IT-kriminalitet

Delbetænkning VIII afgivet af Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet

Betænkning nr. 1417

København 2002

DELBETÆNKNING VIII OM

IT-KRIMINALITET

INDHOLDSFORTEGNELSE

KAPITEL 1
INDLEDNING

1.1. Udvalgets nedsættelse og kommissorium

Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet blev nedsat den 21. oktober 1997.

Udvalgets opgave er beskrevet således i kommissoriet:

> "Udvalget skal have til opgave at fremkomme med forslag, der kan tage højde for den udvikling, som de ændrede økonomiske kriminalitetsmøn-stre og den moderne teknologi fører til.
>
> Med henblik på en sådan forstærket indsats mod den ny tids kriminalitet skal udvalget gennemgå straffelovens berigelsesforbrydelser samt vurdere behovet for skærpelser af strafniveauet for økonomisk kriminalitet, herun-der i forhold til andre forbrydelsestyper.
>
> Udvalget skal behandle særlovgivningen, herunder navnlig behovet for ændringer af skatte- og afgiftslovgivningen med henblik på at imødegå økonomisk kriminalitet. Også selskabslovgivningen, hvidvasklovgivnin-gen og den finansielle lovgivning skal behandles i

denne sammenhæng. Endvidere skal de internationale tiltag på området, herunder i EU-regi, indgå i arbejdet.

Udvalget skal tillige overveje længere forældelsesfrister på en række om-råder.

Af andre spørgsmål, der kan behandles, er revisorernes rolle, medvirken af sagkyndige dommere ved sagernes behandling ved domstolene og en øget forskningsindsats vedrørende forebyggelse og bekæmpelse af økonomisk kriminalitet.

Udvalgets anden opgave bliver at gennemgå navnlig straffeloven og rets-plejeloven med henblik på at sikre tidssvarende bestemmelser om data-kriminalitet.

Gennemgangen skal således bl.a. omfatte straffelovens bestemmelser om urigtige erklæringer og dokumentfalsk og om industrispionage.

Endvidere skal udvalget vurdere de kriminalitetsformer, som informa-tionssamfundet, herunder de elektroniske opslagstavler, giver mulighed for.

Udvalget skal også overveje ændringer af retsplejelovens regler om indgreb i meddelelseshemmeligheden i lyset af de nye telekommunikationsformer.

Endelig skal udvalget vurdere, hvordan ressourcerne anvendes bedst mu-ligt i kampen mod den økonomiske kriminalitet."

1.2. Udvalgets sammensætning

Formand

Landsdommer Hans Henrik Brydensholt
Østre Landsret

Øvrige medlemmer

Professor, dr. jur. Mads Bryde Andersen
Københavns Universitet

Afdelingschef Preben Bialas

Told- og Skattestyrelsen

Kontorchef Susan Bramsen
Fødevareministeriet

Landsdommer Bent Carlsen
Dommerforeningen
(til juli 1999)

Direktør Jørgen Christiansen
Arbejderbevægelsens Erhvervsråd

Politimester Michael Clan
Statsadvokaten for særlig økonomisk kriminalitet
(til december 1999)
Politimesterforeningen
(fra december 1999)

Professor, lic. jur. Vagn Greve
Københavns Universitet

Fuldmægtig Alexander Houen
Skatteministeriet
(fra december 1998 til marts 2001)

Fuldmægtig Annemette Vestergaard Jacobsen
Skatteministeriet
(til oktober 1998)

Fuldmægtig Helle Jahn
Erhvervsministeriet
(fra august 1998)

Statsadvokat Poul Dahl Jensen
Justitsministeriet

Konsulent Claus Kargo
Skatteministeriet
(fra marts 2001)

Statsadvokat Flemming Kjær
Statsadvokaten for særlig økonomisk kriminalitet
(fra december 1999 til november 2000)

Statsautoriseret revisor Jesper Koefoed
Foreningen af Statsautoriserede Revisorer

Juridisk direktør, advokat Lau Kramer
Foreningen Registrerede Revisorer FRR

Fuldmægtig Lisbeth Krener
Erhvervsministeriet
(til august 1998)

Advokat, dr. jur. Sysette Vinding Kruse
Advokatrådet
(til marts 1999)

Professor Lars Bo Langsted
Aalborg Universitet

Landsdommer Kaspar Linkis
Dommerforeningen
(fra juli 1999)

Kontorchef Kirsten Mandrup
Økonomiministeriet

Politimester Annemette Møller
Politimesterforeningen
(til december 1999)

Konsulent Lene Nielsen
Dansk Industri

Advokat Erik Overgaard
Advokatrådet

Advokat Jakob Lund Poulsen
Advokatrådet

(fra november 2001)

Generalsekretær Henrik Rothe
Advokatrådet
(fra marts 1999 til november 2001)

Statsadvokat Henning Thiesen
Statsadvokaten for særlig økonomisk kriminalitet
(fra november 2000)

Sekretariat

Vicestatsadvokat Ulla Høg
Statsadvokaten for særlig økonomisk kriminalitet

Statsadvokatassessor Jens Madsen
Statsadvokaten for særlig økonomisk kriminalitet

Fuldmægtig Birgitte Grønborg Juul
Justitsministeriet
(til marts 1998)

Fuldmægtig Lennart Houmann
Justitsministeriet
(fra marts 1998)

1.3. Udvalgets arbejde

Udvalget har på baggrund af kommissoriets emner nedsat 7 arbejdsgrupper, der udarbejder rapporter til udvalget til brug for udvalgets beslutninger og forslag. Arbejdsgrupperne er opdelt således:

Arbejdsgruppe 1 : Udviklingen i lovgivningen og kriminaliteten.
(Formand : Ulla Høg)

Arbejdsgruppe 2 : Straffeloven.
(Formand : Vagn Greve)

Arbejdsgruppe 3 : Særlovgivningen.

(Formand : Ulla Høg)

Arbejdsgruppe 4 : Rådgivere.
(Formand : Lars Bo Langsted)

Arbejdsgruppe 5 : Domsforhandling m.v.
(Formand : Bent Carlsen (til juli 1999), Kaspar Linkis (fra juli 1999))

Arbejdsgruppe 6 : Datakriminalitet.
(Formand : Mads Bryde Andersen)

Arbejdsgruppe 7 : Forskning.
(Formand : Lars Bo Langsted)

Udvalget har besluttet, at det afgiver delbetænkninger, når en emnekreds er færdigbehandlet, således at udvalgets indstillinger løbende kan gøres til genstand for de videre politiske overvejelser. Udvalget har herved især lagt vægt på, at nogle af de behandlede spørgsmål skal behandles i flere arbejds-grupper, og at en betænkning vedrørende samtlige de i kommissoriet nævn-te problemstillinger derfor først ville kunne foreligge på et meget senere tidspunkt end færdiggørelsen af en del af de indeholdte problemstillinger.

Udvalget har tidligere afgivet følgende delbetænkninger:

Delbetænkning I vedrørende udviklingen i lovgivningen og kriminaliteten samt hæleri og anden efterfølgende medvirken (betænkning nr. 1371/1999).

Delbetænkning II vedrørende børnepornografi og IT-efterforskning (be-tænkning nr. 1377/1999).

Delbetænkning III vedrørende rådgiveres rolle ved bekæmpelse af økono-misk kriminalitet (betænkning nr. 1379/1999).

Delbetænkning IV vedrørende transaktioner mellem nærtstående parter (be-tænkning nr. 1388/2000).

Delbetænkning V vedrørende straffelovens § 289 m.v. – berigelseskriminali-tet rettet mod offentlige midler (betænkning nr. 1396/2001).

Delbetænkning VI vedrørende straffelovens § 296 og § 302 (betænkning nr. 1415/2002).

Delbetænkning VII vedrørende forskning i økonomisk kriminalitet (betænk-ning nr. 1416/2002).

Denne delbetænkning bygger på en delrapport fra arbejdsgruppe 6, der be-handler spørgsmål vedrørende datakriminalitet. Denne delrapport er deref-ter behandlet i arbejdsgruppe 2, der behandler spørgsmål vedrørende straf-feloven. Betænkningen vedrører spørgsmålet om, hvorvidt udviklingen i IT-kriminaliteten medfører, at der er behov for at foretage ændringer i straffe-loven.

Arbejdsgruppe 6 har ved behandlingen af spørgsmålet om datakriminalitet haft følgende sammensætning:

Professor, dr. jur. Mads Bryde Andersen (formand)
Københavns Universitet

Direktør Jan Carlsen
Instituttet for Datasikkerhed

Fuldmægtig Hans Jakob Paldam Folker
Finanstilsynet

Politiassistent Jan Friis
Statsadvokaten for særlig økonomisk kriminalitet (til august 1998)
Rigspolitichefens afd. A, Rejseafdelingen (fra august 1998)

Advokat Michael Goeskjær
Advokatrådet

Statsautoriseret revisor Carsten Heilbuth
KPMG C. Jespersen

Vicestatsadvokat Ulla Høg
Statsadvokaten for særlig økonomisk kriminalitet

Fuldmægtig Helle Jahn (fra august 1998)
Erhvervs- og Selskabsstyrelsen

Fuldmægtig Gunnar Kappel (til januar 1999)
EU-direktoratet

Fuldmægtig Lisbeth Krener (til august 1998)
Erhvervs- og Selskabsstyrelsen

Kontorchef Jens Kruse Mikkelsen
Justitsministeriet

Sikkerhedschef Kjell Olsen (til november 1998)
UNI-C

Vicekriminalkommissær Ronald Pedersen
Rigspolitichefens afd. A, Rejseafdelingen

Sikkerhedschef Ole Stampe Rasmussen
UNI-C

Kriminalassistent Kim Aarenstrup
Københavns politi, Afdeling B, CCU

Statsadvokatassessor Jens Madsen (sekretær)
Statsadvokaten for særlig økonomisk kriminalitet

Som nævnt er rapporten fra arbejdsgruppen vedrørende datakriminalitet derefter behandlet i arbejdsgruppe 2, der har haft følgende sammensætning ved behandlingen:

Professor, lic. jur. Vagn Greve (formand)
Københavns Universitet

Professor, dr. jur. Mads Bryde Andersen

Københavns Universitet

Politimester Michael Clan
Politimesterforeningen

Vicestatsadvokat Ulla Høg
Statsadvokaten for særlig økonomisk kriminalitet

Statsadvokat Poul Dahl Jensen
Justitsministeriet

Statsadvokatassessor Jens Madsen
Statsadvokaten for særlig økonomisk kriminalitet

Kontorchef Jens Kruse Mikkelsen
Justitsministeriet

Advokat Jakob Lund Poulsen (fra november 2001)
Advokatrådet

Generalsekretær Henrik Rothe (til november 2001)
Advokatrådet

Fuldmægtig Lennart Houmann (sekretær)
Justitsministeriet

1.4. Resumé

Betænkningen omhandler spørgsmålet om, hvorvidt udviklingen på IT-om-rådet gør, at der er behov for at justere de strafferetlige regler. Den om-handler endvidere nogle spørgsmål om påtale og terminalefterforskning.

I kapitel 2 gennemgås den hidtidige udvikling i retstilstanden frem til den 1. januar 2002 og lovgivningen i de andre nordiske lande.

I kapitel 3 behandles forskellige spørgsmål om informationskrænkelser.

Udvalget finder, at der bør indsættes nye bestemmelser i straffeloven, der vedrører handlingerne

1) at skaffe sig eller videregive adgangsmidler til kommercielle informa-tionssystemer samt
2) erhvervsmæssigt at sælge, at udbrede i en videre kreds eller at videregive et større antal adgangsmidler til ikke-kommercielle informationssyste-mer samt at skaffe sig eller videregive adgangsmidler til visse særligt beskyttelsesværdige ikke-kommercielle informationssystemer.

Et mindretal i udvalget finder endvidere, at der tillige bør indsættes en be-stemmelse, der vedrører handlingerne at producere, skaffe sig, besidde eller videregive midler til fremskaffelse af adgangsmidler eller betalingskortnumre med forsæt til uberettiget anvendelse.

Udvalget finder endvidere

1) at strafferammen i straffelovens § 263, stk. 2, bør forhøjes,
2) at markedsføringslovens § 10 bør udvides til også at finde anvendelse på andre med lovlig adgang til virksomheden, og at der bør indsættes en bestemmelse i straffeloven om kvalificerede overtrædelser af markedsfø-ringslovens § 10,
3) at ophavsretslovens § 76, stk. 2, bør ændres således, at også udbredelse i form af placering af ophavsretligt beskyttede værker på net, hvorfra en videre kreds kan downloade, bliver omfattet, og at der bør indsættes en bestemmelse i straffeloven om kvalificerede overtrædelser af bestem-melsen, samt
4) at straffelovens § 153 bør ophæves.

I kapitel 4 behandles forskellige spørgsmål om betalingskriminalitet.

Udvalget finder, at der bør indsættes bestemmelser i straffeloven om

1) falske elektroniske penge samt handlingerne
2) at producere, skaffe sig, besidde med henblik på uberettiget anvendelse eller videregive oplysninger, der identificerer et betalingsmiddel, der er tildelt andre, eller genererede betalingskortnumre.

Udvalget finder, at de gældende regler vedrørende misbrug af andres tele-forbindelser er dækkende og foreslår ingen ændringer på dette område.

I kapitel 5 behandles forskellige spørgsmål om elektroniske dokumenter.

Udvalget finder, at bestemmelsen i straffelovens § 163 er tilstrækkeligt dæk-kende og foreslår ingen ændringer på dette område.

Udvalget finder, at den nugældende bestemmelse om dokumentfalsk i straf-felovens § 171 bør ændres, så den også omfatter elektroniske dokumenter, og begrænses til alene at omfatte hensigtsdokumenter. Ændringen får også betydning for straffelovens § 173 og § 174. Udvalget finder tillige, at straf-maksimum for dokumentfalsk bør nedsættes.

Udvalget finder endvidere, at også straffelovens § 175 bør ændres, så den omfatter elektroniske dokumenter og bøger, samt at brugen af bøger også bør medtages i bestemmelsens stk. 2.

Udvalget har herudover overvejet, om der er behov for en særlig regulering vedrørende meddelelser med vildledende afsenderbetegnelse. Udvalget har ikke fundet, at der på nuværende tidspunkt er grundlag for at foreslå en sær-lig regulering.

I kapitel 6 behandles forskellige spørgsmål om datahærværk.

Udvalget foreslår, at straffelovens § 293, stk. 2, ændres således, at den klart omfatter rådighedshindren ad elektronisk vej. Det foreslås endvidere, at strafferammen forhøjes, og at bestemmelsen undergives betinget offentlig påtale.

Udvalget foreslår endvidere, at strafferammerne i straffelovens § 193 for-højes, og at bestemmelsens stk. 2 kun skal dække groft uagtsomme forhold.

I kapitel 7 behandles spørgsmål om offentlig påtale, terminalefterforskning og Europarådets konvention om IT-kriminalitet.

Udvalget foreslår, at ophavsretslovens § 82, stk. 1, om overtrædelser af op-havsretslovens § 76, stk. 2, og § 77, stk. 2, ændres således, at den betingede offentlige påtale suppleres med, at der endvidere kan påtales, hvis almene hensyn kræver det.

Udvalget foreslår endvidere, at der indsættes en generel bestemmelse i rets-plejelovens § 720 om, at en anmeldelse anses som en begæring om påtale, medmindre andet fremgår af anmeldelsen.

Kapitel 8 indeholder udvalgets udkast med bemærkninger.

KAPITEL 2
ALMENE PROBLEMSTILLINGER

2.1. IT-relateret kriminalitet

Begreberne "datakriminalitet", "edb-kriminalitet" og "IT-relateret krimina-litet" kan defineres – og bliver defineret – på mange måder. F.eks. anvendte Straffelovrådet i betænkning nr. 1032/1985 om datakriminalitet begrebet "datakriminalitet i egentlig forstand" om de strafbare handlinger, der rum-mer en anvendelse af den for databehandling særegne teknik med hensyn til registrering, opbevaring, bearbejdelse og brug af oplysninger[1], og begrebet "datakriminalitet i vid forstand" om de strafbare handlinger, der ligger før eller efter databehandlingen[2] eller består i tyveri af udstyr eller fysisk hær-værk mod det.

Udvalget har valgt at se på et bredt kriminalitetsområde for at dække alle områder, hvor en handlings strafbarhed eller strafværdighed påvirkes af, at den har berøring med informationsteknologi enten derved, at handlingen er udført ved hjælp af informationsteknologi (herefter IT), eller således at den retter sig mod et informationsteknologisk system (herefter IT-system). Det har derfor set på de strafbare eller eventuelt strafværdige handlinger, hvor IT indgår som mål eller middel eller forudsætning for handlingen. Udvalget har dog valgt at holde den kriminalitet udenfor, der alene retter sig mod sy-stemet som en fysisk ting, f.eks. tyveri eller ødelæggelse af hardware, fordi der utvivlsomt allerede er fuldt tilstrækkelig strafferetlig dækning, og fordi det informationsteknologiske aspekt ved sådan kriminalitet ikke har selv-stændig betydning.

---

[1] Som eksempler nævnes uberettiget tilføjelse, ændring eller slettelse af oplysninger, indgreb i programmer etc. og at skaffe sig kendskab til oplysninger eller programmer ved uberetti-get brug af anlægget.

[2] Som eksempler nævnes forfalskning af grundmateriale eller udskrifter, undladelse af at gøre opmærksom på fejl ved en databehandling og modtagelse af penge, der hidrører fra datakriminalitet.

Udvalget har set på informationskrænkelser i bred forstand (både adgangs-midler, spredning og tilegnelse), enkelte spørgsmål om berigelseskriminali-tet, elektroniske dokumenter og hærværk.

2.2. Informationssystemer

Udvalget har beskæftiget sig med, hvorledes et informationssystem kan og bør defineres. Problemet er her – som på andre områder af IT-retten – at informationssystemer med nutidens teknologi ikke fremtræder i nogen homogen form. Hvor de første IT-systemer var forholdsvis enkle at iden-tificere, er der igennem det 50-årige udviklingsforløb, som er gennemløbet, siden de første computere så dagens lys i slutningen af 40-erne, sket en mar-kant ændring i IT-systemernes funktion og opbygning.

Hvor man således tidligere kunne identificere en "computer", indgår infor-mationsteknologi i dag i stort set alle områder af samfundslivet. Vælger man f.eks. at lovregulere den uretmæssige adgang til et informationssystem, vil en sådan lovregulering ramme en vid mangfoldighed af informationssystemer; ikke alene erhvervsmæssige IT-anvendelser (f.eks. til regnskabsføring, pro-duktstyring, planlægning og informationssøgning), men også offentligretlige systemer (f.eks. til skatteopkrævning og trafikstyring) og helt private syste-mer (f.eks. til dekodning af tv-signaler).[3]

Disse afgrænsningsproblemer kan henføres til den eksplosive udvikling, der er sket i forholdet mellem IT-systemers pris og funktion. En almindelig borger i det moderne samfund anvender således adskillige chips og compu-tersystemer hver eneste dag, hvad enten der er tale om indstilling af alarm-funktionen i et digitalt ur, om betjening af digitale voice mails systemer via telefonen eller om søgning i digitale informationssystemer.

---

[3] Se for en nærmere gennemgang af informationsteknologiens historie Mads Bryde Ander-sen, IT-retten (2001), s. 73-92.

Den del af udviklingen, der vedrører netsystemer, er allerede beskrevet i ud-valgets delbetænkning II[4], men gentages for helhedens skyld her:

> "Gennem de seneste år er IT-udviklingen forstærket eksponentielt gen-nem udviklingen af det verdensomspændende Internet. Navnlig udviklin-gen af den internet-teknologi, der almindeligvis går under betegnelsen the World Wide Web (også kaldet WWW), har understøttet en række nye for-mer for informationsudveksling med heraf følgende retlige (herunder strafferetlige) implikationer.
>
> Gennem the World Wide Web forbindes et antal databaser, hvis infor-mationsindhold hver for sig fremtræder med en ensartet grafisk bruger-grænseflade – de såkaldte "hjemmesider". Når en bruger ved hjælp af en computer, der er programmeret med en såkaldt web-browser, retter hen-vendelse til en anden computer, hvori der findes en sådan hjemmeside, reagerer hjemmesiden ved at afgive information til brugeren, hvorved hjemmesiden fremtræder på brugerens skærm eller kopieres til brugerens disk. På denne måde kan brugeren også indgå aftale med hjemmesidens indehaver og ved brug af forskellige teknologier gennemføre betalinger.
>
> Der indgår flere former for operatører i opbygningen af Internettets struk-tur. Disse internetoperatører kan opdeles således[5]:
>
> 1) Netværksoperatører, der alene stiller den overordnede teknologi til rå-dighed.
> 2) Internetudbydere, der etablerer adgangen til Internettet. Disse kan opdeles i:
> a) Content Providers, der tilvejebringer den information, der er tilgæn-gelig.
> b) Hosts, der udlejer plads på serveren til kunder eller stiller nyheds-grupper til rådighed på sin newsserver.
> c) Access Providers, der sælger adgang til Internettet (hvilket almin-deligvis omfatter e-mail funktioner og adgang til the World Wide Web).

---

[4] Betænkning nr. 1377/1999 om børnepornografi og om IT-efterforskning, s. 18 f.

[5] Opdelingen er den, Helen Holdt har anvendt på s. 301 ff. i "IT-retlige emner" af Peter Blume, Helen Holdt, Ruth Nielsen og Thomas Riis, Jurist- og Økonomforbundets Forlag, 1998. Se også Mads Bryde Andersen, IT-retten (2001), s. 158 f., der med udgangspunkt i E-handelsdirektivet 2000 opdeler i tre typer af Internet-leverandørfunktioner: Internetadgang (IAP, Internet Access Provider), Internet-tjenester (ISP, Internet Service Provider) og Internet-informationsindhold (ICP, Internet Content Provider).

> Udviklingen indebærer som en naturlig konsekvens også en øget risiko for retsstridig brug af disse teknologier.
>
> En opgørelse over antallet af værts-computere (hosts)[6] viser 36.739.000 hosts pr. juli 1998 og 43.230.000 hosts pr. januar 1999.
>
> Internettet indebærer næsten ubegrænsede muligheder for formidling af information og kommunikation, men også nye muligheder for kriminalitet og nye efterforskningsproblemer."

De seneste tal vedrørende værtscomputere (hosts) er 56.218.000 pr. juli 1999, 72.398.092 pr. januar 2000, 93.047.785 pr. juli 2000, 109.574.429 pr. januar 2001, 125.888.197 pr. juli 2001 og 147.344.723 pr. januar 2002.

Spørgsmålet om brugen af forskellige sikkerhedsløsninger ved anvendelsen af internet-teknologi – herunder retten til at anvende kryptering, retsvirk-ningerne af såkaldt digitale signaturer, brug af "firewall"-teknologi m.v. – behandles i andre fora.[7] Som det fremgår nedenfor i afsnit 2.3 har udvalget dog fundet anledning til at nævne den strafferetlige betydning af, at ofre for IT-relaterede kriminalitet ikke har taget den slags metoder i anvendelse.

2.3. IT-sikkerhed og strafferetten

Udvalget behandler i det følgende primært spørgsmålet om, hvorvidt udvik-lingen på IT-området indicerer, at der er behov for nye eller ændrede straf-febestemmelser. Udvalget behandler derimod ikke de meget væsentlige spørgsmål om, hvilke sikkerhedstiltag der bør påhvile den enkelte IT-bru-ger.

Det er naturligvis meget væsentligt, at der etableres den bedst mulige sikker-hed omkring betalinger og kommunikation via Internettet,

---

[6] Hobbes' Internet Timeline.
(http://info.isoc.org./guest/zakon/Internet/History/HIT.html.)

[7] Eksempelvis skal IT-sikkerhedsrådet ifølge kommissoriet for rådet således tilbyde offent-lige myndigheder samt virksomheder og borgere den højeste faglige rådgivning inden for IT-sikkerhedsområdet og i den forbindelse påpege de menneskelige og samfundsmæssige risici og interesser, som den moderne informationsteknologi giver anledning til.

således at den strafferetlige beskyttelse kun får betydning i praksis, hvor disse sikkerheds-tiltag viser sig utilstrækkelige.[8]

Domstolene lægger også ved strafudmålingen vægt på, om der har været en rimelig sikkerhed og kontrol, eller om mangelen på samme har øget fristel-sesmomentet (på grund af ringe opdagelsesrisiko) og muliggjort, at krimi-naliteten har fået et særlig stort omfang.[9]

Det er væsentligt, at virksomheder selv sørger for at have en forsvarlig orga-nisation, der giver en rimelig høj grad af IT-sikkerhed både i relation til an-satte og i relation til eksternes mulighed for at få adgang til systemet. Det skal i den forbindelse fremhæves, at revisors generelle edb-kontrol også om-fatter muligheden for ikke-autoriseret brug eller adgang som et almindeligt led i den vurdering af virksomhedens sårbarhed, der indgår i going concern-vurderingen.[10]
Udvalget har imidlertid også lagt til grund, at der kan være uopdagede sik-kerhedsrisici ved systemerne, som brugeren ikke kan tage højde for. Dertil kommer, at sikkerhedskravene må tilgodese systemets praktiske anvende-lighed og være økonomisk realistiske.

2.4. Lovgivning specielt vedrørende IT-relateret kriminalitet

I straffelovens almindelige del findes de generelle bestemmelser om bl.a. straffe, forsøg og medvirken, der som udgangspunkt gælder for alle

---

[8] Dette samspil mellem reguleringerne er også fremhævet i OECDs Guidelines for the Security of Information Systems fra 26/11 1992. Disse guidelines fremhæver både behovet for at sikre systemerne bedst muligt og betydningen af, at misbrug kriminaliseres, og at der er fornøden jurisdiktionskompetence i sagerne. I Danmark er der – med udgangspunkt i britiske normer – i 1999 af Dansk Standard vedtaget Norm for edb-sikkerhed, der dels beskriver de basale krav til sikringsforanstaltninger, der som minimum skal være etableret, for at en virksomhed kan påberåbe sig, at den lever op til normen, og dels en række skær-pede sikringsforanstaltninger, hvor der er krav om eller særligt behov for dette.

[9] Dette kom særlig klart til udtryk i præmisserne til de første domme om berigelse ved hjælp af edb-transaktioner. Nogle af dommene er refereret af Ulla Høg i EDB og EDB-kriminalitet, Anklagemyndighedens Årsberetning 1981, s. 56 ff.

[10] Jfr. Carsten Heilbuth i Inspi nr. 8/89 s. 15 ff. om revisionsvejledning nr. 14 om revision i virksomheder, som anvender edb.

straf-febestemmelser. Straffebestemmelser findes dels i straffelovens specielle del, dels i særlove.

Udvalget har overvejet, om IT-kriminalitet skulle reguleres i en særlov om IT-kriminalitet, i et særligt kapitel i straffelovens specielle del eller i enkelte paragraffer i særlove og straffeloven.

Resultatet af udvalgets overvejelser er, at det findes mest naturligt fortsat at vælge den hidtidige løsning, hvor der i de tilfælde, hvor der skønnes at være behov for specialregler, indsættes sådanne i sammenhæng med den øvrige strafferetlige regulering på det pågældende område. Udvalget har herved især lagt vægt på, at IT-relateret kriminalitet i vidt omfang er og fortsat bør være dækket af de nugældende straffebestemmelser.

Udvalgets udgangspunkt for overvejelserne har været både den lovgivning, der vedrører IT-relateret kriminalitet, og den øvrige straffelovgivning. Den-ne strafferetlige ramme er sammenholdt med IT-udviklingen og de mis-brugssituationer, udvalget enten kender eksempler på eller vurderer som realistiske situationer. På denne baggrund er det vurderet, om misbrugs-situationen allerede er kriminaliseret, og, i det omfang dette ikke er tilfældet, om der bør ske en kriminalisering, herunder om der i nogle situationer skal være en særskilt strafferetlig beskyttelse, der ligger tidligt i handlingsfor-løbet.

Straffelovrådet afgav i marts 1985 betænkning nr. 1032/1985 om datakrimi-nalitet på baggrund af en anmodning fra Justitsministeriet om en udtalelse om, hvorvidt de gældende bestemmelser i straffeloven var tilfredsstillende udformet med henblik på gerningstyper, der havde forbindelse med elektro-nisk databehandling (datakriminalitet).

På grundlag af denne betænkning gennemførtes i 1985[11] en række straffe-lovsændringer: § 193 (omfattende forstyrrelser af bl.a. databehandlingsan-læg og forhøjelse af strafmaksimum fra 3 til 4 år), § 263, stk. 2 og 3 (hacking og industrispionage m.v.), § 279 a (databedrageri) og § 284 (hæleri med hen-syn til databedrageri). Straffelovrådet valgte at holde spørgsmålet om even-tuelle yderligere

[11] Lov nr. 229 af 6/6 1985.

ændringer åbent med henblik på senere at vurdere behovet i lyset af den teknologiske udvikling.

I 1992[12] forhøjedes strafmaksimum i straffelovens § 263, stk. 3, og § 264, stk. 2, fra 2 til 4 år.

I 1996[13] ændredes straffelovens § 163 om urigtige erklæringer til det offent-lige således, at kravet om skriftlighed suppleredes med "eller ved andet læsbart medie". Baggrunden for ændringen var en frifindende dom, der var afsagt af Østre Landsret i 1995.[14]

Det bemærkes, at forskellige reguleringer på særlovsområdet også har betyd-ning. Der kan især henvises til ophavsretslovens bestemmelse om pirat-kopiering[15], der blev indsat i 1985[16] og som tillige gælder for ophavsretligt beskyttede edb-programmer. Efter denne bestemmelse kan forsætlig er-hvervsmæssig fremstilling eller spredning blandt almenheden straffes med fængsel indtil 1 år.

I 1992[17] indsattes en bestemmelse i ophavsretsloven om tekniske kopi-spærringer[18], hvorefter den, der forsætligt eller groft uagtsomt omsætter eller i kommercielt øjemed besidder midler, hvis eneste formål er at lette ulovlig fjernelse eller omgåelse af tekniske indretninger, som måtte være anvendt til at beskytte et edb-program eller andre værker i digitaliseret form, straffes med bøde.

Endvidere ændredes i 1997 lov om radio og fjernsynsvirksomhed[19] således, at der i § 75 a blev indført et forbud mod i erhvervsmæssigt øjemed at frem-stille, importere, omsætte, besidde eller ændre dekodere

---

[12] Lov nr. 6 af 3/1 1992.

[13] Lov nr. 388 af 22/5 1996.

[14] Østre Landsrets dom af 13/2 1995. Sagen vedrørte en virksomheds urigtige indberet-ninger til amtet om spildevandsanalyser. De fleste indberetninger var afgivet på disketter, og landsretten frifandt for overtrædelse af straffelovens § 163, fordi bestemmelsens krav om skriftlighed ikke fandtes at være opfyldt.

[15] Nu § 76, stk. 2.

[16] Lov nr. 274 af 6/6 1985 om ændring af ophavsretsloven.

[17] Lov nr. 1010 af 19/12 1992 om ændring af ophavsretsloven (edb-programmer).

[18] Nu § 78.

[19] Lov nr. 1095 af 29/12 1997.

eller andet dekod-ningsudstyr, hvis formål det er at give uautoriseret adgang til indholdet af en kodet radio- eller tv-udsendelse, samt mod at reklamere for sådant udstyr. Forsætlige eller groft uagtsomme overtrædelser af bestemmelsen straffes ef-ter lovens § 76 a med bøde eller fængsel indtil 6 måneder. Bestemmelserne blev ændret igen i 2000[20], således at der i lovens § 75 a ikke længere stilles krav om, at der skal være tale om erhvervsmæssigt øjemed. Lovens § 76 a blev ændret således, at forsætlige eller groft uagtsomme overtrædelser straf-fes med bøde, men at straffen kan stige til fængsel i 6 måneder, hvis der er tale om erhvervsmæssigt øjemed eller om udbredelse i en videre kreds.

Herudover er de processuelle muligheder for at efterforske IT-relateret kri-minalitet blevet revideret. I 1996[21] blev retsplejelovens § 781 ændret såle-des, at der blev adgang til telefonaflytning og teleoplysninger i hackersager (straffelovens § 263, stk. 2 og 3) og adgang til teleoplysninger i sager om overtrædelse af straffelovens § 279 a eller § 293, stk. 1, begået ved anven-delse af en telekommunikationstjeneste. I 2000[22] er bestemmelsen i overens-stemmelse med dette udvalgs indstilling i delbetænkning II[23] ændret således, at der er adgang til indgreb i meddelelseshemmeligheden i sager om over-trædelse af straffelovens § 235 (børnepornografiske fremstillinger). I 2001[24] er der i overensstemmelse med dette udvalgs indstilling i delbetænkning II indsat en bestemmelse i retsplejelovens § 780 om udvidet teleoplysning (ma-steoplysninger o.l.).

2.5. Lovgivning i de andre nordiske lande

Udvalget har afstået fra at foretage omfattende kortlægning af, hvorledes man i andre lande har lovgivet vedrørende IT-relateret kriminalitet. I det følgende findes en kort oversigt over retsudviklingen i de andre nordiske lande inden for de områder, udvalget har koncentreret sine overvejelser om.

---

[20] Lov nr. 446 af 31/5 2000.

[21] Lov nr. 388 af 22/5 1996.

[22] Lov nr. 441 af 31/5 2000.

[23] Betænkning nr. 1377/1999 om børnepornografi og om IT-efterforskning.

[24] Lov nr. 465 af 7/6 2001.

2.5.1. Island

Den islandske straffelov er blevet ændret ved lov nr. 30/1998 på følgende punkter for at tilpasse loven til den IT-relaterede kriminalitet: Kapitel XVII. Dokumentfalsk og andre forbrydelser angående synlige bevis-materialer.

I § 155 (anvendelse af et forfalsket dokument til at bedrage med i retlige transaktioner, fængsel op til 8 år) er som stk. 2 indsat:

> "På samme måde straffes anvendelse af forfalskede dokumenter, der opbevares i maskinlæsbar form, til bedrageri i retlige transaktioner."

I § 157 (anvendelse af et ægte dokument som vedrørende en anden, fængsel op til 6 måneder) er som stk. 2 indsat:

> "Bestemmelsen i stk. 1 vedrører ligeledes anvendelse af ikke-forfalskede dokumenter, der opbevares i maskinlæsbar form."

I § 158 (uberettigede anførsler i offentligt dokument eller bog m.v., fængsel op til 3 år) er som stk. 3 indsat:

> "Bestemmelserne i stk. 1 og 2 vedrører også forvanskning og anvendelse af oplysninger og dokumenter, der opbevares i maskinlæsbar form."

Kapitel XXV. Ærekrænkelser og brud på privatlivets fred.

I § 228 (brevåbning m.v., fængsel op til 1 år) er som 2. pkt. i stk. 1 indsat:

> "Tilsvarende straffes den, der på ulovlig vis skaffer sig adgang til andres dokumenter eller programmer, der opbevares i maskinlæsbar form."

Kapitel XXVI. Berigelsesforbrydelser.

I § 249 a er indsat en ny bestemmelse med følgende ordlyd:

> "Hvis nogen på ulovlig vis ændrer på, tilføjer til eller ødelægger et edb-anlæg eller dokumenter eller programmer, der opbevares i maskinlæsbar form, eller på anden vis har gjort foranstaltninger med henblik på at indvirke på resultatet af elektronisk databehandling, straffes det med fængsel i op til 6 år."

Kapitel XXVII. Forskellige lovovertrædelser angående formuerettigheder.

I § 257 (hærværk, fængsel op til 6 år) er som stk. 2 indsat:

> "Tilsvarende straffes der for uden tilladelse at ændre, tilføje, slette eller på anden vis ødelægge dokumenter eller programmer, der opbevares i ma-skinlæsbar form og er beregnet på elektronisk databehandling."

2.5.2. Norge

Den norske straffelov indeholder i § 179 en dokumentfalskbestemmelse (fængsel op til 4 år eller 5 år, hvis dokumentet er middel til en forbrydelse, der kan medføre fængsel i 2 år eller derover) med følgende indhold:

> "Ved Dokument forstaas i denne Lov enhver Gjenstand, som i Skrift eller paa anden Maade indeholder et Tilkjendegivende, der enten er af Betyd-ning som Bevis for en Ret, en Forpligtelse eller en Befrielse fra en saadan eller fremtræder som bestemt til at tjene som Bevis."

§ 145 (brevhemmelighed, fængsel op til 6 måneder) indeholder i stk. 2 følgende bestemmelse:

> "Det samme gjelder den som ved å bryte en beskyttelse eller på anden lig-nende måte uberettiget skaffer sig adgang til data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske mid-ler."

§ 270, stk. 1, nr. 2 (bedrageri, fængsel op til 6 år) indeholder følgende be-stemmelse (hvor indledningen er, at "For bedrageri straffes den som i hen-sikt å skaffe seg eller andre uberettiget vinding"):

> "ved bruk af uriktig eller ufullstendig opplysning, ved endring i data eller programutrustning eller på annen måte rettsstridig påvirker resultatet av en automatisk databehandling, og derved volder tap eller fare for tap for no-en."

Hærværksbestemmelserne i §§ 291, 292 og 391 (fængsel op til 4 år) nævner ikke specielt data m.v. Derimod indeholder § 151 b følgende:

> "Den som ved å ødelegge, skade eller sette ut av virksomhet informasjons-samling eller anlegg for energiforsyning, kringkasting, telekommunikasjon eller samferdsel volder omfattende forstyrrelse i den offentlige forvaltning eller i samfunnslivet for øvrig, straffes med fengsel inntil 10 år.
> Uaktsomme handlinger som nevnt i første ledd straffes med bøter eller med fengsel inntil 1 år."

Den norske straffelov har endvidere i § 262 en særlig bestemmelse om piratdekodere, der lyder således:

> "Den som ved å bryte en beskyttelse eller på lignende måte rettsstridigt skaffer seg selv eller andre en vinning ved å få tilgang til fjernsyns- eller radiosignaler eller medvirker til det, straffes med bøter eller fengsel inntil 1 år. Det samme gjelder dersom den berettigede blir utsatt for tap."[25] [26]

2.5.3. Sverige

De svenske dokumentfalskbestemmelser er ikke blevet tilpasset elektroniske dokumenter.

§ 21 i datalagen indeholdt følgende bestemmelse:

> "Den som olovligen bereder sig tillgång till upptagning för automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in sådan opptagning dömes för dataintrång till böter eller fängelse i

---

[25] Bestemmelsen blev indsat, uanset der formentlig efter norsk ret allerede i ophavsretslo-vens og/eller straffelovens bestemmelser (brud på brevhemmeligheden m.v.) var strafferet-lig dækning. Det siges i lovforslaget (Ot prp nr. 4 (1994-95)) som en af begrundelserne for lovændringen, at ophavsretsloven er relativt vanskelig tilgængelig for den, der ikke sædvan-ligvis beskæftiger sig med ophavsretlige spørgsmål, og at det kan medføre, at påtalemyndig-hederne undlader at rejse tiltale, selv om reglerne er overtrådt.

[26] Bestemmelsen er bl.a. anvendt i en norsk herredsrettsdom af 1/7 1998. Den tiltalte hav-de gennem ca. 16 måneder via Internettet og på anden måde fra sin bopæl tilbudt, for-midlet og solgt udstyr og know how for at skaffe kunder gratis adgang til beskyttede tv-kanaler. Han havde haft en bruttoindtægt på mindst 1.885.000 kr. og blev idømt 8 må-neders fængsel, ligesom bruttoindtægten blev konfiskeret.

> högst två år, om ej gärningen är belagd med straff i brottsbalken eller i lagen om skydd för företagshemligheter. Med upptagning anses härvid även upp-gifter som är under befordran via elektroniskt eller annat liknande hjäl-pemedel för att användas för automatisk databehandling ..."

Loven blev ophævet pr. 24/10 1998 og erstattet af følgende bestemmelse i 4. kapitel i brottsbalken:

> "9 c § Den som i annat fall än som sägs i 8 och 9 §§[27] olovligen bereder sig tillgång till upptagning för automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in sådan upptagning döms för dataintrång till böter eller fängelse i högst två år. Med upptagning avses härvid även uppgifter som är under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för automatisk databehandling."

§ 9 i 9. kapitel om bedrägeri och annan oredlighet indeholder i stk. 2 føl-gende bestemmelse:

> "För bedrägeri döms också den som genom att lämna oriktig eller ofull-ständig uppgift, genom att ändra i program eller upptagning eller på annat sätt olovligen påverkar resultatet av en automatisk informationsbehand-ling eller någon annan liknande automatisk proces, så att det innebär vin-ning för gärningsmannen och skada för någon annan."

Hærværksbestemmelserne (fængsel op til 4 år) indeholder ingen særregler om data.

2.5.4. Finland

33. kapitel i den finske strafflagen vedrører förfalskningsbrott (fængsel op til 4 år). Forfalskningen skal vedrøre bevismidler, hvilket i § 6 defineres såle-des:

---

[27] "8 § Den som olovligen bereder sig tillgång till ett meddelande, som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller telemeddelande, döms för brytande av post- eller telehemlighet till böter eller fängelse i högst två år.

9 § Den som, utan att fall är för handen som i 8 § sägs, olovligen bryter brev eller telegram eller eljest bereder sig tillgång till något som förvaras förseglat eller under lås eller eljest tillslutet, dömes för intrång i förvar till böter eller fängelse i högst två år."

> ”Som bevismedel anses i denna lag handlinger och kopior av en handling, märken, stämplar, registerskyltar, ljud- och bildupptagningar, upptagningar som gjorts med registrerande målinstrument, räkneapparat eller annan motsvarende teknisk anordning samt upptagningar som lämpar sig för automatisk databehandling, om de används eller kan användas såsom rätts-ligt betydelsefulla bevis om rättigheter, förpliktelser eller fakta.”

38. kapitel om informations- och kommunikationsbrott indeholder i § 8, stk. 1-2, følgende bestemmelser:

> ”Dataintrång. Den som genom at göra bruk av en användaridentifikation som han inte har rätt till eller genom att annars bryte säkerhetsarrange-mang obehörigen tränger in i ett datasystem där data behandlas, lagres eller overförs elektroniskt eller med någon annan sådan teknisk metod eller i en särskilt skyddad del av ett sådant system, skal för dataintrång dömas till böter eller fängelse i högst ett år.
>
> För dataintrång döms också den som utan att tränga in i datasystemet el-ler en del av detta med tekniska specialordningar obehörigen tar reda på information som finns i ett sådant datasystem som avses i 1 mom.”

36. kapitel om bedrägeri och annan oredlighet (fængsel op til 4 år for bedra-geri) indeholder i § 1, stk. 2, følgende bestemmelse:

> ”För bedrägeri döms också den som i sådant syfte som nämns i 1 mom. genom att mata in oriktiga uppgifter i en dator eller på något annat sätt ingripa i maskinell databehandling förvanskar slutresultatet av databehand-lingen och därigenom orsaker ekonomisk skada för nogon annan.”

35. kapitel om skadegörelse (fængsel op til 4 år) indeholder i § 1, stk. 2, føl-gende bestemmelse:

> ”För skadegörelse döms också den, som för att skada någon orättmätigt förstör, skadar, döljer eller hemlighåller information som har upptagits på et datamedium eller någon annan upptagning.”

Derudover indeholder 34. kapitel om allmänfarliga brott i § 1 om sabotage (fængsel op til 4 år, i særligt kvalificerede tilfælde op til 10 år) følgende stk. 2:

> ”För sabotage döms också den som genom att skada eller förstöra egen-dom eller genom att obehörigen ingripa i ett produktions-, distributions- eller datasystems funktion, förorsaker allvarlig fara för energiförsörjnin-gen, den allmänna hälsovården, försvaret, rättsvården eller någon med des-sa jämförbar viktig samhällsfunktion.”

I 34. kapitel er der ved lov nr. 951/1999 indsat en § 9 a om virus (”Orsa-kande av fara för informationsbehandling”)[28]:

> ”Den som för att orsaka olägenhet för informationsbehandling eller ett data- eller telesystems funktion,
> 1) tillverkar eller ställer till förfogande ett sådant datorprogram eller så-dana programinstruktioner som har planerats för att äventyra infor-mationsbehandling eller ett data- eller telesystems funktion eller för att skada data eller programvara som ingår i ett sådant system, eller sprider ett sådant datorprogram eller sådana programinstruktioner eller
> 2) ställer til förfogande anvisningar för tillverkning av ett sådant dator-program eller sådana programinstruktioner som avses i 1 punkten el-ler sprider sådana anvisningar
>
> skall, om inte strängare eller lika strängt straff föreskrivs för gärningen nå-gon annanstans i lag, för *orsakande av fara för informationsbehandling* dömas til böter eller fängelse i högst två år.”

2.6. Forbudet i straffelovens § 1 mod visse analogislutninger

Udvalget har ved gennemgangen af problemstillingerne bl.a. set på, om an-vendelsen af aktuelle bestemmelser eventuelt forudsætter, at dette sker efter et princip om fuldstændig lovanalogi, jfr. straffelovens § 1, hvorefter straf kun kan pålægges for et forhold, hvis strafbarhed er hjemlet ved lov, eller som ganske må sidestilles med et sådant (fuldstændig analogi). Et analogi-forbud kan også udledes af artikel 7, stk. 1, 1. pkt., i Den Europæiske Menneskerettighedskonvention, der lyder:

---

[28] Det nævnes i lovforslaget, at Holland, Italien, Rusland, Schweiz og Storbritannien har straffebestemmelser om virus, herunder om spredning af virus.

> "Ingen kan kendes skyldig i et strafbart forhold på grund af en handling eller undladelse, der ikke udgjorde en forbrydelse efter national eller inter-national ret på det tidspunkt, da den blev begået."

Danske domstole har ikke ført nogen entydig praksis med hensyn til betydningen af analogiforbudene i relation til nye teknologiske fænomener. Ved dommen i UfR 1940.156 Ø blev en person straffet for overtrædelse af straffelovens § 263 (der i sin daværende udformning alene straffede retsstri-dige brevåbninger) i en situation, hvor gerningsmanden havde foretaget af-lytning af en telefonsamtale gennem tilslutning af en hemmelig lytteanord-ning. Både landsretten og byretten udtalte, at der straffedes efter en analogi af den pågældende bestemmelse. Dommen er ganske vidtgående, formentlig også for vidtgående. Ved den i afsnit 2.4 nævnte Østre Landsrets dom af 13/2 1995, der gav anledning til ændring af straffelovens § 163, fandtes disketter ikke at være omfattet af skriftlighedskravet; bestemmelsens analogi blev ikke anvendt.[29] Omvendt fandt Østre Landsret i UfR 1996.356 Ø, at bestemmelsen i § 2 i lov om offentlige indsamlinger, hvorefter indsamling ved anvendelse af "kædebreve" ikke må finde sted, var anvendelig i en situation, hvor en person havde etableret et system baseret på disketter til pc'ere, der var opbygget i samme form som kædebreve.[30] Endelig kan nævnes Køben-havns byrets dom af 29/5 2001, der er stadfæstet af Østre Landsret den 26/9 2001, jfr. afsnit 5.3, hvor skriftlighedskravet ansås for opfyldt i en situation, hvor tiltalte med angivelse af en andens navn telefonisk meddelte en betalingskortudsteder, at hans kort var bortkommet, og derefter fremsendte en e-mail med oplysning om, at nyt kort skulle sendes til en c/o-adresse.

