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

Delbetænkning II afgivet af Justitsministeriets udvalg om økonomisk kriminalitet og datakriminallitet

Resumé:

I betænkningen foreslår Udvalget om økonomisk kriminalitet og datakriminalitet (Brydensholt- udvalget), at kriminaliseringen af børnepornografi i straffelovens ? 235 udvides og skærpes. Udvalget foreslår således, at ikke kun den erhvervsmæssige udbredelse, men også udbredelse i en videre kreds - f.eks. via Internettet - skal være strafbar. Samtidig foreslås strafferammen forhøjet fra 6 måneders fængsel til fængsel i 2 år. Kriminaliseringen af besiddelse af børnepornografi foreslås udvidet til også at omfatte tilfælde, hvor en person - uden at besiddelseskravet er opfyldt - mod vederlag retsstridigt gør sig bekendt med børnepornografiske fremstillinger. Mere generelt overvejer udvalget, om der er behov for at justere de straffeprocessuelle regler for at sikre, at der kan foretages den fornødne efterforskning i sager om IT-kriminalitet. Udvalget foreslår i den forbindelse bl.a. regler om logning af teletrafik, om adgang til teleoplysninger vedrørende sendemasttrafik og om udvidelse af de kriminalitetsformer,

Udgiver:
Justitsministeriet
Slotsholmsgade 10
DK-1216 København K
33923340
jm@jm.dk

Justitsministeriet Version 1.0 den 8. september 1999
Denne publikation findes på adressen: http://jm.schultzboghandel.dk

---

Indholdsfortegnelse

- BILAG 2 - Edition og indgreb i meddelelseshemmeligheden

[Forside] [Top]

Justitsministeriet Version 1.0 den 8. september 1999
Denne publikation findes på adressen: http://jm.schultzboghandel.dk

Kolofon

Titel
Betænkning nr. 1377/1999 om børnepornografi og IT-efterforskning
Undertitel
Delbetænkning II afgivet af Justitsministeriets udvalg om økonomisk kriminalitet og datakriminallitet
Forfatter
Justitsministeriet
Udgiver/forlægger
Justitsministeriet
Ansvarlig institution
Justitsministeriet,99

Emneord
Brydensholt-udvalget, straffeloven, retsplejeloven, økonomisk, kriminalitet, datakriminalitet, delbetænkning II, børnepornografi, efterforskning, IT, informationsteknologi, Internet
Resumé
I betænkningen foreslår Udvalget om økonomisk kriminalitet og datakriminalitet (Brydensholt- udvalget), at kriminaliseringen af børnepornografi i straffelovens ? 235 udvides og skærpes. Udvalget foreslår således, at ikke kun den erhvervsmæssige udbredelse, men også udbredelse i en videre kreds - f.eks. via Internettet - skal være strafbar. Samtidig foreslås strafferammen forhøjet fra 6 måneders fængsel til fængsel i 2 år. Kriminaliseringen af besiddelse af børnepornografi foreslås udvidet til også at omfatte tilfælde, hvor en person - uden at besiddelseskravet er opfyldt - mod vederlag retsstridigt gør sig bekendt med børnepornografiske fremstillinger. Mere generelt overvejer udvalget, om der er behov for at justere de straffeprocessuelle regler for at sikre, at der kan foretages den fornødne efterforskning i sager om IT-kriminalitet. Udvalget foreslår i den forbindelse bl.a. regler om logning af teletrafik, om adgang til teleoplysninger vedrørende sendemasttrafik og om udvidelse af de kriminalitetsformer,
Sprog
dan
ISBN
ISBN 87-601-8498-1
Pris for læsning
0,- DKK
Pris for download
0,- DKK
URL
jm.schultzboghandel.dk
Version
1.0
Versionsdato
19990908
Format
htm
Den trykte udgaves ISBN
ISBN 87-601-8497-3
Publiceringsstandard
1.0

Justitsministeriet Version 1.0 den 8. september 1999
Denne publikation findes på adressen: http://jm.schultzboghandel.dk

Betænkning nr. 1377/1999 om børnepornografi og IT-efterforskning
Delbetænkning II afgivet af Justitsministeriets udvalg om økonomisk kriminalitet og datakriminallitet

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 kriminalitetsmønstre 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, herunder 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, hvidvasklovgivningen og den finansielle lovgivning skal behandles i denne sammenhæng. Endvidere skal de internationale tiltag på området, herunder i EUregi, indgå i arbejdet.
- Udvalget skal tillige overveje længere forældelsesfrister på en række områder.
- 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 retsplejeloven med henblik på at sikre tidssvarende bestemmelser om datakriminalitet.
- Gennemgangen skal således bl.a. omfatte straffelovens bestemmelser om urigtige erklæringer og dokumentfalsk og om industrispionage.
- Endvidere skal udvalget vurdere de kriminalitetsformer, som informationssamfundet, 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 muligt 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

Direktør Jørgen Christiansen
Arbejderbevægelsens Erhvervsråd

Statsadvokat Michael Clan
Statsadvokaten for særlig økonomisk kriminalitet

Professor, lic. jur. Vagn Greve
Københavns Universitet

Fuldmægtig Alexander Houen
Skatteministeriet
(fra december 1998)

Fuldmægtig Annemette Vestergaard Jacobsen
Skatteministeriet
(til oktober 1998)

Fuldmægtig Helle Jahn
Erhvervsministeriet
(fra august 1998)

Kommitteret Poul Dahl Jensen
Justitsministeriet

Statsautoriseret revisor Jesper Koefoed
Foreningen af Statsautoriserede Revisorer

Kontorchef, advokat Lau Kramer
Foreningen Registrerede Revisorer FRR

Fuldmægtig Lisbeth Krener
Erhvervsministeriet
(til august 1998)

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

Lektor Lars Bo Langsted
Handelshøjskolen i Århus

Kontorchef Kirsten Mandrup
Økonomiministeriet

Politimester Annemette Møller
Politimesterforeningen

Konsulent Lene Nielsen
Dansk Industri

Advokat Erik Overgaard
Advokatrådet

Generalsekretær Henrik Rothe
Advokatrådet
(fra marts 1999)

Sekretariat

Vicestatsadvokat Ulla Høg
Statsadvokaten for særlig økonomisk kriminalitet

Kst. 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 6 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)

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

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 arbejdsgrupper, og at en betænkning vedrørende samtlige af de i kommissoriet nævnte problemstillinger derfor først ville kunne foreligge på et meget senere tidspunkt end færdiggørelsen af en del af de indeholdte problemstillinger.

Udvalget har tidligere afgivet delbetænkning I vedrørende udviklingen i lovgivningen og kriminaliteten samt vedrørende hæleri og anden efterfølgende medvirken.

Denne delbetænkning indeholder to selvstændige emner fra udvalgets kommissorium og bygger på en delrapport fra arbejdsgruppe 6, der behandler spørgsmål vedrørende datakriminalitet. Denne delrapport er derefter tillige behandlet i arbejdsgruppe 2, der behandler spørgsmål vedrørende straffeloven, og i arbejdsgruppe 5, der behandler spørgsmål vedrørende domsforhandling m.v. Betænkningen vedrører dels spørgsmålet om den strafferetlige behandling af personer, der udbreder børnepornografisk materiale, og af de personer, der modtager materialet. Dels vedrører den spørgsmålet om de straffeprocessuelle regler set i forhold til de særlige efterforskningsbehov ved IT-relateret kriminalitet, ikke blot i relation til børnepornografi, men i relation til kriminalitet generelt.

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

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

Kriminalassistent Kim Aarenstrup
Københavns politi, Afdeling B, CCU

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

Professor, lic. jur. Vagn Greve
Københavns Universitet

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

Fuldmægtig Henrik Oftebro-Svendsen
Fødevareministeriet

Sikkerhedschef Kjell Olsen (til november 1998)
UNI-C

Vicekriminalkommissær Ronald Pedersen
Rigspolitichefens afd. A, Rejseafdelingen

Systemrevisionschef Ole Stampe Rasmussen
PBS A/S

Kst. statsadvokatassessor Jens Madsen (sekretær)
Statsadvokaten for særlig økonomisk kriminalitet

Som nævnt er rapporten fra arbejdsgruppen vedrørende datakriminalitet for så vidt angår straffelovsspørgsmål 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

Landsdommer Bent Carlsen
Dommerforeningen

Vicestatsadvokat Ulla Høg
Statsadvokaten for særlig økonomisk kriminalitet

Kommitteret Poul Dahl Jensen
Justitsministeriet

Kst. statsadvokatassessor Jens Madsen
Statsadvokaten for særlig økonomisk kriminalitet

Politimester Annemette Møller
Politimesterforeningen

Generalsekretær Henrik Rothe
Advokatrådet

Fuldmægtig Lennart Houmann (sekretær)
Justitsministeriet

Rapporten er for så vidt angår straffeprocessuelle spørgsmål derefter behandlet i *arbejdsgruppe 5*, der har haft følgende sammensætning ved behandlingen:

Landsdommer Bent Carlsen (formand)
Dommerforeningen

Vicestatsadvokat Ulla Høg
Statsadvokaten for særlig økonomisk kriminalitet

Kontorchef Jens Kruse Mikkelsen
Justitsministeriet

Generalsekretær Henrik Rothe
Advokatrådet

Kst. statsadvokatassessor Jens Madsen (sekretær)
Statsadvokaten for særlig økonomisk kriminalitet

Under hensyntagen til, at arbejdsgruppen vedrørende datakriminalitet helt overvejende har været sammensat med eksperter på området, der ikke er medlemmer af udvalget, har udvalget i denne delbetænkning valgt tillige at anføre, hvordan medlemmerne af denne arbejdsgruppe har forholdt sig til de enkelte forslag.

