstår spørgsmål om tyveri med hensyn til den elektricitet, der er brugt ved ulovlig brug af et dataanlæg (se herom nedenfor).

Man kan diskutere, om der kan tænkes en borttagelse af fremmede ting, der ikke realiseres ved gerningsmandens eller andres fysiske handlinger, men på en mere automatisk virkende måde gennem posteringer eller afgivelse af andre instruktioner via et dataanlæg. I de fleste af de tilfælde, hvor der på denne måde søges opnået en vinding med et tilsvarende tab for en anden,

vil det efter straffelovrådets opfattelse være bestemmelserne om bedrageri og mandatsvig, der kommer i betragtning, og der vil senere blive nævnt eksempler, som hører hjemme i denne sammenhæng. Der kunne muligvis tænkes at blive statueret tyveri i tilfælde, hvor en person opnår udbetaling af penge i en bank med et EDB-styret pengeudbetalingssystem, idet han i maskinen anvender et falsk hævekort. Tilfældet har en vis lighed med det fra den før-elektroniske tid kendte forhold, at en person tilegner sig varer fra en automat ved at indkaste en falsk mønt eller et møntformet metalstykke. Dette anses som tyveri, idet udløsning af automatens mekanik er et middel til at borttage varer. Et sådant tilfælde bør bedømmes på samme måde, som hvis skufferne stod åbne på grund af en defekt i automaten. For så vidt angår dataforhold kan man også tænke sig tilfælde, hvor en person over et dataanlæg afgiver en falsk varebestilling i ejerens eller en fast kundes navn, med den følge at varerne leveres på en nærmere angivet adresse, hvorfra gerningsmanden senere borttager dem. Forholdet bedømmes mest naturligt som bedrageri, såfremt der hos det leverende firma er opstået den vildfarelse, at varebestillingen er gyldig og ægte, og levering sker under indflydelse af denne vildfarelse. Men der kan muligvis tænkes tilfælde, hvor hele ordreafgivelsen og vareleveringen er så gennemautomatiseret, at den ulovlige tilegnelse af varer kan betragtes som et tyveri, der realiseres gennem mekanisk virkende mellemled. Dette problem vil formentlig bortfalde, såfremt der i straffelovens kap. 28 indføjes en ny bestemmelse om databedrageri, se herom nedenfor i kapitel 6.

Man må formentlig konkludere, at kravet om bort-tagelse af en fremmed rørlig ting i § 276 giver tyveribestemmelsen et meget mindre anvendelsesområde i dataforhold end bestemmelserne om brugstyveri, bedrageri og mandatsvig. Der ses ikke at være noget behov for ved lovændring at udvide tyveribestemmelsens område med henblik på dataforhold.

3.3. De synspunkter, som er omtalt vedrørende tyveri, finder til dels anvendelse også på forbrydelsen tingsunderslæb, der består i at tilegne sig en fremmed rørlig ting, der på gernings-

tiden er i gerningsmandens egen besiddelse (§ 278, stk. 1, nr. 1). Det er tingsunderslæb at sælge et lånt eller lejet dataanlæg eller dele af et sådant. Der foreligger også tingsunderslæb, hvis et servicebureau for databehandling tilegner sig data eller programmer, som det har fået i sin besiddelse under udførelsen af en opgave, forudsat at der - ligesom i tyveritilfælde - er tale om tilegnelse af noget, der foreligger som en rørlig ting.

3.4. Til fuldbyrdelse af brugstyveri kræves kun, at en person "uberettiget bruger en ting, der tilhører en anden". Det er uden betydning, om genstanden befinder sig i en andens eller i gerningsmandens egen besiddelse, ligesom det er uden betydning, om genstanden under brugen er flyttet eller ikke flyttet fra det sted, hvor den har sin retmæssige anvendelse. Betegnelsen brugstyveri er for så vidt upræcis, men anvendes af praktiske grunde, fordi den typiske handlemåde består i borttagelse af tingen (f.eks. et befordringsmiddel) fra en andens besiddelse med henblik på brug.

Et dataanlæg som helhed eller dele af dets installationer (f. eks. en terminal) kan være genstand for brugstyveri. Uberettiget brug af en datamaskine kan f.eks. forekomme på den måde, at gerningsmanden benytter den til at udføre opgaver på egne materialer og under anvendelse af egne programmer. Brugen kan også finde sted i forbindelse med, at gerningsmanden fra en terminal skaffer sig adgang til en andens dataanlæg med henblik på at kopiere oplysninger eller programmer fra dette anlæg. Uanset hvorledes man bedømmer selve tilegnelsen af oplysninger eller programmer, vil det fremmede dataanlæg med dets indhold af bånd, disketter m.v. i sådanne tilfælde blive brugt som "ting". Det kan formentlig i nogle tilfælde give anledning til tvivl, om brugen er "uberettiget". Her tænkes på tilfælde, hvor den ansatte, hvis arbejde består i betjening af et firmas dataanlæg, benytter dette til begrænsede private formål som f.eks. beregningsopgaver, modsat tilfælde hvor han som sekretær eller kasserer for en forening benytter firmaets dataanlæg til at føre et medlemsregister. Der foreligger ikke for straffelovrådet oplysninger om, hvorvidt der i forretningsvirksom-

heder forekommer en privat brug af dataanlæg fra ansattes side, som er accepteret eller i hvert fald ikke alvorligt misbilliget. Men principielt må der regnes med tilfælde, hvor en uvedkommende brug er så ubetydelig eller så undskyldelig, at forholdet ikke bør straffes.

Uberettiget brug af programmer eller oplysninger kan som nævnt forekomme i tilfælde, hvor dette er en del af en ulovlig brug af et dataanlæg. Men det kan også være brugstyveri at borttage et magnetbånd, en kassette el.lign. med et program og anvende programmet i sin egen datamaskine for at behandle egne data eller for at kopiere programmet. I disse eksempler er der stadig tale om uberettiget brug af en andens ting. Derimod vil uberettiget brug af oplysninger, som en person under sit arbejde aflæser på en skærm, eller af programmer, som han husker fra sit arbejde, ikke være brugstyveri. Ordet "ting" i § 293 gør det med andre ord nødvendigt at sondre mellem brug af oplysninger eller programmer, når de foreligger indbygget i fysiske genstande, og oplysninger eller programmer betragtet alene som et ideindhold, en sum af forestillinger eller meninger .

Det kan tilføjes, at den norske straffelovs § 393 om brugstyveri indeholder et krav om, at der skal være påført den berettigede "tap eller uleilighet". En lignende begrænsning har engang været gældende i dansk ret, men ordene "tab eller væsentlig ulempe" udgik af § 293 i 1961. Det er ikke en betingelse for anvendelse af § 293, at tingen unddrages ejerens rådighed, medens den ulovlige brug står på.

3.5. Man kan rejse det spørgsmål, om den foran under 3.1 omtalte udvidelse af visse forbrydelser til energimængder kan tænkes at finde anvendelse i dataforhold. Det kunne hævdes, at bestemmelserne om bl.a. tyveri og brugstyveri omfatter den "energi" eller præstationskapacitet, der er knyttet til et dataanlæg og dets tilbehør, og som udløses ved aktivering af anlæggets elektronisk virkende funktioner. Efter straffelovrådets opfattelse kan man ikke anlægge en sådan konstruktion. § 276, 2. pkt., angår energimængder, der frembringer "lys, var-

me, kraft eller bevægelse" eller tjener "andet økonomisk øjemed", og et dataanlægs elektroniske processer kan næppe sidestilles med de typer af ydelser eller varer af økonomisk værdi, som § 276, 2. pkt., tager sigte på. Derimod kan denne bestemmelse omfatte det forbrug af elektrisk strøm, der er forbundet med ulovlig brug af et dataanlæg. Dette vil dog sikkert normalt kun blive bedømt som et sekundært moment i forhold til den ulovlige brug af et dataanlæg.

Kapitel 4

Tingsbeskadigelse og -ødelæggelse

4.1. I straffelovens § 291 findes den almindelige bestemmelse om tingsbeskadigelse m.v. Stk. 1 lyder således: "Den, som ødelægger, beskadiger eller bortskaffer ting, der tilhører en anden, straffes med bøde, hæfte eller med fængsel indtil 1 år." Stk. 2 indeholder et forhøjet strafmaksimum bl.a. med henblik på hærværk af betydeligt omfang", og stk. 3 kriminaliserer den groft uagtsomme forvoldelse af en skade, der er omfattet af stk. 2. Hovedbestemmelsen i stk. 1 kræver forsæt.

Der findes i straffeloven nogle specialbestemmelser om forskellige former for beskadigelse m.v. af ting, bl.a. ildspåsættelse og ødelæggelse af bevismidler. De vigtigste af disse bestemmelser vil blive nævnt i det følgende.

Den strafbare handling efter § 291 består i at ødelægge, beskadige eller bortskaffe en ting. Bortskaffelse omfatter ifølge straffelovsudkast 1923 (U III) mot. sp. 382 f. tilfælde, hvor "tingen skaffes af vejen, således at den ikke eller kun ved vanskelige eller bekostelige foranstaltninger kan fås tilbage". Midlet, som anvendes i forbindelse med en beskadigelse m.v., er uden betydning. Om begrebet "ting" henvises til bemærkninger ovenfor i afsnit 3.1. Det skal tilføjes, at der ikke af § 291 kan udledes noget krav om, at tingen skal have en formueværdi.

4.2. Ødelæggelse, beskadigelse eller bortskaffelse af et dataanlæg eller dele heraf (terminaler, ledninger m.v.) er klart omfattet af § 291. Det samme gælder ødelæggelse, beskadigelse eller bortskaffelse af et datalagringsmiddel (magnetbånd, disketter m.v.) eller af et dataprogram, for så vidt dette foreligger i form af en fysisk genstand. Tilfælde som de nævnte adskiller sig ikke i strafferetlig henseende fra en hvilken som helst anden beskadigelse m.v. af en fysisk genstand, f.eks. et radioanlæg, en skrivemaskine, en grammofonplade o.s.v.

4.3. Med bemærkningerne foran er der tænkt på beskadigelse m.v. ved de typer af fysiske handlinger, der også kunne tænkes foretaget overfor andre genstande, f.eks. slag, fjernelse af maskindele, kortslutning af ledninger etc. Et andet og vigtigere spørgsmål er, om § 291 også finder anvendelse på forhold, der består i ved udnyttelse af dataanlæggets egen teknik at ændre eller slette datalagrede oplysninger eller programmer.

Det kan diskuteres, om man kan tale om beskadigelse eller ødelæggelse af en "ting", når man alene tænker på det indgreb, der sker i systemets mindste enhed, hvor data lagres ved magnetisering af et felt og kan kaldes frem ved aktivering af dette. Straffelovrådet finder det mest sandsynligt, at dette spørgsmål ville blive besvaret bekræftende, såfremt det kom til en principiel afgørelse i en straffesag. Men spørgsmålet er næppe af stor praktisk betydning. Man kan nemlig opfatte forholdet således, at der ved ændring eller slettelse af data sker en beskadigelse af den genstand, som er databærer, f.eks. et bånd eller en diskette. Den, hvis båndoptagelse af en koncert eller et møde er blevet slettet af en uvedkommende person, vil opfatte båndet som beskadiget eller ødelagt, selv om der er blevet plads til en ny optagelse, og det samme gør sig gældende for den lovlige bruger af et dataanlæg, når et bånd eller en diskette er blevet indholdsmæssigt ændret. Der er derfor efter straffelovrådets opfattelse ingen hindringer for at betragte de her omtalte handlemåder som angreb på "ting". Det er også klart, at et bånd må anses for ødelagt, hvis dets indhold helt er slettet, selvom gerningsmanden forinden har overført indholdet til sig selv.

Det skal tilføjes, at begrebet "slettelse" i dataforhold vil række videre end til den totale fjernelse af indholdet, der svarer til slettelse på et lydbånd. Fremgangsmåden kan f.eks. være den, at det blot er indgangen til det registrerede, der slettes, medens det øvrige indhold fortsat findes på disketten, men ikke kan findes. Dette er uden betydning for den strafferetlige bedømmelse efter § 291. I tilfælde, hvor oplysninger

ad datateknisk vej er gjort utilgængelige for den retmæssige bruger, vil det efter straffelovrådets opfattelse være mere nærliggende at anvende § 291 end at henføre forholdet under § 293, stk. 2, om den der lægger hindringer i vejen for retmæssig råden over en ting. Strafferammen i § 293, stk. 2, er i øvrigt begrænset til et maksimum af 6 måneders fængsel.