---

[29] Hvilket svarede til Straffelovrådets vurdering i betænkning nr. 1032/1985 om datakrimi-nalitet, s. 64.

[30] Ved Østre Landsrets dom af 10/3 1999 blev de tiltalte i en sag om pyramidespil frifundet for overtrædelse af indsamlingsloven under henvisning bl.a. til artikel 7 i Den Europæiske Menneskerettighedskonvention. Landsretten lagde vægt på, at der ikke havde været opfor-dringer til deltagelse, men at de deltagende var inviteret til møder af bekendte og havde an-søgt om medlemskab under møder. Denne fremgangsmåde fandtes ikke at kunne sidestilles med "indsamling ved anvendelse af kædebreve". Pyramidespil er nu kriminaliseret ved lov nr. 229 af 4/4 2000.

Det er på denne baggrund ikke muligt at opstille nogen klar prognose om, hvorledes domstolene vil fortolke eksisterende straffebestemmelser i hense-ende til nye teknologiske fremtrædelsesformer, der ikke klart dækkes af de pågældende bestemmelsers ordlyd.

Straffelovens § 1 har ikke blot betydning for eksisterende bestemmelser, men også for, hvordan eventuelle nye bestemmelser skal formuleres, så de er anvendelige på alle de forhold, der tilsigtes kriminaliseret.

Udvalget er opmærksom på, at dette krav om klar lovhjemmel om nødven-digt må gå forud for ønsket om en lovgivning, der er fremtidstilpasset til den mulige teknologiske udvikling, og at man i videst mulige omfang må forsøge at nå frem til formuleringer, der tilgodeser begge hensyn.

Spørgsmålet om betydningen af straffelovens § 1 er bl.a. behandlet af Straf-felovrådet i dets udtalelse af 14/1 1974 om økonomisk kriminalitet[31] i for-bindelse med et forslag foranlediget af ågerudvalgets arbejde om en bestem-melse om strafansvar, der ville dække den, som "i udøvelse af erhverv ved grov tilsidesættelse af sociale hensyn eller god forretningsskik skaffer sig økonomisk fordel eller tilføjer andre formuetab". Straffelovrådet fandt, at indholdet skulle være mere præcist.

Kravet om et præcist indhold udelukker ikke bredt formulerede bestemmel-ser.

2.7. Straffelovens § 21 om forsøg og § 23 om medvirken

Udvalget har i øvrigt særligt været opmærksom på, i hvilken udstrækning reglerne i straffelovens § 21 (hvorefter handlinger, som sigter til at fremme eller bevirke udførelsen af en forbrydelse, når denne ikke fuldbyrdes, straf-fes som forsøg) og § 23 (hvorefter den for en lovovertrædelse givne straffe-bestemmelse omfatter alle, der ved tilskyndelse, råd eller dåd har medvirket til gerningen) – herunder i kombinationerne forsøg på medvirken og med-virken til forsøg – yder

[31] S. 27 ff. og s. 38 ff.

en tilstrækkelig strafferetlig beskyttelse i alle tilfælde, hvor man ellers kunne overveje at lægge en fremskudt kriminalisering.

Uanset denne brede kriminalisering af forsøgs- og medvirkenshandlinger anvendes disse bestemmelser i praksis ikke ofte på de indledende forbere-delseshandlinger. Dette skyldes, at spørgsmålet om forsøgsreglernes anven-delighed i praksis ikke mindst er et spørgsmål om, hvilke krav der stilles til beviset for forsæt og for konkretisering af nærmere angivne forbrydelser. Bevismæssigt vil der ofte kun være det objektivt konstaterbare, der indicerer et videregående forsæt. I praksis vil dette ofte være ensbetydende med, at sagen ikke rejses.

Dertil kommer, at en klar straffebestemmelse eller en omfattende retsprak-sis er lettere at få kommunikeret ud til mulige lovovertrædere og derfor må antages at have større præventiv virkning end en oplysning om, at der kan dømmes for forsøg og/eller medvirken.

På den baggrund er spørgsmålet ikke alene, om der kan være behov for en nykriminalisering ved at give en fremskudt strafferetlig regulering inden for visse områder, men også, om der også i tilfælde, hvor bestemmelserne om forsøg og medvirken i og for sig er anvendelige, i dag kan være behov for en mere fremskudt regulering, der ikke er afhængig af, om der kan føres til-strækkeligt bevis for forsøg eller forsøg på medvirken.

Som eksempler på nogle IT-relaterede sager, hvor forsøgsspørgsmålet har været aktuelt, kan nævnes følgende:

> Ballerup rets dom af 30/8 1994
> I sagen var der rejst tiltale for overtrædelse af ophavsretslovens § 55, stk. 2, (nu § 76, stk. 2) ved, at den tiltalte, der var formand for en edb-klub og annoncerede i "Den Blå Avis", igennem mindst 5 år erhvervsmæssigt havde kopieret og distribueret et stort antal edb-programmer og manualer, der var ophavsretligt beskyttet. Retten fandt det godtgjort, at tiltalte i hvert fald i et vist omfang havde solgt disketter, der angiveligt skulle indeholde ophavsretligt beskyttede edb-programmer, men fandt det overvejende be-tænkeligt at anse det for godtgjort, at disketterne faktisk indeholdt kopiere-de programmer. (Bevisførelsen bestod efter dommens beskrivelse over-vejende i vidneførsel og fremlæggelse af annoncer).

Dommen viser primært, hvordan beviskravene til piratkopiering håndteres i praksis. Retten fandt, at bevisførelsen var utilstrækkelig. Tiltalen vedrørte fuldbyrdede, men uidentificerede forhold. I den konkrete sag var det ikke tilstrækkeligt til forsøgsstraf, at tiltalte havde annonceret med salg af ophavsretligt beskyttede programmer og faktisk er i besiddelse af de aktuelle programmer. Det fremgår i øvrigt af retsbogen, at der var nedlagt foged-forbud mod distribution af en række programmer, og at den tiltalte i en pe-riode på knap 7 måneder havde købt 4.000 disketter. Det fremgår ligeledes, at over 90 af de udbudte programmer var ophavsretligt beskyttet.

UfR 1996.1514 Ø

En sag vedrørende markedsføringslovens § 10, stk. 2, vedrørte to opsagte medarbejdere i et speditionsfirma. Det fremgik af vidneforklaringer, at de to medarbejdere havde taget prislister, manualer, konkrete sager og tilbud til bl.a. faste kunder, agentliste over samarbejdspartnere samt liste over pri-ser for fragt til USA, 3 sagsmapper med konkrete sager i original, rederi-kontrakter, arbejdsmanualer m.v. og et større antal kundejournaler i origi-nal, kundetilbud, diverse prislister og tilbud på fragt m.v. med hjem, og at de påregnede nye ansættelser i andre speditionsfirmaer. Byretten frifandt, idet den lagde til grund, at det ikke var bevist, at de havde benyttet eller videregivet de oplysninger, de var kommet i besiddelse af. Der blev ved afgørelsen lagt vægt på, at de tiltalte stadig var ansat og arbejdede i virk-somheden, da de blev fundet i besiddelse af oplysningerne, der hørte til deres ansættelsesområde. Dommen blev anket af anklagemyndigheden, og Østre Landsret dømte med dommerstemmerne 4-2. Flertallet fandt, at der var tale om en strafbar forsøgshandling, idet i hvert fald kundejournalerne måtte anses for erhvervshemmeligheder. Mindretallet fandt det ikke godt-gjort, at formålet med at have en del af virksomhedens papirer hjemme var for eventuelt senere ubeføjet at viderebringe eller benytte papirerne.

Roskilde rets dom af 19/12 1996

I dommens forhold 13 var der rejst tiltale for overtrædelse af straffelovens § 263, stk. 3, jfr. stk. 2, i forbindelse med, at den ene tiltalte havde videre-udviklet et crackerprogram til brydning af passwords og havde viderefor-midlet dette til medtiltalte med henblik på deres brug som led i hacking eller deres videreformidling til samme formål. (Forhold 7 og 14, XXV, 1, a, vedrører samme problemstilling). Retten siger herom (dommens s. 202), at "udarbejdelse, overladelse eller benyttelse af et crackerprogram kan indgå som et forberedende led i en uberettiget indtrængen i et edb-anlæg, dvs. en overtrædelse af straffelovens § 263, stk. 2, eller det kan være medvirken til andres overtrædelse af bestemmelsen. Dette

forudsætter dog, at der er forsæt til, at udarbejdelsen, overladelsen eller benyttelsen fører til en nærmere bestemt uberettiget indtrængen i angivne edb-anlæg, men det er ikke nok, at det måtte kunne lægges til grund, at handlingen – overvejende sandsynligt – sker med henblik på hacking generelt. Noget andet måtte forudsætte, at udvikling m.v. af cracker-programmer blev selvstændigt kriminaliseret, svarende til våbenbesiddelse i forhold til voldsforbrydelser". Der skete herefter frifindelse i denne type forhold (dommens s. 220 f., 238 og 246), da det ikke var bevist, at de tiltalte ved udviklingen og formidlingen havde haft forsæt til indtrængen i bestemte edb-anlæg.

Dommen indeholder også en række konkrete forsøgsforhold i forbindelse med videregivelse af passwords, hvor retten dømmer under henvisning til, at de videregives på en måde, der må betragtes som en opfordring til at hacke bestemte anlæg.[32] Herudover er der i dommens forhold 14, XXV, 2, b, dømt for forsøg på medvirken til overtrædelse af straffelovens § 263, stk. 2, i forbindelse med, at den tiltalte på et område på sit BBS (Bulletin Board System), hvortil især de medtiltalte havde adgang, videregav oplys-ninger om brugeridentiteter med tilhørende dekrypterede passwords med en udtrykkelig opfordring til at prøve det ene anlæg og til ikke at skifte password, således at andre hackere kunne benytte det samme system (dommens s. 247).

Som det fremgår, anlægges der en klar sondring mellem de tilfælde, hvor forsøgshandlingen vedrører konkrete anlæg, og de tilfælde (crackerprogram-merne), hvor det senere aktuelle anlæg ikke er identificeret. Kun i den første type tilfælde dømmes for forsøg.

Lemvig rets dom af 14/2 1997

Der var i sagen tiltalt for overtrædelse af straffelovens § 235, stk. 1, jfr. § 21, for forsøg på erhvervsmæssigt salg (adgang mod betaling af 20 USD, 30 DM eller 120 kr.) eller anden udbredelse af utugtige fotografier af børn. Der var endvidere rejst tiltale for overtrædelse af samme bestemmelses stk. 2, ved at den tiltalte havde et stort antal børnepornografiske billeder lagret på harddisken. Retten lagde efter bevisførelsen til grund, at tiltalte havde oprettet et BBS med billeder med det formål, at brugere via telefon-nettet kunne skaffe sig adgang til databasen og se eller hente billeder, og at brugerne efter en periode skulle betale herfor eller indlægge billeder i databasen som betaling. Det lagdes endvidere til grund, at en bruger kunne downloade de på en filliste angivne billeder. Det fandtes bevist, at der i en fil var utugtige billeder af børn, men det måtte lægges til grund, at denne fil

[32] Jfr. dommens s. 210, 212 og 225 vedrørende forholdene 1, XXXVI, 3, 1, XL, b, og 8, IV, 1-2.

ikke var tilgængelig for brugere. Det fandtes herefter ikke bevist, at den tiltalte havde forsøgt erhvervsmæssigt at udbrede utugtige billeder af børn, og han blev frifundet i dette forhold. I det andet forhold ansås det kun for bevist, at tiltalte havde haft 1 billede på sin harddisk. (Den fil, der ansås for ikke tilgængelig for brugere, er således heller ikke blevet betragtet som omfattet af stk. 2).

I en nyere dom vedrørte et af forholdene forsøg på databedrageri i forbin-delse med besiddelse af falske betalingskort:

UfR 2000.1881 Ø

Der var i sagen tiltalt for bl.a. overtrædelse af straffelovens § 279 a og for-søg herpå i forbindelse med hævninger og forsøg herpå med falske beta-lingskort i alt 22 gange inden for 2 ½ time. Der blev endvidere tiltalt for forsøg på overtrædelse af straffelovens § 279 a i forbindelse med besiddel-se af 123 falske betalingskort. Alle kort havde forbindelse til kort, der havde været anvendt i en bank i Moskva. Både Københavns byret og Østre Landsret dømte i disse forhold.

KAPITEL 3
INFORMATIONSKRÆNKELSER

3.1. Indledning

Som nævnt indledningsvist har udvalget set på informationskrænkelser i bred forstand. Udtrykket informationskrænkelser i bred forstand dækker over en række situationer, hvor IT-systemer eller den information, der be-handles heri, udsættes for angreb af forskellig karakter. Set i et bredt per-spektiv er der tale om en vid mangfoldighed af processer, der ikke er knyttet til lovlig adgang til informationerne:

1. At tilegne sig informationer, der giver adgang til yderligere informatio-ner.
2. At skaffe sig adgang til informationer.
3. At tilegne sig informationer.
4. At kopiere informationer.
5. At anvende informationer.
6. At videregive informationer.

Udvalget har vedrørende disse processer set på de områder, hvor udvalget finder, at der eventuelt er behov for en ny regulering eller en ændring af den eksisterende regulering.

I det følgende behandles disse områder:

Adgangsmidler (afsnit 3.2).
Strafferammen i straffelovens § 263, stk. 2 (afsnit 3.3).
Industrispionage m.v. (afsnit 3.4).
Piratkopiering (afsnit 3.5).

Særligt vedrørende spredning har udvalget i delbetænkning II om børne-pornografi og om IT-efterforskning[33] set på informationsspredning ikke alene i relation til børnepornografi, men også i relation til ansvar for ind-holdet af informationssystemer og til kursmanipulation, insiderviden og markedsføring på eller via Internettet. For så vidt angår straffelovens § 235 foreslog udvalget, at udbredelse i en videre kreds sidestilles med erhvervs-mæssig udbredelse. Lovændringen er gennemført ved lov nr. 441 af 31/5 2000.
Udvalget har i delbetænkning II anført dets generelle overvejelser således:

---

[33] Betænkning nr. 1377/1999, s. 31 f.

”Lovgivningen regulerer i forskellige henseender (f.eks. i forbindelse med piratkopiering og dekodningsudstyr) spredning af information, som ger-ningsmanden ikke har rettigheder over, eller hvis indhold i sig selv er strafbart. Der stilles normalt krav om, at denne spredning er erhvervsmæs-sig, hvis den skal være omfattet af straffebestemmelser med højere straffe-ramme. For så vidt angår lov om radio- og fjernsynsvirksomhed er kun er-hvervsmæssig spredning af dekodningsudstyr strafbart.[34]

På baggrund af internetudviklingen har udvalget drøftet hensigtsmæssig-heden af sådanne grænsedragninger, navnlig i lyset af, at det nu er blevet så enkelt at sprede informationer til en nærmest helt ubegrænset kreds. Muligheden for effektivt at sprede information gennem teleinformations-teknologi er ikke opstået i og med Internettet. Lignende problemer opstår i trykte medier og i andre elektroniske medier. Retsstridig information har således kunnet spredes gennem radiosendere, men på grund af en for-holdsvis intens regulering af såvel frekvenstildelingen som det informa-tionsmæssige indhold i offentlig radio- og tv-transmission, har disse tek-nologier ikke givet anledning til strafferetlige problemstillinger i samme omfang, som det er tilfældet i forbindelse med brugen af Internettet. Ved fremkomsten af de såkaldte bulletin-boards (dvs. informationssystemer, typisk baseret på en pc, der ved hjælp af telenettet gav mulighed for op-kald og søgning af informationer) rykkede problemstillingen tættere på, om end i en langt mere begrænset skikkelse, eftersom sådanne systemer almindeligvis kun har kunnet nås gennem det begrænsede antal telefon-opkald, der har været til rådighed i den enkelte telefonforbindelse.

Den udbredte anvendelse af WWW har imidlertid givet denne pro-blemstilling en langt større dimension, eftersom WWW-teknologien (der som nævnt i mange tilfælde indebærer, at særligt populære hjemmesider ikke alene er tilgængelige fra den server, der benyttes ved indlæggelse af informationerne, men også fra andre internetudbyderes servere, hvortil informationerne kopieres over for at spare teletrafik) har reduceret disse flaskehalsproblemer til et minimum. Ud over dette rent kvantitative pro-blem om spredningens omfang indebærer WWW-teknologien vanskelig-heder med hensyn til at identificere den gerningsmand, der spreder den pågældende information, og herunder også det land, som den efterfor-skende myndighed i givet fald skal samarbejde med med henblik på at opnå de fornødne tilladelser til straffeprocessuelle tvangsindgreb.

---

[34] Loven er senere ændret, jfr. afsnit 3.2.1.

> Disse forhold – omfanget af informationsspredningen og den gennemgående anonymitet på the WWW – har skabt strukturer, hvor deltagerne ikke i traditionel forstand kender de øvrige deltagere. Der mangler derfor den i et vist omfang kriminalitetshæmmende faktor, at andre ved, hvem man er, og hvad man gør.
> Det er udvalgets opfattelse, at mens et forbud mod erhvervsmæssig spred-ning tidligere har dækket hovedparten af det område, der var behov for at give en strafferetlig beskyttelse for at begrænse krænkelser af beskyttede interesser, så har udviklingen på IT-området ændret denne situation. Dette gælder især Internettet, hvor der distribueres oplysninger om dekodere, oplysninger om passwords m.v., ophavsretligt beskyttede edb-program-mer, børnepornografi m.v.
>
> Udvalget finder på denne baggrund, at den traditionelle begrænsning til erhvervsmæssig spredning i dag kan være en utilstrækkelig strafferetlig be-skyttelse, da spredning via netsystemer må antages i mange tilfælde at have samme skadevirkning som den erhvervsmæssige spredning.
>
> Udvalget har derfor i sit arbejde taget udgangspunkt i, at spredning til en større kreds (f.eks. via Internettet) på nogle områder bør sidestilles med erhvervsmæssig spredning. Ved formuleringen af lovudkast har udvalget valgt at benytte udtrykket "udbredelse i en videre kreds", da dette udtryk i forvejen benyttes i straffeloven, jfr. § 266 b om racediskriminerende udta-lelser m.v."

Herudover er visse spørgsmål vedrørende informationsspredning behandlet i afsnit 3.2 om adgangsmidler.

Udvalget har alene set på informationsspredning i forhold til områder, hvor der ikke allerede er en strafferetlig regulering, og områder, hvor reguleringen er begrænset til f.eks. erhvervsmæssig spredning. Udvalget har ikke set på, om strafferammerne i andre bestemmelser, der vedrører informationsspred-ning, da spørgsmålet om strafferammer for tiden behandles i Straffelov-rådet.

3.2. Adgangsmidler

Som nævnt har udvalget valgt først at se på beskyttelsen af de passwords, koder m.v., der giver adgang til informationssystemer.

I takt med, at informationsudveksling er blevet til selve livsnerven i det mo-derne samfund, er der opstået et behov for at beskytte vitale eller følsomme informationer (som f.eks. erhvervshemmeligheder og personoplysninger) mod uberettiget adgang. Hvad enten denne beskyttelse gennemføres ved en kryptering af information eller på anden måde, er der behov for at reservere den for en berettiget personkreds. Denne reservation kan enten gennemfø-res ad logisk vej (f.eks. ved at systemer kræver indtastning af et password) eller gennem særlige tekniske midler (f.eks. ved indføring af et chipkort eller magnetkort i en læseenhed) eller ved en kombination heraf. Som samlet betegnelse for fysiske og logiske indretninger, der på sådan vis skaffer ad-gang til informationsmængder, der ellers ville være lukket af, benyttes i det følgende betegnelsen "adgangsmidler".

Adgangsmidlerne kan være sammenfaldende for alle brugere, som tilfældet f.eks. er ved dekoderkort eller andet dekodningsmiddel, eller kan være indi-viduelle koder (PIN-koder eller andet individuelt middel), hvis der af sikker-heds- eller betalingsmæssige grunde er behov for at regulere adgangen til sy-stemet og/eller registrere omfanget af brugerens adgang.

Udvalgets overvejelser har taget udgangspunkt i, hvorvidt der inden for følgende kategorier af adgangsmidler er behov for en særskilt strafferetlig beskyttelse:

1. Adgangsmidler til kommercielle informationstjenester. Der er her tale om abonnementsordninger, hvor der i forbindelse med abonnementet tildeles et særligt adgangsmiddel.

2. Adgangsmidler til konteringer i kommercielle systemer til elektronisk databehandling. Der er her tale om ydelser, der faktureres på baggrund af forbruget i fakturaperioden.

3. Adgangsmidler til ikke-kommercielle informationstjenester. Der er her tale om tjenester, der er reserveret for en lukket kreds, og som ikke ud-gør en del af det kommercielle marked.

4. Adgangsmidler til andre systemer til elektronisk databehandling. Der er her tale om et bredt område vedrørende systemer, der har

individuel adgangsbeskyttelse og er reserveret for enkeltbrugere eller en begrænset brugerkreds.

Den første gruppe omfatter udover visse radio- og tv-udsendelser f.eks. "on demand"-tjenester eller informationssamlinger, hvor der abonneres på brug af tjenesten, og hvor der i forbindelse med abonnementet tildeles et særligt adgangsmiddel.

Den anden gruppe omfatter kommercielle systemer, hvor adgangsmidlet, f.eks. et calling card eller en NUI-kode, er en konteringsoplysning til syste-met, der giver adgang til brug mod kontobelastning. Der er ikke nødven-digvis tale om beskyttede systemer, men om, at adgangsformen er kontore-lateret, således at ydelserne faktureres på baggrund af forbruget i fakturape-rioden.

Den tredie gruppe omfatter f.eks. informationssamlinger uden for det kom-mercielle marked, der kun er tilgængelige for en bestemt kreds, f.eks. med-lemmerne af en bestemt faglig organisation.

Den fjerde gruppe omfatter de beskyttede individuelle systemer, f.eks. en virksomheds databehandlingssystem eller en privat PC. Der er således tale om et meget bredt område, der alene er karakteriseret ved, at man ønsker at beskytte systemet mod uvedkommendes adgang.

Der vil kunne være sammenfald mellem gruppe 1 og 2 f.eks. i tilfælde, hvor betaling for brug af en kommerciel informationstjeneste afhænger af om-fanget af benyttelsen i stedet for at være en fast periodisk ydelse.

Tilsvarende vil gruppe 2 og 3 kunne være sammenfaldende, hvor en del af et system er en ikke-kommerciel informationstjeneste (f.eks. med forsk-ningsresultater eller markedsanalyser), der kun er tilgængelig for en bestemt kreds.

Gruppe 1 og 2 vil i sin i dag typiske form vedrøre systemer, der ikke alene er kommercielle, men er tilgængelige for alle mod betaling. Der er imidlertid teoretisk ikke noget i vejen for, at de kommercielle systemer kan være be-grænset til en bestemt kreds.

Der vil – i hvert fald teoretisk set – kunne være adgangsmidler, der konkret anvendes til alle 4 grupper.

Udvalget finder, at det bør være uden afgørende strafferetlig betydning, hvad der er det aktuelle adgangsmiddel, og drøftelsernes udgangspunkt har derfor været, hvad adgangsmidlet giver adgang til.

Udvalget finder, at en relevant sondring i denne forbindelse er, om der er tale om et adgangsmiddel til ikke-kommercielle eller til kommercielle infor-mationssystemer.

Udvalgets overvejelser vedrørende den strafferetlige beskyttelse af adgangs-midler har i øvrigt taget udgangspunkt i en sammenligning med fysiske nøg-ler: Efter gældende ret er det ikke i sig selv strafbart at besidde eller frem-bringe en nøgle eller dirk, selvom denne nøgle eller dirk vil kunne benyttes til at åbne en lås til områder, man ikke har lovlig adgang til. Spørgsmålet har derfor været, om der er forhold omkring de nye adgangsmidler, der gør, at der bør lægges en fremskudt strafferetlig beskyttelse – og om det i givet fald er nok, at man faktisk besidder adgangsmidlet, om man aktivt skal have skaffet sig det, eller om en eventuel udvidet beskyttelse kun skal vedrøre, at man distribuerer adgangsmidlet, og om det i givet fald kun skal være den er-hvervsmæssige distribution.

Udvalget har endvidere overvejet, om der bør være en særskilt strafferetlig regulering vedrørende midler til at tilvejebringe adgangsmidler.

Udvalget har i øvrigt ved sine overvejelser også taget hensyn til Europa-rådets konvention om IT-kriminalitet, jfr. afsnit 7.3 og bilaget.

3.2.1. Adgangsmidler til kommercielle informationssystemer m.v.

3.2.1.1. Radio- og tv-udsendelser

Spørgsmålet om kriminalisering af salg og brug af piratdekodere til radio- og tv-udsendelser blev gennem flere år drøftet, og salg af piratdekodere er i fle-re tilfælde anmeldt til politiet, der imidlertid manglede en klar hjemmel til at strafforfølge, jfr. nedenfor i afsnit 3.2.1.2.

De fleste sager om piratdekodere blev henvist til fogedforbud, og et sådant er blevet nedlagt i flere tilfælde, med mulighed for at straffe overtrædelse heraf efter retsplejelovens § 651. Forbudet vedrører normalt markedsføring og salg af programkort, der kan dekode de kodede signaler fra de aktuelle kanaler, og opgradering af allerede solgte programkort.

Som nævnt i afsnit 2.4 fik Danmark i 1997 en delvis regulering ved en æn-dring af lov om radio og fjernsynsvirksomhed. I loven indsattes som § 75 a:

> "Det er ikke tilladt i erhvervsmæssigt øjemed at fremstille, importere, omsætte, besidde eller ændre dekodere eller andet dekodningsudstyr, hvis formål det er at give uautoriseret adgang til indholdet af en kodet radio- eller tv-udsendelse. Annoncering eller anden form for reklame for sådant udstyr er ikke tilladt."

Loven dækker kun radio- og fjernsynsvirksomhed. Ifølge Berlingske Ti-dende 3/7 1998 og Jyllandsposten 6/7 1998 viste en undersøgelse fra Vil-strup Research, at 49% af brugerne af betalingskanalerne brugte piratde-koderkort. Ved en tilsvarende undersøgelse året før var tallet 37%. Der var bl.a. tale om en stigning i køb af blanke dekoderkort, der opdateres med ko-der, der hentes på Internettet.

Det fremgik af bemærkningerne til lovforslaget[35], at Kulturministeriet på det tidspunkt ikke fandt, at der var behov for at regulere hverken privat brug eller spredning via Internettet. Det fremgik endvidere, at der ikke i dansk ret fandtes et direkte forbud mod erhvervsmæssig omsætning m.v. af piratde-kodere og piratdekoderkort m.v.; det nævntes, at markedsføringslovens § 1 i et vist omfang gav mulighed for at gribe ind over for markedsføring og salg, men ikke gav et tilstrækkeligt sikkert retligt grundlag for at stoppe denne form for piratvirksomhed.[36]

---

[35] FT 1997/98 A 1245.

[36] Se om markedsføringsloven eksempelvis UfR 2001.287 H, hvor den tiltalte gennem ca. 10 måneder havde solgt kodede og blanke piratprogramkort til to satellitkanaler. Han blev dømt for at handle i strid med god markedsføringsskik, jfr. markedsføringslovens § 1, og pålagt at ophøre med markedsføring og salg. Han blev endvidere dømt til at betale er-statning til de to satellitkanaler på henholdsvis 15.000 kr. og 25.000 kr.

Det fremgik ligeledes af bemærkningerne til lovforslaget, at formuleringen dækker piratdekodere, piratdekoderkort og andet udstyr med samme for-mål. Som eksempler nævnes edb-programmer o.l., som alene eller sammen med andre anordninger kan anvendes til uautoriseret dekodning eller kortef-tergørelse, samt blanke dekoderkort med brugervejledning.

Som ligeledes nævnt i afsnit 2.4 ændredes bestemmelsen i 2000[37] således, at "i erhvervsmæssigt øjemed" udgik, dvs. at privat besiddelse og spredning via netsystemer nu også er omfattet. Straffebestemmelsen (§ 76 a) er samtidig ændret således, at den som udgangspunkt er en bødebestemmelse, men at der kan idømmes op til 6 måneders fængsel ved overtrædelser i erhvervs-mæssigt øjemed og ved udbredelse i en videre kreds.

Denne ændring harmonerer med dette udvalgs generelle holdning til krimi-nalisering af udbredelse i en videre kreds, jfr. afsnit 3.2, hvor udvalgets generelle holdning til dette spørgsmål, der er behandlet i delbetænkning II, er gengivet.

Den norske straffelovs § 262 giver, som nævnt i afsnit 2.5.2, mulighed for op til 1 års fængsel.[38] Den i afsnit 2.5.2 i noten til bestemmelsen nævnte dom, hvor den tiltalte blev idømt 8 måneders fængsel, ligesom bruttoind-tægten på 1.885.000 kr. blev konfiskeret, belyser, at det ikke kan betragtes som et område, der kun vedrører mindre omfattende kriminalitet.
Udvalget har ikke noget grundlag for at vurdere, om et strafmaksimum på fængsel i 6 måneder er tilstrækkeligt, og udvalget stiller derfor ikke noget forslag på dette område.[39]

---

[37] Lov nr. 446 af 31/5 2000.

[38] "Den som ved å bryte en beskyttelse eller på lignende måte rettsstridigt skaffer seg selv eller andre en vinning ved å få tilgang til fjernsyns- eller radiosignaler eller medvirker til det, straffes med bøter eller fengsel inntil 1 år. Det samme gjelder dersom den berettigede blir utsatt for tap."

[39] Vedrørende dansk retspraksis kan henvises til UfR 2000.714 Ø, hvor den tiltalte erhvervsmæssigt havde solgt 10 ulovlige dekoderkort og omprogrammeret 60. Hans fortje-neste var på ca. 16.000 kr., og han blev idømt en bøde på 16.000 kr. Erstatningskravet blev henvist til civilt søgsmål. Det siges i byrettens dom, at der ved straffastsættelsen er lagt vægt på tiltaltes fortjeneste, samt at han har optrådt som

3.2.1.2. Andre kommercielle informationstjenester

Andre kommercielle informationstjenester er som nævnt f.eks. "on demand"-tjenester (f.eks. videoer) eller informationssamlinger (f.eks. avisdata-baser), hvor der abonneres på brug af tjenesten, og hvor der i forbindelse med abonnementet tildeles et særligt adgangsmiddel.

EU-direktivet om retlig beskyttelse af adgangsstyrede og adgangsstyrende tjenester[40] anvender udtrykket "adgangsstyringsanordning" og definerer denne som et udstyr eller program, der er udformet eller tilpasset med hen-blik på at muliggøre adgang til en beskyttet tjeneste i forståelig form. Det siges i Kommissionens kommentar til det oprindelige forslag[41], at definitionen omfatter dekodere, omformningsanordninger (set-top boxes), smart-kort og alt andet udstyr, som alene eller sammen med andre anordninger er en forudsætning for, at tjenesten kan modtages i forståelig form. Direktivet dækker ikke alene radio- og tv-spredningstjenester, men også informations-samfundets tjenester, hvilket defineres[42] som enhver tjeneste, der normalt ydes mod betaling og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager. Direktivet er alene rettet mod den erhvervsmæssige piratvirksomhed.

Som eksempler nævnes i Kommissionens kommentar bl.a. elektroniske avi-ser og finansielle informationer, hvor der ventes en vækst på området, samt at der i den nærmeste fremtid ventes music-on-demand on-line. Senere for-ventes video-on-demand at kunne modtages på både

---

forhandler. Det siges i landsrettens dom: "Landsretten kan tiltræde, at et forhold som det foreliggende bør udløse en følelig bødestraf, der tager udgangspunkt i den opnåede fortjeneste." Der var ikke nedlagt på-stand om udbyttekonfiskation.

[40] Europa-Parlamentets og Rådets direktiv af 20/11 1998 (98/84), EFT L 1998 320/54.

[41] KOM(97)356 endelig udg., ændret ved kom.(1998) 332 endelig udg.

[42] Ved en henvisning til Europa-Parlamentets og Rådets direktiv af 22/6 1998 (98/34) om en informationsprocedure med hensyn til tekniske standarder og forskrifter samt forskrifter for informationssamfundets tjenester, EFT L 1998 204/37.

tv-apparater og com-puterskærme. Det er uden betydning, hvilket apparat modtageren bruger (tv, computer eller andet udstyr).

I direktivets betragtning 6 nævnes, at tjenesterne ofte kun vil være rentable, hvis tjenesteudbyderen kan sikres et vederlag ved hjælp af adgangsstyring, og at retlig beskyttelse af tjenesteudbydere mod ulovlige anordninger, der muliggør gratis adgang til disse tjenester, synes at være nødvendig for at sikre disse tjenesters økonomiske bæredygtighed.

Udvalget har drøftet, om der tillige bør reguleres vedrørende adgangsbe-skyttede informationstjenester, og om en eventuel regulering bør ske i straf-feloven.

Med hensyn til informationstjenester er det ikke i dag muligt at se, hvordan udviklingen på dette område vil blive, men det er formentlig et område, hvor der vil ske en markant udvikling i de kommende år.

Det kan diskuteres, om disse informationstjenester skal sidestilles med ud-sendelser (radio og tv). Udvalget har imidlertid fundet, at det, der i direk-tivforslaget beskrives som informationstjenester, adskiller sig væsentligt fra udsendelser, idet der er tale om individuelt bestilte ydelser og ikke om at vælge at se/høre noget, der, uanset om en mulig modtager deltager eller ej, formidles ensidigt. Informationstjenesterne har større lighed med benyttelse af telefonsystemer o.l.

Spørgsmålet om behov for strafferetlig beskyttelse opstår kun for de infor-mationstjenester, der er undergivet særlige brugerbegrænsninger. Piratvirk-somhed vil begrebsmæssigt forudsætte, at der er et betalingsmoment. Der kan imidlertid også tænkes informationstjenester, hvor der ikke skal betales for brugen, men hvor der kun er adgang for en særlig brugerkreds, og der kan således være en glidende overgang til de almindelige informationssyste-mer.

Udvalget har drøftet anvendelsen af de nugældende regler både i relation til anvendelsen af adgangsmidlet og til besiddelse m.v. af adgangsmidlet.

Såfremt adgangsmidlet til den aktuelle informationstjeneste er konterings-relateret, således at der betales for den konkrete anvendelse,

er situationen sammenfaldende med situationen ved calling cards og NUI-koder, jfr. ne-denfor i afsnit 3.2.1.3.

Såfremt der er tale om en fast betaling for ydelsen, kan situationen være den samme, som det tidligere var tilfældet i relation til piratdekodere til radio- og tv-udsendelser. Udvalget har under sit arbejde – forud for den seneste lov-ændring – overvejet anvendeligheden af anden lovgivning ved anvendelse af piratdekodere.

Udvalget har for det første overvejet, om det er dækket af straffelovens § 293 om brugstyveri. Bestemmelsen har været anvendt ved uberettiget tilslut-ning til fællesantenneanlæg[43], men anvendelsen bliver noget atypisk, hvis der skal statueres uberettiget brug af en satellit eller lignende, der ikke er mere central for gerningen end en telefonmast for uberettiget brug af telefon-systemet. Bestemmelsen har været forsøgt anvendt på brug af dekodere i en byretssag fra 1996[44], hvor der var rejst tiltale for gennem ca. 3 uger under anvendelse af et piratparabolkort uberettiget at have modtaget tv-signaler udsendt af et udbyderselskab. Retten udtalte, at det lagdes til grund, at den tiltalte var klar over, at han købte et såkaldt piratparabolkort, og at han ube-rettiget modtog signaler gennem en periode på ca. 3 uger via sin egen para-bolantenne. Det siges herefter: "Retten finder ikke, at tiltalte har gjort sig skyldig i uberettiget brug af ting tilhørende en anden, og han frifindes der-for."

Dernæst har udvalget overvejet, om det er dækket af straffelovens § 298 om uden erlæggelse af den fastsatte betaling at tilsnige sig adgang til forestilling, befordring m.v. eller til benyttelse af anden almentilgængelig indretning. Der kan selvfølgelig – bl.a. under henvisning til kravene om ikke-diskriminering m.v. i satellittjenestebekendtgørelsen[45] – argumenteres for, at der er tale om en almentilgængelig indretning, men "tilsniger" i den nævnte sammenhæng synes alene at vedrøre uberettiget fysisk ophold, således at bestemmelsen i givet fald skulle anvendes analogt. På baggrund af bl.a. den i afsnittene 2.4 og 2.6 nævnte Østre Landsrets dom af 13/2 1995, der gav anledning til æn-dring af straffelovens § 163, kan man ikke antage, at en domfældelse vil væ-re sandsynlig.

---

[43] Jfr. UfR 1978.1003 Ø.

[44] Rødovre rets dom af 6/12 1996.

[45] Bekendtgørelse nr. 265 af 21/4 1995.

En tredje mulig straffehjemmel kunne være bestemmelsen i ophavsretslo-vens § 78, som med bøde straffer den, som forsætligt eller groft uagtsomt omsætter eller i kommercielt øjemed besidder midler, hvis eneste formål er at lette ulovlig fjernelse eller omgåelse af tekniske indretninger, som måtte være anvendt til at beskytte et edb-program eller andre værker i digitaliseret form. Muligheden for at anvende denne bestemmelse forudsætter imidler-tid, at den angrebne anordning enten fremtræder som et edb-program eller som et værk i digitaliseret form. Om den første situation foreligger, beror på, hvilken karakter den pågældende spærreordning har. Det kan ikke ude-lukkes, at bestemmelsen i en række tilfælde vil dække indgreb i disse anordninger, men hidtil har bestemmelsen ikke været påberåbt i sådanne sager. Om bestemmelsen kan anvendes i relation til det transmitterede "værk i di-gitaliseret form" beror ligeledes på en fortolkning, som ikke kan anses for afklaret på nuværende tidspunkt. Ifølge lovmotiverne angår denne del af be-stemmelsen værker, der foreligger i digital form (f.eks. et elektronisk leksi-kon). Forarbejderne[46] har således ikke taget stilling til, om bestemmelsen og-så kan anvendes på værker, der transmitteres i digital form. Som nævnt er bestemmelsen endvidere begrænset til den kommercielle besiddelse og om-fatter således ikke brugerne.

Udvalget har ikke kendskab til, om der eksisterer eller vil komme infor-mationstjenester, hvor de tekniske løsninger må sidestilles med radio- og tv-udsendelser, og hvor ovenstående overvejelser derfor fortsat er relevante i relation til anvendelsen af adgangsmidlet.

De former for informationstjenester, udvalget er bekendt med, kræver, at tjenesten forud for hver anvendelse får en meddelelse, der viser, at der er tale om en legal bruger. Der vil således ved uberettiget brug af adgangs-midler, der ikke giver anledning til særskilte konteringer, være tale om situa-tioner, der minder om straffelovens § 298-situationer, jfr. ovenfor. Det anta-ges imidlertid vedrørende § 298, at hvis "tilsnigelsen" sker ved, at nogen – f.eks. en kontrollør – vildledes, finder bedrageribestemmelsen anvendelse, under forudsætning af, at der opnås uberettiget berigelse.[47] Bestemmelsen om databedrageri i straffelovens §

[46] FT 1994/95 A 1311.

[47] Jfr. bl.a. Hurwitz, Speciel Del s. 454.

279 a er udformet sådan, at der ikke stilles krav om, at en person disponerer på grund af en vildfarelse, men kun om, at systemet f.eks. får urigtige oplysninger, der medfører uberettiget beri-gelse. Det må derfor antages, at § 279 a også vil være anvendelig ved i hvert fald den overvejende del af de informationstjenester, hvor der ikke konteres for det konkrete forbrug, fordi tjenesteudbyderen ikke får indtægt fra en ny kunde, jfr. afsnit 4.5 om misbrug af andres teleforbindelser. I øvrigt vil be-stemmelserne om hacking kunne være anvendelige.

Udvalget finder, at spørgsmålet om strafferetlig beskyttelse af adgangen til informationstjenester bør afgøres på samme måde som den tilsvarende pro-blemstilling omkring calling cards, NUI-koder m.v., jfr. nedenfor.

Der henvises til afsnit 3.2.4 vedrørende reguleringens form.

3.2.1.3. Calling cards, NUI-koder m.v.

Calling cards er en almindelig betegnelse for telefonpinkoder (med eventuel tilhørende bruger-ID). Der er således ikke fysisk tale om et kort, men kun om en kode, der kan indtastes eller oplyses til en telefoncentral, hvorefter udgiften ved samtalen belastes den, der er retmæssig indehaver af pinkoden.

Også NUI-koder[48] og tilsvarende koder falder ind under begrebet. Det er også for disse koder til netadgang karakteristisk, at brugen belastes indeha-veren af den kode, der angives.

I de første telefonmisbrugsdomme vedrørende calling cards[49] var der for-hold, hvor folk var blevet franarret deres pinkode. Der dømtes for bedrageri i forbindelse med anvendelsen. Af den ene dom[50] fremgår, at pinkoden skulle oplyses til en person i forbindelse med samtalen.

---

[48] NUI står for Network User Identification. NUI-koden identificerer den bruger, hvis konto skal belastes for netværksbrugen.

[49] Silkeborg kriminalrets dom af 12/2 1993 og Aalborg rets dom af 1/9 1993.

[50] Aalborg-dommen.

Også calling cards udgør et område med stigende misbrug. Tilegnelsen er i nogle tilfælde sket ved hacking hos telefonselskaberne. Distributionen sker i vidt omfang via Internettet, enten ved en direkte og gratis videregivelse eller ved oplysninger om sælger og pris pr. calling card. Det er ikke ualmindeligt, at et calling card sælges gennem flere led, og at det eventuelt anvendes i fle-re af disse, før misbruget opdages, og koden udgår.

Spørgsmålet om strafbarhed opstår således i flere led: I relation til erhver-velse, anvendelse, videresalg og videregivelse.

For så vidt angår erhvervelsen vil der kunne straffes efter straffelovens § 264 c, hvis man er i stand til at bevise, at der har været forsæt i relation til, at calling cardet er tilvejebragt på en af de måder, der er omfattet af be-stemmelsen.

I Norge er det i en høyesterettskendelse af 6/12 1995[51] antaget, at der i en sådan situation kunne straffes for hæleri. Den domfældte, der havde købt calling cards, var i byretten dømt for forsøg på hæleri, og forsvareren gjorde gældende, at kortnumrene ikke kunne anses for "udbytte" i den norske straffelovs § 317's forstand. Det siges i Højesteretts kendelse, at PIN-ko-derne giver adgang til telefonselskabernes tjenester, og de har derved øko-nomisk betydning og er egnede til at blive disponeret over. En PIN-kode må derfor anses for udbytte i straffelovens § 317's forstand, når den hid-rører fra en strafbar handling.

Udvalget har i delbetænkning I[52] foreslået en hæleribestemmelse, der omfat-ter alle strafbare lovovertrædelser. Det har udtrykkeligt taget stilling til, at udbytte i form af information, der ikke er knyttet til et fysisk medie, ikke skal være dækket af bestemmelsen.[53] Der vil således ikke efter dansk ret kunne straffes efter den almindelige hæleribestemmelse, heller ikke efter gennemførelsen af udvalgets forslag om hæleri.[54]

---

[51] RT 1995.1872.

[52] Betænkning nr. 1371/1999 om bl.a. hæleri og anden efterfølgende medvirken.

[53] Betænkningen s. 81.

[54] Lov nr. 465 af 7/6 2001.

Den retstridige anvendelse af calling cards er i almindelighed strafbar. Som eksempler herpå kan nævnes:

> Roskilde rets dom af 19/12 1996
> I sagens forhold 16 var der rejst tiltale for medvirken eller forsøg på med-virken til overtrædelse af straffelovens § 279 a (databedrageri), subsidiært § 293 (brugstyveri), i forbindelse med, at den tiltalte havde videregivet en NUI-kode til en medtiltalt. Retten dømte (s. 249) for forsøg på data-bedrageri, da den tiltalte måtte regne med, at den medtiltalte ville benytte koden.[55]
>
> Odense rets dom af 4/7 1997
> Der var rejst tiltale og blev dømt for medvirken til databedrageri i et forhold, hvor den tiltalte sammen med andre havde solgt mindst 10 calling cards.
>
> Københavns byrets dom af 23/9 1997
> Der var i det ene forhold rejst tiltale for hæleri med hensyn til data-bedrageri, idet den tiltalte havde modtaget over 800 calling cards fra uiden-tificerede personer og dels selv anvendt dem, dels videresolgt for 100-600 kr. til mindst 52 personer, der via 111 calling cards foretog opkald for ca. 300.000 kr. Retten frifandt for hæleri under henvisning til, at det ikke var bevist, at de aktuelle calling cards var skaffet gennem databedrageri. Der dømtes for databedrageri ved den tiltaltes egen anvendelse af calling cards og medvirken til databedrageri ved andres anvendelse af calling cards, den tiltalte havde solgt til dem. Med hensyn til omfanget anførte retten, at det ikke med den til domfældelse fornødne sikkerhed kunne anses for bevist, at tiltalte selv eller de, han havde solgt calling cards til, havde misbrugt dem således, at samtlige tab, der hidrørte fra Danmark og fra calling cards, som fandtes i tiltaltes computer, kunne henføres til ham. Han dømtes derfor kun for det erkendte omfang, der er beskrevet som, at han selv i mindre omfang havde benyttet calling cards og havde videresolgt et mindre antal calling cards til 22 personer for ca. 4.750 kr.

For så vidt angår videresalget kan sælgeren næppe være i tvivl om, at hans ydelse kun har værdi, fordi den skal bruges til telefonmisbrug. Han må derfor kunne dømmes for medvirken eller forsøg herpå til det senere tele-fonmisbrug. Derimod er der ikke tilstrækkelig praksis til at bedømme, hvil-ke krav domstolene vil stille til forsættet. Ovennævnte dom af 23/9 1997 illustrerer problemerne med at afgrænse forbrydelsens omfang. Det er for det første uvist, i hvilket omfang den

[55] Konkret kendte den medtiltalte allerede koden.

enkelte modtager af et calling card vil anvende det. Dertil kommer, at de samme calling cards kan anvendes af flere personer, og modtagerne af calling cards videregiver dem eventuelt til andre – eventuelt i den form, at de lægges ud på Internettet. Det kan derfor være vanskeligt at afgrænse, hvad forsættet til (forsøg på) medvirken til data-bedrageri har omfattet (og dermed også at afgrænse, om der er tale om en sag, der på grund af sit omfang skal henføres under straffelovens § 286).

Hvad endelig angår videregivelse, hvor et eller flere calling cards er tilgænge-lige via Internettet, er det mere tvivlsomt, om domstolene vil statuere forsæt til den senere forbrydelse. Man kan derfor rejse det samme spørgsmål om en selvstændig kriminalisering af distribution og besiddelse som ved pass-words.