1.4. Resumé

Betænkningen omhandler - med udgangspunkt i de nye problemstillinger, der følger med IT-udviklingen - dels straffelovens § 235 om børnepornografi og dels mere generelt, om der er behov for at justere de straffeprocessuelle regler - især reglerne i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden - for at sikre, at der kan foretages den fornødne efterforskning i IT-sammenhænge.

I *kapitel 2* omtales nogle generelle problemstillinger i forbindelse med IT-anvendelse, især i relation til netsystemer. I den forbindelse gennemgås bl.a. spørgsmålet om dansk straffemyndighed ved kriminalitet via Internettet, særligt for så vidt angår salg og udbredelse af børnepornografi via Internettet. Det er udvalgets umiddelbare opfattelse, at den retstilstand, som de gældende jurisdiktionsbestemmelser må antages at indebære i forhold til salg og udbredelse af børnepornografi, er tilfredsstillende. Udvalget finder derfor ikke på det foreliggende grundlag behov for lovændringer på området. Da retspraksis af betydning for dette område er

sparsom, og da udviklingen hele tiden åbner nye tekniske muligheder, finder udvalget, at udviklingen løbende bør følges nøje for at sikre, at straffelovens regler om straffemyndighed til stadighed er tidssvarende i forhold til den teknologiske udvikling.

I *kapitel 3* behandles spørgsmålet om ansvar for indholdet af informationssystemer. Udvalget finder, at udbredelse i en videre kreds på nogle områder bør sidestilles med erhvervsmæssig spredning, men har herudover ikke foreslået lovændringer på dette område.

I *kapitel 4* behandles straffelovens § 235 om børnepornografi. Udvalget foreslår, at bestemmelsens stk. 1 om udbredelse af børnepornografi ændres således, at ikke kun den erhvervsmæssige udbredelse, men også udbredelse i en videre kreds - f.eks. via Internettet - er omfattet. Udvalget foreslår endvidere, at strafmaksimum i stk. 1 forhøjes fra fængsel i 6 måneder til fængsel i 2 år.

For så vidt angår straffelovens § 235, stk. 2, om besiddelse af børnepornografi foreslår udvalget, at bestemmelsen udvides til også at omfatte den, der, uden at besiddelseskravet er opfyldt, mod vederlag retsstridigt gør sig bekendt med de af bestemmelsen omfattede børnepornografiske fremstillinger. Med hensyn til bestemmelsen i stk. 2 finder udvalget, at den nuværende begrænsning af straffen til bøde bør bevares som normalstrafferammen. Udvalget finder imidlertid, at der bør være mulighed for under skærpende omstændigheder at idømme hæfte eller fængsel indtil 6 måneder.

I *kapitel 5* omtales efterforskningsmuligheder hos Internetudbydere og teleselskaber samt kryptering. Udvalget foreslår, at teletrafikken logges i et omfang, der tilgodeser behovet for at kunne efterforske kriminalitet, og at de loggede oplysninger opbevares i 6 måneder. Et flertal i udvalget foreslår, at disse pligter reguleres i lovform, mens et mindretal finder, at spørgsmålet så vidt muligt skal løses ved en selvregulering i branchen.

I *kapitel 6* behandles retsplejelovens efterforskningsregler set i relation til aktuelle IT-problemstillinger.

Med hensyn til adgang til indholdet af digitale meddelelser finder udvalget, at den gældende retstilstand, hvorefter bestemmelserne om edition eller ransagning og beslaglæggelse finder anvendelse på meddelelser, der befinder sig hos enten afsenderen eller modtageren, bør opretholdes. Med hensyn til adgang til f.eks. email hos Internetudbyderen finder udvalgets flertal, at denne situation skal sidestilles med traditionelle (fysiske) breve og behandles efter de regler om indgreb i meddelelseshemmeligheden, der gælder for sådanne breve. Et mindretal finder, at adgang til email hos Internetudbydere bør behandles efter reglerne om edition.

Med hensyn til teleoplysninger finder udvalgets flertal, at oplysninger herom fortsat bør reguleres i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden. Et mindretal finder, at teleoplysninger bør behandles efter reglerne om edition.

Udvalget finder, at adgang til teleoplysninger vedrørende sendemasttrafik bør reguleres i retsplejelovens § 780 om indgreb i meddelelseshemmeligheden, og at dette indgreb kun skal være muligt i særligt kvalificerede sager.

Et flertal i udvalget finder, at teleselskaber ikke skal kunne meddele samtykke til indhentelse af teleoplysninger vedrørende offentlige telefoner, men at de almindelige betingelser for indgreb i meddelelseshemmeligheden skal være opfyldt. Et mindretal finder, at teleselskaberne bør kunne give samtykke.

Med hensyn til spørgsmålet om, hvorvidt området for, ved hvilke kriminalitetsformer der kan foretages indgreb i meddelelseshemmeligheden, skal udvides, finder udvalgets flertal, at der bør være hjemmel til sådanne indgreb i sager om overtrædelse af straffelovens § 235 om børnepornografi. Et af flertallets medlemmer finder, at det herudover bør overvejes at have hjemmel til at foretage disse indgreb i sager om misbrug af intern viden og kursmanipulation efter lov om værdipapirhandel m.v. Et mindretal finder, at der bør indsættes en generel hjemmel til indgreb i meddelelseshemmeligheden i alle sager, der kan straffes med fængsel i 1 år og 6 måneder eller derover, såfremt der i den konkrete sag reelt ikke er andre efterforskningsmuligheder.

Kapitel 7 indeholder udvalgets forslag med bemærkninger.

KAPITEL 2 - GENERELLE

PROBLEMSTILLINGER

2.1. Netsystemer

Gennem de seneste år er IT-udviklingen forstærket eksponentielt gennem udviklingen af det verdensomspændende Internet. Navnlig udviklingen af den Internetteknologi, der almindeligvis går under betegnelsen the World Wide Web (også kaldet WWW), har understøttet en række nye former for informationsudveksling med heraf følgende retlige (herunder strafferetlige) implikationer.

Gennem the World Wide Web forbindes et antal databaser, hvis informationsindhold hver for sig fremtræder med en ensartet grafisk brugergrænseflade - de såkaldte "hjemmesider". Når en bruger ved hjælp af en computer, der er programmeret med en såkaldt webbrowser, retter henvendelse 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 struktur. Disse Internetoperatører kan opdeles således[(1)]:

1) Netværksoperatører, der alene stiller den overordnede teknologi til rådighed.

2) Internetudbydere, der etablerer adgangen til Internettet. Disse kan opdeles i:

a) Content Providers, der tilvejebringer den information, der er tilgængelig.

b) Hosts, der udlejer plads på serveren til kunder eller stiller nyhedsgrupper til rådighed på sin newsserver.

c) Access Providers, der sælger adgang til Internettet (hvilket almindeligvis omfatter email funktioner og adgang til the World Wide Web).

Udviklingen indebærer som en naturlig konsekvens også en øget risiko for retsstridig brug af disse teknologier.

En opgørelse over antallet af værtscomputere (hosts)[(2)] 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.

Udviklingen har da også allerede medført, at de processuelle muligheder for at efterforske IT-relateret kriminalitet er blevet ændret for at imødekomme de nye behov. I 1996[(3)] blev retsplejelovens § 781 ændret således, 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 anvendelse af en telekommunikationstjeneste.

---

[1].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.
[2]. Hobbes' Internet Timeline.
(http://info.isoc.org./guest/zakon/Internet/History/HIT.html.)
[3]. Lov nr. 388 af 22/5 1996.

2.2. Forskellige internationale anbefalinger

IT-udviklingen indebærer mange internationalt relaterede problemstillinger, og udviklingen i det internationale

arbejde på IT-området har derfor stor betydning for, hvilke reelle muligheder der er for at bekæmpe IT-relateret kriminalitet.[4] Det gælder både spørgsmålet om, hvorvidt der er tilsvarende straffebestemmelser - og dermed mulighed for at bistå med strafprocessuelle tvangsindgreb - og spørgsmålet om, hvilke efterforskningstiltag der kan anvendes.

Blandt de centrale internationale anbefalinger kan nævnes følgende (hvoraf nogle af punkterne nævnes senere i betænkningen ved de enkelte problemstillinger):

OECD påbegyndte i 1984 en analyse af medlemsstaternes lovgivning vedrørende IT- relateret kriminalitet. Resultatet blev publiceret i 1986[5]. Det blev anbefalet i rapporten, at medlemsstaterne overvejede en straffelovgivning vedrørende computerrelateret berigelse, falsk, hærværk, piratkopiering og hacking, jfr. bilag 1.