Der kan muligvis i visse tilfælde være tvivl om, på hvilket tidspunkt en af § 291 omfattet dataforbrydelse skal anses for fuldbyrdet. En ofte omtalt form for datakriminalitet består i, at en person - f.eks. en ansat der er blevet sagt op - programmerer en datamaskine til på et givet tidspunkt at slette alle oplysninger af en vis karakter, f.eks. om firmaets debitorer og de skyldige beløb (den "logiske bombe"). I stedet for at anse dette som et forsøg, der først bliver til en fuldbyrdet forbrydelse, når den tilsigtede ændring eller slettelse finder sted, forekommer det forsvarligt at betragte forbrydelsen som fuldbyrdet allerede ved programmeringen. På dette stadium sker der et indgreb i anlæggets tilbehør, som derfor kan siges at være beskadiget. Fastlæggelsen af forbrydelsens fuldbyrdelsesmoment har i hovedsagen kun betydning ved at bestemme, om der kan indtræde straffrihed ved frivillig tilbagetræden indtil det tidspunkt, da den programmerede slettelse faktisk sker. Dette sidstnævnte tidspunkt vil måske i praksis blive anset som fuldbyrdelsesmomentet i relation til § 291, stk. 2, om "hærværk af betydeligt omfang", selv om deliktet i stk. 1 anses som tidligere fuldbyrdet i tilfældet med den logiske bombe.

I de tilfælde, hvor gerningsmanden leverer et nyt program med en indbygget logisk bombe, må det antages, at der kan straffes for forsøg, indtil firmaet har gjort brug af programmet. Mere nærliggende kan det dog være at statuere fuldbyrdet bedrageri ved levering af en vare med en så alvorlig defekt.

4.4. Data vil også. kunne forvanskes, medens de er under transmission, f.eks. mellem to datamaskiner eller mellem en datamaskine og en terminal. Bortset fra tilfælde, hvor der sker ødelæggelse eller beskadigelse af et ledningsnet o.lign., fo-

rekommer det tvivlsomt, om indgrebet i en kommunikation har en sådan forbindelse med en fysisk genstand, at forholdet kan anses for omfattet af § 291. Det kan vel ikke udelukkes, at domstolene i nogle tilfælde ville anlægge en vid forståelse af § 291, men mest nærliggende er det formentlig at anvende § 263 om lukkede meddelelser m.v.

Kapitel 5

Almenfarlige og almenskadelige forbrydelser

5.1. I forbindelse med § 291 om tingsbeskadigelse og -ødelæggelse skal først nævnes, at der i straffelovens kapitel 20 om "almenfarlige forbrydelser" findes bestemmelser i §§ 180 og 181 om forsætlig ildspåsættelse. Bortset fra afgrænsningen over for § 291 med hensyn til ildspåsættelse på mindre løsøregenstande volder anvendelsen af §§ 180 og 181 ingen problemer med hensyn til ildspåsættelse på dataanlæg eller dele heraf. I praksis vil sådant forhold formentlig oftest være forbundet med ildspåsættelse på fast ejendom. Strafmaksimum for den ukvalificerede forsætlige brandstiftelse i § 181 er fængsel i 6 år, under særligt skærpende omstændigheder fængsel i 10 år.

Med fængsel indtil 12 år straffes efter § 183 bl.a. den, der forvolder sprængning til skade for andres person eller formue. De øvrige i § 183 nævnte forhold - "spredning af skadevoldende luftarter, oversvømmelse, skibbrud, jernbane- eller anden transportulykke" - er formentlig uden praktisk betydning med henblik på dataanlæg. Teoretisk set kan transportulykker dog forvoldes gennem forkerte instruktioner via et dataanlæg. Noget tilsvarende gælder flykapring efter § 183 a og de i § 184 beskrevne handlinger, der består i, at nogen "forstyrrer sikkerheden for jernbaners, fartøjers, motorkøretøjers eller lignende transportmidlers drift eller sikkerhed for færdsel på offentlige færdselsveje".

Der er næppe grund til at overveje ændringer i disse bestemmelser med henblik på datakriminalitet.

5.2. I straffelovens kapitel 21 om "forskellige almenskadelige handlinger" findes i § 193 en bestemmelse, der giver anledning til at overveje en ændring med henblik på dataforhold. § 193 har følgende ordlyd:

"Den, som på retsstridig måde fremkalder omfattende forstyr-

> reise i driften af almindelige samfærdselsmidler, offentlig postbesørgelse, almindeligt benyttede telegraf- eller telefonanlæg eller anlæg, der tjener til almindelig forsyning med vand, gas, elektrisk strøm eller varme, straffes med hæfte eller med fængsel indtil 3 år eller under formildende omstændigheder med bøde.
>
> Stk. 2. Begås forbrydelsen uagtsomt, er straffen bøde eller hæfte."

Bestemmelsen indeholder ingen begrænsninger med hensyn til de anvendte midler. Der er derfor ingen tvivl om, at "omfattende forstyrrelse" på de i § 193 nævnte områder kan forvoldes ved et uretmæssigt indgreb i datastyring af bl.a. jernbanedrift eller luftfart eller i de af dataanlæg benyttede transmissionsledninger m.v., for så vidt disse kan betegnes som "almindeligt benyttede telegraf- eller telefonanlæg". Der kan på den anden side tænkes omfattende forstyrrelser, der ikke kan henføres under de i § 193 opregnede områder, og hvis strafbarhed derfor i denne sammenhæng kan bero på en eventuel analogi af § 193. Som eksempler kan nævnes angreb, der helt lammer eller i betydeligt omfang forstyrrer registrering, behandling og transmission af data inden for værdipapircentralen, kildeskattedirektoratet, politiets motorregister el. lign. Indenfor den private sektor er der bl.a. grund til at være opmærksom på de tilsvarende forstyrrelser, der kan være følgen af et uretmæssigt indgreb i den centrale elektroniske databehandling hos banker og sparekasser, realkreditinstitutter etc.

Strafmaksimum efter § 193 er fængsel i 3 år. Dette maksimum er efter straffelovrådets opfattelse for lavt under hensyn til de meget betydelige skadevirkninger, som de i § 193 beskrevne handlinger kan medføre. De fleste strafbare forhold vil formentlig tillige være omfattet af § 291, hvor straffen for "hærværk af betydeligt omfang" kan blive fængsel indtil 4 år. Men en overtrædelse af § 193 kan tænkes, uden at der foreligger hærværk af betydeligt omfang.

Straffelovrådet foreslår, at § 193 affattes således:

> I § 193, stk. 1, ændres ordene "almindeligt benyttede telegraf- eller telefonanlæg" til "telegraf- eller telefonanlæg, radio- eller fjernsynsanlæg, databehandlingsanlæg (eller

anlæg der tjener ...)".

I stedet for "fængsel indtil 3 år" skrives "fængsel indtil 6 år".

Ved ændringen indføjes radio- og fjernsynsanlæg og databehandlingsanlæg blandt de anlæg, i forhold til hvilke det er strafbart at fremkalde omfattende driftsforstyrrelse. Selv om forslaget om at indføje radio- og fjernsynsanlæg falder uden for rådets kommissorium, har rådet fundet det naturligt at benytte lejligheden til at foreslå angreb mod disse anlæg kriminaliseret, hvis der herved fremkaldes omfattende forstyrrelse af driften. Rådet har i den forbindelse lagt vægt på, at radio- og fjernsynsanlæg har en betydelig lighed med flere af de anlæg, der i dag omfattes af bestemmelsen, og at de siden bestemmelsen blev udformet i 1930 har fået en stadig stigende samfundsmæssig betydning som kommunikationsmidlet:.

Rådet har overvejet, om man i § 193 burde begrænse kredsen af de radio- og fjernsynsanlæg og databehandlingsanlæg, som er beskyttet efter bestemmelsen. Man er nået til den konklusion, at bestemmelsens rækkevidde i tilstrækkeligt omfang begrænses ved kravet om, at driftsforstyrelsen skal være "omfattende".

Rådet har i konsekvens heraf fundet det forsvarligt og hensigtsmæssigt at foreslå udtrykket "almindeligt benyttede" telegraf- og telefonanlæg ophævet, idet der ellers ville kunne opstå tvivl om, hvorvidt dette udtryk knytter sig til de følgende led. Rådet tilsigter ikke herved nogen realitetsændring af bestemmelsens anvendelsesområde.

Som anført foran vil angreb mod databehandlingsanlæg og andre af de i bestemmmelsen nævnte anlæg kunne medføre så omfattende forstyrrelser af væsentlige samfundsfunktioner, at en strafferamme på fængsel i 3 år må forekomme alt for lav. Rådet foreslår strafferammens maksimum forhøjet til fængsel i 6 år. Der tilsigtes ikke herved nogen almindelig forhøjelse af strafudmålingsniveauet efter bestemmelsen, men der skabes ved ændringen mulighed for at anvende straf af fængsel op til 6 år, når der konkret foreligger særligt skærpende omstændigheder,

f.eks. meget omfattende eller indgribende driftsforstyrrelser af de pågældende anlæg.

Kapitel 6

Bedrageri

6.1. Straffelovens § 279 om bedrageri lyder således:

> "For bedrageri straffes den, som, for derigennem at skaffe sig eller andre uberettiget vinding, ved retsstridig at fremkalde, bestyrke eller udnytte en vildfarelse bestemmer en anden til en handling eller undladelse, hvorved der påføres denne eller nogen, for hvem handlingen eller undladelsen bliver afgørende, et formuetab".

Til bedrageriet hører, at en person skal have været i en vildfarelse, som gerningsmanden har fremkaldt, bestyrket eller udnyttet, og at den pågældende under indflydelse af denne vildfarelse skal have foretaget en disposition, der ellers ikke ville være blevet foretaget. Hertil kommer, at gerningsmanden skal have handlet med berigelsesforsæt, og at der ved hans handlemåde skal være påført en anden et formuetab eller (som bestemmelsen opfattes i retspraksis) en væsentlig risiko for formuetab.

Beslægtet med § 279 er § 300 a, der blev indføjet i straffeloven i 1975 som resultat af den dengang førte debat om en udvidet kriminalisering af skadelige økonomiske handlinger ("bagmandskriminalitet"). Bestemmelsen har fundet meget ringe anvendelse i retspraksis. Den adskiller sig fra § 279 bl.a. ved at kriminalisere det forhold, at en person ved grov uagtsomhed bevirker, at en anden, der befinder sig i en vildfarelse, bestemmes til en tabgivende disposition. Straffelovrådet har ikke fundet anledning til nærmere at drøfte det mulige anvendelsesområde for § 300 a i dataforhold, og der stilles ikke forslag om lovændringer, der berører § 300 a.

Der findes i straffelovens kap. 29 enkelte andre bestemmelser om bedragerilignende formuekrænkelser, bl.a. i §§ 296-298. Heller ikke disse bestemmelser er nærmere omtalt i det følgende. Bestemmelserne handler navnlig om forskellige former for

fremsættelse af urigtige oplysninger om virksomheders økonomiske stilling, og det har ikke større betydning at undersøge, på hvilke måder databehandling kan være et middel til sådanne oplysningers tilvejebringelse eller udbredelse.

Forbrydelsen dokumentfalsk, der kan rumme et bedrageri, men ikke behøver at gøre det, omtales særskilt i kapitel 8.

6.2. For så vidt angår dataforhold vil § 279 om bedrageri omfatte tilfælde, hvor en person uretmæssigt tilføjer, ændrer eller sletter dataoplysninger under omstændigheder, hvor en anden person derefter opfatter de urigtige dataoplysninger og på dette grundlag foretager en handling (i sjældnere tilfælde: undlader at foretage sig noget, f.eks. at debitere eller kreditere en person et beløb). I sådanne tilfælde er der gennem dataanlæggets udvisende på en skærm eller en udskrift af dataoplysninger fremkaldt en vildfarelse og en handling på en måde, der ganske svarer til, at gerningsmanden svigagtigt fremsender eller anbringer urigtige regninger, fakturaer, varerekvisitioner o.lign. eller mundtligt giver urigtige oplysninger.

Ligesom hvor andre midler er benyttet, vil den typiske gerningsmåde i dataforhold være den, der består i, at gerningsmanden har fremkaldt vildfarelsen. Der er næppe grund til at gå i enkeltheder med hensyn til tilfælde, hvor han uden at fremkalde en vildfarelse har bestyrket eller udnyttet en sådan.

Det her anførte gælder i princippet, hvad enten vildfarelse og handling påregnes at følge hurtigt efter ændringen af dataoplysninger (f.eks. ved den daglige aflæsning af skyldige udbetalinger), eller vildledelse af en anden person først bliver aktuel efter nogen tids forløb (f.eks. i forbindelse med årsopgørelser). Fuldbyrdelsen af bedrageri indtræder først, når nogen er blevet vildledt til at foretage en disposition med økonomiske konsekvenser. Indtil da vil selve ændringen af dataoplysninger udgøre et forsøg på bedrageri, når det uretmæssige indgreb i dataoplysninger er foretaget med forsæt til, at nogen senere skal handle i tillid til dataanlæggets udvisende.