Udvalget finder, at der bør være en særskilt strafferetlig beskyttelse af calling cards, NUI-koder m.v.

Der henvises til afsnit 3.2.4 vedrørende reguleringens form.

3.2.2. Adgangsmidler til ikke-kommercielle informationssystemer

Beskyttelseshensynet ved kommercielle informationssystemer vedrører øko-nomiske interesser i relation til produkter, der allerede udbydes til salg på markedet.

Beskyttelseshensynene ved ikke-kommercielle informationssystemer kan være meget forskellige. I en række tilfælde vil der være tale om beskyttelse af privatlivets fred, men der vil også kunne være tale om beskyttelse af sam-fundsvigtige systemer, af erhvervs- eller forskningshemmeligheder, af en kommerciel IT-struktur m.v. Benyttelsen af adgangsmidlet vil typisk være en strafbar handling (hacking, industrispionage).

Spørgsmålet om den strafferetlige beskyttelse af passwords og andre ad-gangsmidler[56] til ikke-kommercielle informationssystemer havde en

[56] I det følgende bruges passwords som eksempel, men tilsvarende gør sig gældende for an-dre adgangsmidler. En beskrivelse af forskellige former for adgangskoder findes

anden karakter tidligere, da systemerne overvejende var stand alone maskiner eller interne netværk (netværk på en arbejdsplads eller inden for en organisation), hvor det overvejende var et spørgsmål om at sikre sig mod internes mis-brug. Heller ikke da hacking blev et fænomen, der gav anledning til en lov-ændring baseret på Straffelovrådets 1985-betænkning om datakriminalitet, var beskyttelsen af passwords et spørgsmål, der blev taget selvstændigt stil-ling til.

Udviklingen har imidlertid medført, at der i vidt omfang er adgang til infor-mationer fra åbne telefonforbindelser, hvor passwords er den eneste beskyt-telse. I dag er spørgsmålet derfor mere aktuelt. Dels anvendes edb i næsten alle sammenhænge. Der er allerede derfor en større mængde beskyttelses-værdige oplysninger i systemerne og en større afhængighed af, at systemerne fungerer kontinuerligt. Dels er der som nævnt en større netværksflade og ik-ke mindst i mange tilfælde en internetopkobling, der er tilsluttet netværket.

Den beskyttelse, der formuleredes i 1985 vedrørende hacking m.v. i straffe-lovens § 263, kriminaliserede det misbrug, der ønskedes forhindret, og for-mulerede en overbygning til kvalificerede forhold.

Det aktuelle spørgsmål i dag er, om der er behov for en yderligere frem-skudt regulering, der refererer sig direkte til passwordbesiddelsen og ikke er afhængig af, om der kan føres tilstrækkeligt bevis for forsøg eller forsøg på medvirken i relation til en senere kriminalitet.

Den omfattende edb-anvendelse gør systemindehaveren sårbar både med hensyn til de oplysninger, systemet indeholder, og med hensyn til, at syste-met fungerer kontinuerligt. Ethvert forsøg på angreb af systemet giver der-for anledning til bekymring. Ethvert angreb, hvor nogen har haft eller har fundet de rigtige passwords, er tabsgivende.[57] Der kan være tale om "en drengestreg", hvis en ung hacker kommer ind i systemet, og han lader det blive ved det. Men står man med et sårbart system, der er helt centralt for ens virksomhed, har man ikke

---

i IT-sik-kerhedsrådets vejledning af august 2001 om adgangskontrol til en hjemmeside (afsnit 3 om brugerautentificering).

[57] Der kan henvises til beskrivelsen i Roskilde rets dom af 19/12 1996, hvor der i hoved-forhold 2 vedrørende straffelovens § 193 i det ene forhold (a) nævnes, at et anlæg til 5.000 brugere måtte tages ud af drift i 9 dage, og i det andet (c), at indgrebet betød undersøgelse af 120 computere samt overvågning af systemet.

råd til at håbe på, at der ingen skade er sket. Der igangsættes derfor en bekostelig procedure, hvor det kontrolleres, om der har været tale om såkaldt malicious code (om der har været adgang til filer med erhvervshemmeligheder, passwords, o.l., om der er udøvet hærværk i form af sletninger, flytninger eller ændringer (herunder om der er sket noget tilsvarende ved en fejl), om der er indlagt virus, om der er indlagt logiske bomber, osv.).

Behovet for beskyttelse er klart, og der er da også en strafferetlig beskyttelse i straffelovens § 263, men den er ikke fremrykket til selve beskyttelsen af passwords. Og kan et videregående forsæt ikke bevises, er maksimumstraf-fen fængsel i 6 måneder, selv om gerningsmanden har været inde i systemet.

Når udgangspunktet imidlertid er, at man skal sørge for, at passwords kun er tilgængelige for indehaveren og eventuelt systemadministratoren, og at der ved en forsvarlig edb-organisation af en virksomhed jævnligt udskiftes passwords, kan man overveje, om der er behov for en strafferetlig be-skyttelse af "passwords på afveje".

Vurderingen heraf må foretages med udgangspunkt i udviklingen. Tidligere blev et password måske distribueret ved mund-til-øre metoden eller i en mindre kreds, der var tilsluttet et BBS (Bulletin Board System). I dag distri-bueres til hele verden via Internettet, nogle gange endda i hele passwordfiler i krypteret eller læsbar form, der er blevet kopieret i forbindelse med hacking.

Med den vældige udvikling, der har været og må forventes fortsat at være i IT-anvendelsen, og den afhængighed af, at systemerne fungerer, der følger med denne udvikling, har beskyttelsen af systemerne fået en ny samfunds-mæssig dimension.[58] Når denne samfundsmæssige IT-

[58] Dette gælder ikke mindst for systemer, hvor ændringer kan give livstruende situationer, som f.eks. systemer med oplysninger vedrørende flysikkerhed eller patientmedicinering. Som eksempel på det sidste kan nævnes en sag fra 1994 (refereret af Ulrich Sieber i afsnit II.D.1. i hans rapport af 1/1 1998 til EU Kommissionen: Legal Aspects of Computer-Related Crime in the Information Society). Sagen vedrørte en hacker, der brød ind i et hospitalssystem og bl.a. ændrede medicineringen, for en af patienternes vedkommende til en livstruende medicin. Baggrunden var blot, at han gerne ville se "what kind of chaos could be caused by penetrating the hospital computer".

afhængighed sam-menholdes med de muligheder, der er for at distribuere andres passwords, kan meget tale for at lægge den strafferetlige beskyttelse endnu tidligere end efter gældende ret.
Passwordtilegnelsen kan ske på flere måder. Passwordet kan f.eks. være op-lyst – på første, anden eller tredie hånd – fra en retmæssig indehaver af passwordet, fundet ved en tilfældighed, fundet ved gennemgang af virk-somhedens affald (dumpster diving), fundet på Internettet, hentet på Inter-nettet på et område med særlige adgangsbegrænsninger for "medlemmer" eller fundet via hacking. En særlig variant (social hacking eller social en-gineering) sås bl.a. i de tidlige sager om telefonmisbrug, hvor man franar-rede folk deres telefonpinkode (calling card) ved urigtigt at oplyse, at man ringede fra telefonselskabet. I senere eksempler har hackere forenklet tek-nikken ved i stedet – via Internettet – at oplyse brugere om, at de mid-lertidigt i forbindelse med systemændringer skulle ændre deres password til et bestemt angivet password.

I øvrigt er passwordsiden kun en del af det samlede kompleks, hvor der ofte samarbejdes i grupper, der står for hver deres del af arbejdet – f.eks. således at én sørger for telefonadgang, én for passwords og andre for den aktuelle hacking.

Hvis et password er tilegnet retsstridigt gennem hacking, jfr. straffelovens § 263, kan den, der skaffer sig eller uberettiget udnytter passwordet, straffes i medfør af straffelovens § 264 c, såfremt det fornødne forsæt kan bevises. Den uberettigede udnyttelse kan være hacking, der er kriminaliseret i § 263, eller f.eks. salg af passwordet.

I en større dansk hackersag[59] blev der bl.a. dømt for overtrædelse af straffe-lovens § 264 c, jfr. § 263, stk. 2, i forbindelse med downloading af pass-wordfiler fra BBS'er. Retten lagde til grund[60], at den tiltalte regnede med, at i hvert tilfælde langt de fleste af passwordfilerne hidrørte fra hacking i de pågældende edb-anlæg, og at uploading til den tiltaltes BBS, der var klart hackerrelateret, var sket efter opfordring fra ham. Retten dømte for forsøg i det omfang, det ikke var bevist, hvorfra passwordfilerne hidrørte.

---

[59] Roskilde rets dom af 19/12 1996, hovedforhold 5.

[60] Dommens s. 219 f.

I et andet forhold dømtes for forsøg på medvirken til overtrædelse af straf-felovens § 263, stk. 2, i forbindelse med, at den ene tiltalte på et område på sit BBS, hvortil især de medtiltalte havde adgang, videregav oplysninger om brugeridentiteter med tilhørende dekrypterede passwords med en udtryk-kelig opfordring til at prøve det ene anlæg og til ikke at skifte password, så-ledes at andre hackere kunne benytte det samme system.

Begge forhold vedrører situationer i en sag mod flere meget aktive hackere med tæt indbyrdes forbindelse. For så vidt angår hele passwordfiler vil der i almindelighed være en formodning for, at de hidrører fra hacking. Skulle de faktisk ikke gøre det, vil det formentlig ofte blive lagt til grund, at der er forsæt til overtrædelse af straffelovens § 264 c, og at der derfor kan dømmes for forsøg på overtrædelse af denne bestemmelse.

Derimod vil der formentlig i en række tilfælde af videregivelse af passwords ikke kunne dømmes for forsøg på medvirken i relation til den fremtidige eventuelle anvendelse af disse passwords til hacking. En videregivelse til en sluttet hackerkreds med direkte opfordring til brug eller i øvrigt videregivel-se, der klart er med henblik på anvendelse, må dog antages altid at kunne opfylde domstolenes beviskrav i sager om forsøg på medvirken, jfr. den i af-snit 2.7 refererede Roskilde rets dom af 19/12 1996.

Udvalget har på baggrund af udviklingen overvejet, om den eksisterende strafferetlige regulering er tilstrækkelig, eller om der bør være en særskilt strafferetlig regulering af såvel produktion, skaffelse, besiddelse og distri-bution af andres passwords.

Udvalget har overvejet, om man skal se problemstillingen som en variation over urigtige identitetsoplysninger, men udvalget har ikke fundet, at person-lige adgangsmuligheder kan sidestilles med identitetsoplysninger, ligesom der kun i særlige sammenhænge er pligt til at give korrekte identitetsoplys-ninger.

Udvalget har også overvejet, om passwords m.v. nyder beskyttelse som er-hvervshemmeligheder. Imod en sådan antagelse taler det, at et password har rent teknisk karakter (ganske som en fysisk nøgle) og dermed ikke i sig selv indeholder oplysninger om den pågældende

virksomheds drift. Udvalget har imidlertid ikke taget stilling til, om der efter omstændighederne kan anlæg-ges en så bred fortolkning af begrebet erhvervshemmeligheder, allerede for-di behovet for regulering også opstår i relation til f.eks. private og offentlige myndigheder, der ikke har erhvervshemmeligheder.

Der er enighed i udvalget om, at der bør være en fremrykket strafferetlig re-gulering vedrørende passwords.[61] Udvalget finder imidlertid, at den særlige beskyttelse bør begrænses til de situationer, hvor beskyttelsesbehovet er størst.

Der henvises til afsnit 3.2.4 vedrørende udvalgets afgrænsning af beskyttel-sen og reguleringens form.

3.2.3. Midler til tilvejebringelse af adgangsmidler

Udvalget har overvejet, om der tillige skal være en særskilt regulering vedrø-rende midler til tilvejebringelse af adgangsmidler. Sådanne midler kan have forskellig karakter, idet der kan være tale om midler, der udelukkende an-vendes uretmæssigt, midler, der overvejende anvendes uretmæssigt, og mid-ler, der tillige kan anvendes uretmæssigt.

Det vanskeliggør en strafferetlig regulering, hvis midlet i vidt omfang an-vendes i retmæssige sammenhænge.

Udvalget har nærmere overvejet nogle kendte midler, der kan illustrere pro-blemstillingerne.

Udvalget har for det første set på cracker-programmer.[62]

---

[61] Alle medlemmer af arbejdsgruppen vedrørende datakriminalitet var også enige om en re-gulering på dette område.

[62] Alle medlemmer af arbejdsgruppen vedrørende datakriminalitet var enige om, at en regu-lering vedrørende crackerprogrammer ville forudsætte, at det var muligt klart at adskille lovlige forhold fra ulovlige forhold i de tilfælde, hvor midlerne også anvendtes lovligt. Et flertal i arbejdsgruppen (Mads Bryde Andersen, Jan Carlsen, Jan Friis, Michael Goeskjær, Carsten Heilbuth, Ulla Høg, Ole Stampe Rasmussen, Kim Aarenstrup) fandt, at en straffe-retlig regulering vedrørende crackerprogrammer har en så naturlig sammenhæng med be-skyttelsen af passwords, at også crackerprogrammer bør være omfattet af reguleringen. Et mindretal i arbejdsgruppen

I den tidligere nævnte store hackersag[63] var der i 2 forhold rejst tiltale for overtrædelse af straffelovens § 263, stk. 3, jfr. stk. 2, ved videreudvikling og overdragelse af et crackerprogram, dvs. et program, der – i kombination med ordbogsfiler, typisk hentet fra Internettet – kan knække pass-words/bryde en passwordkryptering. Retten frifandt med følgende præmis-ser:

> "Retten finder, at udarbejdelse, overladelse eller benyttelse af et cracker-program kan indgå som et forberedende led i en uberettiget indtrængen i et edb-anlæg, d.v.s. en overtrædelse af straffelovens § 263, stk. 2, eller det kan være medvirken til andres overtrædelse af bestemmelsen. Dette forud-sætter dog, at der er forsæt til, at udarbejdelsen, overladelsen eller benyt-telsen fører til en nærmere bestemt uberettiget indtrængen i bestemte edb-anlæg, mens det ikke er nok, at det måtte kunne lægges til grund, at hand-lingen – overvejende sandsynligt – sker med henblik på hacking generelt. Noget andet måtte forudsætte, at udviklingen m.v. af cracker-programmer blev selvstændigt kriminaliseret, svarende til våbenbesiddelse i forhold til voldsforbrydelser."

Det siges i pressemeddelelsen af 19/12 1996 fra retten i Roskilde, at frifin-delsen svarer til, når det i retspraksis er fastslået, at en rocker med skarplad-te skydevåben som udgangspunkt ikke bliver straffet for forsøg på vold, men for ulovlig våbenbesiddelse. Der er blot ingen lov, som gør besiddelse af crackerprogrammer ulovlig.

Det antages, at der ikke kan straffes efter § 263, før cracker-programmet anvendes, men de almindelige forsøgsbestemmelser kan anvendes, når pro-grammet udarbejdes med et konkretiseret forsæt til den senere brug, her-under at det er tilstrækkeligt konkretiseret, hvis passwords der fremfindes.

(Hans Jakob Paldam Folker, Helle Jahn, Jens Kruse Mikkelsen, Ronald Pedersen) kunne ikke tilslutte sig en kriminalisering på dette område ud over, hvad der følger af reglerne om forsøg og medvirken. I en situation, hvor der i mange tilfælde kan være saglige – og lovlige – grunde for at skaffe sig disse programmer, er det efter disse medlemmers opfattelse ikke rigtigt generelt at kriminalisere udvikling og anskaffelse m.v. af crackerprogrammer med forbehold for tilfælde, hvor dette er "uberettiget" eller "ret-stridigt".

[63] Roskilde rets dom af 19/12 1996.

Som ved adgangsmidler til informationssystemer kan det overvejes, om be-siddelse og distribution af crackerprogrammer skal kriminaliseres særskilt. Spørgsmålet har været behandlet i IT-Sikkerhedsrådet på baggrund af dom-merens udtalelse i ovennævnte sag. IT-Sikkerhedsrådet fandt ikke på det tidspunkt[64], at der skulle ske en regulering, idet der også kunne være lovlige praktiske anvendelsesformer for sådanne programmer, f.eks. i tilfælde hvor den lovlige bruger af et passwordbeskyttet system har glemt sit password. IT-Sikkerhedsrådet har den 27/6 2001 afgivet en ny udtalelse om spørgsmå-let, jfr. senere i dette afsnit.

Udvalgt har specielt forholdt sig til programmer som Back Orifice. Pro-grammet er beregnet til fjernbetjening af IT-systemer. Det giver mulighed for, at en gerningsmand kan gøre stort set alt, den lovlige bruger kan gøre, herunder kontrollere passwords, krypteringsprogrammer m.v. Det instal-leres i forbindelse med åbning af programmer, hvori det er placeret som en skjult del.

Programmets lovlige brug er begrænset til brugere, der har installeret det på deres eget system for at kunne fjernbetjene det.

Uberettiget installation af programmet kan straffes som hacking efter straf-felovens § 263, stk. 2, jfr. UfR 2000.1450 Ø[65] (sagen vedrørte et fuldbyrdet forhold, hvor den tiltalte havde tilegnet sig en andens brugeridentitet og password, og et forsøg, hvor forsøget var mislykkedes på grund af et instal-leret anti Back Orifice program; den tiltalte fik bl.a. sin computer konfiske-ret) og Frederikshavns rets dom af 4/4 2000 (vedrørende 5 forsøg og 1 fuldbyrdet forhold).

Udvalget har endelig set på de frontpaneler, der har været anvendt på Dan-kortautomater, og tilsvarende installationer ved f.eks. benzintanke med kort-betaling. (Tilsvarende vil kunne anvendes ved f.eks. togstationers billetau-tomater eller andre steder med mulighed for kortbetjenening). For så vidt angår frontpaneler til Dankortautomater er der tale om en ekstra front, der er påmonteret tastatur, kortlæser og registreringsenhed. Dankortautoma-terne m.v. kan anvendes almindeligt af kunden, men PIN-kode og magnet-strimmeloplysninger

---

[64] IT-Sikkerhedsrådets skrivelse af 10/6 1997 til Forskningsministeren.

[65] Det fremgår ikke af den trykte dom, at programmet er Back Orifice.

gemmes i registreringsenheden. Disse oplysninger kan derefter bruges til at producere falske betalingskort, der kan anvendes med rette PIN-kode i hæveautomater.[66] Her vil produktion af middel, montering af det og besiddelse og udnyttelse af oplysningerne kunne være led, der varetages af forskellige personer. Dette kan især tænkes i sammenhæng med organiserede former for kriminalitet, hvor det på grund af et personopdelt kriminalitetsforløb kan have betydning, at alle led i processen er klart krimi-naliserede. Uanset der eventuelt kan dømmes for forsøg på medvirken til (et eller andet) bedragerisk forhold samt til uretmæssigt at skaffe sig beta-lingskortnumre og pinkoder, kan det overvejes tillige at have en direkte regulering.

Tilsvarende tekniske indretninger eller andre midler kan tænkes i sammen-hænge, der ikke er direkte relateret til betalingskriminalitet, men har til for-mål at få passwords til andre informationssystemer.

Særligt vedrørende tilegnelse af oplysninger fra betalingskort bemærkes, at udviklingen går mod at anvende chipkort i stedet, og at det derfor om få år ikke, som ved magnetstrimmelløsningerne, vil være muligt at tilegne sig an-vendelige oplysninger ved hjælp af frontpaneler m.v. For Dankortets ved-kommende er pengeinstitutterne allerede meget langt i denne udvikling, jfr. Finansrådets plan "Fremtidens kortmarked" fra maj 2000.[67] Se også Kon-kurrencestyrelsens rapport om betalingsmiddelloven fra juni 2001 "Konkur-renceforholdene på betalingskortmarkedet 2001", der nærmere gennemgår udviklingen og bl.a. omtaler[68] initiativerne vedrørende klargøring af infra-strukturen til modtagelse af chipkort.

IT-Sikkerhedsrådet har den 27/6 2001 afgivet en udtalelse til brug ved ud-valgets overvejelser omkring en strafferetlig regulering. Det siges i denne udtalelse:

> "Det spørgsmål, jeg har forelagt rådet, er om det er praktisk-teknisk-ter-minologisk muligt at afgrænse visse typer af "hackerværktøjer" fra

---

[66] I den i afsnit 2.7 refererede UfR 2000.1881 Ø, hvor de falske kort havde forbindelse til kort, der havde været anvendt i en bank i Moskva, blev der peget på, at der kunne være tale om anvendelse af et sådant frontpanel.

[67] http://www.finansraadet.dk.

[68] Rapporten s. 44 f.

andre ud fra et kriterium om, at der er tale om programmer mv., der i praksis udelukkende – eller stort set udelukkende – kan anvendes til retsstridig indtrængen i IT-systemer mv.

IT-Sikkerhedsrådet har drøftet problemstillingen under sine møder den 29. maj og 21. juni d.å., og som jeg kort orienterede om under arbejds-gruppens møde den 31. f.m. kunne rådet ikke opnå fuldstændig enighed om sit svar. Den overvejende opfattelse i rådet var, at en sådan afgræns-ning ikke er mulig, selv om man kan nære sympati for den procesbe-sparelse, der kan ligge i således at fremrykke fuldbyrdelsesmomentet for bl.a. bestemmelsen i straffelovens § 263, stk. 2. Men rådet har delt sig i spørgsmålet, idet et mindretal finder, at det er både praktisk muligt og for-svarligt at foretage en sådan afgrænsning af et område for besiddelse, der som sådant bør være kriminaliseret.

Baggrunden for flertallets betænkelighed er følgende overvejelser:

Den første overvejelse ligger måske en anelse uden for rammerne af det stillede spørgsmål. Den knytter sig nemlig ikke så meget til de pågældende værktøjers tekniske beskaffenhed men snarere til de psykologiske motiver, der kan ligge bag gerningsmandens besiddelse af dem. Selv om der ikke kan føres bevis herfor kan det ikke udelukkes, at der i visse IT-miljøer sy-nes at være en særlig følelse forbundet med selve dette at være i besiddelse af programværktøjer, der rummer *potentialet* for retsstridige handlinger. Også selv om disse værktøjer der fra en umiddelbar betragtning kun synes at give brugeren mulighed for at foretage noget retsstridigt, kan tænkes anvendt – eller i det mindste opbevaret – på måder, der ikke vil bringe besidderen i nærheden af en straffelovsovertrædelse. Opfattelsen kan for så vidt svare til den, man finder hos våbensamlere mv., hvor besiddelsen – inden for våbenlovens grænser – af "værktøjet" er gjort ulovlig i sig selv. Men hvor man typisk vil vide, hvornår man har et våben i sin besiddelse, kan man meget vel tænkes at komme i besiddelse af de nævnte værktøjer, uden (fuldt ud) at kende deres potentiale.

Hertil kommer imidlertid et forhold, der spiller ind med en særlig vægt i vurderingen af det stillede spørgsmål. For ganske mange brugere, der vel at mærke ikke har forsæt til at begå kriminelle handlinger, kan der være en betydelig nyttevirkning forbundet med at kunne anvende sådanne værk-tøjer, der i øvrigt rummer potentialet til at skaffe sig retsstridig adgang til IT-systemer. En sådan anvendelse kan således give indblik i, hvorledes sådanne retsstridige handlinger undgås.

Som nævnt indledningsvis har de fremhævede forhold ikke umiddelbart adresse til det stillede spørgsmål, idet de snarere knytter

sig til forholdene omkring besiddelsen af de nævnte værktøjer. Til disse overvejelser kom-mer imidlertid en række betænkeligheder af praktisk-teknisk art.

For det første vil det være vanskeligt at foretage nogen afgrænsning af, hvad det nærmere bestemt er for værktøjer, der i givet fald vil skulle for-bydes. Et forbud rettet mod bestemte *programmer* (defineret gennem varemærke eller anden produktbetegnelse) vil ramme alt for bredt og også forbyde funktionaliteter i disse programmer, der ingen relation har til det, man ønsker at forbyde. Således indeholder de fleste hackerværktøjer flere – for så vidt lovlige – funktionaliteter ved siden af de, der må formodes tiltænkt retsstridig anvendelse. Som eksempel kan det nævnes, at det navn-kundige *Back Orifice*-program, der må siges at være et eksempel på et pro-gram med i hovedsagen ulovlige anvendelsesformer, udadtil fremtræder som et program, der gør det muligt for brugeren at betjene sit udstyr fra en fremmed terminal.

Skulle man derimod – omvendt – vælge at regulere ud fra værktøjernes funktionalitet, må det erkendes, at der vil være endog meget store van-skeligheder forbundet med at foretage en afgrænsning af de former for funktionalitet, som man måtte ønske at ramme. Ganske mange af de funk-tioner, der i deres kombination fremstår som et tilsyneladende retsstridigt værktøj, vil således hver for sig kunne rumme helt sædvanlige ingredienser i et styresystem eller et programværktøj. Det skyldes netop kombinationen – som alt efter programmørens ønsker kan kombineres på en mangfol-dighed af måder – at programværktøjet får dette "retsstridige præg". En beskrivelse af området for et forbud vil således være forbundet med sær-deles store vanskeligheder. Forholdet adskiller sig således mærkbart fra de programmer, der findes til at omgå kopispærre-anordninger, og som har ført til en særlig regulering, bl.a. i ophavsretslovens § 78. Sådanne anord-ninger kan kun udføre denne ene funktion.

Selv om det imidlertid skulle kunne lade sig gøre at foretage en præcis afgrænsning af de hackerværktøjer, som ønskes omfattet af en strafferetlig regulering med en form for fremrykket fuldbyrdelsesmoment, vil der efter flertallets opfattelse være så store praktiske vanskeligheder ved at følge en sådan regulering til dørs gennem effektiv håndhævelse, at et forsøg af den-ne art må mødes med betænkelighed. Mulighederne for at placere den slags værktøjer på internettet (f.eks. fra en lukket hjemmeside eller lignen-de) er så enkle, at gerningsmanden uden vanskelighed kan sikre sig, at værktøjet aldrig er i hans "besiddelse" udover de gange, han benytter det. Også muligheden for at kryptere værktøjet til ukendelighed (når dette ikke benyttes) vil gøre en effektiv retshåndhævelse særdeles vanskelig.

> Disse medlemmer har stor sympati for bestræbelserne for at opdatere straffeloven, således at den sikrer et effektivt værn mod de forbrydelses-former, som det digitale samfund frembyder. Men af de nævnte grunde kan de ikke anbefale, at man kriminaliserer besiddelsen af programværk-tøjer med det nævnte potentiale for retsstridig indtrængen i IT-systemer.
>
> Et mindretal i rådet (Jan Carlsen) mener, at det trods de anførte betænke-ligheder er muligt at nå frem til en beskrivelse af visse typer af værktøjer, om hvilke det kan siges, at den blotte besiddelse afgiver en så stærk for-modning for et kriminelt forsæt, at der er grundlag for at forbyde besid-delsen som sådan, medmindre de pågældende kan godtgøre et legitimt for-mål med besiddelsen. Dette medlem peger på, at man i visse steder i lov-givningen, herunder navnlig i ophavsretslovens § 78, har gjort tilsvarende forsøg på at nå frem til at kriminalisere besiddelsen af et programværktøj baseret på dets formodede funktionalitet. Den pågældende bestemmelse henviser herved til "midler, hvis eneste formål er at lette ulovlig fjernelse eller omgåelse af tekniske indretninger, som måtte være anvendt til at beskytte et edb-program", uanset det – ud fra synspunkter som dem, fler-tallet gør gældende – netop i ophavsretten må siges at være noget nær umuligt at konstatere, hvornår en sådan fjernelse er ulovlig, eftersom ophavsretsloven giver brugeren en præceptivt beskyttet ret til at foretage sikkerhedskopiering mv. Dette medlem ser derfor ikke noget problematisk principielt skridt ved at gøre noget tilsvarende i relation til straffelovens §§ 193, 263 og 291 og foreslår, at tilsvarende besiddelse kriminaliseres i relation til programværktøjer, hvis eneste formål det er at opnå funktio-nalitet til:
>
> 1. sniffning (aflytning) af kommunikationslinier,
> 2. opsamling af og/eller gætning af passwords, PIN-koder, telefonnumre
>   og andre identifikationer og lign., samt
> 3. udarbejdelse og/eller massedistribution af virus."

Udvalget har lagt til grund, at værktøjer som de ovennævnte er almindelige værktøjer for IT-sikkerhedsansvarlige i større virksomheder m.v.

Udvalget finder på baggrund af IT-Sikkerhedsrådets udtalelse samt udvik-lingen i retning af anvendelse af chipkort, at området er uegnet

til særskilt strafferetlig regulering, og at behovet herfor i løbet af få år vil blive reduceret væsentligt i takt med udviklingen.[69]

3.2.4. Reguleringens indhold og form

Som det fremgår af de forudgående afsnit, er et af udvalgets grundlæggende synspunkter, at der i dag ligger en så væsentlig interesse i at beskytte IT-samfundet mod uberettigede angreb, at hensynet hertil kan begrunde, at der i et vist omfang etableres en meget tidlig strafferetlig beskyttelse.

Som nævnt kan adgangsspørgsmålet løses teknisk på mange måder, og der er en stor udvikling inden for området, der må tages hensyn til ved formu-leringen af en eventuel bestemmelse. Udvalget er ikke bekendt med, i hvilket omfang der uden for radio- og tv-udsendelser anvendes dekodere til forskellige tjenester. Formentlig er situationen den, at de forskellige øvrige adgangsregulerede betalingstjenester lige så godt kan være styret med smart-cards, passwords eller andet som med dekodere.

Udvalget finder på den baggrund ikke, at der skal eller kan formuleres en helt klar afgrænsning af, hvilke adgangsmidler der beskyttes. Der er en sta-dig udvikling i adgangsmidler, og en oplistning af midler må derfor forven-tes med noget nær absolut sikkerhed at ville betyde, at der løbende skal æn-dres i en bestemmelse, og at den strafferetlige regulering vil komme til at halte bagud. Med den udvikling der er, vil der selvfølgelig, uanset hvilken formulering der vælges, være en risiko herfor, men udvalget har tilstræbt at finde formuleringer, der er rimeligt fremtidssikrede.

Udvalget har lagt vægt på, at uberettiget brug af adgangsmidler vedrører meget forskelligartede forhold, og at IT-udviklingen byder på

---

[69] Et flertal i arbejdsgruppen om datakriminalitet (Jan Carlsen, Jan Friis, Michael Goeskjær, Carsten Heilbuth, Ulla Høg, Ole Stampe Rasmussen, Kim Aarenstrup) fandt, at der også bør være en direkte strafferetlig regulering vedrørende midler (f.eks. frontpaneler) til tileg-nelse af passwords. Disse medlemmer ser dette som et naturligt led i beskyttelsen af infor-mationssystemer. Et mindretal (Mads Bryde Andersen, Hans Jakob Paldam Folker, Helle Jahn, Jens Kruse Mikkelsen, Ronald Pedersen) fandt, at de gældende regler om forsøg og medvirken udgør en tilstrækkelig strafferetlig regulering på dette område.

stadig flere integrerede løsninger. Det er bl.a. derfor ikke en egnet løsning at lægge en fremskudt beskyttelse knyttet til f.eks. et password eller et smartcard, der kun regulerer adgangsmidlet i relation til visse former for brug. De pro-blemstillinger, der kan være knyttet til integrerede IT-løsninger, har således ikke betydning for udvalgets vurdering af, hvad der bør være strafbart, men alene for, hvordan straffebestemmelsen eller -bestemmelserne foreslås for-muleret.

Udvalget har også vedrørende denne regulering lagt særlig vægt på, at spred-ning via Internettet, eller i øvrigt i en videre kreds, bliver klart reguleret.

Det er udvalgets grundlæggende vurdering, at den strafferetlige beskyttelse mod IT-relateret kriminalitet skal tage udgangspunkt i, hvilken risiko der er for, at offeret lider skade, og ikke alene i hvad gerningsmanden opnår af fordele.

Vedrørende strafferammer er det udvalgets vurdering, at det er væsentligt, at de straffebestemmelser, der regulerer (eller tillige regulerer) IT-relateret kriminalitet, viser, at kriminaliteten opfattes som alvorlig.

Udvalget har overvejet, om reguleringen bør ske i en samlet bestemmelse eller i flere bestemmelser. Udvalget har valgt den løsning, at adgangsmidler til kommercielle informationssystemer reguleres i én bestemmelse (den foreslåede § 301 a, jfr. afsnit 8.1.1) og adgangsmidler til ikke-kommercielle informationssystemer i en anden bestemmelse (den foreslåede § 263 a, jfr. afsnit 8.1.2). Denne opdeling og placering indgår naturligt i straffelovens systematik.

Udvalget har valgt udtrykket "informationssystemer" frem for det i straffe-lovens § 263, stk. 2, benyttede udtryk "anlæg til elektronisk databehandling" for at vælge et udtryk, der er neutralt i forhold til mulige teknologiske løsninger. I udtrykket ligger samtidig en afgrænsning mod adgang til en "udsendelse", jfr. afsnit 3.2.1.1 om radio- og tv-udsendelser, hvor man ikke kan vælge arten af ydelsen og (i hvert fald ikke for tiden) tidspunktet for den, men alene, om der skal åbnes for den igangværende udsendelse.

Ved kommercielle informationssystemer (informationstjenester) forstås i denne sammenhæng systemer, hvortil adgangen er forbeholdt for betalende brugere, og som er beskyttet med kode eller anden særlig adgangsbegræns-ning. Uden for den foreslåede kriminalisering falder systemer, hvor enhver ved henvendelse gratis kan få tildelt et adgangsmiddel, og hvor hensynet til udbyderens berettigede interesse i at få betaling for sin ydelse derfor ikke gør sig gældende.[70]

For så vidt angår kommercielle informationssystemer finder udvalget, at den fremrykkede strafferetlige beskyttelse bør omfatte den, der retsstridigt skaf-fer sig eller videregiver en eller flere koder eller andre adgangsmidler til sådanne tjenester. En sådan kriminalisering vil betyde, at der vil kunne straffes, selv om adgangsmidlet endnu ikke er anvendt, og selv om der ikke kan føres bevis for forsøg på at anvende adgangsmidlet.

Den blotte besiddelse er ikke omfattet af den foreslåede bestemmelse. For at kunne straffe kræves det, at den pågældende har skaffet sig eller videregivet koden eller andet adgangsmiddel. Såfremt den pågældende uden selv at have udvist aktivitet med henblik på dette modtager andres adgangskoder, vil dette ikke være omfattet, medmindre den pågældende herefter videregiver koderne. Tilsvarende gælder, hvis adgangskoder skaffes ved en handling, der ikke er retsstridig, f.eks. som led i en systemadmini-strators arbejde, eller hvis andre er villige til at videregive deres adgangs-koder (uden at dette skyldes en fremkaldt vildfarelse hos den pågældende som ved social engineering o.l.). Udvalget er opmærksom på, at det vil kunne give anledning til bevisproblemer, at den blotte besiddelse ikke er tilstrækkelig, og at en regulering som den, der er valgt ved den seneste ændring af radio- og fjernsynsloven, jfr. afsnit 2.4 og 3.2.1.1, er enklere at anvende i praksis. Udvalget finder imidlertid, at en kriminalisering af den blotte besiddelse vil være for vidtgående, og antager, at det i de tilfælde, der især kan være behov for at ramme, vil være muligt at bevise, at der

[70] Som eksempel på et grænseområde kan nævnes aktiehandel via Internettet, hvor børs-mæglere tildeler passwords, der giver mulighed for at benytte deres ordresystem. Tildeling af password er her primært udtryk for, at den potentielle kundes adresse er verificeret ved tilsendelsen af password med post. Jfr. bl.a. Helen Holdt i artiklen "Aktiehandel udøvet via Internet", Nordisk Årbog for Retsinformatik, 1997, s. 92.

ikke er tale om en situation, hvor den pågældende passivt har modtaget oplysnin-gerne udelukkende på baggrund af en anden persons initiativ.

For så vidt angår videregivelse bemærkes, at hvis man f.eks. ikke er bekendt med, at andre har indlagt oplysninger om passwords til et kommercielt informationssystem på ens webside, kan man ikke straffes for videregivelse. Det kan man derimod, hvis man efter at være blevet opmærksom på forhol-det ikke sletter eller forhindrer adgang til de pågældende oplysninger. Denne passivitet kan således anses for en videregivelse. Denne fortolkning svarer til, hvad der gælder om formidleransvar for tjenesteydelser efter EU-direk-tivet om elektronisk handel.[71]

Ikke-kommercielle informationssystemer dækker over en mangfoldighed af forskellige systemer, spændende lige fra private pc'ere og systemer, der er reserveret for enkeltbrugere eller en begrænset brugerkreds, over virksom-heders interne informationssystemer, til store centrale systemer i erhvervs-livet eller i den offentlige sektor. For så vidt angår adgangsmidler til sådanne ikke-kommercielle informationssystemer, har udvalget valgt at afgrænse den fremrykkede kriminalisering, således at den som udgangspunkt omfatter erhvervsmæssigt salg, udbredelse i en videre kreds samt videregivelse af et større antal passwords eller andre adgangsmidler. Som udgangspunkt er det at besidde eller skaffe sig passwords eller andre adgangsmidler til ikke-kommercielle informationssystemer således ikke omfattet. Det samme gæl-der videregivelse af et enkelt eller nogle få passwords. I disse tilfælde gives der således som udgangspunkt ikke en strafferetlig beskyttelse, der ligger tidligere end det tidspunkt, hvor der kan dømmes for forsøg på f.eks. hacking.

For så vidt angår de ikke-kommercielle informationssystemer, der må anses for særlig beskyttelsesværdige, bør der dog efter udvalgets opfattelse gælde den samme strafferetlige beskyttelse som den, der gælder for de kommer-cielle informationssystemer. Der sigtes herved til de samfundsvigtige infor-mationssystemer og til informationssystemer, der indeholder særlig person-følsomme

[71] Europa-Parlamentets og Rådets direktiv af 8/6 2000 om visse retlige aspekter af infor-mationstjenester, navnlig elektronisk handel, i det indre marked (2000/31/EF), EFT L 2000 178/1.

oplysninger. Udvalget foreslår, at det gøres strafbart at skaffe sig eller at videregive et eller flere passwords eller andre adgangsmidler til så-danne informationssystemer.

Strafansvar for overtrædelse af de foreslåede bestemmelser kræver forsæt, jfr. straffelovens § 19. Der kræves således forsæt til salg, udbredelse, videregivelse m.v. og til, at der er tale om adgangsmidler til informations-systemer. Der kræves derimod ikke forsæt til en efterfølgende uberettiget brug af adgangsmidlet.

Med hensyn til forholdet mellem de foreslåede nye bestemmelser og muligheden for at anse befatningen med adgangsmidlet som forsøg på (medvirken til) en videregående kriminalitet bemærkes følgende:

Såfremt betingelserne for at straffe for forsøg i relation til anden kriminalitet er opfyldt, vil der uanset de foreslåede nye bestemmelser i § 263 a og § 301 a fortsat kunne dømmes efter forsøgsreglerne. Dette gælder, uanset om den pågældende forsøgshandling i det hele falder uden for anvendelsesområdet for de foreslåede nye bestemmelser, eller om handlingen isoleret set måtte være omfattet af en af de nye bestemmelser som en fuldbyrdet forbrydelse.

Selv om udbredelse via Internettet af et password til en anden persons bankkonto isoleret set indebærer en fuldbyrdet overtrædelse af den foreslåede nye bestemmelse i § 263 a, stk. 1, vil der således kunne straffes for forsøg på medvirken til f.eks. databedrageri (§ 279 a), hvis et sådant videregående forsæt kan bevises.

På samme måde vil der som hidtil kunne straffes for forsøg på hacking (§ 263), hvis en person skaffer sig et password til en virksomheds interne informationssystem med forsæt til uberettiget at trænge ind i systemet. Dette gælder uafhængigt af, om dette forhold i det hele måtte falde uden for anvendelsesområdet for den foreslåede bestemmelse i § 263 a, hvor forskaf-felsen kun er strafbar som en selvstændig forbrydelse, hvis der er tale om et samfundsvigtigt informationssystem eller et system, der indeholder person-følsomme oplysninger.

For så vidt angår midler til tilegnelse af adgangsmidler finder udvalget på baggrund af IT-Sikkerhedsrådets udtalelse samt udviklingen i retning af anvendelse af chipkort, at området er uegnet til særskilt

strafferetlig regulering, og at behovet herfor i løbet af få år vil blive reduceret væsentligt i takt med udviklingen.

Der henvises til afsnit 8.1 vedrørende udvalgets forslag.

3.3. Straffelovens § 263, stk. 2

Udvalgt har dernæst inden for området med informationskrænkelser set på strafferammen i straffelovens § 263, stk. 2, om hacking. Udvalget har i den forbindelse set på, om straffelovens § 263, stk. 3, kan antages at dække alle situationer, hvor der er behov for at have et højere strafmaksimum end fængsel i 6 måneder.

Der er ikke mange fortolkningsbidrag til bestemmelsen i strfl. § 263, stk. 3, om "eller under andre særlig skærpende omstændigheder". Det siges i Straffelovrådets betænkning nr. 1032/1985 om datakriminalitet[72], at det kan være vanskeligt præcist at angive, hvad der bør kunne medføre strafskær-pelse, samt at rådet bl.a. har haft tilfælde for øje, hvor en udnyttelse eller videregivelse af oplysningerne kan være forbundet med betydelige skade-virkninger. Som eksempel nævnes adgang til offentlige edb-registre.

Udvalget har overvejet, hvad der må anses for særligt skærpende. Det synes i hvert fald umiddelbart tvivlsomt, om det tab, der altid påføres ved hacking, der er lykkedes, i form af udgifter til kontrol af alle dele af systemet og eventuel midlertidig driftsstandsning, er en særlig skærpende omstændighed, eftersom det er en normalsituation og ikke en specialsituation.[73]

Udvalget har på den baggrund overvejet, om strafferammen i strfl. § 263, stk. 2, på 6 måneders fængsel er tilstrækkelig i de situationer, der ikke omfattes af stk. 3. I de foreliggende domme er idømt bøder eller givet betin-get dom. Udvalget finder, at der bør være et højere

---

[72] Betænkningen s. 79.

[73] Det svenske Brottsförebyggande rådet har i BRÅ-rapport 2000:2 om IT-relaterad brotts-lighet, s. 32, anført skaderne i forbindelse med hacking (dataintrång) i de tilfælde, hvor det-te var oplyst i forbindelse med en virksomhedsundersøgelse. Udgifterne lå på mellem 98.700 s.kr. og 346.000 s.kr. pr. sag.

strafmaksimum i straffelovens § 263, stk. 2. Udvalget finder, at hacking er så alvorligt et ind-greb for de fleste virksomheder, at strafmaksimum bør afspejle dette også i den ikke kvalificerede bestemmelse.

Der henvises også til afsnit 2.5, hvoraf det fremgår, at kun Norge har et strafmaksimum svarende til det danske på 6 måneders fængsel, hvorimod Island og Finland har strafmaksima på 1 år og Sverige et strafmaksimum på 2 år.

Udvalget finder, at udviklingen på hackerområdet siden 1985, hvor bestem-melsen blev indsat, gør, at der i dag er behov for, at strafmaksimum i straf-felovens § 263, stk. 2, forhøjes til fængsel i 1 år og 6 måneder. Udvalget har herved bl.a. lagt vægt på, at det IT-baserede samfund er meget sårbart, og at selv et forsøg på hacking er meget føleligt for offeret, der er nødt til at gen-nemgå hele systemet for at være sikker på, om der er sket skader.[74]

Der henvises til afsnit 8.2 vedrørende udvalgets forslag.

3.4. Industrispionage m.v.

Som det tredje område inden for informationskrænkelser har udvalget set på industrispionage m.v.

Da straffelovens § 263, stk. 2 og 3, blev revideret i 1985, overvejede Straf-felovrådet, om princippet fra 1972-revisionen af bestemmelsen, hvorefter ansattes industrispionage m.v. blev holdt uden for straffeloven og i stedet straffedes efter markedsføringsloven, skulle bibeholdes.[75] Straffelovrådet fandt, at dette ville medføre en unødvendig og lidt kunstig begrænsning af § 263, stk. 3, og foreslog derfor, at der ikke blev indlagt begrænsninger i, hvilken personkreds der kunne være gerningsmænd. Dette har givet nogle afgrænsningsproblemer vedrørende den korrekte strafferetlige behandling af internes tilegnelse og udnyttelse af erhvervshemmeligheder.

---

[74] Arbejdsgruppen vedrørende datakriminalitet var enig med udvalget.

[75] Betænkning nr. 1032/1985 om datakriminalitet, s. 74.

Der er mange straffebestemmelser, som omfatter sådanne forhold, og hvor tilegnelse eller udnyttelse af erhvervshemmeligheder i nogle tilfælde vil være omfattet af to af dem eller flere. Det drejer sig bl.a. om følgende bestem-melser:

Straffelovens § 263, stk. 3, omfatter bl.a. uberettiget adgang til data eller programmer med forsæt til at skaffe sig eller uberettiget gøre sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder m.v. Det ka-rakteristiske er således angrebet på hemmeligholdelsen, og at forsæt til indu-strispionage er tilstrækkeligt.

Straffelovens § 264, stk. 2, indeholder en tilsvarende regulering, hvor oplys-ningerne er skaffet i forbindelse med en husfredskrænkelse.

Markedsføringslovens § 10, stk. 1, forbyder den, der er i tjeneste- eller sam-arbejdsforhold med en virksomhed, på utilbørlig måde at skaffe sig eller forsøge at skaffe sig kendskab til eller rådighed over virksomhedens er-hvervshemmeligheder. Lovens § 10, stk. 2, bestemmer, at man ikke ube-føjet[76] må viderebringe eller benytte virksomhedens erhvervshemmelighe-der, selv om man har retmæssigt kendskab til dem.

I andre tilfælde vil også straffelovens § 276 om tyveri eller § 280 om man-datsvig være anvendelige.

Straffelovrådets betænkning om datakriminalitet lader spørgsmålet om val-get mellem disse bestemmelser stå åbent. Det siges[77] om forholdet mellem straffelovens § 263, stk. 3, og markedsføringslovens § 9 (nu § 10), at det vil være overladt til anklagemyndigheden og domstolene, om man vil rejse til-tale henholdsvis dømme i sammenstød eller foretrække at give den ene af bestemmelserne forrang. Det siges videre[78] om afgrænsningen mellem mar-kedsføringslovens § 9 (§ 10) og straffelovens § 280, at spørgsmålet om, hvorvidt straffeloven eller særloven bør have forrang, eller begge bør an-vendes i sammenstød, må afgøres af anklagemyndigheden – og i sidste in-stans domstolene – på

---

[76] Dette fortolkes som erhvervsmæssig udnyttelse, jfr. Børge Dahls kommentar til bestem-melsen i Karnov.

[77] Betænkningen, s. 73 f.