Europarådet inkluderede fra 198586 computerrelateret kriminalitet i CDPCs[6] arbejdsprogram. Arbejdet tog bl.a. udgangspunkt i OECDs ovennævnte rapport, og der udfærdigedes i 1989 guidelines - delt i en "minimum list" og en "optional list" - bl.a. med henblik på at opnå en vis harmonisering af lovgivningen, da der ofte var tale om grænseoverskridende kriminalitet. I 1989 vedtoges rekommandation nr. R(89)9, der anbefalede, at medlemsstaterne bl.a. tog hensyn til disse guidelines i deres lovgivning[7]. På "the minimum list" er OECDs rekommandationer i lidt udbygget form, og der er tilføjet to nye emner, idet også henholdsvis aflytning og halvlederbeskyttelse er medtaget. "The optional list" har herudover ændring af data eller programmer, computer spionage og uberettiget brug af computer eller programmer, jfr. bilag 1.

Europarådet nedsatte i 1991 "Committee of Experts on Procedural Law Problems connected with Computerrelated Crime" (PCPC). I 1995 vedtoges rekommandation R(95)13 vedrørende efterforskning, internationalt samarbejde m.v., der anbefalede, at ransagning og beslaglæggelse skulle kunne ske i edbmiljøer som i andre miljøer, at der i visse tilfælde skulle kunne foretages indgreb i meddelelseshemmeligheden, m.v., jfr. bilag 1.

Rådet for EU udfærdigede 17/1 1995 en resolution om lovlig aflytning af telekommunikation[8], der anbefalede, at der i en række henseender blev taget hensyn til de efterforskningsmæssige behov, jfr. bilag 1.

OECD udfærdigede 27/3 1997 rekommandationer vedrørende "Guidelines for cryptography policy", der både fremhævede betydningen af kryptering i relation til datasikkerhed og beskyttelse af privatlivet og betydningen af, at kryptering ikke udgør en risiko for den offentlige sikkerhed og retsforfølgning. Rekommandationerne indeholder dog ingen mere præcise anvisninger til, hvordan disse modstridende interesser tilgodeses samtidig.

Europarådet arbejder fortsat med IT-relateret kriminalitet, og CDPC har i 1997 nedsat en Committee of Experts on Crime in Cyberspace (PCCY)[9], der arbejder med en konvention vedrørende såvel de strafferetlige som de processuelle aspekter, herunder det internationale samarbejde og adgangen til i et vist omfang via en PC at efterforske over grænserne.

Interpol har - især ved arbejdsgruppen The Interpol European Working Party on Information Technology Crime - bl.a. med Europarådets rekommandation nr. R(89)9 som udgangspunkt arbejdet med den strafferetlige dækning på området. Derudover er nedsat igangværende underarbejdsgrupper, der bl.a. ser på kriminelt misbrug af Internettet, elektroniske betalingsmidler og manipulation med kommunikationsnet.

Særligt vedrørende Internettet gælder det i dag for alle internationale organisationer, at de forsøger at få afklaret, hvad de nuværende og fremtidige muligheder for anvendelse af Internettet betyder for de områder, de beskæftiger sig med.

Af mere specielle fora, der har udfærdiget handlingsplaner bl.a. vedrørende kriminelles anvendelse af IT-mulighederne og efterforskningsbehov, kan nævnes Gruppen på Højt Plan, der blev nedsat af det Europæiske Råd og i april 1997 udfærdigede en handlingsplan til bekæmpelse af organiseret kriminalitet[10], og G8landenes erklæring af 10/12 1997 om hightech crime[11].

I EU foreligger der et af Rådet foreløbigt godkendt udkast til fælles aktion vedrørende bekæmpelse af børnepornografi på Internettet[12]. Udkastet påpeger bl.a., at medlemsstaterne skal sikre et hurtigt og effektivt samarbejde i disse sager, og peger bl.a. på en mulighed for at regulere Internetudbydere således, at trafikrelaterede data, hvor det er muligt, opbevares i det tidsrum, der kan være nødvendigt for at kunne sende disse data til de

retsforfølgende myndigheder. Der er ikke angivet noget anbefalet tidsrum for denne opbevaring.

Endvidere foreligger EuropaParlamentets og Rådets beslutning af 25/1 1999 om vedtagelse af en flerårig EUhandleplan til fremme af en mere sikker anvendelse af Internettet ved bekæmpelse af ulovligt og skadeligt indhold på globale net[(13)]. Handleplanen vedrører bl.a. fremme af selvregulering i branchen og af ordninger til overvågning af indhold (f.eks. børnepornografisk indhold og indhold, der opfordrer til had på grund af race, køn, religion, nationalitet eller etnisk herkomst).

---

[4]. Problemstillingerne vedrørende den internationale dimension er meget udførligt gennemgået af professor Ulrich Sieber i en artikelserie - Internet Law - i Computer Law & Security Report 1997 nr. 36 og 1998 nr. 1. Det konkluderes bl.a., at rent nationale kontroltiltag er ineffektive ved internationale net, og at det derfor er absolut nødvendigt at finde supranationale og internationale løsninger.

[5]. OECD-rapport ICCP nr. 10, Computerrelated crime : Analysis of legal policy

[6].Comité Directeure pour les Problèmes Criminelles. På engelsk kaldet the European Committee on Crime Problems.

[7]. Rekommandationen, rapporten og guidelines er trykt af Europarådet i 1990 (Computerrelated Crime).

[8]. EFT 1996 C 329/1.

[9]. Problèmes Criminelles - Comité d'Èxperts sur la Criminalité dans CyberÉspace.

[10]. 6726/4/97 REV 4.

[11]. Nogle punkter fra disse dokumenter er omtalt i afsnit 5 og 6. G8landenes erklæring er gengivet i bilag 1.

[12]. Rådets pressemeddelelse fra mødet 34 december 1998 (13673/98 (Presse 427)), gengivet i bilag 1.

[13]. Nr. 276/1999/EF, EFT 1999 L 33/1.

2.3. Straffemyndighed

2.3.1. Generelt vedrørende straffemyndighed

Generelle regler om dansk straffemyndighed (jurisdiktionskompetence) er fastsat i straffelovens §§ 612.

Hovedreglen om dansk straffemyndighed findes i straffelovens § 6, nr. 1. Efter denne bestemmelse hører handlinger, der foretages i den danske stat, under dansk straffemyndighed (*territorialprincippet*). Forbrydelser, der er begået her i landet, kan således strafforfølges ved danske domstole uanset gerningsmandens nationalitet.

Udtrykket "handlinger, der foretages i den danske stat" betegner sprogligt de forbrydelser, som begås ved en eller flere handlinger på territoriet. I almindelighed vil gerningsmanden (eller en medvirkende) være fysisk til stede på det sted, hvor handlingen foretages. Der er imidlertid ikke noget til hinder for, at en enkeltpersons handling også kan lokaliseres til et sted, hvor gerningsmanden ikke på handlingstidspunktet befinder sig.

Begår en person, der befinder sig i Sverige, ved hjælp af sin computer indbrud i en computer her i landet, må handlingen lokaliseres ikke blot til Sverige, hvor gerningsmanden fysisk befinder sig, men også til Danmark, hvor indbruddet sker. Der vil således foreligge dansk straffemyndighed efter straffelovens § 6, nr. 1. I sådanne tilfælde vil det således ikke være nødvendigt at anvende straffelovens § 9 om virkningsstedet for at statuere dansk straffemyndighed, selv om gerningsmanden ikke på handlingstidspunktet befandt sig på dansk område, jfr. nedenfor.

Ordet "handlinger" i § 6, nr. 1, antages i almindelighed også at omfatte forsøgs og medvirkenshandlinger. Det indebærer, at forsøgs og medvirkenshandlinger, der begås på dansk område, skaber dansk jurisdiktion over for den pågældende, selv om den forbrydelse, som forsøgs eller medvirkenshandlinger knytter sig til, fuldbyrdes eller tænkes fuldbyrdet i udlandet[(14)]. Det må anses for uafklaret, om en på dansk område foretagen forsøgs eller medvirkenshandling skaber jurisdiktion efter § 6, nr. 1, hvis den forbrydelse efter dansk ret, som handlingen knytter sig til, skal fuldbyrdes i et land, hvor forholdet er straffrit. Som eksempel kan nævnes medvirken på dansk grund til samleje med børn mellem 1215 år, der skal finde sted i et land, hvor den seksuelle lavalder er 12 år.

Udvalget er ikke bekendt med retsafgørelser om dette spørgsmål. Det er derfor ikke muligt at sige noget sikkert om, hvorvidt det i det nævnte eksempel vil have betydning, om de pågældende mindreårige er bragt med fra Danmark, eller om der er tale om "lokale" børn. Meget taler efter udvalgets opfattelse for dansk straffemyndighed i hvert fald i de tilfælde, hvor der er tale om medbragte børn.