En ret almindelig form for datakriminalitet består i, at en person, der betjener et dataanlæg eller kan give instruktioner om dettes betjening, opretter fiktive konti for ikke-eksisterende personer (leverandører, forsikringstagere, lønmodtagere, pensionister m.v.) og opnår udbetaling via konti, som han selv eller andre råder over, af de beløb, som foregives at tilkomme de opdigtede personer. De nærmere anvendte fremgangsmåder kan variere meget, bl.a. beroende på hvad det er nødvendigt og muligt for den pågældende at gennemføre af mellemliggende transaktioner for at undgå kontrol. I relation til bedrageriforbrydelsen må det også her fremhæves, at den pågældendes handlemåde skal have fremkaldt, bestyrket eller udnyttet en vildfarelse hos andre og dermed fremkaldt en disposition. Det må antages, at disse krav normalt er opfyldt, når overordnede i virksomheden er blevet motiverede til ikke at foretage sig noget, fordi de er gået ud fra, at opgjorte beløb, foreliggende navnelister etc. svarer til reelle forpligtelser. Kravet om en vildfarelse og en disposition giver imidlertid anledning til nogle problemer, der skal omtales nedenfor under kapitel 6.3.

Foran er omtalt de misbrug, der umiddelbart består i et uretmæssigt indgreb i et dataanlægs oplysninger (herunder f.eks. tilføjelse af fiktive data). Forud for dette stadium kan bedrageri eller forsøg herpå bestå i afgivelse af urigtige oplysninger, f.eks. til et firma eller en offentlig myndighed, når modtageren derefter lader oplysningerne indgå i et dataanlæg. Dette er ikke et forhold, der er specielt for datakriminalitet. Det er uden betydning for den strafferetlige bedømmelse, om afgiveren af urigtige oplysninger har regnet med maskinmæssig eller manuel behandling af oplysningerne, når han dog har haft forsæt til at fremkalde en vildfarelse og en heraf følgende disposition.

Man kan spørge, om det kan være bedrageri eller forsøg herpå at skaffe sig adgang til et dataanlægs oplysninger på svigagtig måde. Dette spørgsmål må formentlig besvares bekræftende, for så vidt angår tilfælde, hvor gerningsmanden, f.eks. ved urigtige oplysninger om sin stilling eller bemyndigelse, fremkal-

der en vildfarelse hos den person, der råder over dataanlægget. Tilfældet er næppe af stor praktisk betydning. En forudsætning for strafansvar efter § 279 vil det som i andre tilfælde være, at den pågældende har handlet med forsæt til at skaffe sig selv eller andre uberettiget vinding og har forvoldt et formuetab eller en væsentlig risiko herfor. Dette vil ikke være tilfældet, hvis han har opnået adgang til dataanlægget for at skaffe sig personoplysninger o.lign., der ikke bringer ham økonomisk vinding og andre et tilsvarende tab. - Hvis den uberettigede person på den anden side skaffer sig adgang til et dataanlæg uden at vildlede en anden person, f.eks. ved at "vildlede" dataanlægget om sin bemyndigelse til at bruge en vis kode, vil bedrageri være udelukket af den nedenfor nævnte grund, at der ikke foreligger en menneskelig vildfarelse og en deraf følgende disposition.

6.3. Udenfor § 279 om bedrageri falder alle tilfælde, hvor en forretningsmæssig arbejdsgang er i den grad automatiseret, at der ikke i forløbet optræder en enkeltperson, der handler på grundlag af de urigtige dataoplysninger. Herhen hører bl.a. tilfælde, hvor beløb krediteres eller debiteres en person (eller overføres fra en person til en anden) ved indtastning i et dataanlæg uden yderligere mellemkommende handlinger, der opfylder kravet om, at nogen er blevet vildledt til at gøre eller undlade noget. Tilsvarende kan nævnes tilfælde, hvor en person ved indgreb i dataregistrerede lageropgørelser i et toldoplæg eller i en lagerbygning, der tilhører flere personer eller firmaer, bevirker en forvanskning af oplysningerne om, hvem bestemte genstande tilhører.

I klasse med de her nævnte tilfælde må formentlig sættes tilfælde, hvor der ganske vist er en person, der handler i tillid til oplysninger fra et dataanlæg, men hvor den pågældende - typisk som følge af sin underordnede stilling - ikke kan siges at udøve nogen reel prøvelse af oplysningernes rigtighed. Dette kan f.eks. understreges af en almindelig instruks til ham om, at han skal udbetale penge eller udlevere varer i overensstemmelse med de oplysninger, der fremkommer på en terminalskærm eller en udskrift af dataoplysninger. Grænsen for anven-

delsen af § 279 i tilfælde af den nævnte art kan næppe angives helt sikkert; den kan bl.a. bero på den pågældendes stilling, f.eks. om den, der aflæser dataoplysninger, er lagerforvalter eller chauffør, hovedkasserer eller assistent på kassererkontoret.

6.4. Også i andre lande har man fremhævet, at straffelovenes krav om en handlingsbestemmende vildledelse udelukker domfældelse for bedrageri i visse dataforhold.

I den norske straffelovs § 270 hedder det, at gerningsmanden "ved å framkalle, styrke eller utnytte en villfarelse rettstridig forleder noen til en handling, som volder tap eller fare for tap for ham eller den han handler for".

Den tilsvarende formulering i den svenske brottsbalk 9:1 siger, at gerningsmanden "medelst vilseledande förmår någon till handling eller underlåtenhet, som innebär vinning för gärningsmannen och skada för den vilseledde eller någon i vars ställe denne är". I den svenske betænkning "Förmögenhetsbrott" (SOU 1983:50) antages det, at der ved visse uretmæssige indgreb i dataoplysninger, f.eks. kreditering hos en uberettiget person, er sket en formueoverførelse til denne person, og det findes utilfredsstillende, at bedrageribestemmelsen i sådanne tilfælde er uanvendelig, fordi dette resultat ikke er opnået ved vildledelse af en person til at foretage en disposition. I sit lovudkast foreslår förmögenhetsbrottsutredningen, at der i BrB 9:1, 1. stk., nr. 2, optages en ny bestemmelse, efter hvilken bedrageri bl.a. omfatter den, som

> "genom att lämna oriktig eller ofullständig uppgift, företa ändring i datorprogramm eller i upptagning för automatisk databehandling eller på annat sätt olovligen påverkar resultatet av automatisk databehandling så att det innebär ekonomisk skada".

I bemærkningerne om den foreslåede bestemmelse hedder det bl.a.:

> "I andra punkten kriminaliseras "datorbedrageri".
>
> Den som genom at förse en dator med oriktiga eller vilseledande uppgifter förorsaker att den gör en disposition

som innebär ekonomisk skada för annan, exempelvis oriktigt tillgodoför gärningsmannen visst belopp, gör sig enligt gällande ordning inte skyldig till bedrägeri, om inte dispositionen ytterst beror på att en fysisk person blivit vilseledd. Huruvida så är fallet beror ofta på tillfälligheter.

För att bedrägeri skall föreligga enligt denna punkt krävs inte att någon fysisk person vilseleds. Brottet består i att någen olovligen påverkar resultatet av automatisk databehandling så att det innebär ekonomisk skada.

Gärningsmannens handling kan bestå i att han avger en oriktig eller ofullständig uppgift som skall bli föremål för databehandling. Uppgiften kan lämnas direkt till datorn på ett maskinläsbart sätt. Den kan också lämnas till en person, som eventuellt överför den till ett maskinläsbart medium före den maskinella databehandlingen. I sistnämnda fall kan ibland, beroende på mottagarens beslutsfunktion, även rekvisiten för bedrägeri enligt punkten 1 vara uppfyllda."

I et foreløbigt finsk udkast til affattelse af en revideret bestemmelse om bedrageri findes følgende:

"För bedrägeri döms också den som i sådant syfte som nämns i 1 mom. genom att mata in felaktiga uppgifter i dator eller på annat sätt ingripa i databehandling förvanskar slutresultatet av databehandlingen eller utnyttjar fel som han observerat i databehandling och därigenom åsamkar annan ekonomisk skada".

6.5. Straffelovrådet foreslår, at der som § 279 a indføjes en ny bestemmelse om databedrageri:

"§ 279 a. 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".

Som anført ovenfor vil en række bedragerilignende forhold vedrørende dataforhold falde uden for bestemmelsen i § 279, hvis der ikke i forløbet optræder en person, som er blevet vildledt til at gøre eller undlade noget. De fleste af disse forhold må i dag - når de er begået af ansatte - antages at være omfattet af straffelovens § 278, stk. 1, nr. 3, om pengeunderslæb eller af § 280 om mandatsvig, jfr. nedenfor i kapitel 7. Ingen af disse bestemmelser er udformet med henblik på at ram-

me datakriminalitet, og der kan derfor tænkes tilfælde, hvor det vil være mindre naturligt at henføre disse nye kriminalitetsformer under bestemmelserne om pengeunderslæb eller mandatsvig.

Straffelovrådet har navnlig på den baggrund fundet det hensigtsmæssigt i lighed med, hvad der påtænkes i de øvrige nordiske lande, at samle disse bedragerilignende forhold i en ny bestemmelse om databedrageri.

Om enkeltheder vedrørende bestemmelsen og om dennes strafferamme henvises til de specielle bemærkninger til lovudkastet.

Kapitel 7

Pengeunderslæb og mandatsvig

7.1. Ligesom andre berigelsesforbrydelser forudsætter pengeunderslæb og mandatsvig, at gerningsmanden handler med forsæt til "at skaffe sig eller andre uberettiget vinding". Fælles for de to forbrydelser er endvidere, at gerningsmanden i kraft af sin stilling, en aftale el. lign. befinder sig i en situation, hvor han har en faktisk mulighed for at disponere med den virkning, at en anden lider et tab. De to forbrydelser grænser op til hinanden og bør derfor omtales i sammenhæng. Mandatsvig er i § 280 beskrevet således, at bestemmelsen sprogligt omfatter tilfælde, der er pengeunderslæb efter § 278, stk. 1, nr. 3. I sådanne tilfælde skal bestemmelsen om pengeunderslæb foretrækkes. Dette fremgår udtrykkeligt af § 280. I dataforhold som i andre økonomiske forhold må man derfor se på, hvad der kan være pengeunderslæb, før det får selvstændig betydning at afgrænse mandatsvig.

7.2. Pengeunderslæb består i, at en person "uretmæssig forbruger ham betroede penge". Det tilføjes, at strafansvaret . også omfatter den, der ikke var forpligtet til at holde de betroede penge adskilt fra sin egen formue. Denne tilføjelse får dog næppe nogen større betydning i dataforhold, hvor der praktisk talt altid vil være tale om penge, der er adskilte fra gerningsmandens person.

Til pengeunderslæb hører således, at penge kan siges at være "betroet" en person, og dernæst at den pågældende uretmæssigt forbruger sådanne penge. Det må herved fremhæves, at strafansvaret ikke kan pålægges en virksomhed som sådan (f.eks. hvor penge er betroet en bank), men kun enkeltpersoner som har et særligt ansvar for beholdningens tilstedeværelse og en faktisk mulighed for at råde over den, således at deres dispositioner kan siges at være et forbrug af penge.

Indenfor de velkendte kriminalitetsformer drejer det sig om

forhold begået af kasserere, inkassatorer, forretningsbestyrere, indkøbskommissionærer o.l., der har andres'penge eller checks mellem hænderne og bruger dem. Sådanne forhold kan også forekomme på områder, hvor databehandling bruges, f.eks. hvor en ansat modtager andres indbetalinger, tilvender sig pengene og forvansker eller fjerner bilag, hvorefter han eller andre foretager en urigtig databehandling eller simpelthen undlader dataregisterering. Dette kan strafferetligt bedømmes på forskellige måder, beroende på den nærmere fremgangsmåde. En af mulighederne er at statuere pengeunderslæb, men der kan også være tale om tyveri, såfremt pengene må siges at være i firmaets besiddelse, medens gerningsmandens fysiske ihændehavelse af pengene ikke udgør en sådan selvstændig besiddelse hos ham, som er forudsætningen for at statuere underslæb. Under alle omstændigheder har datateknikken ikke i sådanne tilfælde været midlet til at begå en berigelsesforbrydelse, men er brugt til at dække over den.

Indenfor traditionel berigelseskriminalitet er det imidlertid også velkendt, at en person kan begå pengeunderslæb uden direkte at beskæftige sig med og anvende pengesedler, f.eks. ved at udskrive uvedkommende checks på en forenings checkkonto eller ved at give en underordnet ansat ordre til at foretage udbetalinger fra en kasse eller konto, som gernignsmanden er ansvarlig for. Det er formentlig tilsvarende former for mere indirekte omgang med penge, der vil være karakteristiske for dataforhold, idet penge gennem instruktioner til et dataanlæg flyttes fra deres lovlige beskyttede tilstand til personer, virksomheder eller konti på en sådan måde, at de overførte penge er forbrugt. Det skal for en ordens skyld fremhæves, at ordet "forbruger" ikke sigter til det, som gerningsmanden foretager sig med pengene (indkøb, betaling af gæld o.l.), men til det forhold, at pengene er fjernet fra det betroede beløb.