[78] Sm.st. s. 74 f.

grundlag af en konkret fortolkning af bestemmel-serne. Straffelovrådet fandt ikke anledning til at forfølge spørgsmålet nær-mere, da det ikke specielt vedrørte datakriminalitet.

Bestemmelserne i straffelovens kapitel 27 om freds- og ærekrænkelser blev på baggrund af Straffelovrådets betænkning nr. 601/1971 om privatlivets fred revideret væsentligt ved lov nr. 89 af 29/3 1972. Efter indsættelsen af bestemmelserne om hacking i 1985, jfr. afsnit 2.4, vil spørgsmålet om for-tolkningen af de øvrige bestemmelser kun sjældent være aktuelt i relation til IT-kriminalitet.

Det bemærkes, at bestemmelsernes strafmaksima er meget forskellige. Straf-maksimum er 2 år ved markedsføringslovens § 10, 4 år ved straffelovens § 263, stk. 3, og § 264, stk. 2, 4 år ved straffelovens § 276 og 8 år ved straf-felovens § 280.[79]

Det kan desuden have en vis interesse, hvilke overvejelser Straffelovrådet har gjort sig omkring strafmaksima. Strafmaksimum i § 263, stk. 1 og 2, er på 6 måneder. I stk. 3 var strafmaksimum ved indsættelsen i 1985 på 2 år[80], svarende til markedsføringsloven, men det blev i 1992 hævet til 4 år.[81]

I betænkning nr. 601/1971 om privatlivets fred siger Straffelovrådet[82], at den almindeligt gældende strafferamme vedrørende fredskrænkelser er bøde eller hæfte. Det siges videre:

> "Denne beskedne strafferamme afspejler den relativt ringe trussel, disse bestemmelser oprindelig skulle værne imod. Fremkomsten af det nye tek-niske udstyr[83] har imidlertid i høj grad forstærket truslen mod privatlivets fred. Dette har selvfølgelig medført en større samfundsmæssig interesse i at sikre et tilstrækkeligt værn.

---

[79] En udførlig gennemgang af de aktuelle bestemmelsers forarbejder og fortolkning findes i Vagn Greves artikel: Erhvervsspionage – i strafferetlig belysning, FSRs årsskrift 1991 (Skatteret – Erhvervsret) s. 79 ff.

[80] Og samtidig blev strafmaksimum for den tilsvarende overtrædelse ved husfredskrænkel-se, jfr. straffelovens § 264, nedsat fra 4 til 2 år.

[81] Lov nr. 6 af 3/1 1992.

[82] Betænkningen s. 57 f.

[83] Ting som diverse former for aflytningsudstyr, teleobjektiver, miniatureudstyr til billed- eller lydtransmission, udstyr til observationer og fotografering i mørke m.v.

> Som en markering af den ændrede samfundsmæssige vurdering, som ud-viklingen har medført, finder straffelovrådet det rigtigt at skærpe den al-mindelige strafferamme, således at den også kommer til at rumme fængsel indtil 6 måneder. Den samfundsmæssige beskyttelse bør yderligere styrkes ved at ændre påtalereglerne til betinget offentlig påtale, således at den krænkede blot ved at indgive anmeldelse har mulighed for at få det of-fentlige til at efterforske sagen og i givet fald føre den for domstolene. Og-så for de alvorligste forhold – herunder bl.a. industriel spionage, hvor større økonomiske interesser kan være involveret – bør den ændrede sam-fundsmæssige vurdering markeres gennem en skærpelse af strafferam-men. Medens det almindelige strafmaksimum efter den gældende bestem-melse i § 264 a er fængsel i 1 år og kun under særlige omstændigheder kan gå op til fængsel i 4 år, foreslår straffelovrådet nu et almindeligt strafmak-simum på fængsel i 4 år for den groveste kriminalitet på dette område."

I Straffelovrådets betænkning nr. 1032/1985 om datakriminalitet nævnes vedrørende strafferammer for de nye regler[84], at normalstrafferammen kan sættes til fængsel i indtil 6 måneder, svarende til normalstrafferammen ved fredskrænkelser, og at straffen i § 264 kan nedsættes til 2 år, samt at en skærpende bestemmelse vedrørende den foreslåede § 263, stk. 2, ligeledes bør have et strafmaksimum på 2 år.

I Straffelovrådets betænkning nr. 1099/1987 om strafferammer og prøve-løsladelser henvises vedrørende fredskrænkelser til de nyere ændringer, der har været, og der foreslås ingen ændringer vedrørende strafmaksima.[85]

Ved lov nr. 6 af 3/1 1992 forhøjedes strafmaksimum i straffelovens § 263, stk. 3, og § 264, stk. 2, til fængsel i 4 år. Det siges herom i lovforslaget[86], at der bl.a. kan være tale om udenforstående, der får informationer om virk-somhedens erhvervshemmeligheder, hvortil der undertiden kan være knyttet betydelige økonomisk interesser. Det siges videre:

---

[84] Betænkningen s. 27 f.

[85] Betænkningen s. 201 f.

[86] Lovforslag nr. L 84 1991-92 (Samfundstjeneste m.v.) s. 34. FT 1991/92 A 1895.

> "Der har i den forbindelse været rejst spørgsmål om, hvorvidt et strafmak-simum på fængsel indtil 2 år kan anses for tilstrækkeligt. Der kan herved bl.a. henvises til, at det kan bero på tilfældige omstændigheder, om tilegnel-sen af informationer strafferetligt skal bedømmes som tyveri, der forudsæt-ter borttagelse af en rørlig ting, med et strafmaksimum efter straffelovens § 286, stk. 1, på 4 års fængsel, eller alene som en fredskrænkelse med et strafmaksimum på 2 års fængsel. De økonomiske konsekvenser af forbry-delsen vil uanset den strafferetlige kvalifikation kunne være de samme.
>
> Efter Justitsministeriets opfattelse må det ud fra lighedsbetragtninger prin-cipielt anses for uheldigt, at strafmaksimum for den form for industrispio-nage, der sker ved en fredskrænkelse, kun er halvt så højt som strafmak-simum for groft tyveri. Der kan tænkes tilfælde af industrispionage, hvor den økonomiske fordel for gerningsmanden og skadevirkningerne for den ramte virksomhed er så store, at forholdet i strafudmålingsmæssig hense-ende i hvert fald må sidestilles med groft tyveri, og at et strafmaksimum på fængsel i 2 år derfor må anses for utilstrækkeligt."

Udvalget har overvejet, om der kan opstilles kriterier for, hvordan bestem-melserne skal afgrænses indbyrdes, og om strafmaksimum i markedsfø-ringsloven bør bringes på højde med i hvert fald straffelovens § 263, stk. 3, og dermed generelt give en bedre beskyttelse af erhvervshemmeligheder. Udvalget har endvidere overvejet, om der tillige bør være en strafferetlig re-gulering af den situation, at virksomhedsgæster udnytter besøget til utilbør-ligt at skaffe sig information (f.eks. ved under besøget at skaffe sig informa-tioner fra lokaliteter i virksomheden, der ikke er omfattet af rundvisningen, eller ved at fotografere eller medtage prøver trods forbud herom) eller ube-føjet viderebringer eller benytter erhvervshemmeligheder, den besøgende tilfældigt eller uagtsomt er kommet i besiddelse af under besøget, uden at dette er sket som led i den almindelige fremvisning. Begrundelsen for disse situationers straffrihed er hidtil blevet søgt i, at virksomheden selv er herre over, hvem den vil lukke ind i virksomheden.

I erhvervslivet er det som regel legitimt, at virksomheder skaffer sig kend-skab til konkurrenternes produktionsformer, markedsføringsplaner, kunde-kredse etc. Det strafværdige er ikke, at de søger sådan kundskab, men må-den, hvorpå det eventuelt sker. Udvalget finder, at en udnyttelse af mulig-heder, der er skabt ved, at

man lovligt befinder sig i virksomheden, f.eks. som virksomhedsgæst, bør være omfattet af den strafferetlige regulering.

Udvalget har endvidere drøftet, om der bør være en samlet bestemmelse i straffeloven vedrørende industrispionage m.v.[87] Under hensyntagen til de lovtekniske og systematiske problemer, der vil være forbundet med en så-dan løsning, har udvalget valgt ikke at foreslå en samlet bestemmelse.

Udvalget finder, at den nævnte regulering vedrørende virksomhedsgæster m.fl. bør indsættes i markedsføringslovens § 10.

Udvalget finder herudover, at der bør være en mere ensartet strafferetlig regulering, således at strafmaksimum ved f.eks. ansattes industrispionage m.v. ikke afhænger af, om de overtræder straffelovens § 263, stk. 3, (fængsel i op til 4 år) eller markedsføringsloven (fængsel i op til 2 år).

Udvalget foreslår derfor, at der indsættes en bestemmelse i straffeloven om særligt grove overtrædelser af markedsføringslovens § 10. Bestemmelsen fo-reslås at dække de situationer, hvor handlingen har medført betydelig skade, eller hvor der har været nærliggende fare derfor.

Udvalget har drøftet, hvilket af de i dag aktuelle strafmaksima, der bør an-vendes i en ny bestemmelse. Udvalget finder, at kriminalitet rettet mod in-formationer i et moderne samfund bør nyde mindst samme beskyttelse som kriminalitet rettet mod mere traditionelle økonomiske værdier i form af penge og ting, da der kan være tale om betragtelige værdier på linie hermed. I betragtning af, at groft tyveri efter de nugældende regler har et straf-maksimum på fængsel i 4 år, har udvalget valgt det samme strafmaksimum. Udvalget vil imidlertid fremhæve, at såfremt Straffelovrådet når frem til en forhøjelse af strafmaksimum for tyveri, finder udvalget, at der bør ske en tilsvarende forhøjelse vedrørende industrispionage m.v.[88]

---

[87] Arbejdsgruppen om datakriminalitet foreslog en sådan samlet bestemmelse.

[88] Arbejdsgruppen om datakriminalitet foreslog et strafmaksimum på fængsel i 8 år.

Udvalget foreslår endvidere, at det nugældende strafmaksimum i markeds-føringslovens § 22, stk. 4, 1. pkt., ændres fra 2 år til 1 år og 6 måneder.

Et strafmaksimum på fængsel i 1 år og 6 måneder svarer til, hvad udvalget generelt synes bør være maksimum i tilfælde, hvor der er en strafferetlig overbygning vedrørende kvalificerede forhold.[89] Reguleringen svarer til, hvad der gælder for berigelsesforbrydelser, jfr. straffelovens § 285 og over-bygningen i § 286.

Der henvises til afsnit 8.3 vedrørende udvalgets forslag.

Herudover har udvalget drøftet, om det, der anføres på private straffeat-tester, dækker det behov for oplysninger, der er i dag ved ansættelser i IT-relaterede stillinger. Udgangspunktet for disse drøftelser har været, at IT-området er meget sårbart, og at det derfor er væsentligt, at en virksomhed ikke udsættes for unødig risiko ved at ansætte IT-kriminelle. De områder, hvor der kan være anledning til at overveje at medtage yderligere oplysnin-ger, er markedsføringslovens § 10 om industrispionage mv. og ophavsrets-lovens § 76 om piratkopiering.

Efter de gældende regler i Justitsministeriets bekendtgørelse om behandling af personoplysninger i Det Centrale Kriminalregister[90] indeholder straffeat-tester til private oplysning om straffelovsovertrædelser og overtrædelser af lov om euforiserende stoffer i 5 år fra endelig løsladelse, hvis den pågæl-dende har været indsat til afsoning. I andre tilfælde er fristen 2-3 år fra den endelige afgørelse afhængig af sanktionens art.

Udvalget finder, at de gældende regler generelt er tilstrækkelige til at give den ønskede beskyttelse.

Hvis de i denne rapport foreslåede ændringer af straffeloven på disse områ-der gennemføres, er der efter udvalgets opfattelse ikke anledning til at over-veje ændringer af reglerne om private straffeattester.

---

[89] Jfr. betænkning nr. 1396/2001 om straffelovens § 289 m.v., s. 66, og forslagene i nærvæ-rende betænkning.

[90] Bekendtgørelse nr. 218 af 27/3 2001.

3.5. Ophavsretslovens § 76 om piratkopiering

Som det fjerde og sidste område inden for informationskrænkelser har ud-valget set på ophavsretslovens § 76 om piratkopiering.

I betænkning nr. 944/1982 om båndafgifter, sanktioner og påtale fra udval-get vedrørende revision af ophavsretslovgivningens blev der fremsat forslag vedrørende piratvirksomhed. Det nævnes[91], at reglerne i det store hele hav-de fungeret tilfredsstillende, og at området tidligere ikke havde været præget af egentlig kriminalitet, men at de senere års tekniske fremskridt, der gav mulighed for billig produktion, havde medført, at der var opstået en egentlig kriminalitet – den såkaldte piratvirksomhed.

Udvalget vurderede på den baggrund[92], at de dagældende regler med straf-maksimum på 3 måneders hæfte og privat påtale var utilstrækkelige til at be-skytte området. Udvalget fremhævede, at der var diskrepans mellem vurde-ringen af f.eks. berigelseskriminalitet og grove ophavsretskrænkelser. Udval-get foreslog et strafmaksimum på fængsel i 1 år og 6 måneder, således at he-le straffebestemmelsen i ophavsretsloven[93] indledtes med "Med bøde eller under skærpende omstændigheder med hæfte eller fængsel i indtil 1 år og 6 måneder".

I det lovforslag, der blev fremsat den 13/12 1984, anvendtes med hensyn til § 55, stk. 2, den formulering[94], der fortsat anvendes (nu i § 76, stk. 2).

Det siges i bemærkningerne til lovforslaget[95], at Ministeriet for kulturelle anliggender er enig i, at der for så vidt angår lovovertrædelser, der kan ka-rakteriseres som piratvirksomhed, er behov for en udvidelse af straffe-rammen. Efter forhandling med Justitsministeriet har man imidlertid fundet det rigtigst, at den

---

[91] Betænkningen s. 64 f.
[92] Betænkningen s. 80 ff.
[93] Betænkningen s. 89 f.
[94] Jfr. lov nr. 274 af 6/6 1985 om ændring af ophavsretsloven.
[95] FT 1984/85 A sp. 1979 ff.

udvidede strafferamme kun omfatter denne type sager. Ordlyden af bestemmelsen blev herefter:

> "Er en forsætlig overtrædelse af de i stk. 1 nævnte bestemmelser begået ved erhvervsmæssigt at fremstille eller blandt almenheden sprede eksem-plarer af litterære eller kunstneriske værker eller af arbejder eller frembrin-gelser, der beskyttes efter §§ 45-49, kan straffen under særlig skærpende omstændigheder stige til hæfte eller fængsel indtil 1 år. Særlig skærpende omstændigheder anses navnlig for at foreligge, hvis overtrædelsen vedrører et betydeligt antal eksemplarer, eller hvis der ved overtrædelsen tilsigtes en betydelig vinding."

Det fremgår ikke af lovforslaget, hvorfor der blev foreslået et strafmaksi-mum på 1 år og ikke som foreslået af udvalget 1 år og 6 måneder.

Piratkopieringsreglen i ophavsretslovens § 76, stk. 2, forudsætter, at der er tale om en erhvervsmæssig fremstilling eller spredning. Da bestemmelsen blev indsat i 1985, var det disse erhvervsmæssige situationer med vinding på ophavsretsindehaverens bekostning, der var behov for at regulere. Udviklin-gen på internetområdet har imidlertid medført, at denne regel rammer en langt mindre del af krænkelserne af ophavsretten end oprindeligt forudsat. Også på dette område kan meget i dag tale for, at man i relation til strafvær-dighed sidestiller, at værker gøres tilgængelige for en større kreds, med en erhvervsmæssig spredning.[96]

Tilgængelighed via Internettet eller andre åbne netforbindelser medfører of-te en større risiko for ophavsretlige krænkelser end det organiserede salg.

De foreliggende domme om piratkopiering af edb-programmer har lagt vægt på piratens udbytte og ikke på rettighedsindehaverens salgspris. I de rene ophavsretslovssager, udvalget er bekendt med, er der idømt bødestraf i alle sager på nær to.[97]

---

[96] Internettet medfører også andre specielle ophavsretlige problemer, jfr. eksempelvis Mads Bryde Andersens artikel "Linking og robottering på Internettet" i UfR 2000 B s. 311 ff.

[97] Ved Rødding rets dom af 8/12 1999 blev en tiltalt, der havde fremstillet ca. 78.000 cd'er med ulovligt kopierede programmer og spil og videresolgt dem til en ikke

Det skal dog fremhæves, at der i erstatningsretlig sammenhæng ikke nød-vendigvis lægges vægt på de samme forhold.

> I en straffesag om piratkopiering blev en direktør og eneanpartshaver samt en sælger i et anpartsselskab ved Københavns byrets dom af 4/12 1995 frifundet for salg af piratkopier, fordi retten fandt, at der kun var udvist simpel uagtsomhed. Ved Østre Landsrets dom af 20/11 1998 i en erstat-ningssag vedrørende samme forhold blev direktøren (der hæftede på lige fod med det konkursramte selskab) dømt til at betale 1 mio. kr. i erstat-ning til rettighedshaveren, jfr. UfR 1999.326 Ø. Erstatningsbeløbet sva-rede til rettighedshaverens påstand. Det fremgår af begge domme, at an-klagemyndigheden havde foretaget en beregning, hvorefter anpartsselska-bet ikke havde opnået nogen fortjeneste ved salget.

Den erstatningsretlige beskyttelse kan således være et væsentligt supplement til den strafferetlige beskyttelse.

Rettighedshavernes eller dennes repræsentants mulighed for at bevise om-fanget af piratkopiering er blevet væsentligt forbedret fra april 2001, idet der er indsat et nyt kapitel 57 a i retsplejeloven[98] om bevissikring ved krænkelse af immaterialrettigheder m.v. Det er herefter muligt at få bistand fra foged-retten til en nærmere undersøgelse for at sikre bevis for krænkelsen og dens omfang, hvis det sandsynliggøres, at der er sket en krænkelse som led i erhvervsvirksomhed eller i øvrigt i ikke ubetydeligt omfang.

Udvalget har under sit arbejde modtaget henvendelser fra flere sammen-slutninger/foreninger, der repræsenterer rettighedshavere, som alle har op-lyst, at omfanget af piratkopiering er meget stort. Det nævnes i henven-delsen af 1/10 1999 fra Business Software Alliance

---

navngiven per-son, der videresolgte til en fast kundekreds, idømt betinget fængsel i 40 dage og fik kon-fiskeret fortjenesten på ca. 204.000 kr. Rettighedshaverne havde nedlagt påstand om er-statning på henholdsvis ca. 869 mio. kr. og ca. 32 mio. kr. Erstatningskravene blev henvist til civilt søgsmål.

Ved Rødding rets dom af 13/11 2000 blev en tiltalt, der i udlandet havde fået fremstillet ca. 56.000 cd'er med ulovligt kopierede programmer og spil og videresolgt dem i Danmark til uidentificerede kunder, idømt betinget fængsel i 30 dage og fik konfiskeret fortjenesten på ca. 300.000 kr. Erstatningskravet blev henvist til civilt søgsmål. (Ifølge Computerworld 8/12 2000 var erstatningskravet på 620 mio. kr.).

[98] Ved lov nr. 216 af 28/3 2001.

(BSA), at ifølge BSAs seneste undersøgelse skønnes det, at 31% af de edb-programmer, som an-vendes i erhvervsmæssig sammenhæng, er ulovlige kopier, og at det skøn-nede tab for softwarebranchen udgør 200-300 mio. kr. på årsplan.

Udvalget finder, at reglerne om piratkopiering bør ændres, således at distri-bution via BBS'er, Internettet m.v. bliver dækket af den strenge bestem-melse. Udvalget har ikke kendskab til anden lovgivning (bortset fra straffe-lovens § 235 om børnepornografi), hvor problemstillingen forekommer.[99]

Udvalget har overvejet, om en regulering skulle ske ved, at kravet om, at handlingen skal begås erhvervsmæssigt, udgår. Udvalget har imidlertid valgt i stedet at supplere med at nævne, at der gives en videre kreds adgang, som kvalifikation.

Udvalget har også overvejet, om et strafmaksimum på 1 år svarer til den beskyttelse, man i dag ønsker at give – også set i sammenhæng med, hvor omfattende potentielle skadevirkninger der er knyttet til internetdistribu-tion.

Udvalget finder, som også foreslået af det udvalg, der i 1985 afgav betæn-ning om spørgsmålet, at der, selv om den hidtidige strafudmåling på områ-det har været mild, bør være et strafmaksimum på fængsel i 1 år og 6 måne-der under hensyn til krænkelsens skadevirkninger.

Udvalget har i den forbindelse også overvejet, om der skal indsættes en ge-nerel overbygning i straffeloven, f.eks. svarende til straffelovens § 289.

---

[99] Markedsføringslovens § 10, stk. 2, om bl.a. ubeføjet viderebringelse af erhvervshem-meligheder, man har lovligt kendskab til, vedrører ganske vist kun erhvervsmæssige dispo-sitioner, men anden videregivelse kan være dækket af straffelovens § 264 d om uberettiget videregivelse af bl.a. meddelelser vedrørende en andens private forhold.

Udvalget finder, at der bør indsættes en sådan overbygning i straffeloven i stil med straffelovens §§ 125 a, 192 a, 196, 289 og § 289 a med et straf-maksimum på 4 år.[100]

Udvalget har herved lagt vægt på, at særligt grove overtrædelser er lige så strafværdige som tyveri, der har et strafmaksimum på 4 år, jfr. straffelovens § 286. Det er efter udvalgets opfattelse en naturlig strafferetlig udvikling, at et stadigt mere IT-afhængigt samfund også giver en strafferetlig beskyttelse af de produkter, der udvikles i et sådan samfund.

Udvalget finder, at de overtrædelser, der skal behandles efter straffeloven, skal begrænses til situationer, hvor der er forsæt til vinding for gernings-manden eller andre. Bestemmelsen kan især tænkes anvendt i tilfælde, hvor der er tale om omfattende og systematiske krænkelser, hvilket typisk vil væ-re tilfælde, hvor der en organiseret fremstillings- og/eller salgsproces. Be-stemmelsen vil også kunne anvendes, hvis krænkelsen vedrører enkelte me-get dyre programmer eller systemer, der f.eks. er udviklet til en eller flere virksomheder.

Der henvises til afsnit 8.4 vedrørende udvalgets forslag.

3.6. Straffelovens § 153

I straffelovens kapitel 16 om forbrydelser i offentlig tjeneste eller hverv m.v. findes følgende bestemmelse:

---

[100] Et flertal i arbejdsgruppen om datakriminalitet (Kim Aarenstrup, Mads Bryde Andersen, Jan Carlsen, Jan Friis, Michael Goeskjær, Carsten Heilbuth, Ulla Høg, Jens Kruse Mikkel-sen, Ronald Pedersen) foreslog som udvalget en overbygning i straffeloven med fængsel i 4 år. Et mindretal i udvalget (Hans Jakob Paldam Folker, Helle Jahn, Ole Stampe Ras-mussen) fandt, at et strafmaksimum i ophavsretsloven på 2 år ville give en tilstrækkelig strafferetlig beskyttelse.

Arbejdsgruppen drøftede ikke spørgsmålet om at ændre strafmaksimum i ophavsretslo-ven fra 1 år til 1 år og 6 måneder.

> § 153. Når nogen, som virker i post- eller jernbanevæsenets tjeneste, ulovlig åbner, tilintetgør eller underslår forsendelser eller understøtter en anden i sådan færd, straffes han med fængsel indtil 3 år.
> Stk. 2. På samme måde straffes den, som virker i statstelegrafvæsenets eller et offentligt anerkendt telegrafanlægs tjeneste, når han tilintetgør, for-vansker eller underslår et samme til befordring overgivet telegram eller understøtter en anden i sådan færd.

Efter privatiseringen af store dele af det offentlige kommunikationsvæsen er det kun en del af det, som dækkes af denne bestemmelse. Udvalget har derfor drøftet, om bestemmelsen er blevet overflødig, eller om den bør be-vares på en anden plads i straffeloven.

Stk. 1 er fuldstændig dækket af de almindelige regler om krænkelse af brev-hemmeligheden (§ 263) og den almindelige regel om tingsødelæggelse (§ 291). Den forhøjede strafferamme i § 153 i forhold til disse bestemmelsers grunddelikter skyldes, at bestemmelsen tog sigte på offentligt ansatte. I dag er der næppe grund til at anvende andre strafferammer end de almindelige, herunder efter omstændighederne § 263, stk. 3 (4 år under "særlig skær-pende omstændigheder") og § 291, stk. 2 (4 år ved "hærværk af betydeligt omfang"). Stk. 1 er derfor overflødig og kan ophæves.

Stk. 2 må anses for overflødig i dag, hvor telegrafsystemet har mistet sin betydning. Misligholdelse af den indgåede kontrakt om befordring af en meddelelse må, hvis der ikke er strafferetlig dækning i straffelovens almin-delige bestemmelser, imødegås af civilretlige reaktioner på samme måde som de fleste andre misligholdelser af tjenesteydelser.

Fremkaldelse af omfattende forstyrrelser inden for post-, telefon- og tele-grafområdet er desuden omfattet af straffelovens § 193, der også omfatter de privatiserede foretagender.

Udvalget foreslår derfor, at straffelovens § 153 ophæves som overflødig.

Der henvises til afsnit 8.5 vedrørende udvalgets forslag.

KAPITEL 4
BETALINGSKRIMINALITET

4.1. Indledning

Udvalgets overvejelser i det følgende vedrører dels elektroniske pengeover-førsler og elektroniske penge, dels spørgsmålet om, hvorvidt der – som ved passwords m.v. – på nogle områder skal formuleres en direkte strafferetlig beskyttelse (i stedet for reglerne om strafbare forsøgshandlinger) vedrøren-de forhold, der ligger forud for berigelseshandlingerne. Desuden ses på spørgsmålet om, hvordan misbrug af andres teleforbindelser skal bedøm-mes, jfr. afsnit 4.5.

De IT-relaterede betalings- og konteringsformer kan groft opdeles i to om-råder: Elektroniske penge (e-penge, elektroniske kontanter, e-money, e-cash) og kontorelaterede produkter.[101]

Det karakteristiske for elektroniske penge er, at der er tale om et forudbetalt betalingsprodukt (et kort eller et software produkt), der anvendes i elektro-niske sammenhænge på samme måde som kontanter. Elektroniske penge er selvstændige betalingsmidler, der i modsætning til de kontorelaterede pro-dukter ikke kan henføres til en bestemt konto.[102]

I Europa-Parlamentets og Rådets direktiv af 18/9 2000[103] om adgang til at optage og udøve virksomhed som udsteder af elektroniske penge og tilsyn med en sådan virksomhed, defineres elektroniske penge som: En penge-værdi som repræsenteret ved et krav på udstederen, der er

i) lagret på det elektroniske medium
ii) udstedt efter modtagelse af midler, der ikke kan beløbe sig til min-dre end den udstedte pengeværdi
iii) anerkendt som betalingsmiddel af andre foretagender end udste-deren.

---

[101] Sådanne produkter betegnes også som access produkter.

[102] Se også Mads Bryde Andersen, IT-retten (2001), s. 802 ff., hvor forskellen mellem be-grebet elektroniske penge og andre elektroniske betalingsmidler beskrives.

[103] EFT L 2000 257/39.

Direktivet er implementeret ved lov om udstedere af elektroniske penge.[104] I lovens § 1, stk. 3, defineres elektroniske penge som "en pengeværdi, som re-præsenteret ved et krav på udstederen, der er lagret på et elektronisk me-dium. Elektroniske penge må ikke udstedes til overkurs og skal være aner-kendt som betalingsmiddel af andre end udstederen."

Det karakteristiske for kontorelaterede produkter er, at de relaterer sig til en identificeret kundes konto. De vedrører således traditionelle konterings- og betalingssystemer, men giver kunden mulighed for elektroniske disposi-tioner. I nogle tilfælde indebærer muligheden for elektroniske dispositioner, at der opstår nye produkter. F.eks. er koder som calling cards og NUI-koder nye produkter, hvor registrering og kontering af brug kun er knyttet til ko-den og ikke til identificerede anlæg på brugernes fysiske adresser. Produk-terne kan underopdeles i:

a. Kontorelaterede betalingskort (credit og debit cards).
b. Konteringskoder (calling cards, NUI-koder o.l.).
c. Home banking/on line banking/elektroniske checks.

Begge produkter (elektroniske penge og kontorelaterede produkter) er om-fattet af lov om visse betalingsmidler og adgangskoder.

Kontorelaterede betalingskort er endvidere behandlet i Rådets rammeafgø-relse af 28/5 2001 om bekæmpelse af svig og forfalskning i forbindelse med andre betalingsmidler end kontanter.

Lov om visse betalingsmidler og adgangskoder[105] omfatter bl.a. "elektronisk registrerede fordringer, som udsteder er forpligtet til at indfri på brugers anmodning", i det omfang de kan benyttes til at erhverve varer eller tjene-steydelser, foranledige overførsel af beløb, hæve penge eller foretage andre betalingstransaktioner. Det anføres i bemærkningerne til lovforslaget,[106] at der er tale om fordringer, som ikke er knyttet til en individualiseret konto. Typisk vil der være tale om forudbetalte kort som f.eks. et telefonkort, men der kan også være

---

[104] Lov nr. 502 af 7/6 2001.

[105] Lov nr. 414 af 31/5 2000.

[106] FT 1999/2000 A 1541.

tale om elektroniske fordringer lagret på en computer. Det nævnes endvidere i lovforslaget, at de elektroniske fordringer har ka-rakter af "elektroniske penge", idet de registrerede fordringer kan bruges til køb af varer eller tjenesteydelser hos udstederen eller andre.

I loven defineres "betalingsmidler" tillige som "koder og biometriske vær-dier, som er beregnet til at legitimere brugeren", i det omfang de kan benyt-tes til at erhverve varer eller tjenesteydelser, foranledige overførsel af beløb, hæve penge eller foretage andre betalingstransaktioner. Det anføres i be-mærkningerne til lovforslaget, at koder, der ikke alene giver adgang, men også benyttes til en debitering af brugeren, vil være omfattet.

Rådets rammeafgørelse af 28/5 2001 om bekæmpelse af svig og for-falskning i forbindelse med andre betalingsmidler end kontanter[107] definerer i artikel 1 bl.a. begrebet "betalingsinstrument (bortset fra kontanter)".[108] Definitionen omfatter kun fysiske instrumenter.

I artikel 2-4 nævnes en række forhold, der skal være strafbare. Bestemmel-serne har følgende indhold:

> "Artikel 2
> Lovovertrædelser i forbindelse med betalingsinstrumenter
>
> Hver medlemsstat træffer de nødvendige foranstaltninger for at sikre, at følgende adfærd er strafbar, når den er forsætlig, i det mindste med hensyn til kreditkort, eurocheckkort, andre kort, der er udstedt af finansierings-institutter, rejsechecks, eurochecks, andre checks og veksler:
> a) tyveri eller anden retsstridig tilegnelse af et betalingsinstrument
> b) forfalskning eller efterligning af et betalingsinstrument med henblik på brug af det i bedragerisk hensigt
> c) modtagelse, opnåelse, transport, salg eller overdragelse til andre eller besiddelse af et stjålet eller på anden vis retsstridigt tilegnet

---

[107] EFT L 2001 149/1.

[108] Defineres som "Et fysisk instrument, bortset fra lovlige betalingsmidler (dvs. sedler og mønter), som i kraft af sin særlige karakter alene eller sammen med et andet (betalings)in-strument gør det muligt for indehaveren eller brugeren at overføre penge, som f.eks. kre-ditkort, eurocheckkort, andre kort, der er udstedt af finansieringsinstitutter, rejsechecks, eurochecks, andre checks og veksler, som er beskyttet mod efterligning eller brug i be-dragerisk hensigt, f.eks. i kraft af udformning, kodning eller underskrift.".

eller for-falsket eller efterlignet betalingsinstrument med henblik på brug af det i bedragerisk hensigt

d) brug af et stjålet eller på anden vis uretmæssigt tilegnet eller forfalsket eller efterlignet betalingsinstrument i bedragerisk hensigt.

Artikel 3
Edb-relaterede lovovertrædelser

Hver medlemsstat træffer de nødvendige foranstaltninger for at sikre, at følgende adfærd er strafbar, når den er forsætlig:

At gennemføre eller forårsage en pengeoverførsel og derved forvolde et uberettiget tab af formuegoder for andre, med den hensigt at skaffe den person, der begår lovovertrædelsen, eller en tredjepart uberettiget økono-misk vinding, ved:

- retsstridigt at indlæse, ændre, slette eller tilbageholde edb-data, især identifikationsdata, eller
- retsstridigt at gribe ind i driften af et edb-program eller -system.

Artikel 4
Lovovertrædelser i forbindelse med særligt tilpassede anordninger

Hver medlemsstat træffer de nødvendige foranstaltninger for at sikre, at følgende adfærd anses for en lovovertrædelse, når den er forsætlig:

Fremstilling, modtagelse, opnåelse, salg eller overdragelse til andre eller besiddelse i bedragerisk hensigt af:

- redskaber, genstande, edb-programmer og alle andre midler, som ifølge deres natur er bestemt til at anvendes ved de lovovertrædelser, der er omhandlet i artikel 2, litra b)
- edb-programmer, der er beregnet til at anvendes ved de lovovertrædelser, der er omhandlet i artikel 3."

Efter artikel 5 skal medvirken til eller anstiftelse af den i artikel 2-4 omhandlede adfærd eller forsøg på den i artikel 2, litra a), b) og d), og artikel 3 omhandlede adfærd være strafbar.

Ifølge Justitsministeriets bidrag til kommenteret dagsorden til brug for råds-mødet i maj 2001 må de i artikel 2-5 nævnte strafbare handlinger – bl. a. set i lyset af straffelovens regler om forsøg og medvirken – anses

for omfattet af navnlig straffelovens bestemmelser om dokumentfalsk, tyveri, bedrageri og databedrageri.

Det er således antaget, at rammeafgørelsen ikke nødvendiggør lovændrin-ger.

4.2. Elektroniske penge

Som nævnt i indledningen til dette afsnit indgår i begrebet elektroniske pen-ge i direktivet om virksomhed som udsteder af elektroniske penge, at det er et multianvendeligt produkt. Mere simple produkter, hvor der er tale om forudbetaling af en bestemt ydelse (f.eks. telefonkort), er således ikke om-fattet. Udvalget anvender begrebet elektroniske penge på samme måde, og det er således et snævrere begreb end de "elektronisk registrerede for-dringer", der er omfattet af lov om visse betalingsmidler, jfr. indledningen til dette afsnit.

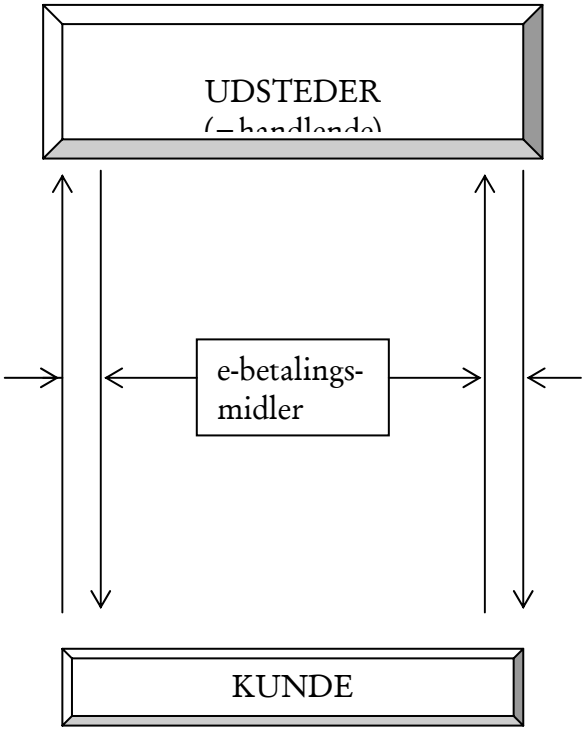
På de følgende sider er anført nogle modeller, der illustrerer nogle af de i dag kendte systemtyper. Modellerne er forenklede, idet der mellem udsteder og køber/indløser typisk vil være placeret formidlerled (f.eks. således at flere banker sælger og indløser på udstederens vegne). Som model 1 er til il-lustration medtaget produkter, hvor der er tale om en forudbetalt, bestemt ydelse og ikke om elektroniske penge.

Som eksempler på nogle af de multianvendelige produkter, der findes i dag, kan nævnes:

- Danmønt (kort, der i sin nuværende skikkelse kan genoplades)
- Mondex (kort, der kan genoplades eller oplades fra andres Mondex-kort (chip-to-chip overførsler))
- DigiCash's eCash og CyberCash's CyberCoin (softwareprodukter, hvor digitale penge er placeret på harddisk)

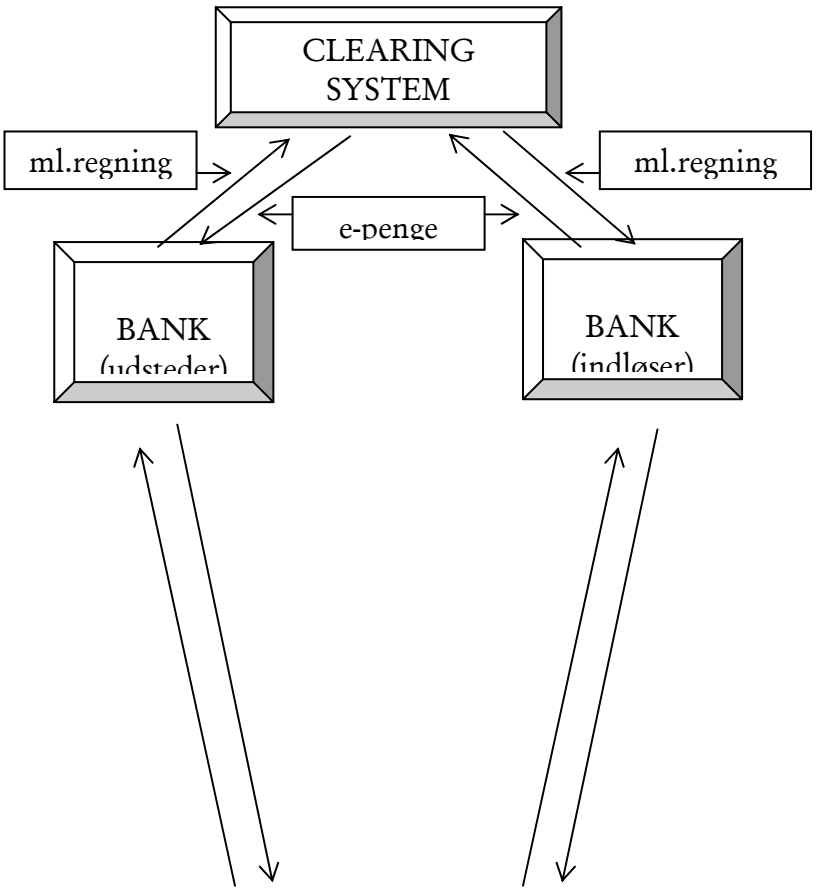
MODEL 1

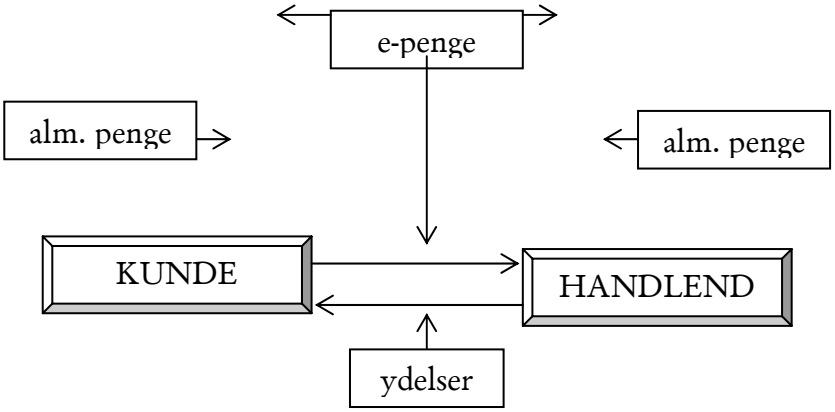
Anvendelsesbegrænsede elektroniske betalingsmidler (ikke bankudstedte)



Eks.: Telefonkort.
MODEL 2

Bankudstedte elektroniske penge (enkelttransaktioner)

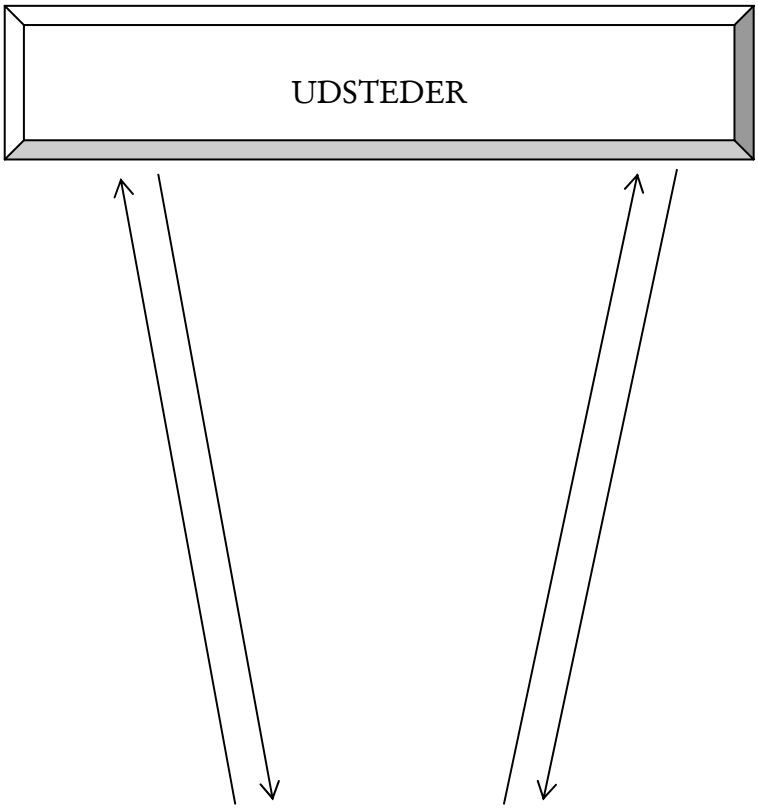


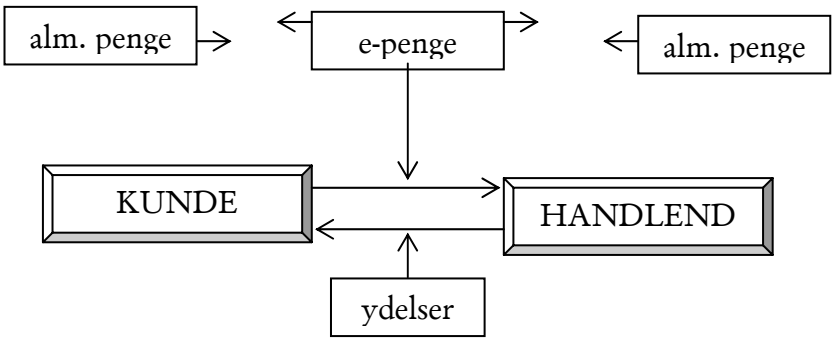


Eks.: Danmønt. (PBS er clearing system).

MODEL 3

Ikke bankudstedte elektroniske penge (enkelttransaktioner)

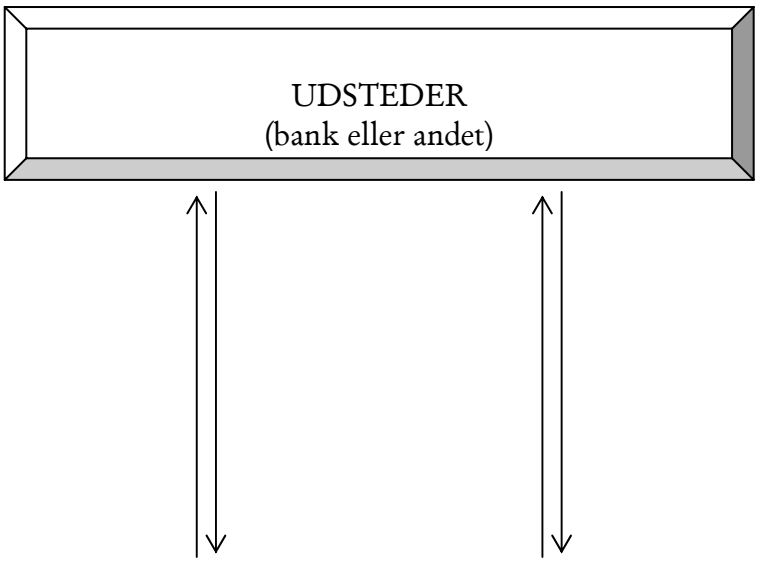


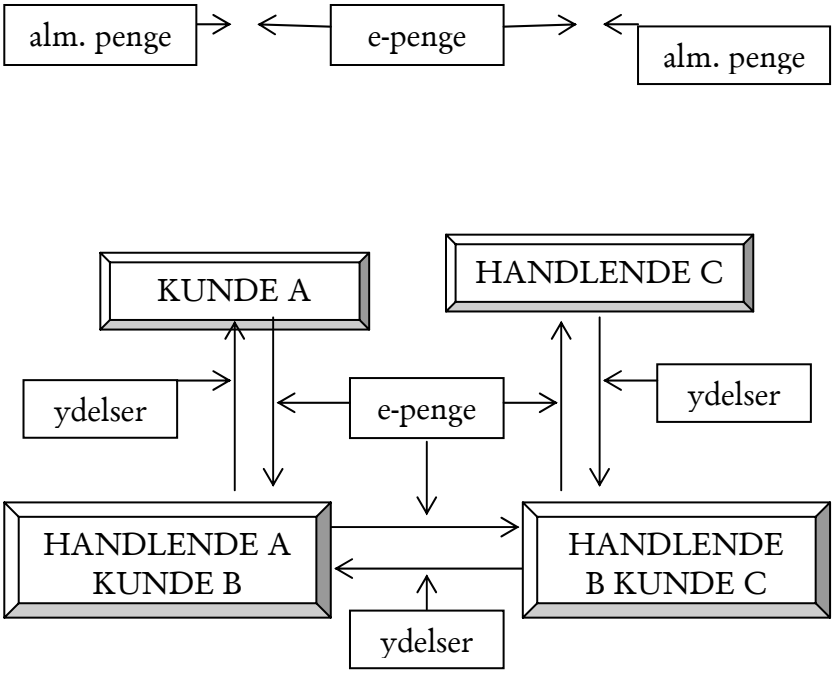


Eks.: CyberCash's CyberCoin og DigiCash's eCash.

MODEL 4

Genopladelige elektroniske penge (multitransaktionsbrug)





Eks.: Mondex' stored value smartcard.

Særligt vedrørende Mondex kan nævnes, at visse af kortene ikke alene kan bruges som et almindeligt forudbetalt betalingskort, men via en computer-tilkoblet kortlæser også kan anvendes, hvis modtageren har en Mondex-modtager-anordning. Der er således tale om et produkt, der giver mulighed for at kombinere det fysiske kort og netværksanvendelsen.