[14.] Hurwitz anfører i Den danske Kriminalret, Alm. Del, s. 102, at det for en anvendelse af § 6 ikke kan kræves, at hele den forbryderiske virksomhed er foregået inden for landets område, når blot væsentlige dele deraf er foregået her i landet. Det fremgår ikke, hvad denne indskrænkende fortolkning af § 6 bygger på.

Som et andet eksempel kan nævnes, at en person i Danmark bistår et søskendepar, der ønsker at have seksuelt forhold til hinanden, med formaliteterne omkring emigration til et land, hvor blodskam ikke er strafbart. I denne situation vil der efter udvalgets opfattelse ikke kunne straffes i Danmark for medvirken.

Der er efter udvalgets opfattelse ikke noget umiddelbart behov for en yderligere lovregulering på dette område. Der foreligger endvidere ikke tilstrækkelig analyse af aktuelle situationer til at vurdere, om der inden for det strafferetlige område i almindelighed findes problemstillinger, der kan give anledning til at overveje en lovregulering.

Spørgsmålet om, hvorvidt forsøgs og medvirkenshandlinger er selvstændigt omfattet af § 6, har den praktiske betydning, at der ved dansk straffemyndighed baseret på § 6 ikke gælder de begrænsninger, der f.eks. følger af § 7 om, at forholdet også skal være strafbart i gerningslandet (det vil her sig det land, hvor forbrydelsen fuldbyrdes eller tænkes fuldbyrdet) og af § 10, stk. 2, hvorefter straffen skal holde sig inden for strafmaksimum i det pågældende andet lands lovgivning.

Fra retspraksis kan nævnes:

I en Østre landsrets dom af 5. oktober 1989 (Domme i kriminelle sager 198789, s. 4) erkendte den tiltalte forsøg på anstiftelse af narkotikakriminalitet vedrørende modtagelse af et parti heroin i Tyskland med henblik på videreoverdragelse i Tyskland og Holland. På grund af pasproblemer havde han formidlet alt fra Danmark (telefonisk formidlet kontakter, mødetider og mødesteder for de implicerede). Byretten anvendte straffelovens § 7, stk. 1, nr. 2, som grundlag for dansk straffemyndighed. Landsretten fandt, at tiltaltes handlinger var undergivet dansk straffemyndighed efter § 6, nr. 1.

I sagen UfR 1998.877 H havde de tiltalte her i landet fremstillet tre brevbomber og adresseret dem til personer i England. Forehavendet mislykkedes dog, dels fordi svensk politi udtog brevbomberne af den postkasse i Sverige, hvori de var blevet anbragt, dels fordi det anvendte sprængstof viste sig ikke at være virksomt. Under sagen var der spørgsmål om, hvorvidt der var straffemyndighed her i landet, når brevbomberne var blevet postet i Sverige, hvor forsøg med utjenligt objekt ikke er strafbart. Højesteret udtalte herom: "Fremstillingen af en brevbombe her i landet hører under dansk straffemyndighed, jfr. straffelovens § 6, nr. 1, uanset hvor modtageren befinder sig, og uanset hvor afgivelse til postbesørgelse sker." Landsrettens domfældelse for forsøg på bombesprængning efter straffelovens § 183, stk. 2, jfr. § 21, samt medvirken hertil blev stadfæstet.

I Nordisk Strafferetskomités betænkning Straffrättslig jurisdiktion i Norden (Nord 1992:17) er spørgsmålet om lokalisering af forsøgs og medvirkenshandlinger kort behandlet side 29 f. og 108 f. Se også Jørn Vestergaard i Kriminalistisk Instituts Årbog 1991 s. 109 ff og (samme artikel) i Juristen 1992 s. 162 ff.

Er handlingen ikke foretaget i Danmark, men har den virkning her i landet, kan den efter omstændighederne være undergivet dansk straffemyndighed. I de tilfælde, hvor en handlings strafbarhed afhænger af eller påvirkes af en indtrådt eller tilsigtet følge, betragtes handlingen således tillige som foretaget dér, hvor virkningen er indtrådt eller tilsigtet at skulle indtræde, jfr. straffelovens § 9 (*virkningsprincippet*).

Bestemmelsen giver bl.a. dansk straffemyndighed i tilfælde, hvor en person fra udlandet afsender et ærekrænkende brev til en person her i landet, eller hvor en person fra udlandet ved et skud over den danske landegrænse dræber en person her i landet. For så vidt angår forsøg og medvirken, indebærer bestemmelsen i § 9 sammenholdt med § 6, at der er dansk straffemyndighed i forhold til personer, der i udlandet begår forsøgs eller medvirkenshandlinger, såfremt den forbrydelse, som forsøgs eller medvirkenshandlingen angår, faktisk fuldbyrdes eller tilsigtes fuldbyrdet

her i landet.

Det kan undertiden give anledning til tvivl, om dansk straffemyndighed følger umiddelbart af § 6, eller om den følger af § 6 sammenholdt med § 9. Spørgsmålet om den indbyrdes afgrænsning mellem handlingssted og virkningssted er imidlertid i denne situation uden selvstændig praktisk betydning.

I UfR 1999.513 Ø havde tiltalte fra udlandet begået insiderhandel ved køb af aktier, der blev effektueret gennem en bank i København. Selv om gerningsmanden befandt sig i udlandet, og købet var formidlet gennem en schweizisk investeringsrådgiver og bankforbindelse, blev forholdet anset for omfattet af straffelovens § 6, nr. 1, under hensyn til, at aktierne blev købt i den danske stat.

Har den kriminelle virksomhed - hverken for så vidt angår handling eller virkning - ingen tilknytning til dansk område, kan der i visse tilfælde være dansk straffemyndighed efter straffelovens § 7 (*personalprincippet*).

Efter straffelovens § 7 hører strafbare handlinger, der er begået i udlandet, under dansk straffemyndighed, såfremt gerningsmanden er dansk statsborger eller bosat her i landet. For så vidt angår handlinger, der er foretaget uden for folkeretligt anerkendt statsområde, kræves det efter § 7, stk. 1, nr. 1, at handlingen kan medføre højere straf end hæfte, mens det for så vidt angår handlinger, der er foretaget inden for sådant område, kræves, at handlingen er strafbar både efter gerningsstedets lov og efter dansk lov, jfr. § 7, stk. 1, nr. 2 (dobbelt strafbarhed).

Personalprincippet udstrækkes ved § 7, stk. 2, til personer, der alene opholder sig her i landet, når de samtidig har indfødsret eller bopæl i Finland, Island, Norge eller Sverige.

De ovennævnte bestemmelser suppleres af straffelovens § 8. Efter denne bestemmelse er der i en række nærmere opregnede tilfælde dansk straffemyndighed i forhold til udlandshandlinger uden hensyn til, hvor gerningsmanden hører hjemme. Det gælder bl.a. med hensyn til handlinger der krænker den danske stats selvstændighed, sikkerhed, forfatning m.v., jfr. § 8, nr. 1. Det gælder også i tilfælde, hvor "handlingen er omfattet af en mellemfolkelig overenskomst, ifølge hvilken Danmark er forpligtet til at foretage retsforfølgning", jfr. § 8, nr. 5.

Når der sker påtale her i landet af udlandshandlinger, skal pådømmelsen finde sted efter dansk lovgivning, jfr. straffelovens § 10. Det er derfor en forudsætning for, at der i anledning af udlandshandlinger kan gøres strafansvar gældende ved de danske domstole, at den pågældende danske straffebestemmelse ikke efter sit gerningsindhold er territorialt begrænset til dansk område. Må man konstatere, at den danske straffebestemmelse, der i givet fald skulle straffes efter, slet ikke er blevet overtrådt, når der er handlet i udlandet, er det selvsagt ikke relevant at overveje spørgsmålet om dansk straffemyndighed, jfr. f.eks. UfR 1998.1027 H.

I de tilfælde, hvor en udlandshandling er undergivet dansk straffemyndighed i medfør af straffelovens § 7, kan der ikke idømmes strengere straf end efter gerningsstedets lovgivning, jfr. straffelovens § 10, stk. 2. Denne begrænsning må formentlig også gælde i tilfælde, hvor grundlaget for dansk straffemyndighed er straffelovens § 8, nr. 6.

2.3.2. Særligt vedrørende salg og udbredelse af børnepornografi via Internettet

Som det fremgår af det ovenfor anførte, bygger udformningen af de gældende regler om dansk straffemyndighed i vidt omfang på, at verden er opdelt i stater med hver deres territorium, hvortil forbrydelser stedligt kan henføres.

Denne opfattelse kan komme under pres i relation til strafbare handlinger, der indbefatter et informationsrelateret gerningsindhold, når denne information spredes ved hjælp af det verdensomspændende Internet. Det kendetegner således al Internetkommunikation, at den involverer et stort antal netforbindelser, der ikke har noget centralt knudepunkt. Uanset om der er tale om afsendelse af en postmeddelelse eller spredning af information fra hjemmesider via "the World Wide Web", ved gerningsmanden derfor ikke - nødvendigvis - hvor den pågældende information modtages: En elektronisk postmeddelelse adresseres altid til en eller flere elektroniske postadresser, men selv om mange af disse postadresser er organiseret under nationale domænenavne (f.eks. ".dk domænet"), siger dette i sig selv intet om, hvor de vil blive læst. En dansk statsborger kan f.eks. uden vanskelighed have elektronisk postadresse under det svenske topdomænenavn, men desuagtet altid læse sin post i Danmark. Ligeledes kan en hjemmeside, som har WWW adresse under det danske topdomænenavn, læses fra hele verden, medmindre der er foretaget særlige tekniske blokeringsforanstaltninger.