Ansvar for pengeunderslæb vil imidlertid altid være betinget af, at der forud for en sådan transaktion forelå "penge" (kontant, i checks eller på en konto), og at disse penge var "betroet" gerningsmanden. Jo mere en virksomheds økonomi og dis-

positioner er baseret på et system af databundne konti og overførsler uden rede penge, desto vanskeligere kan det være at afgøre, hvorvidt der forelå penge, og i bekræftende fald hvem disse penge var betroet. Den omstændighed, at en bank eller anden virksomhed har kasser med rede penge, er fra et praktisk synspunkt af mindre interesse, idet bedømmelsen af datakriminalitet formentlig hyppigst vil være aktuel i tilfælde, hvor det uretmæssige indgreb ikke er gået ud over den kontante beholdning, men har ramt et dataregistreret aktiv. Men naturligvis må man være opmærksom på tilfælde, hvor uretmæssig databehandling har resulteret i ordrer om udbetaling fra en kontant beholdning, og i så fald vil det være klart, hvilke penge indgrebet er gået ud over.

Der kan ikke begås pengeunderslæb af en udefra kommende, uvedkommende person, der skaffer sig mulighed for at foretage pengeoverførsler gennem et dataanlæg. Men det er heller ikke tilfældet med hensyn til en stor del af de i virksomheden ansatte. Det er ikke enhver ansat, der bliver delagtig i betroelsen, blot fordi pengene kan siges at være betroet virksomheden. Der foreligger kun "betroelse" - og dermed grundlag for at statuere pengeunderslæb - hos sådanne ansatte, hvis job det er at være ansvarlige for pengenes tilstedeværelse, og som har en vis adgang til at disponere over dem. Grænserne for en sådan personkreds udviskes imidlertid noget i virksomheder, der som ovenfor nævnt i vid udstrækning er baseret på et system af registrerede oplysninger, konti m.v. og af overførsler gennem et datasytem. I sådanne virksomheder kan registreringer, dispositioner, sikkerhedsforanstaltninger m.v. bero på en kompliceret arbejdsdeling mellem mennesker og maskiner og for menneskers vedkommende mellem forskellige opgaver og stillingstyper, af hvilke ingen helt svarer til den klassiske "kasserer", det vil sige den, der sidder på pengekassen. Afhængigt af den nærmere organisationsform kan pengeunderslæb dog nok i almindelighed begås af direktører, underdirektører, kasserere, regnskabschefer m.v., men ikke af en bogholder, salgschef eller dataoperatør, der ikke har med virksomhedens beholdning af konti eller rede penge at gøre.

Som eksempler på domme, ved hvilke kasserere er fundet skyldige i pengeunderslæb, kan anføres følgende sager:

> Ved Brønderslev rets dom af 7. september 1982 blev en kasserer i en sparekasse straffet for overtrædelse af straffelovens § 278 om underslæb ved gennem ca. 7 måneder at have tilegnet sig 240.000 kr. under følgende omstændigheder: T var kasserer i sparekassen (on-line system) og udfærdigede ca. 125 urigtige kassebilag, hvorved beløb overførtes til en kassemellemregningskonto (overførsler fra andre afdelinger el. kasser). T hævede derefter beløb fra kassen eller overførte beløb til sin egen konto og dækkede ved nye posteringer på kassemellemregningskontoen (hvor uafklarede poster måtte stå i op til 8 dage).
>
> Ved Hillerød kriminalrets dom af 11. august 1983 blev en kasserer i en sparekasse straffet efter straffelovens § 278 om underslæb ved gennem ca. 2 år at have tilegnet sig ca. 280.000 kr. fra konti i sparekassen. T hævede primært på konti, der sjældent blev brugt, men bogførte hævningerne korrekt i sparekassen. Kontrolmateriale fra Sparekassernes Data Center gik til en overordnet, men når T vidste, der kunne komme afslørende materiale, mødte hun tidligere og fjernede det. T, der tilegnede sig pengene for at klare familiens økonomi meldte sig selv, da hun blev klar over, at man undersøgte en af hendes hævninger, som kunden nægtede at have kendskab til.

7.3. Bestemmelsen om mandatsvig kan anvendes i tilfælde, hvor en person i et ansættelsesforhold m.v. forvolder vinding og tab, uden at forholdet kan betegnes som forbrug af betroede penge. Strafferammerne for underslæb og mandatsvig er de samme, jfr. § 285-287. Dette gælder også den særlige skærpelsesregel i § 154 om forbrydelser begået i offentlig tjeneste eller hverv.

§ 280 om mandatsvig har følgende ordlyd:

> "For mandatsvig straffes, for så vidt forholdet ikke falder ind under §§ 276-279, den, som for derigennem at skaffe sig eller andre uberettiget vinding påfører en anden formuetab
> 1) ved misbrug af en for ham skabt adgang til at handle med retsvirkning for denne eller
> 2) ved i et formueanliggende, som det påhviler ham at varetage for den anden, at handle mod dennes tarv."

Bestemmelsen i nr. 2 handler om tilfælde, hvor nogen i medfør af sin ansættelse eller en særlig aftale har en pligt til at varetage et formueanliggende for en anden. Bestemmelsen i nr.

1 rækker videre, idet den kun forudsætter, at der faktisk består en adgang til at handle med retsvirkning for en anden, ikke nødvendigvis en pligt til at foretage sig noget for den anden. Hvis man antager, at der i alle pligtforhold også nødvendigvis må foreligge en adgang til at handle med retsvirkning for en anden, kan bestemmelsen i nr. 2 anses for helt eller i det væsentlige overflødig.

7.4. Området for anvendelse af § 280 om mandatsvig beror navnlig på fortolkning af ordene "(misbrug af) en for ham skabt adgang til at handle med retsvirkning for (en anden)". De klareste eksempler herpå foreligger med hensyn til direktører, forretningsbestyrere, adfdelingsledere og andre personer, der i kraft af en overordnet stilling er legitimerede til at træffe dispositioner med virkning for virksomheden. Der foreligger mandatsvig, hvis en sådan person enten selv eller gennem en underordnet medarbejder, som er blevet instrueret derom, foretager dispositioner, ved hvilke han forsætligt bringer sig selv eller andre uberettiget vinding og påfører virksomheden formuetab eller væsentlig risiko for et sådant. Dette gælder også, når forholdet realiseres gennem et dataanlæg.

I dansk retspraksis har § 280 imidlertid også fundet anvendelse i en række tilfælde, hvor underordnede ansatte med adgang til at benytte EDB-materiel har misbrugt denne adgang, f.eks. ved benyttelse af konti for. fratrådte medarbejdere eller opdigtede personer, urigtig hulning af datamateriale vedrørende arbejdstimer, opsagte forsikringspolicer etc. Anvendelsen af datateknik har øget mulighederne for, at underordnede medarbejdere, som ikke selv er berettigede til at træffe beslutninger om pengeoverførsler eller andre forretningsmæssige dispositioner, misbruger adgangen til at indkode oplysninger med forsæt til berigelse. Kravet om "en for ham skabt adgang o.s.v." kan være opfyldt ved den pågældendes stilling i virksomheden, og hans adgang til at handle kan f.eks. understreges af, at han password er hans legitimation til at betjene anlægget og hans faktiske adgang til at bestemme de transaktioner, der kommer ud af databehandling.

Den norske straffelovs § 275 om forbrydelsen "utroskap", der svarer til mandatsvig, har en snævere afgrænsning af kredsen af gerningsmænd, idet det i denne bestemmelse hedder, at en person "forsømmer en annens anliggender som han styrer eller har tilsyn med". Tilsvarende kan nævnes, at den svenske brottsbalk 10:5 om forbrydelsen "trolöshet mod huvudman" beskriver det strafbare forhold således, at en person "pågrund av förtroendeställning ... fått att för annan sköta ekonomisk angelägenhet eller öva tillsyn å skötseln därav".

Fra dansk retspraksis vedrørende mandatsvig begået af underordnede medarbejdere skal refereres følgende domme:

Ved Østre landsrets dom af 22. maj 1980 blev tiltalte, som var vikar i et forsikringsselskab, idømt 1 år og 3 måneders fængsel for overtrædelse af straffelovens § 276, § 171, § 280, jfr. til dels § 21, ved - for så vidt angår mandatsvigsforholdene - at have udfærdiget urigtige hulleskemaer (med en fortrykt afgangsdato for forsikringer m.v.), hvilket udløste checks forsynet med underskrift i faksimile. Arbejdsprocessen var følgende: Ved forsikriingsopsigelse hentedes policen i arkivet, og T indtastede policen og udfyldte et skema med policens nummer, et kontrolnummer (fremgik af EDB-udskriften), afgangsdatoen og underskrift. Skemaet blev ikke kontrolleret af T's foresatte, men lagt direkte til EDB-afdelingen. Den følgende dag fik T en check (EDB-udskrevet) svarende til ristornoen. Normalt gik checken gennem hans foresatte, men hvis han skrev "check til GP" på hulleskemaet, kom checken direkte til ham. T arkiverede selv både policeudskrift og hulleinstruks. Fejllister gik til T's foresatte, der overlod dem til T uden særskilt gennemgang. T var ikke EDB-kyndig og lavede adskillige fejl. En af dem førte til hans opdagelse, og T tilstod derefter.

Ved Gentofte rets dom af 28. juni 1979 blev tiltalte, der var assistent i et entreprenørfirmas lønningskontor uden bemyndigelse til at disponere over penge idømt 3 års fængsel for overtrædelse af straffelovens § 279 og § 280 ved gennem 2 1/2 måned at have tilegnet sig ca. 400.000 kr. under følgende omstændigheder: T modtog telexer fra en af firmaets arbejdspladser i udlandet vedrørende arbejdstimer m.v. og udfærdigede herefter de nødvendige hullebilag, ligesom han udfærdigede hullebilag vedrørende ændring af kontonumre o.l. T oprettede en række konti og ændrede ved hullebilag nogle af lønmodtagernes konti til egne konti. I flere af forholdene forhøjede T timetallet, mens han i andre blot fik overført den faktiske løn til egen konti. I de tidligste forhold benyttede T afgåede eller syge lønmodtagere. De øvrige forhold måtte nødvendigvis blive opdaget, når de pågældende ikke fik deres løn.

(Bedrageriforholdene adskilte sig kun fra de øvrige ved, at T skulle have en bemyndiget person til at skrive under på forskudsbilag).

Ved Københavns byrets dom af 8. marts 1983 blev en fuldmægtig ansat i Københavns kommunes lønningskontor dømt 3 år og 6 måneders fængsel efter straffelovens § 280, jfr. § 154, og § 171 ved gennem 2 1/2 år at have tilegnet sig ca. 1,2 mill kr. under følgende omstændigheder: T havde været tjenestemandsansat i Københavns kommune siden maj 1971. Fra 1. februar 1979 blev han souschef på kontoret for 14 dages løn og havde bl.a. forbindelse med en EDB-central og et antal hospitaler. Ca. juli 1980 indkodede han en fiktiv lønmodtager (F), men med T's cpr.nr. og adresse. Derefter overførte han løbende penge. T tilbageholdt opgørelserne vedrørende F, der skulle have været udsendt til F's "arbejdsted". På grund af et krav om restskat på ca. 100.000 kr. måtte han ændre F's trækprocent. En medarbejder studsede over ændringen, og T, der derefter forventede opdagelse, orienterede sin overordnede.

Ved Københavns byrets dom af 20. oktober 1983 blev en terminaloperatør på et lønningskontor idømt 1 år og 3 måneders betinget fængsel for efter straffelovens § 280 ved gennem ca. 9 mdr. via EDB at have overført ca. 350.000 kr. til egne konti. T indtastede løn til løsansatte og overførte derefter beløbene til egne konti. Han destruerede normalt testlister, men blev opdaget ved et tilfælde via en testliste, da han var fraværende. Retten betragtede det som en formildende omstændighed, at der - efter det oplyste - ikke blev foretaget egentlig kontrol med eller revisions af T's arbejde med lønanvisning.

7.5. Det er straffelovrådets konklusion, at der ikke er behov for at foreslå nogen ændring i straffelovens bestemmelser om pengeunderslæb og mandatsvig.

For så vidt angår virksomhedsledere og visse andre ansatte i særlig betroede stillinger kan der undertiden være tvivl om, hvorvidt et misbrug af stillingen, foretaget med forsæt til at bevirke uberettiget vinding, bør bedømmes som underslæb med hensyn til penge eller som mandatsvig. Tvivlsspørgsmål af den art kendes også fra andre situationer end dataforhold. andatsvigsbestemmelsen i § 280 er subsidiær i forhold til § 278 om underslæb, men der er på den anden side ingen betænkeligheder ved at foretrække § 280 i tilfælde, hvor der savnes sikkert grundlag for at fastslå, at der er sket et uretmæssigt forbrug af betroede penge.

Med henblik på bedømmelsen af datakriminalitet kan det konstateres, at der ikke i retspraksis har hersket tvivl om, at misbrug foretaget af underordnede ansatte kan henføres under § 280 om mandatsvig. Imidlertid vil en ny bestemmelse om databedrageri (jfr. foran i kapitel 6.5) formentlig bevirke, at denne bestemmelse finder anvendelse i de fleste af de tilfælde, der nu bedømmes som mandatsvig.