Det fysiske kort kan være et éngangskort eller genopladeligt. Muligheden for at genoplade et sådant kort kan eventuelt være kombineret med andre an-vendelsesmuligheder (multiapplikationskort).

I Danmark er udstedere af elektroniske penge, der ikke er pengeinstitutter, reguleret ved lov nr. 502 af 7/6 2001.[109] Disse virksomheder skal, hvis de ikke allerede via anden lovgivning er undergivet sådanne krav, have tilladelse fra Finanstilsynet, der også har tilsyn med dem, og der opstilles nærmere regler om kapital m.v. Loven gælder som hovedregel ikke for udstedere, der kun udsteder kort på 75 EUR eller mindre. Der må ikke udstedes elek-troniske penge med en højere værdi end 300 EUR.

Straffelovens § 170 indeholder følgende bestemmelse:

> "Med bøde eller fængsel indtil 3 måneder straffes den, som uden hjemmel i lovgivningen forfærdiger, indfører eller udgiver på ihændehaveren lydende forskrivninger, der fremtræder som bestemt til i snævrere eller videre kred-se at benyttes som betalingsmiddel mand og mand imellem, eller som må forventes at ville blive benyttet på denne måde. Uden for foranstående bestemmelse falder fremmede pengesedler."

Formålet med bestemmelsen er at værne om Nationalbankens eneret til at udstede pengesedler. Udstedelse af multianvendelige elektroniske penge kræver således lovhjemmel efter dansk ret.[110] En naturlig forståelse af be-stemmelsen er, at den vedrører muligheden for at etablere alternative beta-lingsmiddelsystemer og ikke er anvendelig på personer, der forfalsker sådan-ne produkter.

Selve anvendelsen af falske elektroniske penge vil være strafbar, typisk som bedrageri eller databedrageri.

Udvalget har imidlertid på baggrund af udviklingen overvejet, om der er be-hov for en særlig fremrykket strafferetlig regulering vedrørende elektroniske penge.

---

[109] Udstedere af forudbetalte betalingskort var tidligere reguleret ved lov nr. 375 af 22/5 1996 om sparevirksomheder og udstedere af forudbetalte betalingskort.

[110] Spørgsmål om straffelovens § 170 set i forhold til "digitale kontanter" er behandlet på s. 69 f. i rapporten "Regulering af visse betalingsmidler og adgangskoder", Forbrugerstyrel-sen, Erhvervsministeriet, april 1999.

Straffeloven indeholder i §§ 166-169 bestemmelser om eftergørelse og for-falskning af penge m.v. Hovedbestemmelsen – § 166 – har fremrykket fuld-byrdelsesmoment, idet kriteriet er, at penge er eftergjort eller forfalsket for at bringe dem i omløb som ægte. Strafmaksimum i § 166 er fængsel i 12 år. Bestemmelserne vedrører imidlertid kun landenes autoriserede, almindelige betalingsmidler, og de er derfor ikke anvendelige på elektroniske penge.

Udvalget finder, at der også bør være en særlig strafferetlig beskyttelse af elektroniske penge. Udvalget finder, at et strafmaksimum på fængsel i 6 år er passende i betragtning af, at elektroniske penge, til trods for udviklingen hen imod øget brug af sådanne produkter, har en anden karakter end et lands autoriserede almindelige betalingsmidler, hvor det er hele landets beta-lingssystem, der skal beskyttes.

Der henvises til afsnit 8.6.1 vedrørende udvalgets forslag.

4.3. Betalingskort

Anvendelsen af falske betalingskort og af andres ægte betalingskort er straf-bar som dokumentfalsk, bedrageri eller databedrageri. Forud for denne an-vendelse vil der i et vist omfang kunne straffes for forsøg eller forsøg på medvirken samt – for så vidt angår ægte kort – for hæleri, tyveri m.v.

De aktuelle faser kan være produktion, forskaffelse, besiddelse, videregi-velse og anvendelse. Udvalget har set på, om der i relation til de 4 første fa-ser kan være behov for en direkte strafferetlig beskyttelse, uanset at der i øvrigt allerede er en strafferetlig beskyttelse.

4.3.1. Falske betalingskort

Udvalget har drøftet, i hvilket omfang produktion, forskaffelse, besiddelse og videregivelse af falske kort bør kriminaliseres særskilt (spørgsmålet om betalingskortnumre behandles i afsnit 4.3.3). Udvalget er enigt om, at en eventuel kriminalisering bør omfatte alle kort, hvad enten der er anvendt ægte eller genererede kortnumre, så der ikke er en forskel på kriminali-seringen alt efter, hvordan de nødvendige

betalingskortsoplysninger er tilve-jebragt. En eventuel regulering bør omfatte både kort, der kan karakteriseres som dokumenter, og hvor brugen er omfattet af reglerne om dokument-falsk, og hvide kort uden prægning, hvor de relevante oplysninger er over-ført til magnetstrimlen, og hvor brugen typisk vil være omfattet af reglerne om databedrageri.

Det er indgået i drøftelserne, at der på baggrund af den af Gruppen på Højt Plan, der blev nedsat af det Europæiske Råd, i april 1997 udfærdigede hand-lingsplan til bekæmpelse af organiseret kriminalitet[111], i EU-sammenhæng er arbejdet videre bl.a. med spørgsmålet om ikke-kontante betalingsmidler, jfr. indledningen til afsnit 4 om Rådets rammeafgørelse om dele af dette om-råde.

Udvalget finder, at både produktion, forskaffelse, besiddelse med henblik på at anvende kortene som ægte og videregivelse af falske kort bør krimina-liseres som selvstændige delikter. Udvalget finder derimod ikke, at den blot-te besiddelse bør kriminaliseres, hvis et videregående forsæt til brug ikke kan bevises. Der er herved særlig lagt vægt på, at der bør være en tilstrækkelig strafferetlig beskyttelse af betalingssystemer, og at produktion, forskaffelse, besiddelse med henblik på at anvende kortene som ægte og videregivelse af falske kort ikke har noget legitimt formål. Den traditionelle beskyttelse af betalingssystemer ligger efter reglerne om dokumentfalsk eller bedrageri først ved brugen – medmindre forsøgsforsæt kan bevises – og er knyttet til de traditionelle anvendelser af betalingssystemer, hvor der er personlig kon-takt med gerningsmanden, eller hvor denne er identificeret via et kunde-forhold. De IT-relaterede access-produkter har muliggjort reelt anonyme dispositioner, når f.eks. falske kort bruges, og der er bl.a. derfor behov for at lægge en strafferetlig beskyttelse frem til produktion, forskaffelse, besiddelse med henblik på at anvende kortene som ægte og videregivelse af falske kort.

Udvalget har også lagt vægt på, at falske betalingskort er et kriminalitetsom-råde, der ofte er organiseret, og hvor der opereres i mange lande samtidig.[112] Der kan derfor være behov for at kunne

---

[111] 6726/4/97 REV 4.

[112] F.eks. blev der i et kompleks, hvor kort anvendt i Holland var kopieret, opereret såvel i Danmark, England, Holland, Tyskland og Frankrig.

straffe for produktion, forskaffel-se, besiddelse med henblik på at anvende kortene som ægte og videregi-velse af falske kort, uanset om domstolene finder, at forsøgsforsæt kan bevises.

Danmark ser et stigende antal sager med falske betalingskort – både rent danske sager og sager med international tilknytning, jfr. eksempelvis den i afsnit 2.7 nævnte UfR 2000.1881 Ø vedrørende 130 falske betalingskort. I nogle sager er magnetstrimlen kopieret (skimming) i forbindelse med, at det ægte kort er anvendt til en betalingstransaktion.

Den foreslåede kriminalisering kan ske i den form, at produktion, forskaf-felse, besiddelse med henblik på at anvende kortene som ægte og videre-givelse af falske kort kriminaliseres i en særskilt bestemmelse, eller i den form, at kriminaliseringen knyttes til kortets informationer og reguleres i en bestemmelse, der eventuelt omfatter andre betalingsrelevante informa-tioner.

Der henvises til afsnit 8.6.2 vedrørende udvalgets forslag.

4.3.2. Uretmæssig besiddelse af ægte betalingskort

De hensyn, der taler for en fremrykket kriminalisering af besiddelse af falske kort med forsæt til at anvende dem uretmæssigt, gør sig også gældende ved besiddelsen af andres ægte kort.[113]

---

[113] Et flertal i arbejdsgruppen vedrørende datakriminalitet (Jan Carlsen, Hans Jakob Paldam Folker, Jan Friis, Carsten Heilbuth, Ulla Høg, Ronald Pedersen, Kim Aarenstrup) fandt, at det vil være naturligt tillige selvstændigt at kriminalisere uberettiget besiddelse af ægte be-talingskort. En sådan regulering giver en mere ensartet strafferetlig regulering af betalings-kortområdet, der i dag er et meget centralt kriminalitetsområde. Uanset en uberettiget be-siddelse formentlig vil være opnået på en måde, der er strafbar efter de gældende bestem-melser (f.eks. som tyveri, hæleri eller ulovlig omgang med hittegods), vil det være naturligt at have en samlet regulering. Dette vil samtidig overflødiggøre, at der skal føres bevis for, at det ægte kort er kommet i den pågældendes besiddelse ved et nærmere bestemt strafbart forhold. Et mindretal i arbejdsgruppen (Mads Bryde Andersen, Michael Goeskjær, Helle Jahn, Jens Kruse Mikkelsen, Ole Stampe Rasmussen) fandt, at de gældende regler i tilstræk-keligt omfang dækker besiddelse af ægte kort, og at der ikke er behov for en yderligere re-gulering. Mindretallet pegede i den forbindelse på, at man

Det kan være naturligt tillige selvstændigt at kriminalisere uberettiget besid-delse eller videregivelse af ægte betalingskort. En sådan regulering giver en mere ensartet strafferetlig regulering af betalingskortområdet, der i dag er et meget centralt kriminalitetsområde. Uanset en uberettiget besiddelse for-mentlig vil være opnået på en måde, der er strafbar efter de gældende be-stemmelser (f.eks. som tyveri, hæleri eller ulovlig omgang med hittegods), kan det være naturligt at have en samlet regulering. Dette vil samtidig overflødiggøre, at der skal føres bevis for, at det ægte kort er kommet i den pågældendes besiddelse ved et nærmere bestemt strafbart forhold.
På den anden side kan man vanskeligt forestille sig strafværdige tilfælde af uberettiget besiddelse af ægte kort, hvor der ikke kan straffes for f.eks. tyveri, hæleri eller forsøg på databedrageri. Når dette sammenholdes med, at der vil være en identificeret ejer af kortet, der kan forklare nærmere om, hvordan det er mistet, finder udvalget ikke, at der er fuldt tilstrækkeligt grundlag for at regulere området gennem andre bestemmelser end de nu-gældende. Der er ikke behov for tillige at kunne straffe for videregivelsen uden for de situationer, hvor der er forsæt til den videre anvendelse og kan dømmes for forsøg på medvirken.

Udvalget finder således, at det område, der er behov for at regulere, vedrø-rer de situationer, hvor der er tale om falske betalingsmidler.

Der henvises til afsnit 8.6.2 vedrørende udvalgets forslag.

4.3.3. Betalingskortnumre

En særlig problemstilling vedrører betalingskortnumre. Disse numre er per-sonlige, men ikke fortrolige, og er som udgangspunkt beregnet til at indgå i anvendelsen af kortet sammen med dets PIN-kode eller en underskrift.

---

vanskeligt kan forestille sig til-fælde af uberettiget besiddelse af ægte kort, hvor der ikke kan straffes for tyveri, hæleri eller forsøg på databedrageri.

Betalinger med betalingskort på Internettet kan være beskyttet med f.eks. SET-certifikater[114], der skal sikre, at begge parter i transaktionen er iden-tificerede – en identifikation der for kundens vedkommende er knyttet både til den anvendte pc og eksistensen af et gyldigt kort.

I praksis har anvendelsen imidlertid udviklet sig således, at det er muligt at anvende betalingskortnumre til betaling uden fysisk kontakt med betalings-modtageren, uden brug af kortet, uden anvendelse af PIN-kode og uden un-derskrift.

I tilknytning til accepten af denne anvendelse har Forbrugerombudsman-den i december 1996[115] udstedt "Retningslinier vedrørende fjernsalg m.v. i betalingssystemer med betalingskort", der finder anvendelse på fjernsalgs-transaktioner (bl.a. via Internettet). Bestemmelserne sikrer bl.a., at kortinde-haveren ikke kan gøres erstatningsansvarlig for, at han har videregivet det ikke hemmelige nummer på betalingskortet. Kortindehaveren kan komme med indsigelser om misbrug, ikke levering og fortrydelsesret, og kan indsi-gelsen ikke umiddelbart tilbagevises som uberettiget, må det omstridte be-løb ikke betales (eller det skal straks tilbageføres, hvis det er betalt). Der må ikke fastsættes reklamationsfrister for kontohaverens indsigelser.

Handel på Internettet foregår ofte således, at brugeren indtaster sit beta-lingskortnummer for dermed at igangsætte sin betaling. Sådanne internet-forretninger anses for meget udsatte for hacking med henblik på at finde de modtagne numre. En del sager, hvor betalingskortnumre, der er fundet på Internettet, er misbrugt, er dog sager, hvor kortindehaveren ikke har brugt kortet i internetsammenhæng. F.eks. vedrørte misbrug af et norsk kort ved årsskiftet 1997/98 et kort, der ikke havde været anvendt på Internettet. Den pågældende danske misbruger havde imidlertid fundet nogle kortnumre på en svensk

---

[114] SET står for Secure Electronic Transaction. SET er en sikkerhedsstandard for handel på Internettet. Købere og sælgere udstyres med SET-certifikater, og en softwareløsning sikrer automatisk henholdsvis, at sælgerens certifikat valideres, og at kundens certifikat medsendes. Dette giver sikkerhed for, at handelen foretages mellem certificerede parter.

[115] Efter forhandling mellem Forbrugerombudsmanden og Dansk Postordreforening, Pen-geinstitutternes Betalings Systemer (PBS), Finansrådet, Dansk Handel & Service, Dansk Detail Kreditråd, Diners Club Denmark A/S samt Forbrugerrådet.

homepage på Internettet og havde skrevet 3 af de angivne numre ned. To af dem virkede ikke, men det norske gjorde. Gerningsmanden[116] havde anvendt kortnummeret til betaling af ca. 5.800 kr. for adgang til por-nografiske websites.[117]

I en anden sag anmeldte et selskab, at en person, der havde bestilt varer for over 100.000 kr. (og fået leveret for ca. 50.000 kr.), uberettiget havde an-vendt udenlandske betalingskortnumre.

Anvendelsen af andre personers betalingskortnumre vil typisk kunne straf-fes som databedrageri. Om videregivelse, f.eks. via Internettet, kan straffes som forsøg på medvirken (eller som fuldbyrdet forbrydelse, hvis de bevise-ligt er blevet anvendt), vil afhænge af de konkrete omstændigheder, jfr. af-snit 3.2 om adgangsmidler.

Spørgsmålet er, om der bør være en fremrykket strafferetlig beskyttelse ved-rørende betalingskortnumre.

For så vidt angår midler til produktion af betalingskortnumre henvises til af-snit 4.3.4.

For så vidt angår produktion, forskaffelse, besiddelse og videregivelse finder udvalget, at der bør være en fremrykket beskyttelse af kortnumre, når det sker med forsæt til uberettiget brug af kortnumrene. Betalingsformen er i dag almindeligt brugt og bør derfor også accepteres som en almindelig, be-skyttelsesværdig betalingsform.

---

[116] Den pågældende er ved Københavns byrets dom af 27/1 1999 dømt for databedrageri med hensyn til dette forhold.

[117] Ifølge PBS var der i 1999 11.259 internettransaktioner med internationale betalingskort i udenlandske internetforretninger og i 2000 7.568, hvor kortindehaveren gjorde indsigelser mod internettransaktionen. (Der kan være flere transaktioner i en enkelt sag). For så vidt angår Dankort og Visa/Dankort brugt i danske internetforretninger var der i 1999 33 sa-ger, i 2000 311 sager og i 1. halvår af 2001 154 sager, hvor kortindehaveren gjorde ind-sigelser mod internettransaktionen. (Der kan også her være flere transaktioner i den enkelte sag). Tallene indeholder alle indsigelser og ikke kun indsigelser vedrørende misbrug af kort-indehaverens konto. Af andre typiske indsigelsesårsager kan nævnes: Manglende levering af varen/tjenesteydelsen, uenighed om pris og kvalitet og manglende afmelding af abonne-ment.

Den strafferetlige regulering bør tage sit ud-gangspunkt i, hvilke misbrugssituationer der er faktisk forekommende.

Da der kræves forsæt til uberettiget brug består udvidelsen set i forhold til straffelovens § 21 i, at der ses bort fra konkretiseringskravet. Selv om besid-delse typisk vil indgå i produktion, forskaffelse og videregivelse, har udvalget fundet det rigtigst at nævne disse ting særskilt for at undgå fortolk-ningsproblemer omkring besiddelsesbegrebet.

Udvalget er opmærksom på, at det er en vidtgående beskyttelse, fordi sådan-ne betalingskortnumre ikke i sig selv er særligt beskyttede oplysninger. Ud-valget finder imidlertid, at det afgørende må være, om der er en mulighed for at begrænse de potentielle misbrugssituationer ved at give en fremrykket beskyttelse. Der er på dette område, som ved passwords, calling cards m.v., behov for at straffe distributionen, der skaber misbrugsrisikoen.

Udvalget har i denne forbindelse også lagt vægt på, at der ud over i de rele-vante erhvervsmæssige sammenhænge ikke er nogen rimelig interesse i at kunne forskaffe eller videregive andres betalingskortnumre. Tværtimod vil videregivelsen/besiddelsen typisk følges op af et misbrug.

Udvalget finder, at det, som ved calling cards m.v., også bør være strafbart retsstridigt at skaffe sig sådanne numre.

Udvalget finder, at der herudover ikke er behov for en særskilt beskyttelse vedrørende et eventuelt tilhørende SET-certifikat.

Det fremhæves med hensyn til de foreslåede reguleringer, at det kan bero på tilfældigheder, hvad der konstateres på det tidspunkt, hvor politiet kommer ind i sagen. F.eks. vil disse oplysninger i de sager, hvor gerningsmændene ved hjælp af falske frontpaneler til Dankort-automater har kopieret kortets magnetbånd og registreret pinkoden, kunne foreligge som rene oplysninger og kunne være anvendt til falske kort. I de tilfælde, hvor de pågældende fin-des i besiddelse af betalingskortnumre, men hvor falske kort ikke (endnu) er produceret, vil der næppe kunne straffes for forsøg på produktion af falske kort,

fordi betalingsnumrene også kan anvendes selvstændigt uden sådanne kort.

Der henvises til afsnit 8.6.2 vedrørende udvalgets forslag.

4.3.4. Midler til produktion og tilegnelse af betalingskort/-numre

Udvalget har drøftet, om der tillige bør være en fremrykket beskyttelse, der omfatter midler til produktion og tilegnelse af betalingskort eller betalings-kortnumre. Sådanne midler kan i visse tilfælde være lovlige eller være en integreret del i lovlige midler. I mange tilfælde vil den pågældende ikke alene besidde sådanne midler, men også kort eller kortnumre, der allerede er om-fattet af den af udvalget foreslåede regulering. Der vil dog herudover være tilfælde, hvor en selvstændig regulering vil have betydning, f.eks. fordi den pågældende alene indgår i processen med disse midler uden at kunne ifalde ansvar efter medvirkensreglerne.

Udvalget har i denne forbindelse drøftet de programmer til generering af betalingskortnumre, der distribueres via Internettet. Princippet er, at hvis man f.eks. har fundet en credit card eller en Dankortbon, så kan der ved hjælp af sådanne programmer genereres det ønskede antal kortnumre. Programmet indeholder bankregistreringsnumre og er lavet på baggrund af den algoritme, der bruges til at generere betalingskort. Kortnumrene vil fremtræde som gyldige ved kontrol med et valideringsprogram. Generator-programmet vil også kunne generere kortnumre uden et underliggende bilag. De programmer af denne type fra Internettet, udvalget har kendskab til, er alle programmer, der alene har disse funktioner, og ikke tillige andre (lovlige) funktioner.

Udvalget er enigt om, at genererede betalingskortnumre – der kan være identiske med numre, der allerede er tildelt en betalingskortindehaver – bør behandles på samme måde som andre betalingskortnumre, jfr. afsnit 4.3.3.

Et andet særligt middel, udvalget har drøftet, er de frontpaneler, der har væ-ret anvendt på Dankortautomater. Her vil produktion af middel, montering af det og besiddelse og udnyttelse af oplysningerne

typisk være led, der varetages af forskellige personer. Uanset der eventuelt kan dømmes for for-søg på medvirken til (et eller andet) bedragerisk forhold samt til uretmæssigt at skaffe sig betalingskortnumre og pinkoder, kan det overvejes tillige at have en direkte regulering. Se i øvrigt herom afsnit 3.2.3 om sådanne midler i relation til passwords.

Udvalget finder, at spørgsmålet om, hvorvidt der bør være en direkte strafferetlig regulering vedrørende sådanne midler, må besvares på samme måde som ved midler til tilvejebringelse af adgangsmidler, jfr. afsnit 3.2.3.[118]

Der henvises til afsnit 8.1.3 vedrørende udvalgets forslag.

4.4. Andre elektroniske kontooverførsler

Elektroniske kontooverførsler kan foretages på forskellig måde. De mest kendte former i dag er home banking eller on line banking samt elektroni-ske checks.

Der er på nuværende tidspunkt ikke særlige problemer knyttet til disse kon-tooverførsler. Adgangen er beskyttet med passwords, jfr. udvalgets over-vejelser vedrørende passwords i afsnit 3.2, og misbrug i

---

[118] Et flertal i arbejdsgruppen vedrørende datakriminalitet (Mads Bryde Andersen, Hans Jakob Paldam Folker, Michael Goeskjær, Carsten Heilbuth, Helle Jahn, Jens Kruse Mik-kelsen, Ronald Pedersen) fandt ikke, at der er behov for en selvstændig beskyttelse. Disse medlemmer har for så vidt angår betalingskortnummergeneratorprogrammer særligt lagt vægt på, at der er tale om enkle og kendte algoritmer, der allerede indgår i en række andre sammenhænge, f.eks. programmer til validering af opgivne kortnumre. Et mindretal i arbejdsgruppen (Jan Carlsen, Jan Friis, Ulla Høg, Ole Stampe Rasmussen, Kim Aarenstrup) fandt, at der også bør være en direkte strafferetlig regulering vedrørende sådanne midler. Disse medlemmer ser dette som et naturligt led i beskyttelsen mod misbrug af betalings-kort. For så vidt angår betalingskortnummergeneratorprogrammer er det efter disse med-lemmers opfattelse væsentligt, at en ændret strafferetlig regulering udsender et klart "sig-nal" om, at det ikke accepteres, at Internettet (eller andre netsystemer) direkte eller in-direkte opfordrer til eller muliggør kriminalitet. For så vidt angår frontpaneler og lignende midler er det efter disse medlemmers vurdering af betydning, at der er en direkte regule-ring af dette meget sårbare område.

berigelsesøjemed er dækket af straffelovens bestemmelser om berigelseskriminalitet, hvor især straffelovens § 279 a om datakriminalitet vil være aktuel.

4.5. Misbrug af andres teleforbindelser

Misbrug af andres teleforbindelser kan dels ske på den måde, at der er tale om en handling, der kræver fysisk forbindelse med andres teleapparater eller telelinier, og dels i form af et "fjernmisbrug", der har konteringsmæssige konsekvenser, men ikke kræver, at gerningsmanden har fysisk kontakt med andres ejendele.

Misbrug i forbindelse med fysisk kontakt – typisk uberettiget brug af en andens telefon eller pc – er omfattet af straffelovens § 293, stk. 1, om brugs-tyveri.

Udvalget har drøftet, om det i dag vil være mere naturligt at anvende straf-felovens § 279 a om databedrageri ud fra den betragtning, at anvendelsen af teleforbindelsen er et signal til telesystemet om, at indehaveren af forbin-delsen skal konteres for sin brug, og at der således er tale om en retsstridig påvirkning af en databehandling, der i de typiske tilfælde indebærer vinding og tab.[119] Om tabet rammer indehaveren af teleforbindelsen eller telesel-skabet vil bero på den aktuelle aftaleretlige og erstatningsretlige regulering i den aktuelle situation. Situationen adskiller sig derved fra det mere tradi-tionelle forbrug i forbindelse med brugstyveri (f.eks. forbrug af benzin), hvor indehaveren af genstanden for brugstyveriet og af det, der forbruges, er samme person.

Udvalget har i forbindelse hermed drøftet, om telemisbrug burde reguleres samlet i f.eks. et stk. 2 til straffelovens § 279 a. Udvalget har imidlertid ikke fundet, at der er behov for en sådan særskilt regulering.

Udvalget finder, at selv om der på grund af den teknologiske udvikling er opstået en vis overlapning mellem straffelovens § 293, stk. 1, og dens

---

[119] I nogle situationer – f.eks. hvor der er døgnopkobling til Internettet til fast pris – vil der ikke være et tab for indehaveren af telefonen, men kun for teleselskabet i form af, at den pågældende ikke giver merindtægt som kunde.

§ 279 a på teleområdet, bør udgangspunktet være, at § 293, stk. 1, fortsat anven-des ved telemisbrug, der kræver fysisk forbindelse med andres teleapparater eller telelinier, så dette behandles på samme måde som andre former for uberettiget brug af andres ting. Udvalget vil dog påpege, at der kan være situationer, der ligger så fjernt fra det traditionelle brugstyveri, at det vil være mere naturligt at bruge bestemmelsen om databedrageri. Som eksem-pel kan nævnes, at f.eks. en trådløs telefon benyttes via fjernbetjening fra en anden lokalitet.

Udviklingen på teleområdet har medført helt nye muligheder for "fjern-misbrug" – enten ved brug af gennemvalgstelefoner, ved misbrug af andres calling cards, ved at anvende Internettet via andres computere eller ved at anvende hackede telefonnumre i mobiltelefoner. Dette område var i begyn-delsen af 90'erne genstand for en ret uensartet praksis.
I de første telefonmisbrugssager af denne type tiltaltes for henholdsvis be-drageri og tyveri, subsidiært for brugstyveri, og der dømtes for brugstyveri. I en enkelt sag blev der dog dømt for tyveri. I mobiltelefonsituationen blev der tiltalt og dømt for databedrageri. I de senere sager er der lagt vægt på, at telefonsystemerne og telefonselskabernes betalingssystemer har udviklet sig således, at der i denne type tilfælde, hvis ingen fysiske personer vildledes for at gennemføre handlingen, er tale om databedrageri.

I de første hackersager blev den del af problemstillingen, der vedrørte tele-fonmisbrug, slet ikke medtaget, selv hvor man klart havde hacket sig ind for at benytte anlægget som relæstation for videre datatrafik. Det bemærkes, at mens det er en vanskelig og tidskrævende – eventuelt umulig – opgave at spore, hvad der videre er sket, herunder om gerningsmanden har hacket videre, eller om han helt eller delvist er fortsat til områder, hvortil han havde legal adgang, vil det ofte være lettere at spore, hvad han har belastet telefonregningen med.[120] Det kan derfor i nogle tilfælde være hensigts-mæssigt at vælge databedrageriet, eventuelt kombineret med den indledende hacking, og lade spørgsmålet

[120] I den første kendte større danske sag på området, hvor en dansk computer blev opereret fra Tyskland som relæstation, blev forholdet opdaget, fordi telefonregningen var 8 gange større end normalt, hvorfor man klagede til KTAS. En undersøgelse over 3 uger viste der-efter over 3.000 opkald til hele verden.

om viderehacking ligge, eller – i det omfang man har konkrete oplysninger – overlade sagen til myndighederne i det an-grebne land.

Den norske højesteretskendelse, der er nævnt i afsnit 3.2.1.3 om calling cards m.v., tog også stilling til dette spørgsmål for norsk rets vedkommende og fandt, at både misbrug af gennemvalgstelefoner og videreopkoblinger, så andres telefoner benyttedes, var omfattet af den norske bestemmelse om databedrageri (der indholdsmæssigt svarer til den danske, jfr. afsnit 2.5.2).

Ved lov nr. 388 af 22/5 1996 indførtes adgang til teleoplysninger i telefon-misbrugssager, men der blev på grund af den meget vaklende retspraksis ik-ke taget stilling til, om § 293, stk. 1, eller § 279 a skulle anvendes i disse sa-ger. Justitsministeriet anførte i bemærkningerne til lovforslaget, at forskelle i den tekniske fremgangsmåde eventuelt kunne begrunde anvendelsen af for-skellige straffebestemmelser. En eventuel regulering blev henvist til det ud-valg, der skulle nedsættes (nærværende udvalg).

I den tidligere nævnte hackersag[121] blev der tiltalt og dømt for databedrageri i forbindelse med de tiltaltes misbrug af NUI-brugerkoder i Datapaksy-stemet og af frikaldsnumre. Det nævnes i rettens pressemeddelelse, at "ty-veri af telefontid" er bedømt efter straffelovens § 279 a om databedrageri, og at dette hidtil for det meste er blevet bedømt efter den mildere § 293, stk. 1, om brugstyveri.

Også i de senere domme, udvalget er bekendt med, er det bestemmelsen om databedrageri, der er anvendt, jfr. bl.a. de i afsnit 3.2.1.3 om calling cards nævnte domme. I den ene af dommene[122] blev der dømt for data-bedrageri i forbindelse med telefonsamtaler i 262 timer til en værdi af ca. 300.000 kr. bl.a. som solgte trepartssamtaler. Den tiltalte havde foretaget opkaldene via sin computer med indbygget såkaldt Blue Boxing system, hvori der var indkodet Country Direct 800-numre.

I enkelte sager har calling cards været anvendt således, at de skulle oplyses til en telefonist, der derefter etablerede den ønskede samtale og

[121] Roskilde rets dom af 19/12 1996.
[122] Københavns byrets dom af 23/9 1997.

sørgede for korrekt kontering. Der er her tale om en traditionel bedragerisituation, der efter udvalgets opfattelse fortsat skal behandles efter bedrageribestem-melsen i straffelovens § 279.

Udvalget er ikke bekendt med fjernmisbrugssituationer, der ikke indebærer enten vildledning af personer eller påvirkning af informationssystemer.

Udvalget finder, at de gældende regler er dækkende, og at der ikke er behov for ny lovgivning på området.

Med hensyn til spørgsmålet om at supplere med en fremrykket beskyttelse i de tilfælde, hvor andres calling cards, NUI-koder m.v. benyttes, henvises til afsnit 3.2.1.3.

KAPITEL 5
ELEKTRONISKE DOKUMENTER

5.1. Indledning

IT-samfundet indebærer, at elektronisk kommunikation i stigende grad er-statter den traditionelle skriftlige kommunikation. Som konsekvens

heraf er der behov for at tilpasse lovgivningen til ændrede kommunikationsfor-mer.[123]

I bemærkningerne til lovforslag nr. L 202 (1995-96) om ændring af straffe-lovens og retsplejeloven (datakriminalitet)[124], der bl.a. vedrørte ændring af straffelovens § 163, jfr. afsnit 2.4, siges om Rigsadvokatens indstilling om en ændring af straffelovens § 163, at den er i overensstemmelse med et forslag i Dybkjær-udvalgets rapport fra 1994 "Info-samfundet år 2000", hvor det bl.a. foreslås, at ministerierne vurderer eventuelle krav i lovgivningen om skriftlighed med henblik på at fjerne hindringer for papirløs kommunika-tion.

Det nævnes også, at det er tanken at iværksætte et udvalgsarbejde bl.a. om behovet for at ændre straffelovens kapitel 19 om dokumentforbrydelser, og at der som led i udvalgsarbejdet vil kunne være anledning til mere prin-cipielle overvejelser vedrørende begreberne dokument- og erklæringsfalsk, herunder i relation til edb-medier. Det siges videre, at udvalget i den for-bindelse kunne overveje den nærmere afgrænsning af det strafbare område i straffelovens § 163, også i lyset af eventuelle bevismæssige problemer, der måtte være knyttet til muligheden for at ændre i data på edb-medier.

IT-sikkerhedsrådet udtalte i sit høringssvar til lovforslaget, at rådet var enigt med Justitsministeriet i, at den seneste retspraksis om anvendelsen af straf-felovens § 163, hvor urigtige oplysninger var afgivet på edb-filer, rejste et behov for at tilpasse bestemmelsen, således at den strafferetlige regulering af urigtige skriftlige erklæringer kunne videreføres på det digitale område. Der-imod var IT-sikkerhedsrådet betænkelig ved forslaget om at gennemføre denne ændring ved henvisningen til "andet læsbart medie".

IT-sikkerhedsrådet udtalte bl.a., at en henvisning til "andet læsbart medie", der ikke var ledsaget af yderligere krav om sikkerhed m.v. for de pågælden-de edb-data, kunne efterlade stor bevismæssig tvivl, som det ville være van-skeligt for domstolene efterfølgende at forholde sig

---

[123] Se Mads Bryde Andersen, IT-retten (2001), s. 629 ff., hvor de generelle spørgsmål om elektronisk dokumenthåndtering er behandlet. På s. 203 ff. er forskellen mellem papirme-diet og det digitale medium (og de hertil knyttede bevisspørgsmål) skitseret.
[124] FT 1995/96 A 4068.

til. En fyldestgørende behandling af spørgsmålet ville efter rådets opfattelse bedst ske som led i en samlet regulering af sikkerheden ved digital kommunikation, herunder ved brug af public key-kryptering under anvendelse af troværdige tredjeparter.

Justitsministeriet anførte i forskellige svar til Folketingets Retsudvalg, at det påhvilede anklagemyndigheden at føre bevis for, at der var begået et straf-bart forhold. Justitsministeriet fandt ikke, at der var grundlag for i straffe-loven at fastsætte bestemte sikkerhedskrav til de meddelelser, der afgives på "andet læsbart medie".

Under udvalgets arbejde med denne betænkning er der blevet lovgivet om elektroniske signaturer.

Lov nr. 417 af 31/5 2000 om elektroniske signaturer definerer en "elektro-nisk signatur" som:

> "Data i elektronisk form, der knyttes til andre elektroniske data ved hjælp af et signaturgenereringssystem, og som anvendes til at kontrollere, at disse data stammer fra den person, der er angivet som underskriver, og at de ikke er blevet ændret."

Loven definerer endvidere en "avanceret elektronisk signatur" som:

> "En elektronisk signatur, der
> a) entydigt er knyttet til underskriveren,
> b) gør det muligt at identificere underskriveren,
> c) skabes med midler, som kun underskriveren har kontrol over, og som
> d) er knyttet til de data, den vedrører, på en sådan måde, at enhver ef-terfølgende ændring af disse data kan opdages."

Loven opstiller i øvrigt en række krav til kvalificerede certifikater og de dan-ske nøglecentre, der kan udstede sådanne.

Efter lovens § 13 skal bestemmelser i lovgivningen, hvorefter elektroniske meddelelser skal være forsynet med signatur, anses for opfyldt, hvis medde-lelsen er forsynet med en avanceret elektronisk signatur, der er baseret på et kvalificeret certifikat, og som er fremstillet ved brug af et sikkert signatur-genereringssystem. For så vidt angår offentlige myndigheder gælder dette kun, såfremt andet ikke følger af lov eller bestemmelser fastsat i medfør af lov.

Vedrørende certifikater fra andre lande bestemmer lovens § 23, at kvali-ficerede certifikater udstedt af lande uden for EØS skal anerkendes på sam-me måde som kvalificerede EØS-certifikater, såfremt nøglecentret opfylder kravene i loven og er tilsluttet en frivillig akkrediteringsordning i en med-lemsstat, eller et EØS-nøglecenter indestår for certifikatet, eller certifikatet eller nøglecentret er anerkendt i henhold til bilateral eller multilateral aftale med EU.

For en nærmere oversigt over loven om elektroniske signaturer henvises til Mads Bryde Andersen, IT-retten (2001), s. 196 ff., samt til udredningen samme sted s. 184 ff., der skitserer den tekniske problemstilling, der ligger til grund for denne lovgivning.

Ved loven gennemføres Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13/12 1999 om en fællesskabsramme for elektroniske signaturer.[125]

Direktivets artikel 5, stk. 2, siger om elektroniske signaturer, der ikke kan betragtes som avancerede:

> " Medlemsstaterne sikrer, at en elektronisk signatur ikke nægtes retlig gyl-dighed og anerkendelse som bevis under retssager alene af den grund, at den
> - er i elektronisk form, eller
> - ikke er baseret på et kvalificeret certifikat, eller
> - ikke er baseret på et kvalificeret certifikat udstedt af en akkrediteret certificeringstjenesteudbyder, eller
> - ikke er genereret af et sikkert signaturgenereringssystem."

I betænkning nr. 1400/2000 om e-signatur og formkrav i lovgivningen an-befaler Justitsministeriets udvalg om retsvirkningerne af digital signatur m.v., at der indføres en generel lovregel, som uanset formkrav i lovgiv-ningen gør det muligt for vedkommende minister at bestemme, at der på nærmere angivne områder kan anvendes læsbar digital kommunikation ved henvendelser til den offentlige forvaltning og de nærmere vilkår herfor.[126]

---

[125] EFT L 2000 13/12.

[126] Betænkningen s. 155.

Udvalget finder, at straffeloven bør tilpasses, så den omfatter elektroniske dokumenter og elektronisk kommunikation. Udvalget finder, at spørgsmå-let om elektronisk signatur ikke bør indgå i den vurdering. Betydningen af anvendelse af elektronisk signatur vil således især være, at det vil forenkle en eventuel bevisførelse om, hvorvidt den tiltalte selv har afgivet erklæringen.

5.2. Straffelovens § 163 om erklæringer

Straffelovens § 163 om urigtige erklæringer til offentlige myndigheder lyder således:

> "Den, som i øvrigt til brug i retsforhold, der vedkommer det offentlige, skriftligt eller ved andet læsbart medie afgiver urigtig erklæring eller skrift-ligt bevidner noget, som den pågældende ikke har viden om, straffes med bøde eller fængsel indtil 4 måneder."

Som nævnt i afsnittene 2.4 og 2.6 blev bestemmelsen på baggrund af en fri-findende dom vedrørende disketter ændret i 1996[127], hvor kravet om skrift-lige erklæringer blev suppleret med "eller ved andet læsbart medie". Det fremgår af lovforslaget[128], at erklæringen også skal være læsbar for afsende-ren, og at indtastning af oplysninger på en telefon eller indtaling, der omsæt-tes til læsbar form, ikke er omfattet.

Justitsministeriet anførte i lovforslaget, at en fuldstændig afskaffelse af skriftlighedskravet efter Justitsministeriets opfattelse hverken er ønskelig el-ler hensigtsmæssig. Det nævnes i den forbindelse, at en så vidtrækkende sandhedspligt i forhold til offentlige myndigheder bl.a. vil indebære strafan-svar for urigtige (mundtlige) forklaringer til politiet, medmindre der udtryk-keligt gøres undtagelse for disse tilfælde. Det siges videre, at forarbejderne til straffelovens § 163 – og til den tidligere bestemmelse i 1866-straffelovens § 155 – ikke indeholder nogen udtrykkelig begrundelse for kravet om skrift-lighed, men at det er nærliggende at antage, at man – uden for de tilfælde, hvor erklæringen er pligtmæssig, jfr. § 162 – har villet begrænse strafan-svaret til tilfælde, hvor man gennem erklæringens form sikrer sig, at bor-geren er klar over, at erklæringen tillægges vægt i myndighedens

[127] Ved lov nr. 388 af 22/5 1996.

[128] FT 1995/96 A 4068.

arbejde og eventuelt kan indgå i grundlaget for myndighedens arbejde i en konkret sag.

Rigsadvokaten henviste i sit høringssvar over lovforslaget til, at to statsad-vokater havde påpeget, at det visuelle kriterium måske gjorde bestemmel-sen for snæver. Rigsadvokaten anførte i sit høringssvar af 29/12 1995, at spørgsmålet om en yderligere udvidelse burde behandles i det udvalg, der skulle nedsættes.

Udvalget har nærmere drøftet de forskellige teknikker, der kan indgå i en digital meddelelsesproces. Det er f.eks. blevet almindeligt, at meddelelser afgives ved "tast selv"-ordninger. En indtastning af oplysninger via telefo-nen kombineres ofte med en kontroltilbagemelding om, hvad der er ind-tastet, således at det ikke er muligt at være i tvivl om indholdet af den erklæ-ring, man har afgivet via indtastning. Også muligheden for verbalt at afgive en meddelelse, der konverteres til en digital meddelelse, er et område, der kan forventes at blive stadig mere almindeligt.

Som det fremgår af Justitsministeriets bemærkninger til ovennævnte lovfor-slag indeholder straffelovens forarbejder ikke nogen udtrykkelig begrundel-se for kravet om skriftlighed.

Da straffeloven blev udarbejdet, var der ikke de teknologiske muligheder, der er i dag. Spørgsmålet er, om læsbarhed for borgeren bør være en for-udsætning for strafansvar.

Udvalget finder, at det i hvert fald må være en forudsætning for en re-gulering i straffeloven, at borgeren har mulighed for at konstatere, om der f.eks. er indtalt eller indtastet forkert. Såfremt der ønskes en yderligere re-gulering af indtastede erklæringer o.l., bør dette ske i den aktuelle særlov-givning.

Udvalget finder, at det i relation til en generel regulering i straffeloven er be-hæftet med for stor usikkerhed at gøre en urigtig erklæring strafbar, hvis den både afgives og bekræftes i en form, der ikke er læsbar for afgiveren (ved indtastning uden synligt tekstbillede, talt).[129]

---

[129] Arbejdsgruppen vedrørende datakriminalitet fandt, at der burde ske en regulering også vedrørende erklæringer, der kun er læsbare for modtageren.

Derimod finder udvalget, at er-klæringer, der afgives i en form, der ikke er læsbar for afsenderen, men som bekræftes fra modtageren i en læsbar form, og hvor modtagelsen bekræftes med mulighed for korrektion, bør være omfattet. Udvalget finder, at denne erklæringsform allerede er dækket af ordlyden i straffelovens § 163.

Udvalget har overvejet, om det alligevel burde præciseres i bestemmelsen, at erklæringen kan afgives ved accept af en læsbar bekræftelse, men har fundet, at der ikke er behov derfor. Denne erklæringsvariation adskiller sig kun fra den fra starten for alle læsbare erklæring ved, at den først er afgivet, når afgiveren har haft mulighed for at læse den og har bekræftet modtagelsen.

Der er derimod ikke tale om, at mundtlige forklaringer – f.eks. til politirap-port – som nedfældes i skriftlig form af modtageren, bliver omfattet af be-stemmelsen, fordi de forelægges den afhørte til gennemlæsning og godken-delse.

Der henvises til afsnit 8.7.1.

5.3. Straffelovens §§ 171-175 om dokumenter

Straffelovrådet fandt i betænkning nr. 1032/1985 om datakriminalitet[130], at § 171 ikke var egnet til at blive omformuleret til at dække urigtige erklæringer i form af dataoplysninger, og at der på daværende tidspunkt ikke var behov for særregler om urigtige erklæringer ved hjælp af datateknik. Det anførtes dog, at dokumentbegrebet i norsk ret er defineret således, at ikke-udskrevne dataoplysninger kan udgøre et dokument. Det anførtes videre, at det danske krav om udstederbetegnelse kun har praktisk mening, når det forudsættes, at dokumentet har fået form af et stykke papir eller lignende, og at der til datalagrede oplysninger normalt ikke er knyttet anden udstederbetegnelse end den, der ligger i, at dataanlægget har en retmæssig indehaver.

Den nye § 155 i den islandske straffelov, jfr. afsnit 2.5.1, dækker også dokumenter, der opbevares i maskinlæsbar form.

---

[130] Betænkningen s. 59–64.

Dokumentdefinitionen i § 179 i den norske straffelov, jfr. afsnit 2.5.2, dækker også elektroniske dokumenter.

Også den finske straffelovs 33. kapitel § 6 dækker elektroniske dokumenter, jfr. afsnit 2.5.4.

I Sverige blev der i 1992[131] foreslået en ændring af bestemmelserne i den svenske straffelovs kapitel 14 om förfalskningsbrott, således at begrebet "urkund" erstattedes med "dokument", og at dokumentfalskbestemmelsen i § 1 fik tilføjet et nyt stk. 2 med følgende ordlyd:

> "Med dokument avses i detta kapitel en skriftlig originalhandling eller en bestämd mängd data för automatisk informationsbehandling, om det är möjligt att fast-ställa att innehållet härrör från den som framstår som utställara. Som dokument anses också legitimationskort, biljett och dylikt bevismärke."

Forslaget overvejes ifølge SOU 1998:122[132] i justitiedepartementet.

Med den udvikling, der har været siden 1985, og den, der må forventes vide-re frem, er det nærliggende at etablere et strafferetligt værn omkring dataop-lysninger, der erstatter dokumentanvendelse.

Den nuværende definition af et dokument findes i straffelovens § 171, stk. 2. Straffelovens bestemmelser om dokumentfalsk lyder således:

> "§ 171. Den, der gør brug af et falsk dokument til at skuffe i retsforhold, straffes for dokumentfalsk.
> Stk. 2. Ved dokument forstås 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.
> Stk. 3. Et dokument er falsk, når det ikke hidrører fra den angivne udste-der, eller der er givet det et indhold, som ikke hidrører fra denne.
>
> § 172. Straffen for dokumentfalsk er fængsel, der i tilfælde af, at dokumentet angiver sig at indeholde en offentlig myndigheds afgørelse, eller at det er en offentlig forskrivning, en check, veksel eller andet til

[131] SOU 1992:110 om Information och den nya InformationsTeknologin.

[132] Om E-pengar – civilrättsliga frågor mm, afgivet i oktober 1998.

> almindeligt omløb bestemt dokument eller en testamentarisk bestemmelse, kan stige til 8 år.
> Stk. 2. Er dokumentet efter sin beskaffenhed, eller er forfalskningen eller det, som derved søges opnået, af underordnet betydning, eller har den skyldige ikke tilsigtet at påføre andre nogen skade, såsom når øjemedet alene har været at gennemføre et berettiget eller at afværge et uberettiget krav, er straffen bøde eller fængsel indtil 1 år."

Spørgsmålet om udstederbetegnelse er primært et spørgsmål om, hvorfra dokumentet hidrører, og dette spørgsmål kan antagelig løses på flere måder. Der stilles ikke efter § 171 krav om, at udstederbetegnelsen skal have karak-ter af en underskrift.