Dette forhold, at kommunikation på nettet spredes til en ubekendt flerhed af modtagere, beskrives undertiden således, at Internet har skabt et "elektronisk cyberspace", der bryder med den klassiske geografiske virkelighedsopfattelse. I strafferetlig henseende indebærer dette, at der er skabt nye muligheder for at begå forbrydelser, der uden bistand fra andre personer indtræder på et andet sted end der, hvor gerningsmanden befinder sig. I relation til disse forbrydelser er det dernæst blevet vanskeligt at fastlægge virkningsstedet.

Også fastlæggelsen af selve handlingsstedet kan give anledning til vanskeligheder. At gerningsmanden "lægger information ud på Internet" kan således indebære begivenheder, der udspiller sig inden for flere forskellige jurisdiktioner: Informationen kan f.eks. være placeret under et dansk topdomænenavn, men ligge på en web server, der fysisk er placeret i Sverige, men som drives af en tysk Internetleverandør. Dernæst kan hjemmesiden i kraft af såkaldte links være stillet til rådighed for modtageren via andre hjemmesider og "portaler", til hvilke der tilsvarende kan høre forskellige medaktører med hver deres nationalitet. Ved vurderingen af, om et givet informationsdelikt er undergivet dansk straffemyndighed, kan det derfor - med udgangspunkt i den relevante gerningsbeskrivelse - blive nødvendigt at sondre mellem disse forskelligartede funktioner.

Der sker derudover i et vist omfang det, at information fra udlandet "spejles" på danske Internetudbyderes udstyr, dvs. at særligt populære homepages indlægges på Internetudbyderens server. Formålet med denne spejling er at optimere transmissionstiderne på Internettet, således at kunderne til disse homepages ikke belaster datatrafikken til udlandet.

I det følgende behandles disse jurisdiktionsspørgsmål med henblik på tilfælde, hvor handlingen består i salg eller udbredelse af børnepornografisk materiale via Internettet.

Et *salg* kan stedfæstes til flere forskellige lokaliteter. Som muligheder kan peges på det sted, hvor sælger opholder sig på salgstidspunktet, det sted, hvor køber opholder sig, det sted, hvor købsaftalen indgås, det sted, hvor betalingen sker, det sted, hvor varen befinder sig o.s.v.

Der kan således foreligge mange kombinationer, hvor salget kan have større eller mindre tilknytning til flere forskellige steder. Det er ikke i alle enkeltheder afklaret, hvilke former for tilknytning der kræves, for at et salg i jurisdiktionsmæssig henseende kan lokaliseres til et givet sted.

Som det fremgår af det ovenfor anførte, kan der ikke i straffelovens § 6, nr. 1, indlægges et krav om, at hele den kriminelle virksomhed skal være foretaget i den danske stat. Når blot en del af virksomheden er foretaget her i landet, kan forholdet være undergivet dansk straffemyndighed efter denne bestemmelse.

På den baggrund må et salg efter udvalgets opfattelse anses for foretaget i Danmark, hvis en eller flere af de væsentlige faktorer, der indgår i en salgssituation, har tilknytning til dansk område. Det typiske vil være, at sælgeren eller køberen, eventuelt begge, opholder sig i Danmark. Men et salg vil efter omstændighederne også kunne henføres til dansk område, selv om f.eks. køberen og sælgeren befinder sig i udlandet, jfr. UfR 1999.513 Ø om insiderhandel, der er omtalt ovenfor i afsnit 2.3.1.

Udbredelse af børnepornografisk materiale via Internettet må utvivlsomt lokaliseres til det sted, hvor gerningsmanden opholder sig på det tidspunkt, hvor den pågældende lægger materialet ind på en webserver, der er forbundet med Internettet. En person, der i Danmark lægger børnepornografi ind på en webserver, vil således være undergivet dansk straffemyndighed efter straffelovens § 6, nr. 1, uanset om serveren befinder sig i udlandet, og uanset hvor i verden det pågældende materiale er tilgængeligt.

En sådan handling må imidlertid antages også at kunne lokaliseres til den server, som materialet lægges ind på, og hvorfra den videre udbredelse herefter sker. Lægger en person, der befinder sig i Tyskland, børnepornografi ind på sin hjemmeside, der betjenes via en server i Danmark, er stedet, hvor handlingen (d.v.s. udbredelsen) må anses for foretaget ikke blot Tyskland, men også Danmark. Forholdet er dermed undergivet dansk straffemyndighed i medfør af straffelovens § 6, nr. 1.

Er der ikke lagt særlige begrænsninger ind, er materialet i kraft af Internettets globale karakter tilgængeligt fra hele verden, og "virkningen" af handlingen kan således tænkes at indtræde i alle lande. Spørgsmålet er derfor, om handlingen i kraft af virkningsprincippet i § 9 tillige kan anses for foretaget i alle de lande, hvor materialet er tilgængeligt.

Rækkevidden af virkningsprincippet i § 9 i relation til overtrædelser via Internettet er bl.a. behandlet af Peter

Blume, Helen Holdt, Ruth Nielsen og Thomas Riis i "IT-retlige emner" (Jurist og Økonomforbundets forlag 1998), s. 276:

- "Denne regel har stor betydning ved anvendelse af Internet. Mange handlinger foretaget på Internet kan have virkning i mange af de tilkoblede lande, idet Internet jo netop fungerer uafhængigt af territoriale grænser. Det kan sagtens tænkes, at det ikke var tilsigtet, at de pågældende handlinger skulle have virkning i Danmark, hvorved straffelovens § 9 kan få en uheldig konsekvens for Internetbrugere i andre lande."

Forfatterne synes herved - med en vis beklagelse - at nå frem til, at § 9 medfører, at virkningerne af aktiviteter på Internet ofte vil indtræde her i landet på en sådan måde, at danske domstole vil være kompetente til at behandle sager der udspringer heraf.

De eksempler fra praksis, der refereres i samme fremstilling, er i overvejende grad fra amerikansk ret og vedrører i det væsentlige civilretlige sager. På s. 280 f. resumeres en dom (Telco Communications Inc. v. An Apple A Day Inc.), der vedrører injurierende og ærekrænkende udtalelser. En virksomhed, der drives i én amerikansk delstat, distribuerer via Internet nogle krænkede pressemeddelelser vedrørende en konkurrent, der driver virksomhed i en anden delstat. Dommen fastslår, at distribution via Internet giver en domstol i denne anden delstat jurisdiktion, fordi pressemeddelelserne er tilgængelige i domstolsstaten, og de injurierende virkninger af pressemeddelelserne konkret fandtes at have gjort størst skade dér. Sagsøgte bestred, at domstolen havde jurisdiktion i den pågældende sag, idet sagsøgte ikke (i øvrigt) udførte forretninger i domstolsstaten.

For så vidt angår markedsføring anføres det i "Forbrugernes retsbeskyttelse i grænseoverskridende digitale net" (Erhvervsministeriet 1997), s. 68:

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

Se også Jan Trzaskowski, Forbrugerstyrelsen, i UfR 1998 B, s. 285. Det anføres her, at der ved vurderingen af, hvortil reklame på Internettet retter sig, bl.a. må lægges vægt på, om der er foretaget tekniske begrænsninger i materialets geografiske tilgængelighed, om en vare, der udbydes til salg via Internettet, kun sælges i visse nærmere angivne lande, hvilket sprog oplysningerne er affattet på og valg af Top Level Domain (TLD), f.eks. ".dk".

Den fastlæggelse af markedsføringslovens anvendelsesområde, der er behandlet i de to sidstnævnte fremstillinger, indebærer samtidig en fastlæggelse af dansk straffemyndighed efter straffelovens § 6, nr. 1, i forhold til denne type overtrædelser.

Efter udvalgets opfattelse kan det ikke antages, at straffelovens § 9 uden videre omfatter det forhold, at en person i udlandet placerer materiale på en Internethjemmeside, der er tilgængelig for Internetbrugere her i Danmark. At dette materiale er tilgængeligt her i landet kan således kun siges at være en følge af udbredelsen, hvis tilgængeliggørelsen på den udenlandske hjemmeside specifikt tager sigte på at nå brugere i Danmark (f.eks. gennem særlige foranstaltninger, der specielt retter sig imod de danske Internetbrugere). I sidstnævnte situation vil straffelovens § 6, nr. 1, som udgangspunkt være anvendelig.