Et spørgsmål om forholdet mellem § 280 om mandatsvig og markedsføringslovens § 9 omtales nedenfor i kapitel 9.

Kapitel 8

BevisforbrydeIser

8.1. I det følgende omtales først spørgsmålet om, hvorvidt der ved tilføjelse, ændring eller slettelse af dataoplysninger kan begås et forhold, der er strafbart som dokumentfalsk.

Et dokument defineres i § 171, stk. 2, som "en skriftlig med betegnelse af udstederen forsynet tilkendegivelse, der enten fremtræder som bestemt til at tjene som bevis eller bliver benyttet som bevis for en rettighed, en forpligtelse eller en befrielse for en sådan".

Efter stk. 3 er dokumentet falsk, når det "ikke hidrører fra den angivne udsteder" (det eftergjorte dokument) eller "der er givet det et indhold, som ikke hidrører fra denne" (det forfalskede dokument).

Dokumentfalsk fuldbyrdes efter stk. 1 ved brug af et falsk dokument til at skuffe i retsforhold.

Efter straffelovrådets opfattelse kan det vanskelig tænkes, at en tilføjelse, ændring eller slettelse af dataoplysninger, foretaget af en person der ikke lovligt råder over dataanlægget, opfylder betingelserne for at anses som dokumentfalsk. Efter definitionen i § 171, stk. 2, skal et dokument være en skriftlig tilkendegivelse, og datalagrede oplysninger kan ikke i sig selv udgør skrift. Derimod kan dataoplysninger være et middel til senere frembringelse af en skriftlig tilkendegivelse af bevismæssig betydning, f.eks. et eksamensbevis, en kontoudskrift eller en opgørelse over en beholdning af værdipapirer, og ændringer i data foretaget med forsæt til at fremkalde et sådant skriftligt produkt kan derfor være et forsøg på dokumentfalsk. Men dataoplysninger er ikke i sig selv skrift. I den norske straffelovs § 179 er "dokument" derimod defineret på en sådan måde, at skriftlighed ikke er en nød-

vendig bestanddel: "Ved dokument forståes i denne lov enhver gjenstand, som i skrift eller på annen måte inneholder et tilennegivende der er av betydning som bevis for en rett, en forpliktelse eller en befrielse fra en sådan eller fremtrer som bestemt til å tjene som bevis". Det antages i norsk ret, at dataoplysninger kan udgøre et dokument, idet de - skønt ikke i skrift så dog på anden måde - udgør en "gjenstand" (d.v.s. har en fysisk eksistens i dataanlægget) og indeholder et "tilkjennegivende" (d.v.s. er udtryk for en menneskelig tanke), ligesom de kan opfylde kravet om en bevisfunktion.

Også bortset fra skriftlighedskravet er der i dansk ret vanskeligheder ved at anse dataændringer som dokumentfalsk. Efter § 171, stk. 2, skal et dokument have en udstederbetegnelse. Dette krav har kun praktisk mening, når det forudsættes, at dokumentet er "udstedt", det vil sige har fået form af et stykke papir el.lign. Men datalagrede oplysninger er ikke "udstedt". De er indsamlede efter en vis metode og med visse kortsigtede eller langsigtede formål for øje, og til data er normalt ikke knyttet anden udstederbetegnelse end den, der ligger i, at dataanlægget har en retmæssig indehaver. Noget andet er - som allerede berørt - at der i udskrifter af dataoplysninger kan foreligge en skriftlig tekst med udstederbetegnelse.

Til fuldbyrdelse af dokumentfalsk kræves efter § 171, stk. 1, at nogen "gør brug af et falsk dokument til at skuffe i retsforhold". Det forekommer tvivlsomt, om dette krav er opfyldt på det tidspunkt, hvor en uberettiget person forfalsker dataoplysninger. Når dette sker, bliver de falske oplysninger indtil videre blot en del af dataanlæggets lagerbeholdning, og det vil i hvert fald i mange tilfælde føles kunstigt at sige, at gerningsmanden samtidig har gjort brug af oplysningerne til at skuffe i retsforhold. Men han kan naturligvis have forsæt til, at nogen senere gør brug af dem.

Man må formentlig konkludere, at § 171 om dokumentfalsk i hele sin opbygning og i en række enkeltheder er så klart bestemt af forudsætningen om brug af et udstedt skriftstykke, at bestemmelsen passer dårligt til forfalskning af datatilførsler

og heller ikke egner sig til at udvides til sådanne tilfælde. Man må bl.a. være opmærksom på, at § 171 allerede i sin nuværende form frembyder en række fortolkningsvanskeligheder, og at en udvidelse til dataforfalskning ville gøre gerningsbeskrivelsen og definitionerne endnu mere upræcise. Forbrydelsen ville også komme til at række ud over det, som man naturligt forstår ved "dokumentfalsk".

8.2. De øvrige bestemmelser i straffelovens kapitel 19, bortset fra § 178, angår bevismidler i form af dokumenter, bøger attester, mærker m.v. Ingen af bestemmelserne om sådanne genstande bør søges ændret med henblik på kriminalisering af handlinger, der vedrører dataregistrering.

Straffelovens § 178 omfatter "den, som for at skille nogen ved hans ret tilintetgør, bortskaffer eller helt eller delvis ubrugbargør et bevismiddel, der er tjenligt til at benyttes som sådant i et retsforhold". Bestemmelsen må antages at have et anvendelsesområde med henblik på dataforhold. Dataregistrerede oplysninger og de hertil knyttede programmer kan efter omstændighederne anses som et bevismiddel og være egnet til at benyttes som sådant i en retssag eller ved en administrativ afgørelse af et retsspørgsmål. Beskrivelsen af de strafbare handlinger - at tilintetgøre, at bortskaffe eller helt eller delvis at ubrugbargøre et bevismiddel - svarer i det væsentlige til den, der er benyttet i § 291 om ødelæggelse, beskadigelse eller bortskaffelse af ting (se herom ovenfor i kapitel 4), og vil også i denne forbindelse omfatte praktisk talt alle uberettigede indgreb i en dataregistrering. En vis begrænsning i bestemmelsens område følger af kravet om, at gerningsmanden skal handle "for at skille nogen ved hans ret". Dette betyder formentlig et krav om forsæt til, at en anden stilles ringere i sine muligheder for ved brug af det pågældende bevismiddel at gøre et retskrav gældende eller imødegå et ugrundet retskrav. § 178 er anvendelig både på den, der har bevismidlet i sin varetægt (f.eks. et dataregisters ejer), og på den udefra kommende, der foretager et uberettiget indgreb. Uden for § 178 falder formentlig tilfælde, hvor den for en dataregistrering ansvarlige fra starten foretager en urigtig datare-

gistrering og derfor ikke tilintetgør, bortskaffer eller ubrugbargør et allerede foreliggende bevismiddel. Men hvis bevismidlet havde en selvstændig eksistens, før databehandling skete (f.eks. i form af sedler, skemaer o.l), vil det kunne ødelægges eller bortskaffes i forbindelse med urigtig dataregistrering.

Straffelovrådet har overvejet, om man bør foreslå ordene "for at skille nogen ved hans ret" udeladt af § 178 for derved at opnå en vis udvidelse af bestemmelsens område. Mod denne ændring kan indvendes, at § 178 uden de citerede ord ville omfatte praktisk talt enhver genstand, som under visse omstændigheder kunne tænkes anvendt som bevismiddel. Ordene "for at skille nogen ved hans ret" rummer formentlig en nyttig begrænsning ved at stille et krav om en vis konkretisering af den retlige skadevirkning, som gerningsmanden skal have forsæt til.

Strafmaksimum i § 178 er fængsel i 2 år. Dette maksimum er højere end efter § 291, stk. 1 (1 år), men lavere end efter § 291, stk. 2, om "hærværk af betydeligt omfang" (4 år). Den selvstændige betydning af § 178 vil således være knyttet til tilfælde, hvor der ikke er grundlag for at anvende § 291, stk. 2. Hertil kommer tilfælde, hvor anvendelsen af § 291 er udelukket, f.eks. fordi handlingen har angået dataregistrering i et dataanlæg, der tilhører gerningsmanden selv.

Straffelovrådet har ikke fundet det nødvendigt at omtale de med § 178 beslægtede mere specielle bevisforbrydelser i straffelovens §§ 110, 125, stk. 1, nr. 2, og 164, stk. 2.

8.3. Straffelovrådet er kommet til den konklusion, at der ikke på nuværende tidspunkt er tilstrækkeligt grundlag for at foreslå en ny bestemmelse om dataindgreb o.l. betragtet som en bevisforbrydelse. Man lægger herved navnlig vægt på to forhold. For det første synes det behov for straffebestemmelser om datakriminalitet, der nu kendes i Danmark, i betydeligt omfang at være dækket af allerede gældende bestemmelser, suppleret med de regler, som straffelovrådet har stillet for-

slag om i det foregående. For det andet råder der en betydelig usikkerhed om, hvorledes en ny bestemmelse om en bevisforbrydelse burde udformes. Dette hænger atter sammen med, at der ikke i praksis har vist sig klare holdepunkter for at slutte noget om behovet for en selvstændig kriminalisering af dataindgreb betragtet som en bevisforbrydelse. Det er tænkeligt, at den fremtidige kriminalitetsudvikling vil give flere erfaringer herom, og det er da muligt, at spørgsmålet om nye bestemmelser bedst kan løses i forbindelse med andre ændringer i straffelovens kapitel 19 om forbrydelser vedrørende bevismidler og kapitel 17 om falsk forklaring, urigtige erklæringer m.v.

8.4. For så vidt angår forbrydelserne i kapitel 17 om falsk forklaring og falsk anklage, er det navnlig bestemmelserne i § 162 og § 163 om urigtige erklæringer, som kan tænkes anvendt i forbindelse med datakriminalitet.

Den øgede brug af datateknik vil formentlig i stigende grad medføre, at erklæringer til det offentlige afgives ved brug af sådan teknik, f.eks. ved indlevering af et magnetbånd med de pågældende oplysninger eller ved brug af en terminal, som står direkte i forbindelse med et offentligt register. Efter det over for staffelovrådet oplyste tillader skatte- og toldmyndighederne allerede i dag, at der på nogle få områder indgives oplysninger på datalagringsmidler. Som eksempel herpå kan nævnes, at der efter § 1, stk. 1 og 2, i ministeriet for skatter og afgifters bekendtgørelse nr. 477 af 3. oktober 1983 om administration af realrenteafgiftsloven er pålagt bl.a. visse livsforsikringsselskaber og pensionskasser oplysningspligt ved beregning af realrenteafgiftssats m.v. Normalt skal oplysningerne indgives på et skema, men efter bekendtgørelsens § 1, stk. 3, kan oplysningerne "i stedet indgives på edb-medium." Vilkårene herfor fastsættes af statsskattedirektoratet. Overtrædelse af § 1 straffes efter bekendtgørelsens § 25 med bøde.

Straffelovens § 162 giver mulighed for at straffe den, som afgiver urigtig erklæring for eller til en offentlig myndig-

hed om forhold, angående hvilke han er pligtig at afgive forklaring. Bestemmelsen stiller ikke særlige formkrav til erklæringen og vil således også kunne omfatte urigtige oplysninger, som indgives med hjælp af datateknik.

Straffelovens § 163 omfatter derimod alene urigtige skriftlige erklæringer til brug i retsforhold, der vedkommer det offentlige. Skriftlighedskravet i denne bestemmelse gør den uanvendelig på forhold, hvor gerningsmanden afgiver sin erklæring udelukkende ved hjælp af datateknik. Derimod vil bestemmelsen efter omstændighederne kunne finde anvendelse, hvis gerningsmanden i en skriftlig erklæring indestår for rigtigheden af de oplysninger, som samtidig indleveres på et datalagringsmidde1.

De nævnte bestemmelser i straffeloven suppleres af et betydeligt antal straffebestemmelser om urigtige oplysninger i særlovgivningen.

Der er efter straffelovrådets opfattelse ikke på nuværende tidspunkt påvist behov for nye bestemmelser i straffeloven om urigtige erklæringer, der afgives ved hjælp af datateknik. Sådanne erklæringer afgives i dag kun på meget begrænsede retsområder, og de pågældende myndigheder vil således have anledning til og mulighed for i forbindelse med indførelsen af datateknik at tage stilling til, om der er behov for i det pågældende retsgrundlag at søge gældende straffebestemmelser om urigtige erklæringer ændret.

I lighed med det ovenfor under pkt. 8.2. anførte har straffelovrådet således ikke på nuværende tidspunkt fundet tilstrækkeligt grundlag for at foreslå en ny bestemmelse om urigtige erklæringer afgivet ved hjælp af datateknik indsat i straffelovens kapitel 17.