Det synes umiddelbart at være en for snæver regulering, hvis man ønsker at have strafferetlig dækning for elektronisk dokumentfalsk, hvis man kun dækker området med de af loven omfattede avancerede elektroniske sig-naturer eller dog stiller krav om signatur. Det vil være mere nærliggende at dække alle elektroniske tilkendegivelser, der har en klart angivet udsteder, således at reguleringen svarer til den nuværende regulering.[133]

En ændring af ordet "skriftlig" i straffelovens § 171, stk. 2, til "læsbar" vil eventuelt være tilstrækkeligt. Mod anvendelse af den eksisterende bestem-melse kan imidlertid tale, at den er "skræddersyet" til skriftlige dokumenter, og at der derfor vil kunne opnås en større klarhed ved at formulere en selv-stændig bestemmelse om falske elektroniske dokumenter.

Særligt vedrørende e-mail kan dokumentspørgsmålet diskuteres. I princippet kan e-mail udskrives og blive et skriftligt dokument, men meget ofte vil e-mail blive læst og eventuelt lagret, men ikke udskrevet. Ved Københavns byrets dom af 29/5 2001, der er stadfæstet af Østre Landsret den 26/9 2001, blev der i et forhold dømt for dokumentfalsk i forbindelse med, at den til-talte med angivelse af en andens navn telefonisk meddelte en betalingskort-udsteder, at hans kort var bortkommet, og derefter sendte en e-mail med oplysning om, at et nyt kort skulle sendes til en c/o-adresse.

---

[133] Arbejdsgruppen vedrørende datakriminalitet fandt ligeledes, at der burde indsættes en bestemmelse om elektronisk dokumentfalsk.

Langt de fleste tilfælde af dokumentfalsk begås i praksis i forbindelse med et bedrageri, f.eks. brug af falske checks, kvitteringer eller kontrakter. I sådan-ne tilfælde straffes der i retspraksis som udgangspunkt alene for dokument-falskforbrydelsen, selv om denne forbrydelse ikke begrebsmæssigt kan siges at indbefatte et samtidigt bedrageri. Udvalget har overvejet, om denne rets-tilstand bør opretholdes, eller om der fremover i stedet alene bør straffes for bedrageri, således at et samtidigt dokumentfalsk absorberes, eller om der eventuelt bør statueres sammenstød, således at der straffes både for doku-mentfalsk og for bedrageri. Udvalget finder, at der fremover i de tilfælde, hvor der ved brug af et falsk dokument begås bedrageri, bør statueres sam-menstød, således at der straffes både for dokumentfalsk og for bedrageri. Dette giver efter udvalgets opfattelse den bedst dækkende beskrivelse af det begåede forhold.

Udvalget har drøftet, om en bestemmelse om elektroniske dokumenter bør være mere forenklet end den nugældende dokumentfalskbestemmelse. Re-sultatet af disse drøftelser er, at udvalget finder, at den forenklede bestem-melse bør være en fælles bestemmelse for fysiske og elektroniske dokumen-ter.

Den nugældende bestemmelse hidrører fra en tid, hvor selve brugen af skrift forlenede en meddelelse med en særlig aura. I dag, hvor alt skrives, fysisk eller elektronisk, er dette klart ikke længere tilfældet.

Bestemmelsen skelner mellem hensigtsdokumenter ("der ... fremtræder som bestemt til at tjene som bevis") og lejlighedsdokumenter ("der ... bli-ver benyttet som bevis for en rettighed, en forpligtelse eller en befrielse for en sådan"). Medens hensigtsdokumentbegrebet er klart, opfylder lejligheds-dokumentet ikke nutidens krav til præcision i straffebestemmelser. Skønt der gennem det 20. århundrede blev udfoldet store bestræbelser på at give begrebet et præcist indhold, er det ikke lykkedes for teorien eller praksis at opnå dette.

Straffelovsbetænkningerne fra 1912, 1917 og 1923 indeholder ikke egentlige fortolkningsbidrag til, hvad der er lejlighedsdokumenter.

Hensigtsdokumenter er eksempelvis eksamensbeviser, medlemskort, køre-kort, pas, visa, vielsesattester, dåbsattester, anbefalinger med

faktiske oplys-ninger, attestationer, kvitteringer, kontrakter, bestillinger, ordrebekræftelser, fakturaer, gældsbreve, checks, veksler og fuldmagter. Endvidere vil ansøg-ninger, erklæringer m.v. efter omstændighederne kunne være omfattet.

Der er ikke mange bidrag i trykt praksis til belysning af, hvad der efter omstændighederne i forbindelse med den konkrete brug kan være et lejlig-hedsdokument. Som eksempler kan nævnes UfR 1937.151 V (et privat brev med anerkendelse af, at lån var ydet), VLT 1938.177 (to postkort med tilbud om arbejde) og UfR 1966.462 V (mødekort til hospitalsindlæggelse påført urigtige mødedatoer for at få rejsegodtgørelse).

Udvalget finder, at dokumentfalskbestemmelsen ikke bør omfatte lejlig-hedsdokumenter. Dels mangler denne del af bestemmelsen som nævnt præcision, dels tyder den sparsomme retspraksis ikke på, at der er behov for bestemmelsen. Forholdet er antagelig det, at straf for brug af falske lejlig-hedsdokumenter i praksis ikke behandles efter dokumentfalskbestemmel-sen, men efter andre strafbestemmelser, der vedrører brugen af dokumentet (f.eks. til bedrageri). Såfremt den konkrete anvendelse af (lejligheds)doku-mentet ikke er kriminaliseret, er der næppe heller behov for at kunne straffe for dokumentfalsk i disse tilfælde.

Dokumentfalskbestemmelsen er et formaldelikt. Sådanne absorberes i al-mindelighed af tilsvarende skadedelikter i tilfælde af sammenstød. I praksis er langt hovedparten af tilfældene i praksis dokumentfalsk i forbindelse med berigelsesforbrydelser, f.eks. forfalskning af kvitteringer og kontrakter. Ud-valget er af den opfattelse, at man også på dette område bør drage kon-sekvensen af de hensyn, der ligger bag det almindelige absorptionsprincip, og lade skadedeliktet (berigelsesforbrydelsen) være det primære. Derved vil man opnå, at forholdet betegnes som det, det egentlig er.

I praksis vil de resterende tilfælde af dokumentfalsk vedrøre hensigts-dokumenter, f.eks. eftergørelse eller forfalskning af kørekort, pas, visa, viel-sesattester, dåbsattester osv., der også kan forfalskes af mange andre grunde end for at opnå en berigelse. Der er her tale om delikter, som i grovhed lader sig sammenligne med f.eks. straffelovens §§ 161-163 (der

straffes med bøde eller fængsel indtil 4 måneder, § 161 dog med fængsel indtil 2 år under skærpende omstændigheder).

Udvalget finder på denne baggrund, at bestemmelsen bør omfatte både fy-siske og elektroniske tilkendegivelser, der er bestemt til at tjene som bevis, og at strafmaksimum bør være fængsel i 2 år.

Udvalget finder endvidere, at dokumentdefinitionen bør omfatte begge for-mer for tilkendegivelser. Det er derfor ikke nødvendigt at ændre ordlyden af straffelovens §§ 173-174 for så vidt angår dokumenter, da dokument-begrebet i disse bestemmelser svarer til dokumentfalskbestemmelsen. Disse bestemmelser lyder således:

> "§ 173. Med straf som i § 172 angivet anses den, der benytter et med ægte underskrift forsynet dokument til at skuffe i retsforhold, når underskriften ved hjælp af en vildfarelse er opnået på et andet dokument eller på et dokument af andet indhold end af underskriveren tilsigtet.
>
> § 174. Den, som i retsforhold gør brug af et ægte dokument som vedrørende en anden person end den, hvem det virkelig angår, eller på anden mod dokumentets bestemmelse stridende måde, straffes med bøde eller fængsel indtil 6 måneder."

Udvalget har endvidere overvejet, om der er behov for tillige at ændre straf-felovens § 175. Bestemmelsen lyder således:

> "§ 175. Den, som for at skuffe i retsforhold i offentligt dokument eller bog, i privat dokument eller bog, som det ifølge lov eller særligt pligt-forhold påhviler ham at udfærdige eller føre, eller i læge-, tandlæge-, jordemoder- eller dyrlægeattest afgiver urigtig erklæring om noget forhold, angående hvilket erklæringen skal tjene som bevis, straffes med fængsel indtil 3 år eller under formildende omstændigheder med bøde.
> Stk 2. På samme måde straffes den, der i retsforhold gør brug af et sådant dokument som indeholdende sandhed."

For så vidt angår de i § 175 nævnte dokumenter og bøger, kan der være tale om bøger, der ikke er omfattet af definitionen i dokumentfalskbestemmel-sen, f.eks. fordi tilknytningsforholdet fremgår af, hvor dokumentet eller bogen føres, uden at der tillige er en udstederbetegnelse. Udvalget foreslår derfor, at det præciseres i bestemmelsen, at reguleringen også vedrører andre læsbare medier.

Udvalget foreslår endvidere, at bestemmelsens stk. 2 om straf for den, der i retsforhold gør brug af et sådant dokument som indeholdende en sandhed, udvides til også at omfatte de af stk. 1 omfattede bøger.

Bestemmelsen i stk. 2 kom ind i straffelovsbetænkningen fra 1923. Det fremgår ikke af betænkningen, hvorfor forslaget alene vedrører dokumenter og ikke tillige bøger.

Der synes ikke at være nogen begrundelse for, at alene dokumenter er om-fattet af denne bestemmelse, selv om det må formodes, at den også omfat-ter alle bøger, der opfylder kravene i dokumentdefinitionen. Dertil kommer, at elektronisk førte bøger må forventes i ringere grad end fysiske bøger at indeholde en traditionel udstederbetegnelse.

Udvalget finder endvidere, at bestemmelsens strafferamme bør bringes i overensstemmelse med den af udvalget foreslåede dokumentfalskbestem-melse. Også her vil der i grove tilfælde foreligge (medvirken til) et skade-delikt, f.eks. bedrageri, og i så fald kan der straffes i sammenstød med dette delikt.

Der henvises til afsnit 8.7.2-8.7.3 vedrørende udvalgets forslag.

5.4. Vildledende afsenderbetegnelser

Endnu en ny problemstilling, der er fremkommet med Internettet og e-mailsystemet, har en vis sammenhæng med dokumentfalskspørgsmålet:

Fremsendelse af store mængder e-mail, der fremtræder som hidrørende fra en anden, men ikke har den til dokumentfalsk krævede bevisværdi. Sådanne handlinger kaldes i internetjargonen undertiden "spoofing". Problemstil-lingen er en variant over tilsvarende handlinger med fysiske breve, der imid-lertid aldrig er blevet udsendt i et omfang, der svarer til det, man ser nu. Dette skyldes både, at det er let at maile til et betydeligt antal modtagere, og at det sammenholdt med portoudgifter er næsten omkostningsfrit.

Der kan bl.a. henvises til en sag om udsendelse af e-mail til måske over 100.000 personer i en internetudbyders navn om lukning af internetforbindelsen på en angiven dato på grund af økonomiske problemer.

I en anden sag havde gerningsmanden via en anden abonnents e-mail adres-se udsendt breve til internetudbyderens ca. 2.000 abonnenter med indholdet "I er alle sammen nogle klovnes" og "I alle være nogle klovner". Ved Kø-benhavns byrets dom af 3/10 1997 blev han dømt for overtrædelse af straf-felovens § 263, stk. 2, ved uberettiget at have skaffet sig adgang til internet-udbyderens server og uberettiget at have benyttet programmerne til udsen-delse af de to meddelelser.

Som eksempel kan også nævnes en sag, der er omtalt i Computerworld 5/9 2000, hvor en person er blevet arresteret i USA som mistænkt for at stå bag en falsk pressemeddelelse. Meddelelsen, der blev citeret af flere store inter-nationale nyhedsbureauer, gik ud på, at en chef for en virksomhed var trådt tilbage på grund af store tab i firmaet. Aktierne dykkede med 60% (ca. 2 milliarder USD).

Det kan overvejes, om der i lyset af distributionsmulighederne på Internettet og mulighederne for at hacke kundefiler o.l. bør være en strafferetlig regulering af omfattende distribution i andres navne. Dette kan især over-vejes vedrørende e-mails eller internetmeddelelser, der indeholder urigtige oplysninger om personers eller virksomheders forhold, ikke mindst hvis der er tale om meddelelser, der kan påføre en virksomhed eller person væsentlig økonomisk skade.

En tilsvarende problemstilling er udbredelse af informationer via urigtige pressemeddelelser, hvad enten meddelelsen er elektronisk eller ej.

I en række situationer er de aktuelle meddelelser på grund af deres indhold omfattet af allerede eksisterende straffebestemmelser (f.eks. reglerne om kursmanipulation og bedrageri eller straffelovens § 296, stk. 1, nr. 1), eller adresser på modtagerkredsen er opnået ved hacking som i ovennævnte dom. Visse dispositioner, der kan påføre en virksomhed skade f.eks. ved kundetab, er reguleret i markedsføringsloven (men ikke nødvendigvis straf-belagt, før der er påbud om at ophøre, hvilket ikke hjælper meget ved ska-devoldende éngangsdispositioner).

Udvalget finder, at der muligvis er områder, hvor urigtige meddelelser sen-des eller kommunikeres (f.eks. via falske pressemeddelelser) til en videre kreds, hvor der kan være behov for en regulering eller en mere klar regu-lering. Dette gælder ikke mindst i tilfælde, hvor meddelelsen er egnet til at påføre en anden væsentlig økonomisk skade. Udvalget finder imidlertid ik-ke, at der på nuværende tidspunkt foreligger oplysninger nok til, at behovet for en særlig regulering kan vurderes, ligesom det ikke på det foreliggende grundlag er muligt at tage endelig stilling til, hvordan en strafferetlig regule-ring af aktuelle områder kan formuleres i en tilstrækkelig præcis straffe-bestemmelse.

Udvalget finder på den baggrund, at der ikke på nuværende tidspunkt skal ske en regulering, men at området bør følges med henblik på at få et bedre overblik over både omfanget og arten af meddelelser, således at der senere kan tages stilling til en regulering, såfremt udviklingen viser, at der er behov for en særskilt strafferetlig regulering.[134]

Der henvises til afsnit 8.7.4.

KAPITEL 6
HÆRVÆRK M.V.

6.1. Indledning

Ved nogle af de problemstillinger, der behandles i de følgende afsnit, er et aktuelt spørgsmål bl.a. anvendeligheden af straffelovens § 291 og § 293. Forarbejderne til disse bestemmelser, der gengives nedenfor, har naturligvis ikke haft IT-problemstillinger for øje.

Straffelovens § 291

Den tilsvarende hærværksbestemmelse i 1866-straffeloven havde følgende ordlyd:

---

[134] Arbejdsgruppen vedrørende datakriminalitet fandt, at der burde ske en regulering ved-rørende visse indholdsmæssigt kvalificerede meddelelser.

> "§ 296. Ødelægger eller beskadiger Nogen ellers[135] forsætlig fremmed Eiendom, bliver han, forsaavidt Forholdet ikke falder ind under strængere Straffebestemmelser, at straffe med Bøder eller Fængsel. Offentlig Paatale finder kun Sted, naar Handlingen har medført Forstyrrelse af den offent-lige Fred eller været forbunden med Overtrædelse af Politiforskrifter."

§ 292 i lovudkastet fra 1864[136] indeholder intet nærmere om, hvad der er omfattet af beskrivelsen.[137]

I straffelovsbetænkningerne fra 1912, 1917 og 1923 formuleredes i udka-stenes henholdsvis § 313, § 260 og § 265 hærværksbestemmelser.

Straffelovsbetænkningen fra 1912[138] beskrev i § 313 området som "Den, som retstridig ødelægger, beskadiger, ubrugbargør eller paa anden Maade forspilder en Ting, der tilhører en anden, straffes ...". Det siges i bemærk-ningerne[139], at der inddrages "ubrugbargøre" og "forspilde", så at f.eks. også det tilfælde, at tingen bortkastes, så den ikke kan fås tilbage, utvivlsomt fal-der ind under bestemmelsen.
Straffelovsbetænkningen fra 1917[140] beskrev i § 260 området som "Den, som ødelægger, beskadiger eller bortfjerner Ting, der tilhører en anden, straffes ...". Det siges i bemærkningerne[141], at den ændrede beskrivelse i forhold til 1912-udkastet ikke tilsigter nogen realitetsændring, men giver en kortere beskrivelse af de tre måder, forbrydelsen kan udføres på. "Bort-fjerner" er benyttet i stedet for det i øvrigt nærliggende "bortkaster", fordi det formentlig er noget mere omfattende.

---

[135] De foregående §§ 294-295 indeholdt særregler om monumenter, gadelygter m.v. samt telegrafledninger m.v.

[136] Jfr. Udkast til Straffelov for Kongeriget Danmark af 25/2 1864, udarbejdet af "Den ved allerhøiste Kommissorium af 22de Februar 1859 til at udarbejde et endeligt Udkast til en Straffelovbog for Danmark allernaadigst anordnede Kommission".

[137] Jfr. bemærkningerne s. 360 f.

[138] Afgivet af Kommissionen nedsat til at foretage et Gennemsyn af den almindelige bor-gerlige Straffelovgivning.

[139] S. 274.

[140] Udarbejdet af professor, dr. jur. Carl Torp.

[141] S. 250.

I straffelovsbetænkningen fra 1923[142] formuleredes den nugældende ordlyd: "Den, som ødelægger, beskadiger eller bortskaffer Ting, der tilhører en an-den, straffes ...". Det siges i bemærkningerne[143], at der udtrykkeligt medta-ges bortskaffelse af ting, hvorved forstås, at tingen skaffes af vejen, således at den ikke eller kun ved vanskelige eller bekostelige foranstaltninger kan fås tilbage. Det siges videre, at ordet "ting" omfatter såvel løsøre som fast ejen-dom. Med hensyn til straffen nævnes, at den er betydeligt skærpet i forhold til 1866-straffeloven, og det nævnes som begrundelse herfor, at "Hele Kom-missionen er enig i, at Ødelæggelse af fremmed Ejendom kan være Udtryk for en saa ondartet Ødelæggelseslyst og et saa samfundsfjendtligt Sindelag, at en kraftig Repression gennem Straf maa anses for paakrævet".

Bestemmelsen fik herefter i 1930-straffeloven sin nuværende formulering (bortset fra at hæfte indgik i strafferammen frem til 1/7 2001):

> "§ 291. Den, som ødelægger, beskadiger eller bortskaffer ting, der tilhører en anden, straffes med bøde eller fængsel indtil 1 år.
> Stk. 2. Øves der hærværk af betydeligt omfang, eller er gerningsmanden tidligere fundet skyldig efter nærværende paragraf eller efter §§ 180, 181, 183, stk. 1 og 2, 184, stk. 1, 193 eller 194, kan straffen stige til fængsel i 4 år.
> Stk. 3. Forvoldes skaden under de i stk. 2 nævnte omstændigheder af grov uagtsomhed, er straffen bøde eller fængsel indtil 6 måneder."

I Straffelovrådets betænkning nr. 1032/1985 om datakriminalitet gennem-gås[144] anvendeligheden af straffelovens § 291 ved datakriminalitet. Det siges herom bl.a.:

> "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 sletning af

[142] Afgivet af Straffelovskommissionen af 9. November 1917.

[143] Sp. 382 ff.

[144] I kapitel 4, s. 36 ff.

> 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 er helt 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 af et lydbånd. Fremgangsmåden kan f.eks. være den, at det blot er indgangen til det regi-strerede, der slettes, medens det øvrige fortsat findes på disketten, men ikke kan findes. Dette er uden betydning for den strafferetlige bedøm-melse 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 6 måneders fængsel.
> (...)
>
> 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., forekommer 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."

I Straffelovrådets betænkning nr. 1099/1987 om strafferammer og prøve-løsladelse foreslog rådet[145], at strafmaksimum i stk. 1 nedsættes til fængsel i 6 måneder. Dette forslag var dog ikke medtaget i betænkningens lovudkast. Bestemmelsen i stk. 2 blev foreslået ændret til:

[145] Betænkningen s. 131 f. og 291.

> "Øves der hærværk af betydeligt omfang, eller foreligger der i øvrigt særligt skærpende omstændigheder, kan straffen stige til fængsel i 3 år."

Vedrørende stk. 3 blev det foreslået, at der kun skulle være bødestraf. Det nævnes[146] vedrørende den foreslåede ændring af stk. 2, at "særligt skær-ende omstændigheder" vil kunne omfatte tilfælde, hvor skaden isoleret set er af begrænset omfang, men hvor dens økonomiske eller ideelle virkninger, f.eks. på et dataanlæg eller et kunstværk, er meget betydelige.

De foreslåede ændringer af § 291 blev ikke gennemført.

Straffelovens § 293

Den tilsvarende bestemmelse om uberettiget brug i 1866-straffeloven havde følgende ordlyd:

> "§ 236. Sætter Nogen sig paa ulovlig Maade i Besiddelse af anden Mands Gods uden Hensigt til at tilegne sig det eller skille Eieren derved, men alene for at benytte sig af samme til et bestemt Brug, straffes han med Fængsel eller Bøder. Offentlig Paatale finder kun Sted efter den Forurettedes Begæring."

I straffelovsbetænkningerne fra 1912, 1917 og 1923 formuleredes i udka-stenes henholdsvis § 314, § 262 og § 267 bestemmelser om uberettiget brug og rådighedshindring.

Straffelovsbetænkningen fra 1912 beskrev i § 314, nr. 1 og 3, forholdene som: "1) den, som retstridig bruger eller raader over en Ting, som en anden har Ret over eller Krav paa, eller som er i en andens Besiddelse," og "3) den, der retstridig hindrer nogen berettiget i at bruge eller raade over en Ting eller fratager en Besidder Tingen". Det siges i bemærkningerne[147], at nr. 1 dækker brugstyveri og brugsunderslæb, herunder tilfælde hvor ejeren bruger en ting, han f.eks. har udlejet til en anden, og at nr. 3 giver bestem-melse om visse negative indgreb, hvad enten de rammer ejeren eller en per-son, der har en begrænset tinglig ret over tingen.

---

[146] Betænkningen s. 92.

[147] S. 275.

Straffelovsbetænkningen fra 1917 beskrev i § 262 første led "Den, som uberettiget bruger en Ting, der tilhører en anden, saaledes at der derved paaføres denne et Tab eller væsentlig Ulempe", mens andet led blev beskrevet som "den, som hindrer nogen i at udøve en gyldig stiftet Brugsret eller den ved en Haandpanteret eller Tilbageholdsret hjemlede Beføjelse til at raade over en Ting". Det siges i bemærkningerne[148], at 1912-forslaget fin-des for bredt, og at en blot tilnærmelsesvis så vidtgående regel ikke kendes i nogen lov eller i noget andet udkast, og at de fleste fremmede lovgivninger overhovedet ikke straffer den blotte uberettigede brug.

I straffelovsbetænkningen fra 1923 formuleredes indholdet som i 1917-ud-kastet.

Under Rigsdagens behandling af lovforslaget blev det ændret således, at bestemmelsen "ogsaa rammer Tilfælde, hvor nogen hindrer Ejeren selv i at raade over sine Ting".[149]

Bestemmelsen fik herefter i 1930-straffeloven følgende formulering:

> "§ 293. Den, som uberettiget bruger en ting, der tilhører en anden, således at der derved påføres denne tab eller væsentlig ulempe, straffes med bøde eller hæfte. Under skærpende omstændigheder, navnlig når tingen er af betydelig værdi, kan straffen stige til fængsel i 2 år.
> Stk. 2. Den, som lægger hindringer i vejen for, at nogen udøver sin ret til at råde over eller tilbageholde en ting, straffes med bøde eller hæfte eller under skærpende omstændigheder med fængsel indtil 6 måneder."

I Straffelovskommissionens betænkning nr. 232/1959 vedrørende ungdomskriminaliteten behandledes spørgsmålet om brugstyverier af motorkø-retøjer[150], og det blev foreslået, at der blev lavet et særligt nyt stk. 1 ved-rørende denne form. Dette forslag blev ikke fulgt, og ved lov nr. 163 af 31/5 1961 fik § 293, stk. 1, sin nuværende formulering (bortset fra at hæfte indgik i strafferammen frem til 1/7 2001):

---

[148] S. 251.

[149] RT 1929/30 B sp. 1875 f.

[150] Betænkningen s. 91 ff.

> "Den, som uberettiget bruger en ting, der tilhører en anden, straffes med bøde eller fængsel indtil 1 år. Under skærpende omstændigheder, navnlig når tingen ikke bringes tilbage efter brugen, kan straffen stige til fængsel i 2 år."

I Straffelovrådets betænkning nr. 1032/1985 om datakriminalitet siges ved-rørende anvendelsen af § 293, stk. 1, bl.a.[151]:

> "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"."

I Straffelovrådets betænkning nr. 1099/1987 om strafferammer og prøve-løsladelse foreslog rådet[152], at ordene "navnlig når tingen ikke bringes tilbage efter brugen" skulle udgå af stk. 1, og at strafmaksimum skulle nedsættes til 1 år og 6 måneder. Vedrørende stk. 2 nævnes, at bestemmelsen muligvis helt kunne undværes, og det foreslås, at straffen begrænses til bøde.[153]

De foreslåede ændringer af § 293 blev ikke gennemført.

6.2. Sletning

Sletning af data eller programmel er omfattet af straffelovens § 291 om hær-værk, der har et strafmaksimum på 1 år, men i kvalificerede tilfælde (hær-værk af betydeligt omfang samt visse gentagelsessituationer) et strafmak-simum på 4 år. Også tilfælde af grov

---

[151] S. 30 f.

[152] Betænkningen s. 132 ff. og s. 291.

[153] Se i øvrigt om strafudmåling i sager om IT-kriminalitet, Mads Bryde Andersen, IT-ret-ten (2001), s. 697 f.

uagtsomhed er omfattet med et straf-maksimum på fængsel i 6 måneder. I tilfælde, hvor hærværket fremkalder omfattende forstyrrelser i driften af almindelige samfærdselsmidler, databehandlingsanlæg m.v., vil forholdet i stedet være omfattet af straffelovens § 193, der ligeledes har et strafmaksimum på 4 år, men tillige har en almin-delig uagtsomhedsbestemmelse med straf af bøde eller fængsel indtil 4 må-neder.

Straffelovens § 291 har været anvendt i flere domme, jfr. bl.a. UfR 1987.216 Ø, hvor det siges :

> "Landsretten finder, at databærende medier med indlagte data må anses for "ting", således som dette begreb anvendes i straffelovens § 291. Så-fremt der uberettiget sker sletning af data på datamedierne, eller adgangs-mulighederne til data i øvrigt uberettiget ændres på en sådan måde, at en hidtidig benyttelse umuliggøres – eller dog kun er mulig for personer med større EDB-indsigt end den sædvanlige bruger – finder landsretten yder-ligere, at der foreligger "ødelæggelse" af en ting, da de databærende medier ikke længere – i hvert fald ikke uden særlige foranstaltninger – kan anven-des efter deres formål".

Landsrettens dom sondrer således ikke mellem det fysiske medie og indhol-det, men lægger i stedet vægt på helheden.

Med hensyn til anvendelsen af den skærpede bestemmelse siger landsretten, at samtlige de i anklageskriftet beskrevne handlinger findes efter deres ind-gribende karakter, der nødvendiggjorde tilkaldelse af ekstern ekspertbistand, med rette henført under straffelovens § 291, stk. 2. Den hovedtiltalte i sa-gen, der bl.a. havde indlagt logiske bomber, der slettede alle relevante ar-bejdsfiler, blev idømt 6 måneders ubetinget fængsel for edb-hærværk.

I en anden sag vedrørte anmeldelsen straffelovens § 193 i forbindelse med, at en person via Internettet gik ind på en internetudbyders system og fik eksekveret en sletningskommando, der gik i gang med at slette alt i sy-stemet. Da man straks opdagede angrebet, kunne man begrænse skaden til 10 timers nedbrud.[154]

---

[154] I Computerworld 16/5 2000 er omtalt en amerikansk dom, hvor en tidligere netværks-chef havde placeret en logisk bombe i systemet, der ødelagde systemet 3 uger efter hans fratræden. Efter det oplyste kostede sammenbruddet virksomheden 10 millioner USD og havde senere afskedigelse af 80 medarbejdere til konsekvens.

Den strafferetlige regulering ved sletning synes at være fuldt dækkende, jfr. dog for så vidt angår straffelovens § 193 nedenfor i afsnit 6.7.

Endvidere kan det overvejes at indsætte en selvstændig bestemmelse om edb-hærværk, der tillige omfatter andre typer af indgreb.

Der henvises til afsnit 6.6.

6.3. Ændring

I ovennævnte dom[155] dømtes tillige for hærværk i et forhold, hvor der ikke var sket sletning, men hvor en UFD (User File Directory) var flyttet, så den lå under en anden MFD (Master File Directory), ligesom UFD'ens navn var blevet ændret, hvilket betød, at breve ikke kunne udskrives. Også dette forhold, der vedrørte ændringer, hvorved filer blev gjort utilgængelige, er omfattet af landsrettens beskrivelse af, hvad der anses for ødelæggelse.

En anden ændringssituation, der synes at være blevet mere udbredt, består i, at man ændrer indholdet af en homepage. Det er bl.a. sket med CIA's homepage. Situationen vil indebære hacking, hvis der ikke er almindelig ad-gang til ændring. Ændringer er også sket i priser m.v. i markedsføringsma-teriale.

En yderligere situation, der kan indeholde en mulighed for ændring af registrerede data i forbindelse med forsætlig forkert opdatering, kan opstå i forbindelse med ekstern online opdatering i Erhvervs- og Selskabsstyrel-sens selskabsregister, hvor kun en mindre del af selskaberne har valgt at hin-dre online registrering ved hjælp af særlig passwordbeskyttelse. Det særlige password sikrer, at kun brugere med kendskab til passwordet har online adgang til selskabets datafil. Ændring i et selskabs datafil vil kunne være et led i en berigelsesforbrydelse, hvor personen skal fremstå som legitimeret til at repræsentere selskabet, men vil også kunne ske isoleret f.eks. som chika-ne. Bestemmelsen i straffelovens § 163 om urigtige erklæringer til det of-fentlige vil formentlig være anvendelig i nogle tilfælde, ligesom

[155] UfR 1987.216 Ø.

handlingen isoleret set vil kunne være hærværk, hacking eller forsøg på dokumentfalsk.

Ændringerne vil også kunne ske i indholdet af erklæringer m.v., jfr. afsnit 5.2, eller i beregningsprogrammer.

Ændringer ses også i forbindelse med hacking, hvor der opnås kontrol over systemet, især i den form, at loggen ændres, når hackeren er færdig med sine aktiviteter.

På baggrund af, at databærende medier med data er "ting", vil det være na-turligt at anvende straffelovens § 291 også på sådanne forhold, men måske henføre dem under "beskadiger" og ikke under "ødelægger".

En særlig ændringsform er forvanskning af data i transmissionsforløbet. I Straffelovrådets betænkning nr. 1032/1985 om datakriminalitet nævner rå-det, at det er tvivlsomt, om straffelovens § 291 er anvendelig, men at § 263 formentlig vil være mest nærliggende (lukkede meddelelser m.v.).

Det kan ligeledes overvejes at lade sådanne handlinger indgå i en samlet bestemmelse om edb-hærværk.

Der henvises til afsnit 6.6.

6.4. Hindren af brug

En særlig hærværksvariant er Denial-of-Service angreb (DoS-angreb), der hindrer almindelig brug af systemerne ved at udvirke overbelastning eller nedbrud af disse.
En variant er blokering af et anlæg gennem uafbrudt transmission. Det er især sket ved, at Internet Protocol-pakker er sendt i så store mængder, at anlægget ikke kan klare andet. Pakkerne har typisk falske afsenderadresser. (Der kan være tale om en særlig målrettet variation af såkaldt spamming, der i sin typiske form er masseudsendelse af enslydende meddelelser på et netværk). I begyndelsen af 2000 sås dette i

en ny form, hvor bl.a. flere store internettjenester blev lammet af sådanne angreb.[156]

En anden af de nye hærværksvarianter – bl.a. Ping of Death – ligner på mange måder ovennævnte e-mail bomber, men består i, at serveren uafbrudt bliver bedt om at sende dens IP-nr., eller i, at der sendes en for stor datapakke, hvilket får den modtagende computer til at gå ned.

I IT-Sikkerhedsrådets rapport "Datasikkerheden i Danmark år 2000" er besvarelser fra 441 virksomheder (ud af 1.600 spurgte) på en række spørgs-mål vedrørende perioden 1/1-31/12 2000. Et af spørgsmålene vedrørte, om virksomheden havde været udsat for DoS-angreb. 4% (16 af 418) svarede ja. Der var tale om i alt i hvert fald 78 tilfælde, hvoraf det værste tilfælde forvoldte IT-stop i 48 timer.

Spørgsmålet er, hvilken strafferetlig dækning der er ved e-mail bomber o.l. Der er ikke nogen ødelæggelse, ikke nogen ændring og ikke nogen uberet-tiget adgang. Der er kun brug i form af chikane.

Man kan overveje at anvende straffelovens § 293, stk. 1, om uberettiget brug og se på den samlede brug, men det vil være en ret atypisk anvendelse af denne bestemmelse. Man kan også overveje at anvende straffelovens § 293, stk. 2, der bl.a. vedrører, at man lægger hindringer i vejen for, at nogen udøver sin ret til at råde over en ting. Man har her muligvis en situation, hvor der ikke er helt klar strafferetlig dækning, selv om forholdet som ind-greb betragtet må sidestilles med situationer, der er omfattet af hærværks-bestemmelsen.

Det vil i nedbrudssituationerne være nærliggende at overveje, om sådanne nedbrud er omfattet af hærværksbestemmelsen, dvs. at indgrebet kan karak-teriseres som en beskadigelse. Som ved e-mail bomber kan man også overveje anvendelsen af straffelovens § 293.

Der henvises til afsnit 6.6.

---

[156] I IT-Sikkerhedsrådets udredning om Internet sårbarhed (februar 2001) s. 50 f. nævnes, at rådet ikke ser grund til at antage, at angreb mod internet-infrastrukturen ikke kan prak-tiseres, f.eks. ved angreb mod DNS-servere (der styrer adressering af internettrafik via domænenavne) eller routere (der er nødvendige for transport af trafik på Internettet).

6.5. Virus

Virusproblemstillingen er typisk en variant af ovenstående punkter. Virusen sletter, ændrer (herunder tilføjer) eller blokerer. Det er sandsynligt, at en vi-rus normalt vil opfylde betingelserne i hærværksbestemmelsen i straffelo-vens § 291, fordi den indgår som en del af systemet og dermed ændrer det-te.

Også i forbindelse med virus kan udgifterne være betragtelige.[157]

I IT-Sikkerhedsrådets i afsnit 6.3 nævnte rapport "Datasikkerheden i Danmark år 2000" vedrørte et andet af spørgsmålene, om virksomheden havde været udsat for virusangreb. 57% (239 af 418) svarede ja. Der var ta-le om i alt i hvert fald 11.281 tilfælde, hvoraf det værste tilfælde gav drifts-problemer i 30 kalenderdage. Det højeste tilfælde af anvendt tid til bekæm-pelse og opretning var på 55 persondage.

Nogle af de nye virusformer har en anden karakter end de tidligere. F.eks. har Back Orifice, Netbus, Masters Paradise og Sockets de Troie den egen-skab, at de (efter at være blevet spredt f.eks. via elektroniske julekort, der åbnes) etablerer en bagdør til den aktuelle computer og giver adgang til dens dokumenter.

En særlig variation, en mail med titlen "I love you", dukkede op i foråret 2000. Når man åbnede, kopierede den sig selv og sendte sig til alle adresser i det pågældende adressekartotek. I næste omgang forsøgte den at ændre regi-streringsdatabasen. Denne virus lammede i vidt omfang systemer over hele verden. En version ("Newlove"), der dukkede op kort efter, mailede til-svarende sig selv, men skiftede navn til navnet på det dokument, der sidst var sendt til den pågældende adresse. Siden da er en række andre vira af samme eller værre karakter dukket op ("Anna Kournikova", "Nimbda" m.fl.).

---

[157] Det svenske Brottsförebyggande rådet har i BRÅ-rapport 2000:2 om IT-relaterad brottslighet, s. 27, anført skaderne i forbindelse med virus i de tilfælde, hvor det var oplyst i forbindelse med en virksomhedsundersøgelse. Udgifterne lå på mellem 48.200 s.kr. og 67.200 s.kr. pr. sag.

Hovedproblemet med den strafferetlige behandling af virus er at finde ger-ningsmanden. Dels bevæger virus sig verden rundt ad uransagelige veje, og dels er Internettet fyldt med opskrifter på virus. I et vist omfang kommer de ind i systemer via arbejdstageres benyttelse af fremmede disketter i systemet.

Der henvises til afsnit 6.6.

6.6. Udvalgets overvejelser vedrørende hærværk

Med hensyn til spørgsmålet om, i hvilken udstrækning de gældende bestem-melser i straffelovens § 291 og § 293 dækker de aktuelle situationer, hen-vises til indledningen til afsnit 6, der indeholder en gennemgang af for-arbejder m.v. Som det fremgår, har bestemmelserne et bredt anvendelses-område.

Udvalget finder, at der i hvert fald overvejende må antages at være straffe-retlig dækning i straffelovens § 291 om hærværk. Dækningen er imidlertid ikke utvivlsom i alle tilfælde, hvilket kan tale for en klar regulering. Dertil kommer, at selv når hærværksbestemmelsen må antages at være anvendelig, ligner den edb-mæssige ødelæggelse i dens forskellige former ikke de øde-læggelser, der kendes fra traditionelt hærværk. Der rejser sig derfor også det principielle spørgsmål, om det under alle omstændigheder er hensigtsmæs-sigt, at straffeloven tilpasses IT-udviklingen også i tilfælde, hvor den kan eller måske kan dække handlingen med den nugældende formulering. Om-vendt giver det afgrænsningsproblemer, hvis man indfører særbestemmel-ser.

Som eksempler på tilsvarende overvejelser kan henvises til de tidligere lov-ændringer på baggrund af Straffelovrådets betænkning fra 1985 om data-kriminalitet[158]. Det nævnes her vedrørende hacking[159] bl.a., at spørgsmålet om anvendelsen af straffelovens § 263 på dataforhold ikke kunne anses for afgjort i retspraksis. Det nævnes videre, at datalagrede oplysninger måske er en optegnelse, der er omfattet af straffelovens § 263, stk. 1, og at det er sandsynligt, at danske domstole – bl.a. på

[158] Betænkning nr. 1032/1985.

[159] Betænkningen s. 22 f.

baggrund af registerudvalgets opfattelse – vil anlægge denne vide fortolkning. Straffelovrådet fandt imid-lertid, at man ved en lovændring burde gøre det klart, at det er strafbart at skaffe sig adgang til et dataanlægs informationer.

Vedrørende den foreslåede bestemmelse om databedrageri anfører Straffe-lovrådet[160], at der kan være bedragerilignende situationer, der ikke er omfat-tet af straffelovens § 279 om bedrageri, fordi der ikke optræder personer, der vildledes. Rådet anfører, at de fleste af disse forhold må antages at være omfattet af § 278 eller § 280, og siger herefter:

> "Ingen af disse bestemmelser er udformet med henblik på at ramme data-kriminalitet, og der kan derfor tænkes tilfælde, hvor det vil være mindre naturligt at henføre disse nye kriminalitetsformer under bestemmelserne om pengeunderslæb eller mandatsvig."

Straffelovrådet fandt det bl.a. derfor hensigtsmæssigt at samle disse bedrage-rilignende forhold i en ny bestemmelse om datakriminalitet.

Med hensyn til hærværk foreslog Straffelovrådet ingen ændringer[161], idet straffelovens § 291 fandtes at være dækkende i situationer, hvor data blev slettet eller ændret. I situationer, hvor data blev gjort utilgængelige for bru-geren, fandt Straffelovrådet også, at § 291 var anvendelig og mere nær-liggende end § 293, stk. 2, om at lægge hindringer i vejen for retmæssig råden.[162]

Under hensyntagen til, at der inden for området for elektronisk databehand-ling er hærværksområder, hvor der ikke er helt klar strafferetlig dækning, og hærværksområder, der antagelig dækkes af forskellige bestemmelser, finder udvalget, at der er behov for en vis justering og præcisering af straffeloven. Udvalget finder ikke, at der er behov for en særskilt straffelovsbestemmelse om datahærværk.[163] Udvalget finder, at den gældende hærværksbestemmelse i straffelovens

---

[160] Betænkningen s. 49 f.

[161] Se betænkningen s. 36 ff.

[162] De hærværkserfaringer, der forelå på dette tidspunkt, vedrørte især de forhold om logiske bomber m.v., der blev medtaget i UfR 1987.216 Ø.

[163] Arbejdsgruppen vedrørende datakriminalitet fandt, at der skulle være en særskilt bestemmelse om datahærværk.

§ 291 er tilstrækkeligt klart dækkende, og at der ikke er behov for ændring af den bestemmelse. Derimod finder udvalget, at straffelovens § 293, stk. 2, bør ændres på flere punkter. Dels bør strafferammen svare til bestemmelsens stk. 1, og dels bør påtalereglerne være de samme som ved hærværk (dvs. betinget offentlig påtale i stedet for privat påtale, jfr. straffelovens § 305). Desuden bør bestemmelsen formuleres, så det klart fremgår, at den også omfatter rådighedshindren ad elektronisk vej.

Der henvises til afsnit 8.8.1 vedrørende udvalgets forslag.

6.7. Straffelovens § 193

Som nævnt i afsnit 2.4 gennemførtes i 1985[164] en ændring af straffelovens § 193 (omfattende forstyrrelser i driften af bl.a. databehandlingsanlæg og for-højelse af strafmaksimum fra 3 til 4 år) på baggrund af Straffelovrådets be-tænkning nr. 1032/1985 om datakriminalitet.

Ændringen var bl.a. begrundet i[165], at der kunne tænkes forstyrrelser, der ik-ke var omfattet af de dengang i straffelovens § 193 opregnede områder, og hvis strafbarhed derfor ville afhænge af, om den kunne anvendes analogisk. Som eksempler nævntes angreb, der helt lammer eller i betydeligt omfang forstyrrer registrering, behandling og transmission af data inden for værdi-papircentralen, kildeskattedirektoratet, politiets motorregistrering eller lig-nende samt den centrale elektroniske databehandling hos banker og spare-kasser, realkreditinstitutter etc. Straffelovrådet overvejede, om man i be-stemmelsen skulle begrænse kredsen af de beskyttede dataanlæg, men fandt, at rækkevidden blev begrænset i tilstrækkeligt omfang ved kravet om, at driftsforstyrrelsen skal være omfattende.

Justitsministeriet anførte i et svar til Folketinget[166] bl.a.:

---

[164] Lov nr. 229 af 6/6 1985.

[165] Betænkningen s. 41 f.

[166] FT 1984/85 B 1922.

> ”De anførte udtryk ”omfattende forstyrelse af driften” og ”almenskadelig karakter” angiver, at der må anlægges en kvantitativ vurdering af angrebets omfang. Man må formentlig herved lægge afgørende vægt på størrelsen af den personkreds, der berøres af angrebet. Forbrydelsen får denne almen-skadelige karakter f.eks. hvis et af storbankernes centrale dataanlæg helt sættes ud af funktion, eller hvis f.eks. en tilsvarende lammelse af stats-skattedirektoratets centrale dataanlæg fremkaldes. Derimod vil en lammel-se eller betydelig driftsforstyrrelse af en bankfilials eller et skattekontors dataterminal ikke være omfattet af straffelovens § 193, da virkningerne af driftsforstyrrelsen i disse tilfælde ikke antager den almenskadelige karak-ter, som bestemmelsen forudsætter.”

Straffelovrådet havde foreslået et strafmaksimum på 6 år[167], og lovforslaget[168] var i overensstemmelse hermed. Under udvalgsbehandlingen af lovforslaget blev der stillet forslag om at ændre til 4 år, hvilket blev vedtaget. Det fremgår ikke af Retsudvalgets betænkning, hvad der var baggrunden for ændringsforslaget.

Som eksempel på dens anvendelse kan nævnes Roskilde rets dom af 19/12 1996:

> I dommens forhold 2 a var der rejst tiltale for at have fremkaldt omfat-tende forstyrrelse i driften af et militært anlæg i USA, der bl. a. indeholdt visse sensitive oplysninger udelukkende til tjenstligt brug, og til hvilket der var knyttet ca. 5.000 brugere, hvilket bevirkede, at anlægget måtte tages ud af drift i 9 dage. Tab i produktionskapacitet blev anslået til knap 4,7 mio. USD. Forhold 2 c vedrørte tilsvarende forstyrrelse i driften af 3 anlæg hos en vejrtjeneste i USA, der indholdt operationelle systemer til daglig brug til udarbejdelse af vejrmeldinger over store dele af verden samt forsknings- og udviklingssystemer til forbedring af operationelle systemer. Vejrtjenesten måtte anvende ressourcer til overvågning af den tiltaltes aktiviteter og til at undersøge operativsystemet på over 120 computersystemer, ligesom den tiltaltes dekryptering af passwordfiler gav en betydelig forsinkelse i autoriseret arbejde på anlægget, hvilket videre indebar, at autoriserede brugere blev afskåret fra at benytte det.
>
> I dommen lagdes i forhold 2 a til grund, at brugerantal og driftsstop var som anført, at anlægget ikke indeholdt klassificerede oplysninger, men bl.a. forskellige personfølsomme data, samt at tabet ikke kunne opgøres, men at der var tale om en omfattende driftsforstyrrelse med

---

[167] Betænkningen s. 42 f.

[168] FT 1984/85 A 4375.

et betydeligt øko-nomisk tab til følge, og den tiltalte fandtes skyldig i overtrædelse af § 193.

I dommen lagdes i forhold 2 c til grund, at det forholdt sig som anført i tiltalen, og at det ene anlæg var operationelt og de to andre til forskning og udvikling. De sidstnævnte anlæg fandtes ikke på baggrund af de forelig-gende oplysninger at indgå i en sådan sammenhæng, at de objektivt var omfattet af straffelovens § 193. Det anføres i dommen, at det ikke er be-vist, at den tiltalte var klar over, at anlæggene tilhørte den amerikanske vejrtjeneste eller overhovedet anlæggenes præcise karakter og brug. Den tiltalte havde dog vidst, at anlæggene tilhørte den amerikanske regering, at uautoriseret adgang var forbudt, og at det ene anlæg havde særlig stor reg-nekraft. Den tiltalte havde haft en almindelig forståelse af situationen og var klar over, at det drejede sig om regeringscomputere. Når han i over 200 tilfælde var brudt ind i computere, havde han accepteret de faktiske konsekvenser af sine handlinger og således handlet forsætligt. Der dømtes for fuldbyrdet overtrædelse af straffelovens § 193 for så vidt angik det operationelle anlæg og for forsøg for så vidt angik de 2 andre anlæg.

Som det fremgår af afsnit 6.6 finder udvalget, at også andre forstyrrelser af informationssystemer bør reguleres klart i straffeloven. Udvalget finder ikke anledning til at foreslå ændringer i, hvad der er omfattet af straffelovens § 193. Derimod finder udvalget, at udtrykket "databehandlingsanlæg" bør erstattes med det af udvalget anvendte "informationssystemer".