En generel anvendelse af § 9 i disse tilfælde ville i øvrigt føre til en uacceptabel vidtgående jurisdiktion. Danmark ville i så fald have jurisdiktion i forhold til alle informationer på Internettet, som er tilgængelige i Danmark, og som er strafbare efter dansk ret. Tænker man sig tilsvarende regler i andre lande, ville det betyde, at en person, der her i landet f.eks. indlægger voksenpornografisk materiale på Internettet, ville kunne straffes i lande, hvor sådant materiale er strafbart, selv om den pågældende i øvrigt er uden indflydelse på, om nogen i det pågældende land skaffer sig adgang til materialet. Tilsvarende ville gælde for oplysninger, der efter dansk ret er lovlige, men som efter lovgivningen i visse lande er strafbare, f.eks. som blasfemi.

En så vidtgående jurisdiktion ville betyde, at personer, der lægger materiale ind på Internettet, forinden måtte foretage nærmere retlige undersøgelser for at sikre sig, at materialet er lovligt efter lovgivningen i alle de lande,

hvor det er tilgængeligt for andre brugere af Internettet. Hvis man ønsker et globalt Internet, giver det ikke mening at stille et sådant uopfyldeligt krav til brugerne.

Det kan også give anledning til tvivl, om en straffemyndighed i forhold til handlinger, der har så begrænset tilknytning til landet, i alle tilfælde vil være forenelig med folkeretten.

Sammenfattende må det således antages, at der er dansk straffemyndighed efter straffelovens § 6, nr. 1, i forhold til handlinger, der består i salg eller udbredelse af børnepornografi via Internettet, hvis salget eller udbredelsen har tilknytning til dansk område. Tilknytningen kan bestå i, at gerningsmanden har ophold i Danmark på handlingstidspunktet, eller i anvendelse af salgs eller udbredelsesmidler, der befinder sig eller målrettet tager sigte på dansk område. Det er derimod ikke tilstrækkeligt til at anse udbredelse af materiale for foretaget indenlands, at brugere her i landet kan hente materialet ned fra servere, der er placeret i udlandet.

Straffelovens § 235 er efter sit gerningsindhold ikke begrænset til salg, udbredelse m.v., der kan lokaliseres til Danmark. Kan salg og udbredelse af børnepornografi efter det ovenfor anførte ikke anses for foretaget her i landet, kan der således være dansk straffemyndighed efter § 7, hvis betingelserne i denne bestemmelse er opfyldt. En dansk statsborger, der under ophold i Tyskland via Internettet udbreder børnepornografi via en server i Frankrig, vil således kunne straffes herfor i Danmark, hvis forholdet tillige er strafbart efter tysk eller fransk ret, d.v.s. efter lovgivningen i de lande, hvor handlingen (udbredelsen) må anses for foretaget.

Det er udvalgets umiddelbare opfattelse, at den retstilstand, som de gældende jurisdiktionsbestemmelser må antages at indebære i forhold til salg og udbredelse af børnepornografi, er tilfredsstillende. Udvalget finder derfor ikke på det foreliggende grundlag behov for lovændringer på området./P

Da retspraksis af betydning for de her behandlede spørgsmål imidlertid indtil nu har været sparsom, og da udviklingen hele tiden åbner nye tekniske muligheder, som stiller lovgivningen og retsanvendelsen over for nye udfordringer, kan det ikke udelukkes, at der i fremtiden kan forekomme tilfælde, der vil afsløre mangler ved de gældende jurisdiktionsregler. Der kan derfor være grund til løbende at følge udviklingen nøje for at sikre, at straffelovens regler om straffemyndighed til stadighed er tidssvarende i forhold til den teknologiske udvikling.

2.4. Informationsspredning

2.4.1. Generelt om kriminalisering af spredning

Lovgivningen regulerer i forskellige henseender (f.eks. i forbindelse med piratkopiering og dekodningsudstyr) spredning af information, som gerningsmanden ikke har rettigheder over, eller hvis indhold i sig selv er strafbart. Der stilles normalt krav om, at denne spredning er erhvervsmæssig, hvis den skal være omfattet af straffebestemmelser med højere strafferamme. For så vidt angår lov om radio og fjernsynsvirksomhed er kun erhvervsmæssig spredning af dekodningsudstyr strafbart.

På baggrund af Internetudviklingen har udvalget drøftet hensigtsmæssigheden 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 teleinformationsteknologi 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 forholdsvis intens regulering af såvel frekvenstildelingen som det informationsmæssige indhold i offentlig radio og tvtransmission, har disse teknologier ikke givet anledning til strafferetlige problemstillinger i samme omfang, som det er tilfældet i forbindelse med brugen af Internettet. Ved fremkomsten af de såkaldte bulletinboards (dvs. informationssystemer, typisk baseret på en PC, der ved hjælp af telenettet gav mulighed for opkald 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 telefonopkald, der har været til rådighed i den enkelte telefonforbindelse.

Den udbredte anvendelse af WWW har imidlertid givet denne problemstilling en langt større dimension, eftersom WWWteknologien (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 problem om spredningens omfang indebærer WWWteknologien

vanskeligheder med hensyn til at identificere den gerningsmand, der spreder den pågældende information, og herunder også det land, som den efterforskende myndighed i givet fald skal samarbejde med med henblik på at opnå de fornødne tilladelser til straffeprocessuelle tvangsindgreb.

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 spredning 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 edbprogrammer, børnepornografi m.v.

Udvalget finder på denne baggrund, at den traditionelle begrænsning til erhvervsmæssig spredning i dag kan være en utilstrækkelig strafferetlig beskyttelse, 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(15). 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 udtalelser m.v.

---

15. Dette er i overensstemmelse med, hvad arbejdsgruppen vedrørende datakriminalitet har foreslået.

2.4.2. Særlige eksempler på spredning

Spørgsmålet om spredning af børnepornografisk materiale behandles særskilt i afsnit 4.

De eksempler, der nævnes i det følgende, giver ikke anledning til forslag om ændring af de strafferetlige regler(16). De giver derimod anledning til overvejelser omkring, hvorvidt der kan være anledning til at forbedre mulighederne for at efterforske kriminalitet, der begås under anvendelse af store netsystemer. Der henvises til afsnit 5 og 6 vedrørende disse overvejelser.

---

16. Som eksempel på spredning kan også nævnes antisemitisk materiale. Ifølge en rapport af 4/3 1998 fra The InterParliamentary Council Against Antisemitism er der mere end 600 websites med denne type materiale, og tallet er voksende. Rådet opfordrer både til en effektiv strafferetlig beskyttelse, og til at Internetudbydere for så vidt angår krænkende, men ikke strafbart materiale, i videst mulig omfang ikke giver adgang til det.

2.4.2.1. Kursmanipulation og insiderviden

Ved børsreform I i 1986, insiderloven i 1991 og børsreform II i 1995 blev der henholdsvis indført meget omfattende generelle insiderregler og et generelt forbud mod kursmanipulation. Reglerne har en almindelig maksimumstraf på fængsel i 1 år og 6 måneder, men straffen kan stige til fængsel i 4 år ved forsætlig og særlig grov overtrædelse eller ved et større antal forsætlige overtrædelser. Der er tale om et område, der er blevet markant ny og opkriminaliseret i de senere år.

Sideløbende hermed er Internettet blevet et forum for udveksling af investeringsoplysninger. Brugerne kan på forskellige websites indlægge oplysninger om selskaber, investeringserfaringer m.v. - og de kan gøre det anonymt. Vil de være helt sikre på, at de ikke kan lokaliseres via registreringer af brugen i deres egen eller Internetudbyderes log over brugen, kan de enten bruge en PC, der er almindelig adgang til, eller de kan gå via dækadresser, hvor det oftest reelt vil være umuligt at finde frem til brugeren.

Kan man finde frem til den, der har videregivet insideroplysninger ved at lægge dem på Internettet, vil han kunne straffes efter værdipapirhandelloven. Tilsvarende gælder for brugere, der handler på baggrund af sådanne oplysninger - hvis man er i stand til at bevise, at de ikke betragtede oplysningerne som almindelig kendte. Det vil være nærliggende at betragte oplysningerne som offentliggjorte, når de er spredt ud på Internettet, selv om den korrekte fremgangsmåde via Fondsbørsen ikke er fulgt, ligesom en del brugere formentlig vil gå ud fra, at oplysningerne allerede er offentliggjort på korrekt vis.

De samme problemer opstår ved kursmanipulation, hvor især overtrædelse af værdipapirhandellovens § 34, stk. 3, nr. 1, jfr. § 39, om offentliggørelse eller udspredelse af urigtige oplysninger om en værdipapirudsteder, der er egnet til at påvirke kursen, kan tænkes at foregå via Internettets kommunikationsmuligheder. Tilsvarende gælder for straffelovens § 296, stk. 1, nr. 1, om udspredelse af løgnagtige meddelelser, hvorved prisen på varer, værdipapirer eller lignende genstande kan påvirkes.

I en sag fra foråret 1997 var der på en investeringswebside i Danmark indlagt en urigtig oplysning om, at en aktieanalyse var på vej, der ville anbefale aktiekøb i et selskab op til kurs 90, hvor kursen aktuelt lå på 75. Bl.a. på grund af manglende opbevaring af al relevant logning har det indtil nu ikke været muligt at identificere gerningsmanden.