Kapitel 9

Særlovgivningen

9.1. Straffelovrådet har efter sit kommissorium ikke haft til opgave at foretage en gennemgang af særlovgivningen med henblik på at vurdere behovet for lovændringer af hensyn til datakriminalitet. En del særlove har imidlertid en så tæt tilknytning til de foran beskrevne bestemmelser i straffeloven, at rådet har fundet det hensigtsmæssigt kort at omtale de - i forhold til spørgsmålet om datakriminalitet - vigtigste af disse særlove: registerlovene, lov om betalingskort, markedsføringsloven og ophavsretsloven. De nævnte særlove falder i to hovedgrupper: registerlovene og loven om betalingskort har i forhold til datakriminalitet et meget klart præventivt sigte ved bl.a. at fastsætte regler om sikkerhedsforanstaltninger mod misbrug o.lign. af lagrede data, medens markedsføringsloven og ophavsretsloven i højere grad supplerer de foran beskrevne regler i straffeloven ved at fastsætte regler om forbud mod og straf for misbrug af dataprogrammer eller lagrede oplysninger .

9.2. Registerlovene

Hovedformålet med lov nr. 293 af 8. juni 1978 om private registre m.v. og lov nr. 294 af 8. juni 1978 om offentlige myndigheders registre er at sikre retsbeskyttelsen af private i forbindelse med oprettelsen og brug af EDB-registre. Dette formål søges bl.a. opnået ved lovenes bestemmelser om sikkerhedsforanstaltninger i forbindelse med brugen af EDB-registre. Som tidligere nævnt er sådanne sikkerhedsforanstaltninger af væsentlig kriminalpræventiv betydning og er formentlig ofte en langt mere effektiv måde at sikre sig mod datakriminalitet end regler om datakriminalitet i straffeloven.

Loven om private registre finder bl.a. anvendelse på EDB-registrering, der omfatter personoplysninger. Sådan registrering må kun finde sted efter reglerne i lovens kapitel 2 og 3, som

fastsætter nærmere betingelser for oprettelsen af registre og brugen heraf, herunder om ret til at videregive registrerede oplysninger og pligt til at slette oplysninger, som f.eks. på grund af alder har mistet deres betydning for varetagelsen af registrets opgaver. Endvidere fastsætter lovens § 6, stk. 3 og 4, en pligt for virksomheder til at foretage kontrol til sikring af, at der ikke indføres urigtige eller vildledende oplysninger i EDB-registre, og en pligt til at træffe de fornødne sikkerhedsforanstaltninger mod, at oplysninger i et EDB-register misbruges eller kommer til uvedkommendes kendskab.

Registertilsynet fører tilsyn med, at der ikke sker overtrædelse af loven. Herudover er der tillagt registertilsynet beføjelser til at give pålæg af forskellig art til virksomhederne, herunder pålæg om at foretage foranstaltninger til sikring eller forbyggelse mod, at de registrerede oplysninger misbruges eller kommer til uvedkommendes kendskab. Efter lovens § 27 kan bl.a. overtrædelser af en lang række af lovens bestemmelser og undladelse af at efterkomme registertilsynets forbud eller påbud straffes med bøde eller hæfte, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Loven om offentlige myndigheders registre gælder for EDB-registre, der føres for den offentlige forvaltning, og som indeholder personoplysninger. Sådanne registre må kun oprettes efter godkendelse af vedkommende minister eller kommunalbestyrelse. Brug af registeret forudsætter, at der er fastsat forskrifter for registrets opbygning og drift, og at der forinden er indhentet en udtalelse om registrets oprettelse og forskrifterne for dette fra registertilsynet. Herudover indeholder loven visse bestemmelser om, hvilke oplysninger der må registreres, og hvorledes disse oplysninger skal opbevares, herunder om sikkerhedsforanstaltninger mod at oplysningerne misbruges eller kommer til uvedkommendes kendskab. Endelig fastsættes der i loven bestemmelser om registrerede personers adgang til oplysninger om sig selv, om offentlige myndigheders videregivelse af oplysninger til private, om videregivelse af oplysninger til andre offentlige myndigheder og om registertilsynets funktioner. I § 29 i loven om offentlige registre

findes straffebestemmelser, som i et vist omfang supplerer straffelovens regler om tjenesteforseelser. Hvis ikke højere straf er forskyldt efter disse eller andre bestemmelser, giver § 29 mulighed for med bøde eller hæfte at straffe personer, som i visse situationer uberettiget videregiver oplysninger eller uberettiget benytter sådanne oplysninger. Endvidere kan der med hjemmel i § 29 i de forskrifter, som udfærdiges vedrørende registerets oprettelse og drift, fastsættes straf af bøde for overtrædelse af bestemmelser i forskrifterne.

I modsætning til de danske registerlove indeholder den svenske datalov af 11. maj 1973 i § 21, stk. 1, følgende generelle bestemmelse om indtrængen i dataanlæg:

> "21 §. Den som olovligen bereder sig tillgång till upptagning för automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in sådan upptagning dömes för dataintrång till böter eller fängelse i högst två år, om ej gärningen är belagd med straff i brottsbalken."

Efter straffelovrådets opfattelse er der ikke behov for at foreslå en tilsvarende generel straffebestemmelse om indtrængen i dataanlæg indføjet i de danske registerlove eller i straffeloven. Straffelovrådet har, som det fremgår af de foranstående kapitler, fundet det mere hensigtsmæssigt at indføje de fornødne ændringsbestemmelser i straffelovens enkelte kapitler, således at indtrængen i dataanlæg afhængigt af formålet hermed straffes som f.eks. fredskrænkelse, brugstyveri, dokumentforbrydelse, tingsødelæggelse, berigelsesforbrydelse o.s.v.

9.3. Lov om betalingskort.

Da kontant betaling for varer, tjenesteydelser m.v. må forventes i stadig stigende omfang at blive erstattet af automatiske pengeoverførelser under anvendelse af betalingskort eller lignende legitimation, har lovgivningen på dette område en vis interesse for; spørgsmålet om datakriminalitet. Også på dette område må effektive sikkerhedsforanstaltninger mod misbrug af betalingskort m.v. således antages at kunne have en betydelig kriminalpræventiv virkning.

Ved lov nr. 284 af 6. juni 1984 om betalingskort m.v., der trådte i kraft den 1. januar 1985, er der fastsat regler om betalingssystemer med betalingskort og om betalingssystemer, der kan sidestilles hermed. Lovens formål er en øget forbrugerbeskyttelse på dette område, som søges opnået ved lovens regler om anmeldelse og registrering af betalingssystemer, om forbrugerombudsmandens beføjelser og tilsyn med betalingskortsystemerne og om betalingskortsudstederens oplysningspligt m.v. samt om erstatnignsansvar som følge af uberettiget brug af betalingskort m.v.

Af særlig betydning for spørgsmålet om datakriminalitet kan nævnes, at forbrugerombudsmanden bl.a. kan udstede påbud til virksomheder om betryggende indrettelse af kontrol- og sikkerhedsprocedurer vedrørende betalingskortsystemernes indretning og virkning, jfr. lovens § 10. Efter forarbejderne til bestem-' melsen skal der ved afgørelsen af, om et betalingssystem kan anses for betryggende indrettet, bl.a. lægges vægt på, om den valgte transmissionsform er sikker, om systemet er driftssikkert, og om etablerede sikkerhedsprocedurer yder tilstrækkelig beskyttelse mod tilsigtet uretmæssig brug. Tilsidesættelsen af et sådant påbud fra forbrugerombudsmanden kan straffes med bøde, jfr. lovens § 30.

I øvrigt finder med de ændringer, som loven selv fastsætter, loven om private registre anvendelse på de registre, der føres til brug ved betalingssystemerne.

9.4. Ophavsretsloven.

Den ofte omfattende forskningsmæssige indsats, der ligger bag fremstillingen af EDB-materie og programmer, betyder, at fremstilleren heraf kan have en betydelig økonomisk interesse i, at produktet er retligt beskyttet mod uberettiget udnyttelse, herunder navnlig kopiering fra konkurrenternes side.

Hvis et dataanlæg eller en programdiskette stjæles, kan gerningsmanden straffes for tyveri. Vælger gerningsmanden i stedet at plagiere dataanlægget eller kopiere programmet, behø-

ver han ikke at borttage nogen ting, og tyveri- og underslæbsbestemmelserne er i den sitaution uanvendelige, jfr. ovenfor kapitel 3.2. I stedet vil gerningsmanden efter omstændighederne kunne straffes efter straffelovens regler om husfredskrænkelser, anden fredskrænkelse, eller brugstyveri.

Det har herudover været diskuteret i den retsvidenskabelige litteratur, om den, der har fremstillet en datamaskine eller et dataprogram, er beskyttet mod andres efterligning, kopiering o.lign. efter eneretslovgivningen.

Det antages, at en datamaskine kan opnå retsbeskyttelse efter patentlovgivningen ved udtagelsen af patent, således at fremstilleren herved opnår eneret til at udnytte opfindelsen erhvervsmæssigt. Derimod kan dataprogrammer ikke patenteres, jfr. patentlovens § 1, stk. 2, nr. 3.

Omvendt antages det i den ophavsretlige litteratur, at dataprogrammer, men ikke datamaskiner, kan være beskyttede efter ophavsretsloven, jfr. nærmere Mogens Koktvedgaard, Retsbeskyttelse af EDB-programmer, U.f.R. 1983 side 317 ff. Afgørende for, om et dataprogram nyder beskyttelse efter ophavsretsloven, er, at det i lovens forstand kan betegnes som et "værk". Hertil kræves en vis orginalitet, således at dataprogrammet må fremtræde som selvstændig frembringelse, der med rimelig klarhed adskiller sig fra det almene, åndelige fælleseje på området, jfr. Koktvedgaard, sm.st. s. 322.

Den ophavsretlige beskyttelse af EDB-programmer medfører en lovbestemt eneret til at råde over programmerne ved at fremstille eksemplarer af programmerne og ved at gøre dem tilgængelige for almenheden i oprindelig eller ændret skikkelse, jfr. ophavsretslovens § 2, stk. 1.

En uberettiget kopiering af et ophavsretligt beskyttet dataprogram vil således være en krænkelse af eneretten til programmet og vil kunne straffes efter ophavsretslovens § 55, stk. 1, nr. 1, med bøde eller under skærpende omstændigheder med hæfte indtil 3 måneder. Subjektivt kræves det, at gerningsman-

den har handlet forsætligt eller groft uagtsomt.

Den blotte uautoriserede brug af et program antages, jfr. Koktvedgaard sm.st, side 323, - medmindre det drejer sig om rent private forhold, jfr. herved ophavsretslovens § 11 - normalt at indebære en krænkelse af ophavsretten og derfor være strafbar efter ophavsretsloven. Dette beror på, at benyttelsen typisk forudsætter, at programmet indlæses i det maskinanlæg, der ønskes benyttet, og herved fremstilles et ulovligt eksemplar, jfr. ophavsretslovens § 2, stk. 2.

Ophavsretten til et dataprogram indehaves som udgangspunkt af den, som har fremstillet dataprogrammet, uanset om den pågældende er selvstændig eller ansat hos en anden. Da hovedparten af ophavsmændene til dataprogrammer i dag fremstiller dataprogrammerne som led i et ansættelsesforhold, vil der meget naturligt kunne opstå spørgsmål om, hvorvidt ophavsretten til dataprogrammet i kraft af stiltiende eller udtrykkelig aftale eller sædvane er overgået til arbejdsgiveren. Ophavsretsloven indeholder ingen udtrykkelige bestemmelser om forholdet mellem arbejdsgivere og arbejdstagere, og det antages i den ophavsretlige litteratur, at parterne - i mangel af lovgivning om spørgsmålet - derfor må henvises til at træffe aftaler om spørgsmålet eller følge eventulle sædvaner i branchen, jfr. nærmere Koktvedgaard sm.st. side 324-325.

Som nævnt er det gældende strafmaksimum i ophavsretsloven i dag hæfte i 3 måneder. Straffelovrådet er bekendt med det forslag til lov om ændring af ophavsretsloven, som ministeren for kulturelle anliggender fremsatte den 13. december 1984 i Folketinget. Lovforslaget indeholder i § 55 en straffebestemmelse hvorefter bl.a. en forsætlig eller groft uagtsom krænkelse af en andens eneret til et litterært eller kunstnerisk værk, jfr. ophavsretslovens § 2, straffes med bøde. Som en nyskabelse foreslås en særlig udvidet strafferamme for "piratvirksomhed" i § 55, stk. 2. Efter denne bestemmelse kan straffen for en forsætlig Krænkelse af bl.a. enerettigheder, jfr. ophavsretslovens § 2, under særligt skærpende omstændigheder stige til hæfte eller fængsel indtil 1 år, hvis overtrædelsen er be-

gået ved erhvervsmæssigt at fremstille eller blandt almenheden sprede bl.a. eksemplarer af litterære eller kunstneriske værker. Særligt skærpende omstændigheder anses ifølge lovforslaget navnlig at foreligge, hvis overtrædelsen vedrører et betydeligt antal eksemplarer eller, hvis der ved overtrædelsen tilsigtes en betydelig vinding.

Lovforslagets bemærkninger berører ikke forholdet til EDB-programmer, men formuleringen af forslaget til § 55, stk. 2, synes at omfatte krænkelser af enerettigheder til EDB-programmer.