Udvalget finder, at strafmaksimum i straffelovens § 193, stk. 1, bør forhøjes, så der ikke er samme strafmaksimum som ved groft hærværk. Udvalget har i den forbindelse lagt vægt på, at samfundets stigende afhængighed af edb og-så betyder, at driftsforstyrrelser kan have meget mere indgribende konse-kvenser end tidligere. Det er på den baggrund ønskeligt, at der i helt ekstra-ordinære situationer kan idømmes en ligeledes ekstraordinær høj straf.

I f.eks. Norge og Finland er der mulighed for at idømme op til fængsel i 10 år, jfr. afsnit 2.5, ved særligt kvalificeret hærværk. Udvalget har imidlertid ved de nærmere overvejelser omkring, hvordan strafniveauet efter denne bestemmelse skulle ligge i forhold til den almindelige hærværksbestemmel-se, valgt et strafmaksimum på 6 år, svarende til det, der blev foreslået af Straffelovrådet og Justitsministeren i 1985.

Udvalgets forslag tager udgangs-punkt i de gældende strafferammer, der for tiden er genstand for overvejel-ser i Straffelovrådet.

Udvalget finder herudover, at straffelovens § 193, stk. 2, bør harmonere med den tilsvarende bestemmelse vedrørende groft hærværk, således at be-stemmelsen ligesom straffelovens § 291, stk. 3, begrænses til at dække grov uagtsomhed og får et strafmaksimum på 6 måneders fængsel i stedet for 4 måneders fængsel.

Der henvises til afsnit 8.8.2 vedrørende udvalgets forslag.

KAPITEL 7
TILTALE- OG EFTERFORSKNINGSSPØRGSMÅL

7.1. Offentlig påtale

En række af de bestemmelser, der vedrører (eller tillige vedrører) IT-rela-teret kriminalitet, er undergivet privat påtale eller betinget

offentlig påtale. Det gælder bl.a. straffelovens § 263 om hacking m.v., der efter § 275 er un-dergivet privat påtale med alternativ betinget offentlig påtale. Markedsfø-ringslovens § 10 om erhvervshemmeligheder er efter lovens § 22, stk. 4, ale-ne undergivet privat påtale, og ophavsretslovens § 76 er efter lovens § 82, stk. 1, kun undergivet betinget offentlig påtale.

De forskellige påtaleformer har også betydning for efterforskningsmulighe-der og for forældelsesfrister.

Retsplejelovens § 727, stk. 2, indeholder en bestemmelse om, at offentlig påtale af en lovovertrædelse, der er henvist til privat forfølgning, kan ske, hvis almene hensyn kræver det.

Der findes ikke en tilsvarende bestemmelse vedrørende betinget offentlig påtale, men efter retsplejelovens § 720, stk. 3, kan der foretages uopsættelige handlinger, til en påtalebegæring kan indhentes. Det er således begrænset, i hvilket omfang politiet kan tilrettelægge efterforskningen, og der er ikke mulighed for at fortsætte sagen, hvis den forurettede ikke begærer påtale, uanset om det vurderes, at almene hensyn kræver påtale, medmindre der måtte være en særlig hjemmel herfor, jfr. f.eks. straffelovens § 305.

Der findes en særlig forældelsesfrist for både privat og betinget offentlig på-tale. Efter straffelovens § 96, stk. 1, skal sag være anlagt eller begæring frem-sat inden 6 måneder efter, at den berettigede har fået sådan kundskab, at han har tilstrækkeligt grundlag herfor[169] [170]. I

---

[169] Fristen blev på baggrund af Straffelovrådets forslag i betænkning nr. 433/1966 om straf-feretlig forældelse m.v. forlænget fra 3 til 6 måneder. Fristens længde skyldes især en afvej-ning af på den ene side risikoen for misbrug af privat påtaleret og på den anden side den mulige procesbesparelse ved, at forlig kunne forhandles. Det siges vedrørende fristens begyndelsestidspunkt kun, s. 26, at beskrivelsen er mere dækkende end den tidligere (der vedrørte kundskab om gerningsmanden) for det, der bør lægges vægt på.

[170] Som eksempel på, at den særlige forældelsesfrist kan føre til frifindelse, kan nævnes Roskilde rets dom af 1/5 1996 vedrørende overtrædelse af markedsføringslovens § 10. Der var indgivet anmeldelse i december 1992 mod 2 ingeniører, men anmelderen kunne ikke udelukke, at den tidligere direktør var gerningsmanden. Først efter en landsretskendelse af 27/9 1993 kunne direktørens materiale forevises de forurettede, og kurator bekræftede her-efter i november 1993, at sagen ønskedes fremmet, såfremt efterforskningen førte til, at der rejstes tiltale

det omfang påtale sker i medfør af bestemmelsen i retsplejelovens § 727, stk. 2, om offentlig påtale begrundet i almene hensyn, gælder de almindelige forældelsesfrister.

Bestemmelsen i retsplejelovens § 727, stk. 2, kom ind i 1916-retsplejeloven (som § 725, stk. 3). Den dagældende bestemmelse anvendte "offentlig in-teresse" i stedet for "almene hensyn". Det siges i det forslag, der dannede grundlag for bestemmelsen[171]:

> "Dels er der givet det offentlige en i den nugældende Ret oftere savnet Adgang til at gøre en Handling, der i Almindelighed er henvist til privat Forfølgning, til Genstand for offentlig Forfølgning. Betingelse er, at Over-anklageren finder, at en offentlig Interesse (f. Eks. Hensynet til en Dom-stols Værdighed og Autoritet, naar et af dens Medlemmer er Genstand for Sigtelser eller Haan) kræver offentlig Forfølgning."

Udtrykket "almene hensyn" blev indsat i 1969. Det siges i lovforslaget[172], at forbrugerrådet havde anmodet om, at det blev overvejet at undergive straffelovens § 294 om selvtægt offentlig påtale, således at der var effektive regler ved selvtægtshandlinger fra afbetalingssælgeres side. I høringssvarene vedrørende dette forslag blev der navnlig henvist til, at der typisk lå civil-retlige mellemværender bag, hvis udredning falder uden for politiets sæd-vanlige arbejdsområde, og at det ville være urimeligt at bebyrde politiet med et betydeligt arbejde, der ikke modsvares af nogen almen interesse. Justits-ministeriet foreslog derfor ikke ændringer, men henviste til, at bestemmel-sen i den dagældende retsplejelovens § 725, stk. 3, kunne anvendes i de und-tagelsestilfælde, hvor der er en klar samfundsmæssig interesse i en offentlig forfølgning. Justitsministeriet antog således, at bestemmelsen kunne bruges i tilfælde, hvor en forretningsmand regelmæssigt begik selvtægtshandlinger i forbindelse med tilbagetagelse af ting solgt på afbetaling.

---

mod direktøren. Retten tiltrådte, at det først efter landsretskendelsen havde været muligt at tage stilling til begæring om påtalerejsning, men fandt ikke, at anklagemyn-digheden på det foreliggende havde godtgjort at have fornøden, rettidig begæring fra den forurettede for tiltalen.

[171] RT 1901 A (II), sp. 2964.

[172] FT 1968/69 A sp. 2910 f.

Bestemmelsen i retsplejelovens § 725, stk. 3, blev foreslået præciseret ved en ændret formulering bl.a. ved at anvende udtrykket "almene hensyn", hvor-ved formuleringen blev bragt i overensstemmelde med straffelovens § 305, stk. 1.

Ifølge straffelovens § 305, stk. 1, er overtrædelser af lovens § 291, stk. 1 og 3, § 298 og § 299 undergivet betinget offentlig påtale, medmindre almene hensyn kræver påtale. Motiverne indeholder ikke bidrag til, hvad der ligger i begrebet "almene hensyn".

Hurwitz anfører vedrørende opdelingen i privat påtale, betinget offentlig påtale og offentlig påtale[173], at området for privat påtale er betydelig ind-snævret i forhold til ældre lovgivning og yderligere indsnævret ved ind-førelse af bestemmelsen i (nu) retsplejelovens § 727, stk. 2. Han nævner, at et fælles karaktermærke for de forhold, der er undergivet privat påtale, er, at det drejer sig om angreb på blot individuelle retssfærer, at straffen i almin-delighed kun er bøde, samt at gerningsmanden normalt er kendt, således at politimæssig undersøgelse ikke er påkrævet. Der tages således hensyn til den forurettede, der ikke ønsker en offentlig sag, og til, "at de almene hensyn, der begrunder strafforfølgning, kun gør sig svagt gældende, idet man bevæ-ger sig i nærheden af grænserne for det strafbares naturlige område".

Vedrørende sidstnævnte betragtning henviser Hurwitz til straffelovsbetænk-ningen fra 1917, bemærkningerne s. 44. Det siges her vedrørende straffe-lovens påtaleregler, at hvis privat påtale skyldes, at en lovovertrædelse gen-nemsnitligt er af så ringe betydning, eller at grænsen mellem det strafbare og det ikke strafbare er så flydende og ubestemt, at det er unødvendigt og stri-dende mod sund økonomi at strafforfølge, hvis den forurettede ikke ønsker det, kan det være naturligt at undergive den forurettedes skøn en korrektur ud fra mere samfundsmæssige hensyn. Påtale bør kunne ske, hvis sagen undtagelsesvist er så alvorlig, at almene hensyn kræver straf.

Hurwitz anfører vedrørende sager, der er undergivet betinget offentlig på-tale, at denne form normalt anvendes ved lovovertrædelser, der er grovere end dem, der er undergivet privat påtale, men hvor særlige

---

[173] Den Danske Strafferetspleje, 3. rev. udg., 1959, s. 242 ff.

hensyn kan tale imod at skåne den forurettede for en uønsket strafforfølgning.

Vedrørende det af Hurwitz anførte om, at gerningsmanden normalt er kendt (og at der derfor ikke er efterforskningsbehov), nævner Krabbe[174], at valget mellem privat påtale og betinget offentlig påtale som regel vil have sammenhæng med, om gerningsmanden er kendt, og at dette bl.a. har med-ført, at 1930-straffeloven er gået over til (betinget) offentlig påtale ved for-sætligt hærværk.

Endvidere er det karakteristisk, at det ofte vil skade offeret yderligere, hvis der føres en offentlig straffesag f.eks. i anledning af freds- og ærekrænkelser.

Det fremgår af bemærkningerne til 1996-lovforslaget om datakriminalitet[175], at Rigsadvokaten i sit høringssvar vedrørende datakriminalitet havde anført vedrørende straffelovens § 263 om hacking, at det kunne overvejes, om der fortsat burde være betinget offentlig påtale. Rigsadvokaten bemærkede, at en af statsadvokaterne i sit høringssvar havde anført, at specielt private er-hvervsdrivende af hensyn til virksomhedens omdømme må påregnes at væ-re yderst tilbageholdende med at anmelde konstaterede "hacker-angreb" til politiet eller fremsætte anmodning om offentlig påtale, hvis kriminaliteten mod virksomheden afsløres uden anmeldelse fra denne.

Det siges videre i bemærkningerne vedrørende § 263, stk. 2 og 3, at Justits-ministeriet ikke på det foreliggende grundlag finder anledning til at foreslå ændringer i reglerne om adgangen til offentlig påtale, men dette spørgsmål kan overvejes af det udvalg, der skal overveje eventuelle yderligere lovæn-dringer med henblik på bekæmpelse af datakriminalitet.

Det har været omdiskuteret, om retsplejelovens § 727 er anvendelig i til-fælde, hvor der både er privat påtale og betinget offentlig påtale. Spørgs-målet er omtalt i 1996-lovforslaget om datakriminalitet. Der henvises her til UfR 1979.435 Ø[176], hvor det antoges at være tilfældet,

---

[174] Forhandlinger paa det sekstende nordiske Juristmøde, 1935, s. 189.

[175] FT 1995/96 A 4068.

[176] Vedrørende overtrædelse af straffelovens § 264 b, jfr. påtalereglen i § 275.

og UfR 1992.187 V[177], hvor det antoges ikke at være tilfældet. Det siges videre, at der efter Justitsministeriets opfattelse er adgang til offentlig påtale efter retspleje-lovens § 727, stk. 2, i sager, hvor der som alternativ til privat påtale er hjem-mel for betinget offentlig påtale.

Der henvises som nævnt til, at spørgsmålet om offentlig påtale kan over-vejes af det udvalg, der skal overveje eventuelle yderligere lovændringer med henblik på bekæmpelse af datakriminalitet. Det siges, at det forudsættes i den forbindelse, at der – hvad der må anses for at være gældende ret – er adgang til offentlig påtale i sager om overtrædelse af straffelovens § 263, stk. 2 og 3, hvis almene hensyn kræver det.[178]
Ophavsretslovens § 76 om piratkopiering er ikke omfattet af Justitsmini-steriets bemærkninger i lovforslaget.

I UfR 1998.1445 Ø lagde landsretten til grund, at en overtrædelse af straf-felovens § 264, stk. 1 – der lige som § 263 er omfattet af påtalereglen i § 275 – kunne påtales af det offentlige efter bestemmelsen i retsplejelovens § 727, stk. 2, uden begæring fra den forurettede.

Udvalget finder, at der i almindelighed ikke er et særligt behov for, at de bestemmelser, der (tillige) vedrører IT-kriminalitet, og som er undergivet privat og/eller betinget offentlig påtale, generelt undergives offentlig påtale. De hensyn, der ligger bag valg af påtaleform, vil i formentlig de fleste til-fælde gøre det velbegrundet, at den forurettede kan bestemme, om tiltale skal rejses.

I visse tilfælde kan situationen imidlertid være den, at det vurderes, at alme-ne hensyn kræver, at forholdet påtales. Udvalget har derfor overvejet, om bestemmelsen i retsplejelovens § 727 bør udvides således, at der ved over-trædelser, der er undergivet betinget offentlig påtale, i

---

[177] Vedrørende overtrædelse af straffelovens § 264, jfr. påtalereglen i § 275.

[178] Dette er også forudsat i Roskilde rets dom af 9/12 1996 i en større hackersag. Der var altovervejende ikke påtalebegæringer, og retten henviser, dommens side 195, til almene hensyn, uden at problemstillingen dog fremgår udtrykkeligt af dommen.

alle tilfælde skal kun-ne ske offentlig påtale, hvis almene hensyn kræver det.

Udvalget har især drøftet, at en række situationer vedrørende IT-kriminalitet kan adskille sig væsentligt fra de situationer, der var forudsat, da påta-lereglerne blev formuleret. For så vidt angår straffelovens § 263, stk. 2 og 3, er spørgsmålet løst i praksis gennem den valgte fortolkning af retsplejelo-vens § 727, stk. 2. Udvalget finder imidlertid, at det kan overvejes, om rets-tilstanden – under hensyntagen til tidligere modstridende fortolkninger – bør fremgå mere klart af lovteksten.

Ophavsretskrænkelsesområdet har i dag på IT-området i vidt omfang en anden karakter. For det første er gerningsmanden måske ikke kendt (hvis der er distribueret anonymt via Internettet), og for det andet kan det være problematisk at finde frem til, hvem der (i et eller andet land) kan komme med påtalebegæring på den forurettedes vegne.

Udvalget finder i øvrigt, at det med den nugældende fortolkning, hvor der er mulighed for offentlig påtale, hvis der er både privat og betinget offentlig påtale, kan virke uharmonisk, at denne ikke også er en mulighed i situatio-ner, hvor der alene er betinget offentlig påtale – ikke mindst i betragtning af, at denne kategori må antages at vedrøre mere grove (eller mere anonyme) overtrædelser end dem, hvor der alene er privat påtale.

Udvalget har derfor overvejet, om der ved betinget offentlig påtale bør ind-føres en generel hjemmel til offentlig påtale, hvis almene hensyn kræver det.[179]

Udvalget finder imidlertid ikke grundlag for at stille et sådant forslag, der i givet fald vil forudsætte en generel gennemgang af lovgivningen, herunder også af områder, der ikke har berøring med IT-kriminalitet.

For så vidt angår hovedparten af de områder, udvalget beskæftiger sig med i denne betænkning, vil der enten være offentlig påtale eller mulighed for på-tale, hvis almene hensyn kræver det. Dette gælder dog ikke for ophavsrets-loven, idet den alene indeholder en bestemmelse

[179] Arbejdsgruppen vedrørende datakriminalitet fandt, at der skulle være hjemmel hertil.

om betinget offentlig påta-le ved overtrædelser af lovens § 76, stk. 2, og § 77, stk. 2. Udvalget finder, at denne påtalebestemmelse i ophavsretsloven bør ændres, så den kommer til at svare til straffelovens § 305, dvs. at betinget offentlig påtale bibeholdes som hovedreglen, men at der åbnes mulighed for offentlig påtale, hvis alme-ne hensyn kræver det. Ændringen vil give en retstilstand, der harmonerer med de øvrige straffebestemmelser i ophavsretsloven, hvor der enten er privat påtale (med mulighed for at anvende retsplejelovens § 727, stk. 2, om offentlig påtale på grund af almene hensyn) eller offentlig påtale.

Udvalget finder, at den foreslåede bestemmelse ikke i almindelighed skal be-tyde en ændret tiltalepraksis. Udvalget finder, at såfremt de hensyn, der har ført til påtalereglerne, gør sig fuldt ud gældende, skal retstilstanden forblive uændret.

Ændringen vil betyde, at den indledende efterforskning i sager om ophavs-retskrænkelser ikke begrænses af reglen i retsplejelovens § 720, stk. 3, til uopsættelige handlinger. Det kan i visse tilfælde være til fordel for efter-forskningen, at den forurettede først underrettes senere, f.eks. hvis den for-urettede kan tænkes at kontakte den eller de mistænkte eller gå til pressen i en situation, hvor der er behov for at afvente, at andre lande iværksætter be-vissikring. Endvidere vil bestemmelsen kunne have betydning i relation til den særlige forældelsesfrist for påtalebegæringer, der ikke gælder ved of-fentlig påtale.

Udvalget finder herudover, at den ret restriktive fortolkning af, hvad der skal betragtes som en påtalebegæring, jfr. eksempelvis frifindelsen i UfR 2000.342 H, hvor der forelå anmeldelse, men ikke særskilt påtalebegæring, er uhensigtsmæssig, da en anmelder i almindelighed ikke har kendskab til, at en anmeldelse skal suppleres med en påtalebegæring, og da det kan ske, at politiet ikke – eller først for sent, jfr. forældelsesreglen i straffelovens § 96 – konstaterer, at en egentlig påtalebegæring mangler.

Udvalget foreslår på den baggrund, at der indsættes en bestemmelse i retsplejeloven om, at en anmeldelse fra den berettigede anses som en begæring om offentlig påtale, medmindre andet fremgår af anmeldelsen.

Der henvises til afsnit 8.9 vedrørende udvalgets forslag.

7.2. Terminalefterforskning

Den teknologiske udvikling kan ikke undgå at give nye efterforsknings-problemer. Dette problem er derfor også nævnt af Gruppen på Højt Plan, der blev nedsat af det Europæiske Råd, i dens handlingsplan til bekæmpelse af organiseret kriminalitet fra april 1997[180]. Det siges i den detaillerede hand-lingsplans punkt 5:

> "Der bør inden for EU foretages en undersøgelse på tværs af søjlerne af kriminalitet inden for højteknologi samt brugen heraf og forbindelsen med organiseret kriminalitet. Denne undersøgelse bør bane vejen for en poli-tik, der sikrer effektiv offentlig beskyttelse. Uden at der indføres unødven-dige restriktioner, bør de retshåndhævende og retlige myndigheder have midler til, som et supplement til det specifikke ansvar, der påhviler leve-randører af teknologi og tjenesteydelser, at forebygge og bekæmpe mis-brug af disse nye teknologier. Man skal være opmærksom både på ulovlig praksis (som f.eks. kriminelle organisationers brug af disse teknologier for at lette deres aktiviteter) og på ulovligt indhold (som f.eks. børneporno-grafi eller formidling af opskrifter på syntetisk narkotika)."

Den efterforskning, der er behov for at foretage på Internettet, vedrører dels traditionel efterforskning i områder, der er tilgængelige for alle, og dels efterforskning i områder, der kun er tilgængelige for en udvalgt medlems-kreds. I den sidste sammenhæng kan der være behov for at at bruge en ind-skudt Internetadresse til sløring af, hvorfra der opereres, og for anvendelse af særlige dæknavne, som almindeligt er i det forum.

Et væsentligt spørgsmål ved efterforskning af IT-kriminalitet er de folke-retlige begrænsninger i adgangen til at foretage efterforskning i andre lande. Denne problemstilling forstærkes af, at man i mange tilfælde ved en termi-nalefterforskning ikke ved, hvilket land serveren findes i.

---

[180] 6276/4/97 JAI 7 REV 4.

Dette spørgsmål opstår også i tilfælde, hvor det strafbare forhold ikke er IT-relateret, men hvor der f.eks. er behov for at indhente bogføring, der føres i udlandet, fra en terminal på et ransagningssted.

For så vidt angår spørgsmålet om agentvirksomhed opstår der både det na-tionale spørgsmål om, hvad der er agentvirksomhed, og det internationalt relaterede spørgsmål om, hvad Danmark accepterer, at udenlandske myn-digheder med efterforskningskompetence foretager sig i Danmark.

Spørgsmålet om, hvornår en efterforskning bliver omfattet af agentregler-ne[181], og i hvilken udstrækning der bør være adgang til efterforskning på Internettet, opstår i relation til alle former for kriminalitet, der foregår via eller muliggøres via Internettet.

I Justitsministeriets Strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter be-skriver udvalget[182] den nedre grænse for agentvirksomhed, dvs. grænsen mellem tilladelig agentvirksomhed og almindelige efterforskningsskridt.

Det siges[183], at infiltration falder uden for agentbegrebet. Infiltration beskri-ves som f.eks. den situation, at en person efter aftale med politiet søger kon-takt i et kriminelt miljø for at kunne give politiet oplysninger. Det siges vi-dere:

---

[181] Der er afgrænset til visse kvalificerede sagstyper og har et særligt mistankekrav, jfr. retsplejelovens §§ 754 a – 754 b:
§ 754 a. Politiet må ikke som led i efterforskningen af en lovovertrædelse foranledige, at der tilbydes bistand til eller træffes foranstaltninger med henblik på at tilskynde nogen til at udføre eller fortsætte lovovertrædelsen, medmindre:
1) der foreligger en særligt bestyrket mistanke om, at lovovertrædelsen er ved at blive be-gået eller forsøgt,
2) andre efterforskningsskridt ikke vil være egnede til at sikre bevis i sagen, og
3) efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, eller en overtrædelse af straffelovens § 289, 2. pkt.

§ 754 b. De foranstaltninger, som er nævnt i § 754 a, må ikke bevirke en forøgelse af lovovertrædelsens omfang eller grovhed.
Stk. 2. Foranstaltningerne må alene udføres af polititjenestemænd.

[182] S. 155 ff.

[183] S. 160.

> ”Dette gælder også, selv om den pågældende deltager i kriminalitet for at gøre sig troværdig i miljøet. Hvis den pågældende imidlertid på de i lov-udkastet angivne måder griber direkte ind i selve den lovovertrædelse, som efterforskningen angår, kan der dog være tale om en foranstaltning, der ligger over den nedre grænse og derfor er omfattet af reguleringen. Deri-mod er tilfælde af infiltration, hvor den pågældende kun tager del i sådan mindre kriminalitet, som efterforskningen ikke er rettet imod, ikke omfat-tet af reguleringen.”

Det siges endvidere[184], at en agent ikke vil kunne blive ansvarlig for med-virken til lovovertrædelsen, fordi forholdet mangler materiel typicitet.

I det omfang, de efterforskningsskridt, der vil være nødvendige for at opkla-re kriminaliteten, falder ind under agentreglerne, vil politiet i vidt omfang være afskåret fra at efterforske den IT-relaterede kriminalitet, fordi den ak-tuelle kriminalitetsform ikke er omfattet af reglerne. Det gælder f.eks. for kursmanipulation, ophavsretskrænkelser m.v.

Spørgsmålet er derfor, om der er behov for at udvide området for, i hvilke sager agenter kan anvendes.

I Strafferetsplejeudvalgets ovennævnte betænkning fra 1984 fremhæves[185], at kriminalitetsudviklingen, især narkotikakriminaliteten, har ført til en forøget anvendelse af ikke-traditionelle efterforskningsskridt. Det fremhæves, at narkotikakriminaliteten er ”offerløs” i den forstand, at offeret er solidarisk med den kriminelle. På den baggrund er udviklingen gået mod en aktiv ef-terforskning, der er karakteristisk ved, at den ikke angår en anmeldt, begået kriminalitet, og at politiet ”er med i marken” og foretager undersøgelser, samtidig med at kriminaliteten er på forsøgsstadiet eller ved at blive begået.

Tilsvarende kan anføres om dele af den IT-relaterede kriminalitet, ikke mindst for så vidt angår spredningen af børnepornografi.

---

[184] S. 168 f.

[185] S. 125 f.

Umiddelbart synes de efterforskningsskridt, der er relevante, snarere at kun-ne karakteriseres som infiltration end som agentvirksomhed. Eventuelle lov-overtrædelser, der er nødvendige for at infiltrere f.eks. en børnepornografi-kreds eller en hackerkreds, vil formentlige ikke være strafbare, hvis de – som ved agentens medvirken – mangler materiel typicitet. Det kan derimod ikke udelukkes, at de betragtes som en overskridelse af, hvor langt politiet tjenst-ligt kan gå i den konkrete sammenhæng. Der kan derfor være behov for, at der formuleres administrative forskrifter om politiets efterforskning ved IT-infiltration.

Udvalget finder ikke, at der med den kendte kriminalitet er behov for at kunne anvende de særlige agentregler i IT-relaterede sager, der ikke er omfattet af de gældende regler.[186]

De regler, der gælder for politiets virksomhed i Danmark, kan imidlertid ikke uden videre overføres på internationale forhold. Det er forskelligt, i hvilket omfang andre lande tillader, at udenlandske myndigheder foretager myndighedshandlinger med tilknytning til deres territorium. F.eks. er der flere lande, der ikke accepterer, at politiet eller anklagemyndigheden sender breve – f.eks. brevforkyndelser eller meddelelse om slutning af en sag – di-rekte til personer på deres territorium. Sådanne lande kan ikke forventes at acceptere, at politiet i andre lande infiltrerer på deres territorium.

I G8-landenes erklæring af 10/12 1997 om high-tech crime[187] nævnes i prin-ciperklæringens punkt VII, at der ikke skal kræves tilladelse fra det land, der har data, hvis retshåndhævelsesmyndigheder har elektronisk adgang til åbne kilder.

Tilsvarende anføres i Europarådets konvention om IT-kriminalitet, jfr. ne-denfor.

Internationalt arbejdes der på at løse i hvert fald nogle af de efterforsknings-mæssige problemer, der er knyttet til det globale IT-samfund. Som det fremgår af det følgende, bevæger man sig mod en vis

---

[186] Arbejdsgruppen vedrørende datakriminalitet var af samme opfattelse.

[187] Erklæringen er gengivet i sin helhed i betænkning nr. 1377/1999 om børnepornografi og om IT-efterforskning, s. 122 f.

opblødning på de om-råder, hvor det traditionelle retshjælpssystem ikke er i harmoni med de IT-løsninger, der anvendes i dag.

I konventionen af 29/5 2000 om gensidig retshjælp mellem EU-landene[188] er der i afsnit III en regulering vedrørende aflytning af telekommunikation.

Artikel 20 vedrører aflytning af telekommunikation uden teknisk assistance fra en anden stat. I tilfælde, hvor telekommunikationsadressen anvendes på en anden stats område, skal den aflyttende stat underrette (med oplysning om retsgrundlag, sigtelse m.v.) den anden stat inden aflytningen, hvis den er bekendt med, at den aflyttede person befinder sig på den anden stats om-råde, og ellers straks den bliver bekendt hermed. Den underrettede stat skal som udgangspunkt inden 96 timer meddele, om den tillader aflytningen, Hvis den meddeler afslag (af nærmere angivne grunde), kan den kræve, at det indhentede materiale ikke anvendes eller kun anvendes på nærmere an-givne betingelser.

I Europarådets konvention om IT-kriminalitet jfr. bilaget, er der i artikel 32 en regulering vedrørende grænseoverskridende access til data, hvor gensidig retshjælp ikke er påkrævet. Efter denne bestemmelse er dette tilladt ved offentligt tilgængeligt materiale (open source). Det er endvidere tilladt, hvis der er givet samtykke fra en person på statens eget territorium, der har lovlig adgang til de aktuelle data i det andet land. Bestemmelsen finder så-ledes ikke anvendelse, hvis indgrebet sker uden samtykke i forbindelse med en ransagningkendelse. De øvrige situationer reguleres ved bestemmelser om hurtig kommunikation, hurtige indgreb m.v., hvilket selvfølgelig vil betyde forbedrede efterforskningsmuligheder.

Uden for disse situationer vil det være nødvendigt at anvende det almin-delige retshjælpssystem. Den risiko, der er for, at dette på grund af tidsfak-toren reelt umuliggør en gennemførelse af det ønskede efterforsknings-skridt, må reduceres ved et særligt kontaktsystem. I mange tilfælde vil situ-ationen dog være den, at handlingen også er kriminel i det pågældende land, således at landet på baggrund af en information om, hvad der sker eller er sket, straks kan iværksætte sin

[188] EFT C 2000 197/1.

egen efterforskning, der i disse situationer ikke er afhængig af en retsanmodning.

Forudsætningen for, at man kan anmode et land om noget eller orientere det om noget, er imidlertid, at man ved, hvilket land man skal rette hen-vendelse til. Kan man se, hvilket land der umiddelbart er aktuelt, kan problemet med at efterforske, mens der stadig er logning af de foretagne transaktioner, herefter være, at der måske er anvendt værtscomputere i mange lande frem til den computer, et angreb har været rettet mod.

Spørgsmålet om de folkeretlige begrænsninger i adgangen til for dansk politi at foretage efterforskning med tilknytning til udlandet kan i sagens natur ikke løses ved dansk lovgivning.

Udvalget påpeger behovet for, at de internationale regler får et sådant ind-hold, at efterforskning over landegrænserne kan gennemføres på en smidig måde.

Problemstillingen er ikke kun aktuel ved IT-kriminalitet, men også i relation til en dansk virksomheds bogføring i udlandet eller placering af andre sel-skabsfunktioner i udlandet (hvad enten der er tale om placering i koncernen eller outsourcing af opgaver).

Der henvises til afsnit 8.10.

7.3. Europarådets konvention om IT-kriminalitet

Europarådets konvention af 23/11 2001 om IT-kriminalitet (Budapestkon-ventionen) er optrykt som bilag til denne betænkning.

Udvalget har overvejet, om konventionen nødvendiggør strafferetlige regu-leringer, der er mere vidtgående end de i denne betænkning foreslåede. Konventionen indeholder på det strafferetlige område helt overvejende krav om en kriminalisering, der harmonerer med den nugældende regulering i straffeloven.

Særligt vedrørende artikel 5 om at forhindre et edb-systems funktion i alvor-lig grad ved at indlæse, overføre, slette, forringe, ændre eller

undertrykke elektronisk data henvises til udvalgets forslag om at præcisere anvendelses-området for straffelovens § 293, stk. 2, om rådighedsberøvelse, jfr. afsnit 6.6.

Særligt vedrørende artikel 6 om at gøre det strafbart at fremstille, sælge, fremskaffe til brug, importere, forhandle eller i øvrigt tilgængeliggøre samt besidde anordninger, herunder edb-programmer, og forskellige former for adgangsmidler til edb-systemer med forsæt til at anvende dem til at begå en af de handlinger, der er nævnt i artikel 2-5, bemærkes, at den konventions-mæssige forpligtelse må anses for at være dækket af straffelovens regler om forsøg og medvirken. Efter det for udvalget oplyste er det ikke et krav, at der skal udfærdiges særskilte straffebestemmelser, dvs. i det omfang, be-stemmelserne om forsøg og medvirken dækker det, der skal kriminaliseres, er dette tilstrækkeligt. Udvalgets forslag vedrørende adgangsmidler, jfr. afsnit 3.2, giver på flere områder en udvidet strafferetlig dækning på områ-det.

Særligt vedrørende artikel 7 om at kriminalisere elektronisk dokumentfalsk bemærkes, at udvalgets forslag vedrørende dokumentfalsk, jfr. afsnit 5.3, dækker denne forpligtigelse.

KAPITEL 8
UDVALGETS FORSLAG MED BEMÆRKNINGER

8.1. Adgangsmidler

Der henvises til afsnit 3.2.4 vedrørende udvalgets overvejelser.

8.1.1. Adgangsmidler til kommercielle informationssystemer

Udvalget foreslår følgende formulering af bestemmelsen vedrørende kom-mercielle informationssystemer:

"§ 301 a. Med bøde eller fængsel indtil 6 måneder straffes den, der retsstri-digt skaffer sig eller videregiver koder eller andre adgangsmidler til informa-tionssystemer, hvortil adgangen er forbeholdt betalende brugere, og som er beskyttet med kode eller anden særlig adgangsbegrænsning.
Stk. 2. Sker den i stk. 1 nævnte videregivelse erhvervsmæssigt, i en videre kreds eller under omstændigheder, hvor der er særlig risiko for omfattende misbrug, er straffen fængsel indtil 4 år."

Der henvises til bemærkningerne til den foreslåede § 263 a i afsnit 8.1.2.

I modsætning til § 263 a dækker den foreslåede bestemmelse alle adgangs-midler, såfremt der er tale om kommercielle systemer, d.v.s. systemer, hvor brugerbetaling (enten som en fast, typisk periodisk, ydelse eller som betaling for den konkrete brug eller en kombination heraf) er en forudsætning for brugen af systemet. Der er efter udvalgets opfattelse behov for, at der er en fremskudt regulering, der ikke er afhængig af, om betingelserne for at straffe for forsøg (allerede) er opfyldt.

Bestemmelsen er også anvendelig ved forskaffelse eller videregivelse af en enkelt kode eller et enkelt andet adgangsmiddel.

Forslagets stk. 2 giver mulighed for fængsel i op til 4 år i kvalificerede vide-regivelsessituationer, hvor der videregives erhvervsmæssigt eller i en videre kreds. Det dækker også videregivelse med "særlig risiko for omfattende mis-brug". Det vil afhænge af de konkrete omstændigheder, om der kan siges at være en særlig risiko for omfattende misbrug. Det vil f.eks. kunne være til-fældet, hvis der videregives calling cards eller NUI-koder til mange personer (der eventuelt også kan videregive) med besked om, fra hvilket tidspunkt de skal anvendes, således at en kontobelastning må forventes at kunne blive omfattende, før misbruget opdages og standses. Det vil også kunne være til-fældet, hvis der er tale om "bestillingsarbejde" på et større antal adgangs-midler, ikke mindst hvis der betales et større beløb

for adgangskoderne, for-di det i disse situationer må forventes, at formålet er et omfattende mis-brug.

Der kan eventuelt idømmes bøde i forbindelse med en betinget dom, jfr. straffelovens § 58, stk. 2.

8.1.2. Adgangsmidler til ikke-kommercielle informationssystemer

Udvalget finder, at der til beskyttelse af privatlivets fred og til beskyttelse mod hærværk m.v. i en række situationer bør være en beskyttelse af pass-words og andre adgangsmidler, der ligger tidligere end forsøget på at anven-de disse midler. Udvalget har valgt at begrænse denne tidlige beskyttelse således, at den som udgangspunkt omfatter videregivelse i form af erhvervs-mæssigt salg, udbredelse i en videre kreds samt videregivelse af et større antal passwords eller andre adgangsmidler. Som udgangspunkt er det at besidde eller at skaffe sig passwords eller andre adgangsmidler til ikke-kommercielle informationssystemer således ikke omfattet. Det samme gæl-der videregivelse af et enkelt eller nogle få passwords. For så vidt angår ikke-kommercielle informationssystemer, der må anses for særlig beskyt-telsesværdige, finder udvalget dog, at der bør gælde den samme strafferetlige beskyttelse, som den, der gælder for de kommercielle informationssystemer. Der sigtes herved til de samfundsvigtige informationssystemer og til informationssystemer, der indeholder særlig personfølsomme oplysninger. Udvalget foreslår, at det gøres strafbart at skaffe sig eller at videregive et eller flere passwords eller andre adgangsmidler til sådanne informations-systemer.

Udvalget har derimod ikke fundet, at der er behov for herudover at give en strafferetlig beskyttelse, der efter omstændighederne kan ligge tidligere end det tidspunkt, hvor der kan dømmes for forsøg på f.eks. hacking. Udvalget har således ikke fundet, at adgangsmidler til private pc'ere eller til infor-mationssystemer, hvor der ikke er et helt specielt behov for at beskytte oplysningerne, skal omfattes af stk. 2.

Udvalget foreslår følgende formulering af bestemmelsen:

"§ 263 a. Med bøde eller fængsel indtil 6 måneder straffes den, der retstri-digt

1) erhvervsmæssigt sælger eller
2) i en videre kreds udbreder

en kode eller andet adgangsmiddel til et ikke offentligt tilgængeligt informa-tionssystem, hvortil adgangen er beskyttet med kode eller anden særlig ad-gangsbegrænsning.

Stk. 2. På samme måde straffes den, der retsstridigt videregiver et større an-tal koder eller andre adgangsmidler som nævnt i stk. 1.

Stk. 3. På samme måde straffes den, der retsstridigt skaffer sig eller videregi-ver en kode eller andet adgangsmiddel som nævnt i stk. 1 til

1) et samfundsvigtigt informationssystem eller
2) et informationssystem, der behandler fortrolige oplysninger, der er om-fattet af § 7, stk. 1, og § 8, stk. 1, i lov om behandling af personoplys-ninger, om flere personers personlige forhold.

Stk. 4. Sker den i stk. 1 og stk. 2 nævnte videregivelse i særligt stort omfang eller indebærer den særlig risiko for betydelig skade, er straffen fængsel ind-til 4 år."

Bestemmelsen har til formål at give en mere effektiv strafferetlig beskyttelse af informationssystemer.

Med hensyn til forholdet mellem de foreslåede nye bestemmelser og mulig-heden for at anse befatningen med adgangsmidlet som forsøg på (medvir-ken til) en videregående kriminalitet bemærkes følgende:

Såfremt betingelserne for at straffe for forsøg i relation til anden kriminalitet er opfyldt, vil der uanset de foreslåede nye bestemmelser i § 263 a og § 301 a fortsat kunne dømmes efter forsøgsreglerne. Dette gælder, uanset om den pågældende forsøgshandling i det hele falder uden for anvendelsesområdet for de foreslåede nye bestemmelser, eller om handlingen isoleret set måtte være omfattet af en af de nye bestemmelser som en fuldbyrdet forbrydelse.

Selv om udbredelse via Internettet af et password til en anden persons bankkonto isoleret set indebærer en fuldbyrdet overtrædelse af den foreslåede nye bestemmelse i § 263 a, stk. 1, vil der således kunne straffes for forsøg på medvirken til f.eks. databedrageri (§ 279 a), hvis et sådant videregående forsæt kan bevises.

På samme måde vil der som hidtil kunne straffes for forsøg på hacking (§ 263), hvis en person skaffer sig et password til en virksomheds

interne informationssystem med forsæt til uberettiget at trænge ind i systemet. Dette gælder uafhængigt af, om dette forhold i det hele måtte falde uden for anvendelsesområdet for den foreslåede bestemmelse i § 263 a, hvor forskaf-felsen kun er strafbar som en selvstændig forbrydelse, hvis der er tale om et samfundsvigtigt informationssystem eller et system, der indeholder person-følsomme oplysninger.

Begrænsningen i de informationssystemer, der er omfattet af den foreslåede bestemmelse i § 263 a, ligger i, at de ikke er offentligt tilgængelige og har særlige adgangsbegrænsninger. Bestemmelsen vil således omfatte informationssystemer til almindelig databehandling i f.eks. private virksomheder eller den offentlige sektor. Bestemmelsen vil ligeledes omfatte informationstjenester, hvor der er særlige adgangskrav og adgangsmidler, og hvor adgang f.eks. er betinget af, at man tilhører en særlig erhvervskreds. Den vil derimod ikke omfatte koder, der giver en særlig kontorelateret adgang til at benytte teletjenester, idet det er en adgang til, at udgifterne føres på kodeindehaverens konto (konteringsmidler). Den vil heller ikke omfatte koder m.v. til andre informationssystemer, der er tilgængelige for alle mod betaling. Efter udvalgets forslag skal betalingsrelaterede koder m.v. reguleres i en selvstændig bestemmelse, jfr. afsnit 8.1.1. Bestemmelsen vil også dække situationer, hvor informa-tionssystemet er reserveret for en enkelt person, der konkret udgør hele brugerkredsen.

I kravet om retstridighed ligger f.eks., at hvis midlerne skaffes eller vide-regives til lovlige formål, f.eks. som led i en systemadministrators arbejde, er dette ikke omfattet af bestemmelsen.

Tilsvarende gælder, hvis andre uopfordret videregiver deres passwords (uden at dette skyldes en af gerningsmanden fremkaldt vildfarelse hos den pågældende som ved social engineering o.l.).

Udtrykket "beskyttet" tilsigter at udelukke, at bestemmelsen kan finde an-vendelse, hvor adgangsmidlet kan tildeles alle uden nærmere vilkår, hvis de anmoder om det.

Forslagets stk. 1, nr. 1, vedrører de situationer, hvor adgangsmidlerne sælges erhvervsmæssigt. Udvalget finder, at det er væsentligt, at

adgangsmidlerne ikke bliver handelsobjekter uden for det legitime område.

Forslagets stk. 1, nr. 2, vedrører udbredelse i en videre kreds. Der er tale om videregivelse, der har karakter af eller kan sammenlignes med offentliggø-relse, f.eks. ved at oplysningerne er almindeligt tilgængelige eller tilgængelige for en større lukket kreds på Internettet.

Forslagets stk. 2 vedrører videregivelse af "et større antal" adgangsmidler. Udvalget finder, at begrebet typisk skal forstås som 10 adgangsmidler eller derover. Det er en forudsætning for anvendelse af bestemmelsen, hvis der flere gange er videregivet færre end 10, at der er en sådan tidsmæssig sam-menhæng, at det reelt må betegnes som én samlet videregivelse.

Forslagets stk. 3 omfatter ikke alene videregivelse af adgangsmidler til de nævnte informationssystemer, men også at skaffe sig sådanne midler.

I udtrykket "skaffe sig" ligger bl.a. den begrænsning, at det ikke er omfattet, hvis man uforvarende er kommet i besiddelse af midlerne, f.eks. ved at an-dre har indlagt dem på ens computer.

Den foreslåede bestemmelse dækker også den situation, at en person skaffer sig kendskab til et password og blot husker dette.

Udvalget er opmærksom på, at det vil kunne give bevisproblemer, at den blotte besiddelse ikke er tilstrækkelig, og at en regulering som den, der er valgt ved den sidste ændring af radio- og fjernsynsloven, jfr. afsnit 3.2.1.1, er enklere at anvende i praksis. Udvalget antager imidlertid, at det i de tilfælde, der især kan være behov for at ramme, vil være muligt at bevise, at der ikke er tale om en situation, hvor den pågældende passivt har modtaget oplys-ningerne på baggrund af en anden persons initiativ.

En sådan kriminalisering findes allerede nu i straffelovens § 264 c. Straffe-lovens § 264 c forudsætter imidlertid, at den skaffede information er tilveje-bragt på bestemte måder (bl.a. ved hacking eller ved husfredskrænkelser). Efter udvalgets forslag skal forskaffelsen gøres

strafbar, uanset hvordan op-lysningen er tilvejebragt, selv om overdrageren lovligt besidder adgangsmid-let.

For så vidt angår de tilfælde, der er omfattet af både straffelovens § 264 c og den af udvalget foreslåede § 263 a kan anklagemyndigheden vælge, hvilken bestemmelse der skal rejses tiltale efter. Straffelovens § 264 c vil i øvrigt fortsat dække det samme som i dag og vil således for så vidt angår f.eks. hackede adgangsmidler have et bredere anvendelsesområde end den af ud-valget foreslåede § 263 a. Det er ikke tanken, at udvalgets forslag skal inde-bære en udvidelse af anvendelsesområdet for straffelovens § 264 c, jfr. sidst i dette afsnit.

Forslagets stk. 3, nr. 1, vedrører de informationssystemer, der kan være om-fattet af straffelovens § 193. Der henvises til afsnit 6.7, hvor bestemmel-sens anvendelsesområde er beskrevet. Adgangsmidlet skal give adgang på et niveau, der giver mulighed for at begå en overtrædelse af straffelovens § 193. Eksempelvis vil passwordet til en kontohavers konto ikke være omfat-tet af denne bestemmelse, uanset om data er placeret i bankens centrale in-formationssystem, hvorimod en af bankens driftsansvarliges password vil være omfattet. (Salg, udbredelse i en videre kreds eller videregivelse sammen med flere andre adgangsmidler af kontohaverens password vil være dækket af bestemmelsens stk. 1).

Forslagets stk. 3, nr. 2, omfatter offentlige og private informationssystemer, der behandler fortrolige oplysninger om flere personers private forhold. Bestemmelsen finder kun anvendelse på informationssystemer med oplys-ninger, der er omfattet af § 7, stk. 1 i lov om behandling af personoplys-ninger (racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om hel-bredsmæssige og seksuelle forhold), og § 8, stk. 1 (strafbare forhold, væsent-lige sociale problemer og andre rent private forhold end de i § 7, stk. 1, nævnte).

Med hensyn til begrebet "andre rent private forhold" nævnes som ek-sempler i lovforslaget[189] andre foreningsmæssige tilhørsforhold, familiestri-digheder, separations- og skilsmissebegæringer og

[189] FT 1999/2000 A 3971.

adoptionsforhold. Det fremgår i øvrigt af lovforslaget, at det samlede område ikke er mere snævert end efter den tidligere registerlovgivning.

Forslagets stk. 4 giver mulighed for fængsel i op til 4 år i særligt kvalifice-rede videregivelsessituationer. Dette gælder, hvis videregivelsen har et sær-ligt stort omfang. Dette vil typisk indebære, at der er særlig risiko for bety-delig skade, men udvalget finder, at der i disse situationer bør kunne idøm-mes højere straf, uden at der nødvendigvis skal tages stilling til skaderisiko-en.

Bedømmelsen af risikoen for skade vil være konkret i den enkelte sag. I vur-deringen af, om risikoen er væsentligt større end den, der altid ligger i vide-regivelsen, kan bl.a. indgå, hvem der videregives til (om der f.eks. er tale om en organiseret hackergruppe eller om bestillingsarbejde), og hvad der videre-gives. F.eks. må en målrettet videregivelse af adgangsmidler til samfunds-vigtige informationssystemer forventes normalt at blive omfattet af be-stemmelsen i modsætning til en videregivelse via Internettet af mindre følsomme adgangskoder. Et naturligt udgangspunkt vil være, hvor tæt man er på forsøg på medvirken, udover om det pågældende informationssystem indeholder oplysninger eller har en størrelse, der kan indebære risiko for betydelig skade.