I en sag fra USA gav gerningsmanden urigtige oplysninger om en mulig takeover på en tilsvarende website og rådede til aktiekøb, mens han selv solgte sine aktier i stedet.

Det må formodes, at straffebestemmelsen i værdipapirhandellovens § 94, der både dækker insiderhandel og kursmanipulation, giver mulighed for at henføre en spredning via Internettet til den kvalificerede bestemmelse om forsætlig, grov overtrædelse, der har et strafmaksimum på 4 år. Der er således en tilstrækkelig strafferetlig dækning også i relation til formidling af sådan information via Internettet.

Set i relation til netsystemerne er det efterforskningsmæssige et væsentligt problem i disse sagstyper, herunder især spørgsmålet om, hvorvidt den relevante logning fortsat eksisterer på efterforskningstidspunktet. For så vidt angår Internetudbyderes logning behandles dette spørgsmål i afsnit 5.1. Endvidere vil der i nogle sager kunne være behov for indgreb i meddelelseshemmeligheden, jfr. afsnit 6.5.

2.4.2.2. Markedsføring på eller via Internettet

Den almindelige markedsføring på Internettet - med de tilknyttede problemstillinger omkring muligheden for at kontrollere, at reglerne om moms og skat overholdes - behandles ikke i denne sammenhæng. Ved siden af den lovlige markedsføring af produkter og ydelser åbner Internettet imidlertid for nye muligheder i forbindelse med kriminalitet, der for at kunne begås kræver markedsføring.

Ud over de muligheder, der ligger i markedsføring direkte på nettet, er der også åbnet for en omfattende markedsføring via Internettet. I modsætning til traditionel direkte markedsføring, der er forbundet med betydelige portoudgifter, er det minimale omkostninger, der er forbundet med at emaile. Såkaldt junk mail eller spamming (uopfordrede email tilbud) er derfor blevet et tiltagende problem.

Ifølge EuropaParlamentet og Rådets direktiv af 20/5 1997 om forbrugerbeskyttelse i forbindelse med aftaler vedrørende fjernsalg[(17)] skal medlemslandene fastsætte regler om begrænsninger i anvendelsen af visse fjernkommunikationsteknikker. Der kræves forudgående forbrugersamtykke ved anvendelse af et automatisk opkaldssystem uden menneskelig medvirken (opkaldsautomat) og af telefax. For andre fjernkommunikationsteknikker, som tillader en individuel kommunikation, skal medlemsstaterne sørge for, at de kun kan anvendes, hvis forbrugeren ikke klart modsætter sig det. Efter direktivets artikel 3 og bilag II finder direktivet ikke anvendelse på visse finansielle tjenesteydelser, herunder investeringsservice og tjenester vedrørende termins og optionsforretninger.

Med hensyn til de ydelser, der er omfattet af investeringsservicedirektivet (ISD)[(18)], har Kommissionen afgivet en erklæring om, at den anerkender forbrugerbeskyttelsens betydning i forbindelse med aftaler om finansielle tjenesteydelser og vil undersøge, hvorledes forbrugerbeskyttelse kan integreres i politikken vedrørende finansielle tjenesteydelser. ISD artikel 13 indeholder følgende bestemmelse:

- "Bestemmelserne i dette direktiv er ikke til hinder for, at investeringsselskaber, der har fået meddelt tilladelse

i en anden medlemsstat, kan gøre reklame for deres tjenesteydelser med alle de kommunikationsmidler, som står til rådighed i værtslandet, dersom de overholder de regler for den pågældende reklames form og indhold, der er begrundet i hensynet til samfundsmæssige interesser."

---

17. 97/7/EF - fjernsalgsdirektivet.
18. Direktiv 93/22/EØF

De eksempler af strafferetlig relevans, der ses anvendt, har både form af markedsføring på Internettet og af junk mail.

Pyramidestrukturer (der bl.a. kendes fra de traditionelle indsamlingssager, hvor hver ny deltager skal få flere nye til at betale, mod at alle på et tidspunkt selv er modtagere) er et eksempel. Gerningsmand og gerningsland kan være svære at identificere, for Internetadressen kan være en dækadresse (eller sendt via en anonym remailer) og navnet forkert, selv om der kunne lokaliseres en adresse eller konto. Med hensyn til omfanget af udbydere bemærkes, at Forbrugerombudsmanden i oktober 1997 holdt "International Internet Sweep Day" (en søgning på Internettet efter aktuelle tilbud) sammen med 29 lande efter pyramidearrangementer, Multilevelmarketing og Networkmarketingkoncepter(19). Det resulterede for Danmarks vedkommende i, at Forbrugerombudsmanden skrev til 74 udbydere af betænkelige markedsføringskoncepter. Nogle af de mest graverende af disse sager er efterfølgende sendt til Rigsadvokaten(20). I september 1998 holdt over 30 lande en ny "International Internet Sweep Day". Danmark koncentrerede sig især om de såkaldte "getrichquick"sider. Der blev fundet tegn på pyramidespil eller vildledende markedsføring på 32 Internetsider, heraf 12 danske. Forbrugerombudsmanden har som tidligere i første omgang skrevet til de pågældende.

Advanced fee fraud er et andet eksempel. Forholdet består her i, at der tilbydes varer eller lån eller credit cards uden bankkontakt og sikkerhedsstillelse (eventuelt i kombination med en pyramidestruktur) mod forudbetaling af et relativt beskedent beløb, hvorefter der typisk lukkes ned, når der er modtaget tilstrækkeligt med penge, og helst før politiet underrettes og iværksætter efterforskning.

---

19. Sweep Day er omtalt på s. 17 i Forbrugerstyrelsens årsberetning for 1997. Det nævnes også, at sagerne blev indberettet til Erhvervsministeriet og Justitsministeriet, og at Forbrugerombudsmanden påpegede, at han fandt lovgivningen på området utilstrækkelig, både med hensyn til politiets efterforskningsmuligheder og med hensyn til at forbyde pyramidespil og pyramidearrangementer.
20. Rigsadvokaten har i fortsættelse heraf bedt Statsadvokaten for særlig økonomisk kriminalitet om at være ansvarlig for at koordinere efterforskningen i sager om pyramidespil m.v.

Også ved *investeringsbedragerier* - et område der i forvejen har tiltagende international karakter - anvendes Internettet. Det kan nævnes i den forbindelse, at de såkaldte "sidegadevekselerer", hvis virksomhed nu er omfattet af regler om tilladelse og tilsyn i EUlandene, uhindret kan fortsætte deres virksomhed fra et land, der ikke har tilsvarende reguleringer, og markedsføre via Internettet. Der kendes allerede eksempler herpå.

Spørgsmålet er, om den meget omfattende udbredelsesform via Internettet kvalificerer de handlinger, der allerede er strafbelagt.

Ofte vil der være tale om forhold, der er omfattet af straffelovens § 279 om bedrageri. Denne bestemmelse har en kvalificeret straffebestemmelse i straffelovens § 286, hvorefter den sædvanlige maksimumstraf på fængsel i 1 år og 6 måneder kan stige til 8 år, når forbrydelsen er af særlig grov beskaffenhed, eller når et større antal forbrydelser er begået. Udvalget er ikke bekendt med domme, hvor markedsføring via Internettet er indgået i tiltalen, men forsøg på via Internettet at nå en stor kreds af potentielle ofre enten ved generelt udbud eller ved at maile til potentielle kunder kan indgå i domstolenes vurdering af forholdenes grovhed.

Det bemærkes, at den til bedrageri krævede vildfarelse kan stamme fra indholdet af annoncering (bedrageri mod almenheden).

Desuden vil der kunne straffes for overtrædelse af markedsføringsloven, hvis markedsføringen sker til eller fra Danmark[(21)]. Muligheden for at læse indholdet i Danmark er næppe nok til, at loven kan anvendes, hvis indholdet ikke er målrettet mod Danmark.

Hvis man vil udtrykke, at markedsføring via Internettet bør være et særligt kvalificerende moment, kan man overveje at ændre straffelovens § 286, stk. 2, således, at der efter "når et større antal forbrydelser er begået" indsættes "eller er forsøgt begået" med tilhørende bemærkninger om, at der især er tænkt på markedsføring via Internettet eller tilsvarende brede forsøg.

Udvalget har overvejet dette spørgsmål, men ud fra den betragtning, at det må antages allerede at være gældende ret, og at en præcisering måske vil kunne medføre uheldige modsætningsslutninger på andre områder, har udvalget valgt ikke at foreslå ændringer.

Set i relation til netsystemerne kan der også i disse sagstyper være særlige efterforskningsmæssige problemer, herunder især spørgsmålet om, hvorvidt den relevante logning fortsat eksisterer på efterforskningstidspunktet. For så vidt angår Internetudbyderes logning behandles dette spørgsmål i afsnit 5.1. Endvidere vil der i nogle sager kunne være behov for indgreb i meddelelseshemmeligheden, jfr. afsnit 6.5.