Spørgsmålet om ophavsretlige beskyttelse af dataprogrammer m.v. indgår i kommissoriet for udvalget vedrørende revision af ophavsretslovgivningen, der blev nedsat af ministeren for kulturelle anliggender den 4. maj 1976. Efter det over for straffelovrådet oplyste vil spørgsmål vedrørende dataprogrammer blive taget op til drøftelse i udvalget i løbet af foråret 1985.

9.5. Markedsføringsloven.

Siden 1912 har konkurrenceloven indeholdt bestemmelser om beskyttelse af erhvervshemmeligheder, som har haft til formål at beskytte virksomheder mod, at oplysninger om visse forhold vedrørende produktionen eller indkøbs- og salgsorganisationen, der har særlig betydning for virksomhedens konkurrenceevne, uberettiget er blevet videregivet til eller udnyttet af andre. De gældende bestemmelser om erhvervshemmeligheder findes i § 9 i markedsførsloven (lov nr. 297 af 4. juni 1974 som ændret ved lov nr. 252 af 8. juni 1977), der i 1975 afløste konkurrenceloven. Lovens § 9 er identisk med bestemmelsen i den tidligere konkurrencelovs § 11, således som denne blev udformet i 1972 i forbindelse med den samtidige revision af straffelovens regler om fredskrænkelser. Straffelovrådet foreslog i betænkningen om privatlivets fred (nr. 601/1971) bl.a., at der i straffeloven og i konkurrenceloven fastsattes bestemmelser, som kunne ramme udnyttelsen af erhvervshemmeligheder. Straffelovrådet fandt det rimeligt, at man byggede videre på antagelsen i konkurrencelovbetænkningen (nr. 416/1966) om, at man inden for konkurrencelovgivningen gør op med udnyttelsen af op-

lysninger fra ansatte m.v., medens der i straffeloven gives bestemmelser vedrørende tilfælde, hvor oplysningerne tilvejebringes af uvedkommende. Resultatet blev, at der ved lovændringen i 1972 i straffelovens § 264, stk. 2, fastsattes regler om industrispionage i forbindelse med en husfredskrænkelse, og at der i § 264 c fastsattes en "hæleribestemmelse" om den, der skaffer sig eller uberettiget udnytter oplysninger, som er fremkommet ved en overtrædelse af bl.a. § 264, stk. 2. I konkurrenceloven fastsattes bestemmelser om de ansattes industrispionage og om andres udnyttelse af oplysninger, som er fremkommet ved ansattes industrispionage.

Bestemmelserne i markedsføringslovens § 9 kan kort beskrives således:

Markedsføringslovens § 9, stk. 1, forbyder den, der er i tjeneste- eller samarbejdsforhold til en virksomhed eller udfører et hverv for denne, på utilbørlig måde at skaffe sig eller forsøge at skaffe sig kendskab til eller rådighed over virksomhedens erhvervshemmeligheder. Bestemmelsen omfatter ikke besøgende eller andre med lovlig adgang til virksomheden, som ikke er ansat eller udfører et særligt hverv for virksomheden, og heller ikke personer, som skaffer sig uberettiget adgang til virksomheden f.eks. ved indbrud og i forbindelse hermed skaffer sig kendskab til virksomhedens erhvervshemmeligheder. Det sidstnævnte tilfælde kan imidlertid som nævnt være omfattet af bestemmelsen i straffelovens § 264, stk.2.

Hvis en ansat eller samarbejdende person m.v. på retmæssig måde har fået kendskab til en virksomheds erhvervshemmeligheder, forbyder markedsføringslovens § 9, stk. 2, at den pågældende indtil 3 år efter tjenesteforholdets ophør ubeføjet viderebringer eller benytter sådanne hemmeligheder. I en mere speciel bestemmelse i § 9, stk. 3, forbydes det den, der i erhvervsøjemed er blevet betroet tekniske tegninger, beskrivelser, opskrifter, modeller eller lignende, ubeføjet at benytte sådant materiale eller sætte andre i stand hertil. De sidstnævnte tegninger m.v. behøver ikke at have karakter af en erhvervshemmelighed.

I en særlig "hæler i bestemmelse" i § 9, stk. 4, forbydes det erhvervsdrivende at benytte en erhvervshemmelighed, såfremt kendskabet hertil eller rådigheden over erhvervshemmeligheden er opnået i strid med reglerne i § 9, stk. 1-3. Erhvervshemmeligheden skal således stamme fra en ansat eller samarbejdende person, jfr. stk. 1-3. Hidrører erhvervshemmeligheden fra en person uden for denne personkreds, falder forholdet uden for bestemmelsen, men kan, hvis den er opnået i forbindelse med en husfredskrænkelse, være omfattet af straffelovens § 264 c, jfr. § 264, stk. 2.

Forsætlig eller uagtsom overtrædelse af markedsføringslovens § 9 straffes med bøde, hæfte eller fængsel i 2 år, jfr. lovens § 19, stk. 5. Strafferammen i den tilsvarende bestemmelse i konkurrenceloven blev væsentligt skærpet i 1972 bl.a. under hensyn til, at de forhold der omfattes af markedsføringsloven ikke behøver at adskille sig væsentligt fra de forhold, der omfattes af straffelovens § 264, stk. 2, som har et strafferammemaksimum på fængsel i 4 år.

I almindelighed vil det ikke være vanskeligt at vurdere, om et tilfælde af industrispionage skal straffes efter straffelovens bestemmelser om fredskrænkelser eller efter markedsføringslovens § 9, idet ansattes og samarbejdende personers forhold som nævnt typisk vil være omfattet af markedsføringsloven og de udenforståendes af straffeloven. Der kan forekomme tilfælde, hvor de to love begge er anvendelige, f.eks. hvor en ansat i forbindelse med sin industrispionage bryder eller gør sig bekendt med arbejdsgiverens lukkede meddelelser eller optegnelser.

Hvis der gennemføres en ændring af straffelovens § 263 som foreslået ovenfor i kapitel 2, vil fredskrænkelser, der begås af ansatte i en virksomhed med forsæt til at gøre sig bekendt med virksomhedens erhvervshemmeligheder, - f.eks. indsigt i datalagerede erhvervshemmeligheder -, være omfattet af såvel den foreslåede bestemmelse i § 263, stk. 3, jfr. stk. 2, som af markedsføringslovens § 9, stk. 1. Tilsvarende vil en kon-

kurrerende virksomheds benyttelse af en erhvervshemmelighed, som hidrører fra en ansats uberettigede indsigt i arbejdsgiverens datalager, kunne være omfattet af såvel straffelovens § 264 c, jfr. § 263, stk. 2 og 3, som af markedsføringslovens § 9, stk. 4. Strafferammemaksimum er i forslaget til § 263, stk. 3, og i markedsføringsloven fængsel i 2 år.

Straffelovrådet har overvejet, om man burde videreføre princippet fra revisionen i 1972 af fredskrænkelsesbestemmelserne om, at ansattes industrispionage m.v. holdes uden for straffeloven og i stedet straffes efter markedsføringsloven. Man er nået til den konklusion, at det vil medføre en unødvendig og lidt kunstig begrænsning af § 263, stk. 3, hvis den skulle undtage ansatte i en virksomhed. Bl.a. på den baggrund foreslår rådet, at bestemmelsen i § 263, stk. 3, udformes således, at der ikke indlægges begrænsninger i, hvilken personkreds der kan være gerningsmænd til forbrydelsen. Det vil herefter være overladt til anklagemyndigheden og domstolene, om man vil rejse tiltale henholdsvis dømme i sammenstød mellem bestemmelserne i straffeloven og markedsføringsloven eller foretrække at give den ene af bestemmelserne forrang. Det vil formentlig på et senere tidspunkt i forbindelse med en revision af markedsføringsloven være nærliggende at overveje, om det efter en ændring af straffelovens § 263 vil være hensigtsmæssigt at begrænse anvendelsesområdet for markedsføringslovens § 9 tilsvarende.

Også afgrænsningen mellem markedsføringslovens § 9 og straffelovens § 280 om mandatsvig kan i visse tilfælde give anledning til tvivl. Hvis en ansat i en virksomhed uberettiget udnytter en af virksomhedens erhvervshemmeligheder med forsæt til at skaffe sig berigelse, f.eks. ved brug af kopierede magnetbånd i eget firma, kan der således opstå spørgsmål om, hvorvidt forholdet bør straffes efter straffelovens § 280 eller efter markedsføringslovens § 9, idet handlingen er dækket af gerningsindholdet i begge bestemmelser. Problemet er et blandt mange eksempler på det velkendte strafferetlige fortolkningsspørgsmål, om straffeloven eller bestemmelser i særlovgivningen bør have forrang eller eventuelt bør anvendes i sammenstød.

Spørgsmålet, der henhører under anklagemyndigheden og i sidste instans afgøres af domstolene, må besvares på grundlag af en konkret fortolkning af de pågældende bestemmelser. Da spørgsmålet ikke specielt vedrører datakriminalitet, har straffelovrådet ikke fundet anledning til forfølge spørgsmålet nærmere.

Straffelovrådets lovudkast med bemærkninger

Efter de ovenfor anførte forslag til ændring af straffeloven vil bestemmelserne i § 193, § 263, § 264, § 279 a, § 280, § 284 og § 286, stk. 2, få følgende affattelse:

§ 193. Den, som på retsstridig måde fremkalder omfattende forstyrrelse i driften af almindelige samfærdselsmidler, offentlig postbesørgelse, telegraf- eller telefonanlæg, radio- eller fjernsynsanlæg, databehandlingsanlæg eller anlæg, der tjener til almindelig forsyning med vand, gas, elektrisk strøm eller varme, straffes med hæfte eller med fængsel indtil 6 år eller under formildende omstændigheder med bøde.

Stk. 2. Begås forbrydelsen uagtsomt, er straffen bøde eller hæfte.

§ 263. Med bøde, hæfte eller fængsel indtil 6 måneder straffes den, som uberettiget

1) bryder eller unddrager nogen et brev, telegram eller anden lukket meddelelse eller optegnelse eller gør sig bekendt med indholdet,
2) skaffer sig adgang til andres gemmer,
3) ved hjælp af et apparat hemmeligt aflytter eller optager udtalelser fremsat i enrum, telefonsamtaler eller anden samtale mellem andre eller forhandlinger i lukket møde, som han ikke selv deltager i, eller hvortil han uberettiget har skaffet sig adgang.

Stk. 2. 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.

Stk. 3. Begås de i stk. 1 eller 2 nævnte forhold med forsæt til at skaffe sig eller gøre sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder eller under andre særligt skærpende omstændigheder, kan straffen stige til fængsel indtil 2 år.

§ 264. Med bøde eller hæfte eller fængsel indtil 6 måneder straffes den, som uberettiget

1) skaffer sig adgang til fremmed hus eller andet ikke frit tilgængeligt sted,
2) undlader at forlade fremmed grund efter at være opfordret dertil.

Stk. 2. Begås det i stk. 1, nr. 1, nævnte forhold med forsæt til at skaffe sig eller gøre sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder eller under andre særligt skærpende omstændigheder, kan straffen stige til fængsel indtil 2 år.

§ 279 a. 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.

§ 280. For mandatsvig straffes, for så vidt forholdet ikke falder ind under §§ 276-279a, den, som for derigennem at skaffe sig eller andre uberettiget vinding påfører en anden formuetab
1) ved misbrug af en for ham skabt adgang til at handle med retsvirkning for denne eller
2) ved i et formueanliggende, som det påhviler ham at varetage for den anden, at handle mod dennes tarv.

§ 284. For hæleri straffes den, som modtager eller skaffer sig eller andre del i en ved tyveri, ulovlig omgang med hittegods, underslæb, bedrageri, databedrageri, mandatsvig, afpresning, skyldnersvig eller røveri erhvervet vinding, samt den, som ved fordølgelse, hjælp til afhændelse eller på lignende måde virker til at sikre en anden udbyttet af en sådan forbrydelse.

§ 286, stk. 2. Straffen for underslæb, bedrageri, databedrageri, mandatsvig og skyldnersvig kan, når forbrydelsen er af særlig grov beskaffenhed, eller når et større antal forbrydelser er begået, stige til fængsel i 8 år.

Bemærkninger til de enkelte bestemmelser

Til § 193.

Ved ændringen af § 193 indføjes databehandlingsanlæg blandt de anlæg, der efter bestemmelsen er beskyttet mod omfattende driftsforstyrrelser. Der stilles ikke krav til størrelsen eller karakteren af de beskyttede dataanlæg, men en begrænsning i bestemmelsens anvendelsesområde opnås gennem kravet om, at driftsforstyrrelsen skal være omfattende, jfr. nærmere herom i kapitel 5.

Som omtalt ovenfor i kapitel 5 har man benyttet anledningen til samtidig at indføje radio- og fjernsynsanlæg blandt de beskyttede anlæg. Endvidere er udtrykket "almindeligt benyttede" telegraf- og telefonanlæg ophævet, jfr. ovenfor i kapitel 5.