Der kan eventuelt idømmes bøde i forbindelse med en betinget dom, jfr. straffelovens § 58, stk. 2.

Som nævnt tilsigter den foreslåede bestemmelse ikke at udvide anvendelses-området for straffelovens § 264 c. Hvis bestemmelsen placeres som § 263 a bliver den imidlertid omfattet af henvisningen til §§ 263-264 a i § 264 c.

Udvalget foreslår derfor, at straffelovens § 264 c ændres således, at "§§ 263-264 a" ændres til "§§ 263, 264 og 264 a".

8.1.3. Midler til tilegnelse af bl.a. adgangsmidler

Udvalget har overvejet, om der bør være en regulering vedrørende midler, der udelukkende eller overvejende er beregnet til tilegnelse af adgangsmid-ler, betalingskortnumre m.v., jfr. afsnit 3.2.3 og 4.3.4.

Udvalget finder på baggrund af IT-Sikkerhedsrådets udtalelse samt udvik-lingen i retning af anvendelse af chipkort, at området er uegnet til særskilt strafferetlig regulering, og at behovet herfor i løbet af få år vil blive redu-ceret væsentligt i takt med udviklingen.

8.2. Straffelovens § 263, stk. 2

Der henvises til afsnit 3.3 vedrørende udvalgets overvejelser.

Udvalget har overvejet, om strafferammen i strfl. § 263, stk. 2, på 6 måne-ders fængsel er tilstrækkelig i de situationer, der ikke omfattes af stk. 3. I de foreliggende domme er idømt bøder eller givet betinget dom. Udvalget finder, at der bør være et højere strafmaksimum i straffelovens § 263, stk. 2. Udvalget finder, at hacking er så alvorligt et indgreb for de fleste virksom-heder, at strafmaksimum bør afspejle dette også i den ikke kvalificerede be-stemmelse.

Udvalget finder, at udviklingen på hackerområdet siden 1985, hvor bestem-melsen blev indsat, gør, at der i dag er behov for, at strafmaksimum i straf-felovens § 263, stk. 2, forhøjes til fængsel i 1 år og 6 måneder. Udvalget har herved bl.a. lagt vægt på, at det IT-baserede samfund er meget sårbart, og at selv et forsøg på hacking er meget føleligt for offeret, der er nødt til at gen-nemgå hele systemet for at være sikker på, om der er sket skader.[190]

Udvalget foreslår derfor, at straffelovens § 263, stk. 2, ændres således, at "fængsel indtil 6 måneder" erstattes med "fængsel indtil 1 år og 6 måne-der".

Det foreslås endvidere, at "et anlæg til elektronisk databehandling" ændres til "et informationssystem".

8.3. Industrispionage m.v.

Der henvises til afsnit 3.4 vedrørende udvalgets overvejelser.

---

[190] Arbejdsgruppen vedrørende datakriminalitet var enig med udvalget.

Udvalget foreslår, at der i markedsføringslovens § 10 som et nyt stk. 3 ind-sættes følgende bestemmelse:

"Reglerne i stk. 1 og 2 finder tilsvarende anvendelse på andre personer, der har lovlig adgang til virksomheden."

Markedsføringslovens § 10, stk. 3 og 4, bliver herefter stk. 4 og 5.

Udvalget foreslår endvidere, at markedsføringslovens § 22, stk. 4, 1. pkt., ændres således, at der i stedet for "bøde eller fængsel indtil 2 år" indsættes "bøde eller fængsel indtil 1 år og 6 måneder, medmindre højere straf er forskyldt efter straffelovens § 299 a".

Et strafmaksimum på fængsel i 1 år og 6 måneder svarer til, hvad udvalget generelt synes bør være maksimum i tilfælde, hvor der er en strafferetlig overbygning vedrørende kvalificerede forhold.[191] Reguleringen svarer til, hvad der gælder for berigelsesforbrydelser, jfr. straffelovens § 285 og over-bygningen i § 286.

Udvalget finder endvidere, at særligt grove overtrædelser af markedsføringsloven bør reguleres i straffeloven, og at strafmaksimum skal være på li-nie med straffelovens § 263, stk. 3, og § 276. Udvalget foreslår derfor føl-gende bestemmelse indsat i straffeloven:

"§ 299 a. Med fængsel indtil 4 år straffes den, der gør sig skyldig i overtrædelse af markedsføringslovens § 10, hvor handlingen har medført bety-delig skade, eller der har været nærliggende fare herfor."

Ved nogle overbygningsbestemmelser i straffeloven (f.eks. ved tyveri (§ 286, stk. 1), hærværk (§ 291, stk. 2) og skattesvig (§ 289)) anvendes i praksis ret faste beløbsgrænser ved afgørelsen af, om overbygningsbestemmelserne skal an-vendes. I andre tilfælde (f.eks. ved grov miljøkriminalitet (§ 196) og visse former for hacking m.v. og husfredskrænkelse (§ 263 og § 264)) er det ikke muligt at have en fast afgrænsning. Den foreslåede bestemmelse hører til sidstnævnte gruppe. Det må således afgøres efter en konkret vurdering i den enkelte sag, om

[191] Jfr. betænkning nr. 1396/2001 om straffelovens § 289 m.v., s. 66, og forslagene i nærvæ-rende betænkning.

der er tale om "betydelig skade". Udvalget har herved bl.a. lagt vægt på, at krænkelser, der finder sted i udviklingsfasen, kun medfører skade, der kan opgøres i penge, hvis den planlagte udvikling er succesfuld, hvorimod beskyttelseshensynet ikke afhænger af, om det endelige resultat er vellykket.

8.4. Piratkopiering

Der henvises til afsnit 3.5 vedrørende udvalgets overvejelser.

Udvalget finder, at bestemmelsen i ophavsretsloven om piratkopiering bør ændres således, at det at gøre værker tilgængelige for en videre kreds tillige er omfattet af den kvalificerede bestemmelse, og at strafmaksimum forhø-jes fra 1 år til 1 år og 6 måneder. Som nævnt i afsnit 8.3 svarer et straf-maksimum på fængsel i 1 år og 6 måneder til, hvad udvalget generelt synes bør være maksimum i særlovgivningen i tilfælde, hvor der er en strafferetlig overbygning vedrørende kvalificerede forhold.

Det foreslås derfor, at ophavsretslovens § 76, stk. 2, affattes således:

"Stk. 2. Er en overtrædelse af de i stk. 1, nr. 1 og 2, nævnte bestemmelser begået ved forsætligt og under skærpende omstændigheder at gengive de af bestemmelserne omfattede værker eller frembringelser eller blandt almen-heden at sprede eksemplarer heraf, kan straffen stige til fængsel i 1 år og 6 måneder måneder, medmindre højere straf er forskyldt efter straffelovens § 299 b. Skærpende omstændigheder anses navnlig for at foreligge, hvis overtrædelserne sker erhvervsmæssigt, hvis der fremstilles eller blandt almenheden spredes et betydeligt antal eksemplarer, eller hvis værker og frembringelser gengives på en sådan måde, at almenheden får adgang til dem på et individuelt valgt sted og tidpunkt."

Bestemmelsen dækker både de situationer, hvor gerningsmanden fremstiller alle eksemplarer selv, og de situationer, hvor gerningsmanden uploader vær-ket eller frembringelsen (og dermed fremstiller et eksemplar), der derefter er tilgængeligt, således at en videre kreds har adgang og eventuelt kan down-loade.

Baggrunden for forslaget er, at der i vid udstrækning gives adgang til pro-grammer via netværk, især Internettet, der downloades til brug eller benyt-tes på anden måde, der krænker den ophavsretlige eneret. Denne udbredelse indeholder i hvert fald potentielt, men formentlig også faktisk, krænkelser i et omfang, der er langt mere omfattende end de krænkelser, der sker i er-hvervsmæssig sammenhæng.

Beskrivelsen af, hvad der er skærpende omstændigheder, er ikke udtøm-mende, men dækker de typisk forekommende tilfælde. Bestemmelsen vil imidlertid også være anvendelig ved f.eks. et enkelt salg af et meget dyrt pro-gram eller system. I den nugældende formulering anvendes "særlig skær-pende omstændigheder". Der er ikke ved ændringen til "skærpende" tilsigtet en ændring i bestemmelsens anvendelsesområde. Den ændrede formulering har alene sammenhæng med, at der foreslås indsat en overbygning i straffe-loven, der dækker "særligt" skærpende omstændigheder ("overtrædelse af særlig grov karakter").

Med hensyn til strafmaksimum finder udvalget, at der vil kunne være behov for i særlig grove tilfælde at idømme fængsel i mere end 1 år og 6 måneder.

Udvalget har i den forbindelse særligt lagt vægt på beskyttelsesbehovet i relation til edb-programmer. Den digitale teknik betyder, at det er muligt og meget let at fremstille helt identiske eksemplarer. Programudviklingen er of-te meget omkostningskrævende og det er oftest ikke muligt at beskytte pro-grammer effektivt mod kopiering. Det er efter udvalgets opfattelse et na-turligt modstykke til overgangen til IT-samfundet, at der skabes en væ-sentlig strafferetlig beskyttelse af de midler, der er en forudsætning for IT-samfundet.

Udvalget har i den forbindelse også overvejet, om der skal indsættes en ge-nerel overbygning i straffeloven. Udvalget finder, at der bør indsættes en så-dan overbygning i straffeloven i stil med straffelovens §§ 125 a, 192 a, 196, 289 og § 289 a med et strafmaksimum på 4 år.[192]

---

[192] Et flertal i arbejdsgruppen om datakriminalitet (Mads Bryde Andersen, Jan Carlsen, Jan Friis, Michael Goeskjær, Carsten Heilbuth, Ulla Høg, Jens Kruse Mikkelsen, Ronald Pedersen, Kim Aarenstrup) foreslog som udvalget en overbygning i straffeloven med fæng-sel i 4 år. Et mindretal i udvalget (Hans Jakob Paldam Folker,

Udvalget har herved lagt vægt på, at særligt grove overtrædelser er lige så strafværdige som tyveri, der har et strafmaksimum på 4 år, jfr. straffelovens § 286.

Udvalget finder, at de overtrædelser, der skal behandles efter straffeloven, skal begrænses til situationer, hvor der er forsæt til vinding for gernings-manden eller andre.

Udvalget foreslår, at de foreslåede ændringer suppleres med, at der i straffe-lovens kapitel 28 indsættes en bestemmelse med følgende indhold:

"§ 299 b. Med fængsel indtil 4 år straffes den, der for at skaffe sig eller an-dre uberettiget vinding gør sig skyldig i overtrædelse af ophavsretslovens § 76, stk. 2, af særlig grov karakter."

Bestemmelsen kan især tænkes anvendt i tilfælde, hvor der er tale om om-fattende og systematiske krænkelser, hvilket typisk vil være tilfælde, hvor der en organiseret fremstillings- og/eller salgsproces. Bestemmelsen vil også kunne anvendes, hvis krænkelsen vedrører et enkelt meget dyrt program el-ler system, der f.eks. er udviklet til en eller flere virksomheder.

8.5. Straffelovens § 153

I straffelovens kapitel 16 om forbrydelser i offentlig tjeneste eller hverv m.v. findes følgende bestemmelse:

> "§ 153. Når nogen, som virker i post- eller jernbanevæsenets tjeneste, ulovlig åbner, tilintetgør eller underslår forsendelser eller understøtter en anden i sådan færd, straffes han med fængsel indtil 3 år.
> Stk. 2. På samme måde straffes den, som virker i statstelegrafvæsenets eller et offentligt anerkendt telegrafanlægs tjeneste, når han

---

Helle Jahn, Ole Stampe Ras-mussen) fandt, at et strafmaksimum i ophavsretsloven på 2 år ville give en tilstrækkelig strafferetlig beskyttelse.
Arbejdsgruppen drøftede ikke spørgsmålet om at ændre strafmaksimum i ophavsretsloven fra 2 år til 1 år og 6 måneder.

> tilintetgør, forvansker eller underslår et samme til befordring overgivet telegram eller understøtter en anden i sådan færd."

Efter privatiseringen af store dele af det offentlige kommunikationsvæsen er det kun en del af det, som dækkes af denne bestemmelse. Udvalget har derfor drøftet, om bestemmelsen er blevet overflødig, eller om den bør be-vares på en anden plads i straffeloven.

Stk. 1 er fuldstændig dækket af de almindelige regler om krænkelse af brevhemmeligheden (§ 263) og den almindelige regel om tingsødelæggelse (§ 291). Den forhøjede strafferamme i § 153 i forhold til disse bestem-melsers grunddelikter skyldes, at bestemmelsen tog sigte på offentligt ansat-te. I dag er der næppe grund til at anvende andre strafferammer end de almindelige, herunder efter omstændighederne § 263, stk. 3 (4 år under "særlig skærpende omstændigheder") og § 291, stk. 2 (4 år ved "hærværk af betydeligt omfang"). Stk. 1 er derfor overflødig og kan ophæves.

Stk. 2 må anses for overflødig i dag, hvor telegrafsystemet har mistet sin betydning. Misligholdelse af den indgåede kontrakt om befordring af en meddelelse må, hvis der ikke er strafferetlig dækning i straffelovens almin-delige bestemmelser, imødegås af civilretlige reaktioner på samme måde som de fleste andre misligholdelser af tjenesteydelser.

Fremkaldelse af omfattende forstyrrelser inden for post-, telefon- og tele-grafområdet er desuden omfattet af straffelovens § 193, der også omfatter de privatiserede foretagender.

Udvalget foreslår derfor, at straffelovens § 153 ophæves som overflødig.

8.6. Betalingskriminalitet

8.6.1. Elektroniske penge

Udvalgets overvejelser, jfr. afsnit 4.2, har både omfattet elektroniske penge og generatorer til elektroniske penge.

Udvalget har særligt overvejet, om området er så nyt, at en strafferetlig regulering bør afvente den videre udvikling. Udvalget finder imidlertid, at netop det forhold, at området er i hastig udvikling, taler for, at området reguleres nu. Der er herved lagt særlig vægt på, at i det omfang, det lykkes at producere falske elektroniske penge, vil der ikke være noget, der adskiller dem fra de ægte. Modtageren har vanskeligt ved at opdage, at der ikke er ta-le om ægte elektroniske penge. Området er opklarings- og bevismæssigt endnu mere vanskeligt end falske penge.

Udvalget finder, at elektroniske penge bør nyde en kvalificeret beskyttelse, selv om anvendelsen af dem typisk vil være omfattet af straffelovens § 279 eller § 279 a.

Udvalget finder, at problemstillingen er så nært forbundet med spørgsmålet om betalingsmidler, at reguleringen bør indsættes i straffelovens kapitel 18 om forbrydelser vedrørende penge.

Udvalget foreslår, at bestemmelsen indsættes som § 169 a, og at kapitlets overskrift ændres til "Forbrydelser vedrørende betalingsmidler".

"§ 169 a. Med bøde eller fængsel indtil 6 måneder straffes den, der uretmæs-sigt fremstiller, skaffer sig eller udbreder falske elektroniske penge med for-sæt til, at de anvendes som ægte.
Stk. 2. Ved elektroniske penge forstås elektronisk lagrede pengeværdier, der anerkendes som betalingsmidler af andre end udstederen.
Stk. 3. Ved falske elektroniske penge forstås midler, der uden at være ægte elektroniske penge er egnede til at blive brugt som sådanne.
Stk. 4. Er handlingen af særlig grov beskaffenhed på grund af den måde, hvorpå den er udført, eller på grund af beløbets størrelse, er straffen fængsel indtil 6 år."

Udtrykket "betalingsmiddel", der også anvendes i EU-direktivet[193] og den danske lov om udstedere af elektroniske penge[194], dækker et

[193] Europaparlamentets og Rådets direktiv af 18/9 2000 om adgang til at optage og udøve virksomhed som udsteder af elektroniske penge og tilsyn med en sådan virksomhed (EFT L 2000 257/39).

middel, der re-præsenterer en given værdi og kan benyttes som betalingsmiddel uden trediemands mellemkomst. Det dækker således ikke "betalingsinstrumen-ter", der alene er pengeanvisninger, dvs. anmodninger til en anden (f.eks. en bank) om at udbetale et vist beløb til trediemand.

Såfremt handlingen ligger tidligere end det gerningsindhold, der er omfattet af bestemmelsen, finder de almindelige forsøgsregler anvendelse.

Udvalgets forslag omfatter ikke brugen af falske elektroniske penge. Udval-get finder, at brugen fortsat skal være dækket af de almindelige bestemmel-ser, i praksis typisk straffelovens § 279 a om databedrageri.

8.6.2. Betalingskort, betalingskortnumre m.v.

Der henvises til afsnit 4.3 vedrørende udvalgets overvejelser.

Udvalget har vurderet, i hvilket omfang betalingskort kan give anledning til overvejelser om en fremrykket beskyttelse eller om en ændret regulering. Udvalget finder, at følgende områder er aktuelle:

1. Falske betalingskort.
2. Betalingskortnumre.

Udvalget finder, at både produktion, forskaffelse, besiddelse med henblik på uberettiget brug og videregivelse af falske betalingskort bør kriminaliseres.

Udvalget finder endvidere, at kriminaliseringen også bør omfatte betalings-kortnumre.

Udvalget har valgt at foreslå en regulering, der ikke er knyttet til fysiske kort, men er knyttet til de relevante betalingsinformationer.

Udvalget foreslår følgende formulering af bestemmelsen:

---

[194] Lov nr. 502 af 7/6 2001.

"§ 301. Med bøde eller fængsel indtil 6 måneder straffes den, der med for-sæt til uberettiget anvendelse producerer, skaffer sig, besidder eller videre-giver oplysninger, der identificerer et betalingsmiddel, der er tildelt andre, eller genererede betalingskortnumre.
Stk. 2. Sker den i stk. 1 nævnte videregivelse i en videre kreds eller under i øvrigt særligt skærpende omstændigheder, er straffen fængsel indtil 4 år.
Stk. 3. Bestemmelsen i stk. 1 finder ikke anvendelse på ægte betalingskort."

Da der kræves forsæt til uberettiget brug består udvidelsen set i forhold til straffelovens § 21 i, at der ses bort fra konkretiseringskravet. Selv om besid-delse typisk vil indgå i produktion, forskaffelse og videregivelse, har udvalget fundet det rigtigst at nævne disse ting særskilt for at undgå fortolk-ningsproblemer omkring besiddelsesbegrebet.

Efter forslagets stk. 1 er alle betalingskortnumre omfattet, uanset om de er ægte, genererede eller frit konstruerede. De er endvidere omfattet, hvad en-ten de alene foreligger som oplysninger uden tilhørende kort, eller de fore-ligger på falske kort. Hovedområdet vil imidlertid være konstruerede eller eftergjorte betalingsmidler, herunder hvide kort med konstrueret eller eftergjort magnetstrimmel m.v.

Forslagets stk. 2 angiver videregivelse i en videre kreds som en af de skær-pende omstændigheder, der kan medføre, at forholdet henføres under stk. 2. "I øvrigt skærpende omstændigheder" vil f.eks. kunne foreligge, hvis oplysningerne er skaffet ved, at en pengeautomat er forsynet med en falsk front, så kundernes betalingskortnummer og pinkode har kunnet aflæses.

Efter forslagets stk. 3 er ægte kort ikke omfattet af reguleringen. Udvalget har fundet, at de gældende regler i tilstrækkeligt omfang dækker dette om-råde, jfr. afsnit 4.3.2.

Vedrørende midler til produktion og tilegnelse af betalingskortnumre hen-vises til afsnit 4.3.4 og 8.1.3.

8.6.3. Misbrug af andres teleforbindelser

Der henvises til afsnit 4.5.

Udvalget finder, at de gældende regler er dækkende, og at der ikke er behov for ny lovgivning på området.

8.7. Elektroniske dokumenter

8.7.1. Straffelovens § 163

Der henvises til afsnit 5.2 vedrørende udvalgets overvejelser.

Udvalget finder, at erklæringer, der afgives i en form, der ikke er læsbar for afsenderen, men som bekræftes fra modtageren i en læsbar form med mu-lighed for korrektion, bør være omfattet.

Udvalget finder imidlertid, at denne erklæringsform er dækket af ordlyden i straffelovens § 163. Udvalget har overvejet, om det alligevel burde præcise-res i bestemmelsen, at erklæringen kan afgives ved accept af en læsbar be-kræftelse, men har fundet, at der ikke er behov derfor.

8.7.2. Dokumentfalsk og straffelovens §§ 173-174

Der henvises til afsnit 5.3 vedrørende udvalgets overvejelser.

Udvalget har taget udgangspunkt i de bestemmelser, der gælder for fysiske dokumenter.

For så vidt angår straffebestemmelsen i straffelovens § 172 har Straffelov-rådet imidlertid i 1987[195] foreslået en ændret formulering, bl.a. for at tilpasse bestemmelsen til det forhold, at der, når dokumentfalsk indgår i et bedra-geri, typisk kun straffes for dokumentfalsk. Straffelovrådet foreslog på den baggrund[196] en normalstrafferamme på fængsel indtil 2 år. Ved dokument-falsk af

[195] Straffelovrådets betænkning nr. 1099/1987 om strafferammer og prøveløsladelse.

[196] Betænkningen s. 184.

særlig grov karakter eller ved et større antal forhold foreslog Straffelovrådet strafmaksimum på 8 år bibeholdt, mens der ved forhold af min-dre strafværdighed skulle være tale om bøde (med forsøgsstraf). Sidstnævnte forslag havde især sammenhæng med den dengang gældende sondring mel-lem politisager (typisk bødesager) og statsadvokatsager.

Udvalget finder, at der bør være en regulering vedrørende falske elektro-niske dokumenter. Udvalget har drøftet, om en bestemmelse om elektro-niske dokumenter bør være mere forenklet end den nugældende doku-mentfalskbestemmelse. Resultatet af disse drøftelser er, at udvalget finder, at den forenklede bestemmelse bør være en fælles bestemmelse for fysiske og elektroniske dokumenter.

Den nugældende bestemmelse lider af en række svagheder. Bestemmelsen hidrører fra en tid, hvor selve brugen af skrift forlenede en meddelelse med en særlig aura. I dag, hvor alt skrives, fysisk eller elektronisk, er dette klart ikke længere tilfældet.

Bestemmelsen skelner mellem hensigtsdokumenter ("der ... fremtræder som bestemt til at tjene som bevis") og lejlighedsdokumenter ("der ... bliver benyttet som bevis for en rettighed, en forpligtelse eller en befrielse for en sådan"). Medens hensigtsdokumentbegrebet er klart, opfylder lejlig-hedsdokumentet ikke nutidens krav til præcision i straffebestemmelser. Skønt der gennem det 20. århundrede blev udfoldet store bestræbelser på at give begrebet et præcist indhold, er det ikke lykkedes for teorien eller praksis at opnå dette.

Hensigtsdokumenter er eksempelvis eksamensbeviser, medlemskort, køre-kort, pas, visa, vielsesattester, dåbsattester, anbefalinger med faktiske oplys-ninger, attestationer, kvitteringer, kontrakter, bestillinger, ordrebekræftelser, fakturaer, gældsbreve, checks, veksler og fuldmagter. Endvidere vil ansøg-ninger, erklæringer m.v. efter omstændighederne kunne være omfattet.
Der er ikke mange bidrag i trykt praksis til belysning af, hvad der efter om-stændighederne i forbindelse med den konkrete brug kan være et lejligheds-dokument. Som eksempler kan nævnes UfR 1937.151 V (et privat brev med anerkendelse af, at lån var ydet), VLT 1938.177 (to postkort med tilbud om arbejde) og UfR 1966.462 V (mødekort til

hospitalsindlæggelse påført urig-tige mødedatoer for at få rejsegodtgørelse).

Udvalget finder, at dokumentfalskbestemmelsen ikke bør omfatte lejligheds-dokumenter. Dels mangler denne del af bestemmelsen som nævnt præci-sion, dels tyder den sparsomme retspraksis ikke på, at der er behov for bestemmelsen. Forholdet er antagelig det, at straf for brug af falske lejlig-hedsdokumenter i praksis ikke behandles efter dokumentfalskbestemmel-sen, men efter andre strafbestemmelser, der vedrører brugen af dokumentet (f.eks. til bedrageri). Såfremt den konkrete anvendelse af dokumentet ikke er kriminaliseret, er der næppe heller behov for at kunne straffe for do-kumentfalsk i disse tilfælde.

Dokumentfalskbestemmelsen er et formaldelikt. Sådanne absorberes i al-mindelighed af tilsvarende skadedelikter i tilfælde af sammenstød. I praksis er langt hovedparten af tilfældene i praksis dokumentfalsk i forbindelse med berigelsesforbrydelser, f.eks. forfalskning af kvitteringer og kontrakter. Ud-valget er af den opfattelse, at man også på dette område bør drage kon-sekvensen af de hensyn, der ligger bag det almindelige absorptionsprincip, og lade skadedeliktet (berigelsesforbrydelsen) være det primære. Derved vil man opnå, at forholdet betegnes som det, det egentlig er.

I praksis vil de resterende tilfælde af dokumentfalsk vedrøre hensigtsdo-kumenter, f.eks. eftergørelse eller forfalskning af kørekort, pas, visa, vielses-attester, dåbsattester osv., der også kan forfalskes af mange andre grunde end for at opnå en berigelse. Der er her tale om delikter, som i grovhed lader sig sammenligne med f.eks. straffelovens §§ 161-163 (der straffes med bøde eller fængsel indtil 4 måneder, § 161 dog med fængsel indtil 2 år under skærpende omstændigheder).

Udvalget finder på denne baggrund, at bestemmelsen skal omfatte både fy-siske og elektroniske tilkendegivelser, der er bestemt til at tjene som bevis, og at strafmaksimum skal være fængsel i 2 år.

Udvalget foreslår, at §§ 171-172 affattes således:

"§ 171. Den, der gør brug af et falsk dokument for at skuffe i retsforhold, straffes for dokumentfalsk med bøde, fængsel indtil 4 måneder eller under skærpende omstændigheder fængsel indtil 2 år.

§ 172. Ved et dokument forstås en skriftlig eller elektronisk med betegnelse af udstederen forsynet tilkendegivelse, der fremtræder som bestemt til at tjene som bevis.
Stk. 2. Et dokument er falsk, når det ikke hidrører fra den angivne udsteder, eller der er givet det et indhold, som ikke hidrører fra denne."

Da dokumentdefinitionen omfatter både skriftlige og elektroniske tilkende-givelser, er det ikke nødvendigt at ændre ordlyden af straffelovens §§ 173-174 for så vidt angår dokumenter, da dokumentbegrebet i disse bestem-melser svarer til dokumentfalskbestemmelsen.

8.7.3. Straffelovens § 175

Der henvises til afsnit 5.3 vedrørende udvalgets overvejelser.

For så vidt angår de i § 175 nævnte dokumenter og bøger, kan der være tale om bøger, der ikke er omfattet af definitionen i dokumentfalskbestem-melsen, f.eks. fordi tilknytningsforholdet fremgår af, hvor dokumentet eller bogen føres, uden at der tillige er en udstederbetegnelse. Udvalget foreslår derfor, at det præciseres i bestemmelsen, at reguleringen også vedrører an-dre læsbare medier.

Udvalget foreslår endvidere, at bestemmelsens stk. 2 om straf for den, der i retsforhold gør brug af et sådant dokument som indeholdende en sandhed, udvides til også at omfatte de af stk. 1 omfattede bøger.

Bestemmelsen i stk. 2 kom ind i straffelovsbetænkningen fra 1923. Det fremgår ikke af betænkningen, hvorfor forslaget alene vedrører dokumen-ter og ikke tillige bøger.

Der synes ikke at være nogen begrundelse for, at alene dokumenter er omfattet af denne bestemmelse, selv om det må formodes, at den også om-fatter alle bøger, der opfylder kravene i dokumentdefinitionen.

Dertil kom-mer, at elektronisk førte bøger må forventes i ringere grad end fysiske bøger at indeholde en traditionel udstederbetegnelse.

Udvalget finder endvidere, at bestemmelsens strafferamme bør bringes i overensstemmelse med den af udvalget foreslåede dokumentfalskbestem-melse. Også her vil der i grove tilfælde foreligge (medvirken til) et skadede-likt, f.eks. bedrageri, og i så fald kan der straffes i sammenstød med dette delikt.
Udvalget har tidligere foreslået den ændring i bestemmelsen, at "lov eller" skal udgå, jfr. delbetænkning VI om straffelovens § 296 og § 302 (betænk-ning nr. 1415/2002).

Udvalget foreslår, at § 175 affattes således:

"§ 175. Den, som for at skuffe i retsforhold i offentligt dokument eller bog, i privat dokument eller bog, som det ifølge særligt pligtforhold påhviler ham at udfærdige eller føre, eller i læge-, tandlæge-, jordemoder- eller dyrlæge-attest afgiver urigtig erklæring om noget forhold, angående hvilken erklæ-ringen skal tjene som bevis, straffes med bøde, fængsel indtil 4 måneder eller under skærpende omstændigheder fængsel indtil 2 år.
Stk. 2. På samme måde straffes den, der i retsforhold gør brug af et sådant dokument eller bog som indeholdende sandhed.
Stk. 3. Bestemmelserne i stk. 1 og 2 finder tilsvarende anvendelse, når dokumentet eller bogen er udfærdiget eller føres på andet læsbart medie."

8.7.4. Vildledende afsenderbetegnelser

Der henvises til afsnit 5.4 vedrørende udvalgets overvejelser.

Udvalget finder, at der ikke på nuværende tidspunkt skal ske en regulering, men at området bør følges med henblik på at få et bedre overblik over både omfanget og arten af meddelelser, således at der senere kan tages stilling til en regulering, såfremt udviklingen viser, at der er behov for en særskilt strafferetlig regulering.

8.8. Datahærværk m.v.

8.8.1. Datahærværk

Der henvises til afsnit 6.6 vedrørende udvalgets overvejelser.

Under hensyntagen til, at der inden for området for elektronisk databehand-ling er hærværksområder, hvor der ikke er helt klar strafferetlig dækning (de situationer – f.eks. e-mail bomber – hvor rådigheden over systemet forhin-dres eller begrænses væsentligt), og hærværksområder, der antagelig dækkes af forskellige bestemmelser, finder udvalget, at der er behov for en vis justering og præcisering af straffeloven. Udvalget finder ikke, at der er behov for en særskilt straffelovsbestemmelse om datahærværk. Udvalget finder, at den gældende hærværksbestemmelse i straffelovens § 291 er til-strækkeligt klart dækkende, og at der ikke er behov for ændring af den bestemmelse.

Derimod finder udvalget, at straffelovens § 293, stk. 2, bør ændres på flere punkter. Dels bør strafferammen svare til bestemmelsens stk. 1, og dels bør påtalereglerne være de samme som ved hærværk (dvs. betinget offentlig påtale i stedet for privat påtale, jfr. straffelovens § 305). Endvidere bør bestemmelsen formuleres, så det klart fremgår, at den også omfatter rådighedshindren ad elektronisk vej.

Udvalget foreslår, at straffelovens § 293, stk. 2, affattes således:

"Stk. 2. På samme måde straffes den, som uberettiget hindrer en anden i helt eller delvist at råde over en ting."

Kravet om, at handlingen skal være "uberettiget" indebærer, at f.eks. lovlig tilbageholdsret ikke er en overtrædelse af bestemmelsen. Endvidere omfat-ter bestemmelsen kun lovlig råden, og den vil således ikke omfatte et ind-greb rettet mod ulovlig råden.

Udtrykket "uberettiget hindrer" er valgt i stedet for det nuværende "lægger hindringer i vejen" for at præcisere, at der ikke kræves en fysisk hindring, men at også elektroniske rådighedshindringer er omfattet. Bestemmelsen dækker også andre typer hindringer – f.eks.

hvis man via anvendelse af mis-lyd på særlige frekvenser forhindrer andre i at bruge deres radioforbindelse.

Udtrykket "helt eller delvist at råde" er valgt for at præcisere, at også en hindren, der f.eks. betyder, at den berettigede begrænses væsentligt i sin rådighed, er omfattet. Dette vil f.eks. kunne være situationen, hvis et DoS-angreb (Denial-of-Service angreb) kun delvist umuliggør anvendelsen af et informationssystem.

Tilbageholdsret nævnes ikke særskilt ved siden af rådighed, da udvalget fin-der, at en sådan ret er omfattet af almindelig rådighedsret.

De i stk. 1 nævnte skærpende omstændigheder vil navnlig vedrøre varighe-den og omfanget af rådighedshindring.

Udvalget foreslår endvidere, at stk. 2 ligesom straffelovens § 291, stk. 1, undergives betinget offentlig påtale. Det foreslås derfor, at "§ 293, stk. 2" flyttes fra straffelovens § 305, stk. 2, til bestemmelsens stk. 1.

8.8.2. Straffelovens § 193

Der henvises til afsnit 6.7 vedrørende udvalgets overvejelser.

Udvalget finder, at strafmaksimum i straffelovens § 193, stk. 1, bør være højere end i hærværksbestemmelserne i straffelovens § 291. Udvalget fore-slår derfor følgende ændring:

I straffelovens § 193, stk. 1, ændres "4 år" til "6 år".

Udvalget foreslår endvidere, at "databehandlingsanlæg" ændres til "infor-mationssystemer".

Udvalget finder herudover, at straffelovens § 193, stk. 2, bør harmonere med den tilsvarende bestemmelse vedrørende groft hærværk, således at bestemmelsen lige som straffelovens § 291, stk. 3, begrænses til at dække grov uagtsomhed og får et strafmaksimum på 6 måneders fængsel i stedet for 4 måneders fængsel.

Udvalget foreslår, at straffelovens § 193, stk. 2, formuleres således:

"Begås forbrydelsen groft uagtsomt, er straffen bøde eller fængsel indtil 6 måneder".

8.9. Offentlig påtale

Udvalget har overvejet, om der generelt bør være offentlig påtale ved IT-kriminalitet. Udvalget finder imidlertid, at der ikke er behov herfor. De hen-syn, der ligger bag valg af påtaleform, vil i formentlig de fleste tilfælde gøre det velbegrundet, at den forurettede kan bestemme, om tiltale skal rejses.

I dag er situationen den, at der er en sådan hjemmel i retsplejelovens § 727 i sager, der er undergivet privat påtale. I situationer, hvor der både er privat påtale og betinget offentlig påtale, har Justitsministeriet givet udtryk for, at retsplejelovens § 727 finder anvendelse, og praksis er i overensstemmelse hermed, jfr. eksempelvis UfR 1998.1445 Ø.

Hvis der alene er betinget offentlig påtale, foreligger denne mulighed ikke, medmindre der måtte være en særlig hjemmel herfor, jfr. f.eks. straffelovens § 305.

Udvalget finder derfor, at det bør overvejes at indføre en generel hjemmel til offentlig påtale, hvis almene hensyn kræver det. [197]

Udvalget finder imidlertid ikke grundlag for at stille et sådant forslag, der i givet fald vil forudsætte en generel gennemgang af lovgivningen, herunder også af områder, der ikke har berøring med IT-kriminalitet.

For så vidt angår hovedparten af de områder, udvalget beskæftiger sig med i denne betænkning, vil der enten være offentlig påtale eller mulighed for på-tale, hvis almene hensyn kræver det. Dette gælder dog ikke for ophavsrets-loven, idet den alene indeholder en bestemmelse om betinget offentlig påta-le ved overtrædelser af lovens § 76, stk. 2, og § 77, stk. 2. Udvalget finder, at denne påtalebestemmelse i ophavsretsloven bør ændres, så den kommer til at svare til straffelovens

[197] Arbejdsgruppen vedrørende datakriminalitet fandt, at der skulle være hjemmel hertil.

§ 305, dvs. at betinget offentlig påtale bibeholdes som hovedreglen, men at der åbnes mulighed for offentlig påtale, hvis alme-ne hensyn kræver det. Ændringen vil give en retstilstand, der harmonerer med de øvrige straffebestemmelser i ophavsretsloven, hvor der enten er privat påtale (med mulighed for at anvende retsplejelovens § 727, stk. 2, om offentlig påtale på grund af almene hensyn) eller offentlig påtale.

Udvalget foreslår, at ophavsretslovens § 82, stk. 1, affattes således:

"Overtrædelser, som omfattes af § 76, stk. 2, eller § 77, stk. 2, påtales kun efter den forurettedes begæring, medmindre almene hensyn kræver påtale."

Udvalget finder, at den foreslåede bestemmelse ikke i almindelighed skal be-tyde en ændret tiltalepraksis. Udvalget finder, at såfremt de hensyn, der har ført til påtalereglerne, gør sig fuldt ud gældende, skal retstilstanden forblive uændret.

Ændringen vil betyde, at den indledende efterforskning i sager om ophavs-retskrænkelser ikke begrænses af reglen i retsplejelovens § 720, stk. 3, til uopsættelige handlinger. Det kan i visse tilfælde være til fordel for efter-forskningen, at den forurettede først underrettes senere, f.eks. hvis den for-urettede kan tænkes at kontakte den eller de mistænkte eller gå til pressen i en situation, hvor der er behov for at afvente, at andre lande iværksætter be-vissikring. Endvidere vil bestemmelsen kunne have betydning i relation til den særlige forældelsesfrist for påtalebegæringer, der ikke gælder ved of-fentlig påtale.

Udvalget finder herudover, at den ret restriktive fortolkning af, hvad der skal betragtes som en påtalebegæring, jfr. eksempelvis frifindelsen i UfR 2000.342 H, hvor der forelå anmeldelse men ikke særskilt påtalebegæring, er uhensigtsmæssig, da en anmelder i almindelighed ikke har kendskab til, at en anmeldelse skal suppleres med en påtalebegæring, og da det kan ske, at po-litiet ikke – eller først for sent, jfr. forældelsesreglen i straffelovens § 96 – konstaterer, at en egentlig påtalebegæring mangler.

Udvalget foreslår på den baggrund, at der indsættes følgende bestemmelse i retsplejelovens § 720, stk. 2, som nyt 2. punktum:

”En anmeldelse fra den berettigede anses som en begæring om offentlig på-tale, medmindre andet fremgår af anmeldelsen.”

8.10. Terminalefterforskning

Udvalget har set på to problemstillinger vedrørende terminalefterforskning, jfr. afsnit 7.2.

Den ene problemstilling vedrører politiets efterforskning på Internettet, når den er rettet mod at opdage kriminalitet.

Udvalget finder ikke, at der med den kendte kriminalitet er behov for at kunne anvende de særlige agentregler i IT-relaterede sager, der ikke er omfattet af de gældende regler.

Udvalget finder imidlertid, at der kan være behov for, at der formuleres ad-ministrative forskrifter om politiets efterforskning ved IT-infiltration.

Den anden problemstilling vedrører politiets efterforskning på Internettet vedrørende strafbare forhold med igangværende efterforskning.

Spørgsmålet om de folkeretlige begrænsninger i adgangen til for dansk politi at foretage efterforskning med tilknytning til udlandet kan i sagens natur ikke løses ved dansk lovgivning.

Udvalget påpeger behovet for, at de internationale regler får et sådant ind-hold, at efterforskning over landegrænserne kan gennemføres på en smidig måde.

Problemstillingen er ikke kun aktuel ved IT-kriminalitet, men også f.eks. i relation til en dansk virksomheds bogføring i udlandet eller placering af an-dre selskabsfunktioner i udlandet (hvad enten der er tale om placering i koncernen eller outsourcing af opgaver).

BILAG

Europarådets konvention om IT-kriminalitet
23. november 2001

CONVENTION ON CYBER-CRIME

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned at the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international level, and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights, as enshrined in the 1950

Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, as well as other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the protection of personal data, as conferred e.g. by the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field as well as similar treaties which exist between Council of Europe member States and other States and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrimes, including actions of the United Nations, the OECD, the European Union and the G8;

Recalling Recommendation N° R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, Recommendation N° R (88) 2 on piracy in the field of copyright and neighbouring rights, Recommendation N° R (87) 15 regulating the use of personal data in the police sector, Recommendation N° R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services as well as Recommendation N° R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and Recommendation N° R (95) 13 concerning problems of criminal procedural law connected with Information Technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, June 1997), which recommended the Committee of Ministers to support the work carried out by the European Committee on Crime Problems (CDPC) on cybercrime in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation concerning such offences, as well as to Resolution N° 3, adopted at the 23rd Conference of the European Ministers of Justice (London, June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions so as to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation,

which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe, on the occasion of their Second Summit (Strasbourg, 10 - 11 October 1997), to seek common responses to the development of the new information technologies, based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a. "computer system" means any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c. "service provider" means:

i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the

intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent**,** or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5;

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed

with intent that it be used for the purpose of committing any of the offences established in Articles 2 - 5; and

b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (2).

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:

a. any input, alteration, deletion or suppression of computer data,

b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a. producing child pornography for the purpose of its distribution through a computer system;

b. offering or making available child pornography through a computer system;

c. distributing or transmitting child pornography through a computer system;

d. procuring child pornography through a computer system for oneself or for another;

e. possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above "child pornography" shall include pornographic material that visually depicts:

a. a minor engaged in sexually explicit conduct;

b. a person appearing to be a minor engaged in sexually explicit conduct;

c. realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraph 1(d) and 1(e), and 2(b) and 2(c).

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations done in Rome (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of

any moral rights conferred by such Conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 – 10 of the present Convention with intent that such offence be committed.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, 9 (1) a and 9 (1) c of this Convention.

3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that a legal person can be held liable for a criminal offence established in accordance with this Convention, committed for its benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

a. a power of representation of the legal person;

b. an authority to take decisions on behalf of the legal person;

c. an authority to exercise control within the legal person.

2. Apart from the cases already provided for in paragraph 1, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 – 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this Section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically otherwise provided in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 to:

a. the criminal offences established in accordance with articles 2-11 of this Convention;

b. other criminal offences committed by means of a computer system; and

c. the collection of evidence in electronic form of a criminal offence.

3. a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b. Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system

i. is being operated for the benefit of a closed group of users, and

ii. does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, a Party shall consider the impact of the powers and procedures in this Section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 - Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative or other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control;

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3. For the purpose of this article, "subscriber information" means any information, contained in the form of computer data or any other form, that is held by a service provider, relating to subscribers of its services, other than traffic or content data, by which can be established:

a. the type of the communication service used, the technical provisions taken thereto and the period of service;

b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c. any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a. a computer system or part of it and computer data stored therein; and

b. computer-data storage medium in which computer data may be stored

in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1 (a), and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to :

a. seize or similarly secure a computer system or part of it or a computer-data storage medium;

b. make and retain a copy of those computer data;

c. maintain the integrity of the relevant stored computer data; and

d. render inaccessible or remove those computer data in the accessed computer system.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a. collect or record through application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability, to:

i. collect or record through application of technical means on the territory of that Party, or

ii. co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications in its territory through application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a. collect or record through application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability, to:

i. collect or record through application of technical means on the territory of that Party, or

ii. co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data of specified communications in its territory through application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 – 11 of this Convention, when the offence is committed :

a. in its territory; or

b. on board a ship flying the flag of that Party; or

c. on board an aircraft registered under the laws of that Party; or

d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs (1) b – (1) d of this article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph (1) of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him/her to another Party, solely on the basis of his/her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised in accordance with domestic law.

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1. a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 – 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this Article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as in the case of any other offence of a comparable nature under the law of that Party.

7. a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and addresses of each authority responsible for the making to or receipt of a request for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 - 35.

3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communications, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4. Except as otherwise specifically provided in Articles in this Chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 to 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual

criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominates the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1. A Party may, within the limits of its domestic law, without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2. Prior to providing such information, the providing Party may request that it be kept confidential or used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation is available, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. a. Each Party shall designate a central authority or authorities that shall be responsible for sending and answering requests for mutual assistance, the execution of such requests, or the transmission of them to the authorities competent for their execution.

b. The central authorities shall communicate directly with each other.

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph.

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3. Mutual assistance requests under this Article shall be executed in accordance with the procedures specified by the requesting Party except where incompatible with the law of the requested Party.

4. The requested Party may, in addition to grounds for refusal available under Article 25, paragraph (4), refuse assistance if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b. it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. If the request is refused or postponed, reasons shall be given for the refusal or postponement. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. The requesting Party may request that the requested Party keep confidential the fact and substance of any request made under this Chapter except to the extent necessary to execute the request. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9. a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to subparagraph (a) and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation, is available unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. The requested Party may make the furnishing of information or material in response to a request dependent on the condition that it is:

a. kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b. not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information is nevertheless provided. When the requesting Party accepts the condition, it shall be bound by it.

4. Any Party that furnishes information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, which is located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2. A request for preservation made under paragraph 1 shall specify:

a. the authority that is seeking the preservation;

b. the offence that is the subject of a criminal investigation or proceeding and a brief summary of related facts;

c. the stored computer data to be preserved and its relationship to the offence;

d. any available information to identify the custodian of the stored computer data or the location of the computer system;

e. the necessity of the preservation; and

f. that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data may, in respect of offences other than those established in accordance with Articles 2 – 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reason to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5. In addition, a request for preservation may only be refused if :

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of, or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than 60 days in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made under Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting

Party a sufficient amount of traffic data in order to identify that service provider and the path through which the communication was transmitted.

2. Disclosure of traffic data under paragraph 1 may only be withheld if :

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2. The requested Party shall respond to the request through application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this Chapter.

3. The request shall be responded to on an expedited basis where:

a. there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b. the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without obtaining the authorisation of another Party:

a. access publicly available (open source) stored computer data**,** regardless of where the data is located geographically; or

b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance regarding the real-time collection of traffic data

1. The Parties shall provide mutual assistance to each other with respect to the real-time collection of traffic data associated with specified communications in its territory transmitted by means of a computer system. Subject to paragraph 2,

assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other with respect to the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted by their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1. Each Party shall designate a point of contact available on a 24 hour, 7 day per week basis in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out:

a. provision of technical advice;

b. preservation of data pursuant to Articles 29 and 30; and

c. collection of evidence, giving of legal information, and locating of suspects.

2. a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20 (d) of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become

effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

- the European Convention on Extradition opened for signature in Paris on 13 December 1957 (ETS No. 24);

- the European Convention on Mutual Assistance in Criminal Matters opened for signature in Strasbourg on 20 April 1959 (ETS No. 30);

- the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters opened for signature in Strasbourg on 17 March 1978 (ETS No. 99).

2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or otherwise have established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Article 2, Article 3, Article 6, paragraph 1 (b), Article 7, Article 9, paragraph 3 and Article 27, paragraph 9 (e).

Article 41 – Federal clause

1. A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2. When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3. With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the European Committee on Crime Problems (CDPC) and,

following consultation with the non-member State Parties to this Convention, may adopt the amendment.

4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the European Committee on Crime Problems (CDPC), to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

a. the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b. the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c. consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The European Committee on Crime Problems (CDPC) shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this Article.

Article 47 – Denunciation

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a. any signature;

b. the deposit of any instrument of ratification, acceptance, approval or accession;

c. any date of entry into force of this Convention in accordance with Articles 36 and 37;

d. any declaration made under Article 40 or reservation made in accordance with Article 42;

e. any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.