Straffelovrådet foreslår endelig, at strafferammens maksimum forhøjes fra 3 til 6 års fængsel, medens der ikke sker nogen ændring af de øvrige straffebestemmelser, herunder om adgangen til under formildende omstændigheder at give bøde.

Til §§ 263-264.

Straffelovrådets forslag indebærer, at den gældende bestemmelse i § 263, stk. 1, opretholdes.

Efter straffelovrådets opfattelse kan det som anført ovenfor i kapitel 2 diskuteres, om bestemmelsen i § 263 i sin nuværende form med fornøden klarhed omfatter indtrængen i et dataanlægs oplysninger. Straffelovrådet foreslår, at det ved en ny bestemmelse i § 263, stk. 2, præciseres, at det er strafbart uberettiget at skaffe sig adgang til et dataanlægs oplysninger eller programmer.

Efter gældende ret findes der kun i forbindelse med husfredskrænkelser en bestemmelse om strafskærpelse i tilfælde, hvor forholdet er begået med forsæt til at gøre sig bekendt med forretnings- eller fabrikationsforhold, jfr. § 264, stk. 2, hvorefter straffen kan stige fra 6 måneders fængsel og indtil 4 års fængsel. Den skærpede strafferamme for husfredskrænkelser finder efter den nuværende formulering i øvrigt også anvendelse i tilfælde, hvor gerningsmanden har forsæt til at gøre sig bekendt "med dokumenter eller optegnelser".

Som nævnt i kapitel 2.7. finder straffelovrådet, at der også bør være mulighed for at skærpe straffen ved de fredskrænkelser, der skal bedømmes efter den gældende § 263 eller den af straffelovrådet foreslåede nye bestemmelse i § 263, stk. 2. Straffelovrådet finder, at skærpelsesgrundene i § 263 og § 264 bør være de samme, og straffelovrådet finder i den forbindelse, at den nugældende formulering af § 264, stk. 2, bør indsnævres, således at den skærpede straffebestemmelse ikke kommer til at omfatte ethvert tilfælde, hvor forholdet begås med forsæt til at gøre sig bekendt med dokumenter eller optegnelser. Det centrale i skærpelsesbestemmelsen bør efter straffelovrådets opfattelse være, at der er forsæt til at gøre sig bekendt med oplysninger, som er hemmelige.

Straffelovrådet har på den baggrund udformet skærpelsesbestem-

meiser i § 263, stk. 3, og i § 264, stk. 2, således at strafskærpelse knyttes til, at den pågældende fredskrænkelse er begået med forsæt til at skaffe sig eller gøre sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder eller under andre særligt skærpende omstændigheder.

Første led svarer i væsentlig grad til første led i den gældende § 264, stk. 2, og formuleringen er den samme som den, der anvendes i markedsføringslovens § 9, således at det præciseres, at kun oplysninger, der har karakter af hemmeligheder, være sig kommercielle eller driftstekniske eller af anden erhvervsmæssig karakter, er omfattet.

Udtrykket "andre særligt skærpende omstændigheder", som anvendes i andet led, kendes også i straffelovens § 191 om overdragelse af narkotika, sml. straffelovens §§ 181, 216 og 288 om henholdsvis brandstiftelse, voldtægt og røveri. Med dette udtryk angives det, at strafskærpelse for de nævnte fredskrænkelser kan indtræde også i andre tilfælde end dem, hvor der er forsæt til at skaffe sig eller gøre sig bekendt med en virksomheds erhvervshemmeligheder. Det kan efter rådets opfattelse være vanskeligt mere præcist at angive, hvilke andre omstændigheder der bør kunne medføre strafskærpelse. Rådet har bl.a. haft tilfælde for øje, hvor en udnyttelse eller videregivelse af oplysningerne kan være forbundet med betydelige skadevirkninger for offentlige eller private interesser. Herunder vil f.eks. falde tilfælde, hvor gerningsmanden skaffer sig adgang til offentlige EDB-registre.

Bestemmelserne om strafskærpelse er udformet således, at forbrydelsen i sin skærpede form fuldbyrdes på det tidspunkt, som er angivet i § 263, stk. 1 eller 2, eller § 264, stk. 1, f.eks. når gerningsmanden har skaffet sig adgang til oplysninger i et EDB- register, jfr. stk. 2. Fuldbyrdelsesmomentet er for så vidt angår indsigten i erhvervshemmeligheder (§ 263, stk. 3, og § 264, stk, 2) fremrykket, således at det ikke kræves, at gerningsmanden faktisk har opnået kendskab til erhvervshemmelighederne.

Efter straffelovrådets forslag skal straffen i de i § 263, stk. 3, og § 264, stk. 2, nævnte tilfælde kunne stige til fængsel i 2 år, hvilket efter straffelovrådets opfattelse vil være et passende strafmaksimum i tilfælde med særligt skærpende omstændigheder. Dette indebærer en lempelse i forhold til den gældende bestemmelse i § 264, stk. 2 (4 år), idet der ikke kan være praktisk behov for et så højt strafmaksimum. I forhold til den gældende bestemmelse i § 263 og i forhold til andre skærpelsestilfælde, der ikke i dag omfattes af § 264, stk. 2, vil dette omvendt indebære en væsentlig forhøjelse af maksimum (fra 6 måneder til 2 år).

Efter straffelovrådets forslag fastholdes det, at de omhandlede fredskrænkelser kun er strafbare i forsætlig form.

Til § 279 a.

Om begrundelsen for bestemmelsen, der er ny, henvises til bemærkningerne ovenfor i kapitel 6.

Den foreslåede bestemmelse har indholdsmæssigt og med hensyn til betegnelsen for den nye forbrydelse (databedrageri) tilknytning til § 279 om bedrageri. Straffelovrådet finder det praktisk, at den nye bestemmelse ikke indføjes som et stk. 2 i § 279, men i en selvstændig paragraf.

Den vigtigste forskel mellem de to bestemmelser er, at § 279 a fraviger kravet i § 279 om, at en person som følge af gerningsmandens forhold skal være blevet vildledt til at foretage en disposition. I stedet for denne vildledelse træder ved databedrageri et indgreb i grundlaget for den elektroniske databehandling.

Efter straffelovrådets udkast kan databedrageri efter § 279 a i sit første led bestå i, at en person retsstridigt ændrer, tilføjer eller sletter oplysninger eller programmer. Udtrykket ændre vil formentlig dække de fleste forhold, men rådet har for tydeligheds skyld valgt at supplere dette udtryk med udtrykkene tilføje eller slette. Herved fremhæves bl.a. til-

fælde, hvor gerningsmanden indlægger et nyt supplerende program i dataanlægget eller fuldstændig sletter et program. Gerningsmandens ombytning af et program vil kunne være omfattet af udtrykket ændre programmer.

Det er uden betydning, hvorledes det indgreb, som bevirker en ændring, tilføjelse eller sletning af oplysninger eller programmer, foretages. Indgrebet kan tænkes foretaget ved hjælp af datateknik, f.eks. ved brug af en terminal. Men også andre indgreb kan være omfattet, f.eks. fysisk ødelæggelse af et magnetbånd, der indgår i en databehandling. Det vil i sådanne tilfælde være berigelsesforsættet, der adskiller forholdet fra forbrydelsen tingsødelæggelse i § 291.

Indgrebet i databehandlingen kan rettes mod både oplysninger og programmer. Det er efter bestemmelsen uden betydning, hvorledes disse oplysninger eller programmer er lagret, eller om de er under transmission.

Til de foran omtalte udtryk føjes i § 279 a, 2. led, ordene: "eller i øvrigt retsstridigt søger at påvirke resultatet af sådan databehandling". Udtrykket vil bl.a. kunne omfatte tilfælde, hvor gerningsmanden i stedet for at gribe ind i den elektroniske databehandling ændrer de oplysninger, som senere af en person skal indtastes eller lignende med henblik på elektronisk databehandling. Herved kan den pågældende person, som handler ud fra en forudsætning om oplysningernes rigtighed, i visse tilfælde blive bragt i en bestemmende vildfarelse, og forholdet kan derfor være omfattet af § 279. Men som anført ovenfor i kapitel 6.3. vil den pågældende person i nogle situationer - typisk som følge af sin underordnede stilling - ikke kunne siges at udøve nogen reel prøvelse af oplysningernes rigtighed og derfor ikke blive bragt i bestemmende vildfarelse som anført i § 279. Forholdet har således en betydelig lighed med det i bestemmelsens første led omtalte direkte indgreb i databehandlingen.

Bestemmelsen i § 279 a, 2. led, om at påvirke resultatet af en databehandling er ikke i almindelighed anvendelig på for-

hold, hvor gerningsmandens indgreb har til formål at bevirke, at der slet ikke foretages nogen databehandling, og hvor databehandlingen således ikke blot skal påvirkes, men helt udeblive. Dette kan f.eks. være tilfældet ved afbrydelse af elektriciteten til databehandlingsanlægget eller ved ødelæggelse af anlægget. Ofte vil det tillige i disse tilfælde formentlig være vanskeligt at godtgøre noget berigelsesforsæt.

Udtrykket "søger at påvirke" i § 279 a, 2. led, peger hen på en aktivitet, men udtrykket skal dog her forstås som på andre områder af strafferetten, hvor passivitet i visse situationer kan sidestilles med en aktiv handling. Det vil f.eks. kunne være tilfældet, hvor den pågældende person har en handlepligt i forbindelse med databehandlingen, f.eks. som terminaloperatør .

Om databedrageriets fuldbyrdelsesmoment bemærkes følgende. Almindeligt bedrageri efter § 279 anses for fuldbyrdet, når der med berigelsesforsæt er fremkaldt en disposition med den følge, at nogen har lidt et tab eller er blevet udsat for en væsentlig risiko for tab. For så vidt angår handlinger, der har virkning gennem et automatisk virkende dataanlæg, må det efter straffelovrådets opfattelse anses for nødvendigt at fastsætte et tidligere fuldbyrdelsesmoment, idet det vil kunne være vanskeligt og i nogle tilfælde ligefrem umuligt at fremskaffe nærmere oplysninger om, hvorvidt og i givet fald hvornår den databehandling har fundet sted, i hvilken den ændrede oplysning m.v. er blevet anvendt. I forslagets § 279 a, 1. led, er dette udtrykt således, at fuldbyrdelsen indtræder, når en person med det i bestemmelsen angivne videregående forsæt ændrer, tilføjer eller sletter oplysninger eller programmer. Tilsvarende vil forbrydelsen efter § 279 a, 2. led, være fuldbyrdet, når der er foretaget en anden handling med berigelsesforsæt og forsæt til at påvirke resultatet af en databehandling, jfr. ordene "i øvrigt ... søger at påvirke". Med disse formuleringer undgår man at tage stilling til, om der umiddelbart ved indtastning af data eller lignende kan siges at være sket en databehandling, hvor et resultat er blevet påvirket, eller om dette først er tilfældet på et senere tidspunkt.

Bestemmelsen kræver subjektivt, at gerningsmanden har handlet forsætligt, herunder har haft forsæt til berigelse. Dette subjektive krav er i overensstemmelse med kravene i de øvrige bestemmelser i kapitlet om berigelsesforbrydelser.

Til § 280.

Ved ændringen indføjes § 279 a i rækken af berigelsesforbrydelser, som er primære i forhold til mandatsvigsbestemmelsen. Den nye bestemmelse i § 279 a om databedrageri vil i sammenhæng med ændringen af § 280 formentlig betyde, at størstedelen af de sager om datakriminalitet, som efter gældende ret er henført til § 280, i fremtiden vil blive henført under den nye bestemmelse i § 279 a om databedrageri.

Til § 284.

Ved ændringen indføjes databedrageri i rækken af berigelsesforbrydelser, med hensyn til hvilke der kan begås forsætligt hæleri efter § 284.

Tilsvarende bør straffelovens § 303 om uagtsomt hæleri principielt kunne omfatte udbyttet fra databedrageri, selv om udbyttet formentlig relativt sjældent vil være en "ting", som § 303 forudsætter. Dette nødvendiggør imidlertid ikke nogen ændring af § 303, som efter sin ordlyd blot kræver, at tingen er erhvervet ved "en berigelsesforbrydelse".

Til § 286, stk. 2.

Efter straffelovrådets opfattelse bør databedrageri på grund af forbrydelsens nære forbindelse til bedrageri og mandatsvig have samme strafferamme som disse forbrydelser. Dette betyder, at normalstraffen efter straffelovens § 285, stk. 1, bør være fængsel indtil 1 år og 6 måneder, i gentagelsestilfælde 2 år og 6 måneder. Dette nødvendiggør ingen ændring af § 285, stk. 1. Tilsvarende bør den lavere strafferamme i § 287 vedrørende forhold af mindre strafværdighed også kunne finde anvendelse

på databedrageri. Dette nødvendiggør ikke nogen en ændring af denne bestemmelse. Derimod kræver det ændring af straffelovens § 286, stk. 2, at indføje databedrageri blandt de berigelsesforbrydelser, som under skærpende omstændigheder kan medføre fængsel i indtil 8 år.