---

21. Jfr. afsnit 2.3 om straffemyndighed.

KAPITEL 3 - ANSVAR FOR INDHOLDET AF INFORMATIONSSYSTEMER

Et spørgsmål, der har været aktuelt siden de tidlige BBS'er[(22)] startede med opskrifter på bomber og narkotika, oplysninger om passwords og calling cards m.v., er, om den, der administrerer BBS'et[(23)] - eller den aktuelle homepage på Internettet - kan gøres ansvarlig for indholdet. Det må i den forbindelse bemærkes, at som ved de ovennævnte investeringshomepages er situationen ofte den, at andre også uploader, og at indehaveren derfor ikke nødvendigvis ved, hvad han har liggende.

Har den pågældende selv indlagt strafbar information, kan der dømmes derfor, uanset om handlingen er knyttet til et netsystem eller ej. F.eks. dømtes en mand ved Københavns byrets dom af 15/6 1998 og Østre landsrets ankedom af 22/3 1999 for overtrædelse af straffelovens § 266 b for spredning af racistiske ytringer, idet han havde indlagt adskillige racistiske udtalelser på en website for en nyhedsgruppe.

Den svenske højesteret har i en dom af 22/2 1996[(24)] antaget (efter domfældelse i byretten og frifindelse i landsretten), at sysop'en ikke kunne gøres ansvarlig, når hans eneste aktivitet bestod i, at ophavsretligt beskyttede programmer kunne downloades fra hans BBS. Tiltalen lød på, at sysop'en havde gjort programmerne tilgængelige for almenheden. Højesteret anførte, at der var en åbenbar mangel i den ophavsretlige beskyttelse af programmer[(25)].

Igen ligger problemstillingen i udbredelsen. Man kan også gå på biblioteket og finde opskrifter på mange ting, så forskelligheden beror for noget af indholdets vedkommende mere på, at man typisk her udbreder til en større kreds, der har let adgang til materialet fra deres PC, og som måske føler sig fristet til at afprøve opskrifterne[(26)]

Formidling af opskriften på eller oplysningen om noget, der kan benyttes til at begå noget strafbart, er ikke efter den almindelige fortolkning af forsøgs og medvirkensbestemmelserne i straffelovens § 21 og § 23 generelt omfattet af disse bestemmelser. Hvis selve indholdet er strafbart (f.eks. børnepornografi eller salg af tyvekoster), vil sysop'en eller indehaveren af homepagen antagelig kunne dømmes for medvirken ved passivitet, hvis hans kendskab (evt. burde viden) til indholdet kan bevises. Hans ejerskab vil formentlig betyde, at han har en handlepligt, dvs. at han skal slette indhold, der realiserer gerningsindholdet i en straffebestemmelse.[(27)]

[22.] Bulletin Board Systems eller elektroniske opslagstavler.

[23.] Kaldet sysop'en (systemoperatøren).

[24.] "BBSmålet", NJA 1996 s. 79.

[25.] Ifølge Thomas CarlénWendels, Nätjuridik - Lag och rätt på Internet, Juristförlaget 1997, s. 52, er dommens resultat omdiskuteret i Sverige.

[26.] Ikke mindst tilvirkning af bomber er meget udførligt beskrevet i "The Terrorist's Handbook", der i hvert fald siden 1993 har cirkuleret på BBS'er m.v. I forbindelse med en hærværkssag om sprængning af hjemmelavede bomber oplyste én af de afhørte, at han havde fremstillet og sprængt bomber, og at han havde opskriften fra den nævnte håndbog, der lå på en PC på en dansk erhvervsskole.

[27.] Der kan i den forbindelse henvises til UfR 1996.209 H, hvor udgiveren af et annoncehæfte (der ikke var omfattet af medieansvarsloven) blev idømt en bøde for overtrædelse af markedsføringsloven ved medvirken til en annoncørs reklamering med ulovlig tilgift. Det siges ved Højesterets vurdering af, om den pågældende havde udvist uagtsomhed: "Højesteret finder det herved afgørende, om tiltalte ved et umiddelbart gennemsyn af annoncerne - et gennemsyn, som det naturligt må påhvile en udgiver af et annoncehæfte at foretage som en rutine - burde have indset, at der i de pågældende annoncer utvivlsomt reklameredes med ulovlig tilgift."

Formidling af opskrifter og hjælpemidler kan under særlige omstændigheder være strafbar, jfr. Roskilde rets dom af 19/12 1996, hvor der dømtes for forsøg på medvirken til hacking i et tilfælde, hvor der var en udtrykkelig opfordring til en mindre, kendt kreds til at prøve (og til ikke at ændre) passwords, der var lagt på BBS'et.

Derudover kan man overveje, om de stort set aldrig brugte bestemmelser i straffelovens § 136 og § 266 a kan udstrækkes til at omfatte dele af indholdet.

Efter straffelovens § 136, stk. 1, straffes den, som uden derved at have forskyldt højere straf offentlig tilskynder til forbrydelse, med op til 4 års fængsel. Det antages, at § 136, stk. 1, er uanvendelig ved mindre alvorlige lovovertrædelser. Efter straffelovens § 266 a straffes den, der, uden at forholdet omfattes af §§ 136 og 266, offentligt fremsætter udtalelser, der tilstræber at fremkalde voldshandlinger eller hærværk, med op til 1 års fængsel. Straffelovens § 136 er brugt i UfR 1938.407 Ø, hvor en redaktør blev dømt for i en artikel om et bombeattentat mod forsvarsministerens villa delvis indirekte at have opfordret til at anvende kraftigere bomber over for ministre. Straffelovens § 266 a er brugt i Odense rets dom af 1/7 1986, hvor en politiker blev dømt for i en valgudsendelse i tv at have fremsat udtalelser, der tilstræbte ødelæggelse af karlitlofter i skoler og institutioner.

Udvalget er ikke bekendt med andre domme om overtrædelse af disse bestemmelser. Bestemmelserne er klart forudsat at kunne anvendes, hvor betingelserne for at dømme for forsøg på medvirken ikke er opfyldt, men de indeholder begge et tilskyndelses/tilstræbningsmoment, der nok skal være mere målrettet end det typiske indhold på et BBS eller en homepage. Derimod vil offentlighedskravet formentlig være opfyldt i langt de fleste tilfælde, hvor der distribueres via BBS eller Internettet.

Selv om der i nogle tilfælde således vil kunne dømmes for medvirken til et strafbart indhold ved passivitet og i særlige tilfælde for forsøg på medvirken til den forbrydelse, indholdet (password, calling card o.l.) kan bruges til, og selv om det kunne være af interesse ved et særligt opfordrende indhold at afprøve en eventuel anvendelse af straffelovens § 136 og § 266 a, er der for en del af indholdet af opskrifter eller passwords o.l. næppe nogen anvendelig straffebestemmelse.

Det skal dog anføres, at indehaveren - såfremt han har (eventuelt burde have) kendskab til indholdet - vil blive dækket af de af udvalgets forslag, der regulerer spredning til en større kreds, i det omfang der er tale om et kriminaliseret indhold.

Man kunne overveje at opstille et krav om, at informationssystemer såsom BBS'er og homepages skal underkastes et anmeldelseskrav. I tilknytning til en sådan ordning kunne man f.eks. stille betingelse om kontrolforanstaltninger mod informationer af retsstridigt eller anstødeligt indhold. Regler af et sådant indhold kan dog tænkes at komme i strid med de principper, der er udtrykt ved reglerne om den formelle ytringsfrihed i grundlovens § 77 og i Den Europæiske Menneskerettighedskonventions artikel 10. Hertil kommer, at en regulering, der i realiteten kun er anvendelig ved nationale BBS'er - selv om den tillige krævede, at sysop'en havde pligt til at være bekendt med indholdet - næppe vil få den fornødne gennemslagskraft, når Internettets internationale struktur tages i betragtning. Endvidere er det praktisk umuligt for en sysop løbende at gøre sig bekendt med alt det materiale, som der kan

skaffes adgang til over sådanne. Endelig er det vanskeligt at afgrænse BBS'er og homepages og gennemføre kontrolforanstaltninger, når et stort antal private og juridiske personer etablerer sådanne.

Sverige har i 1998 vedtaget en lov [(28)] om ansvar for elektroniske opslagstavler. Lovens § 1 definerer en elektronisk opslagstavle som en tjeneste til elektronisk formidling af meddelelser, hvor der ved meddelelser forstås tekst, billede, lyd eller information i øvrigt. Efter lovens § 2 gælder loven ikke for almindelig kommunikation, interne formidlinger, tjenester, der er beskyttet af trykkefrihedsforordningen eller ytringsfrihedsgrundloven, eller email. Efter lovens § 3 skal indehaveren af en elektronisk opslagstavle underrette den, der tilslutter sig, om sin identitet og om, i hvilken udstrækning indkomne meddelelser bliver tilgængelige for andre brugere. Efter lovens § 4 skal den, der administrerer (tillhandahåller) en elektronisk opslagstavle, for at kunne opfylde sin pligt efter § 5, have et sådant overblik over tjenesten, som med rimelighed kan kræves under hensyntagen til virksomhedens omfang og indretning.

Lovens § 5 indeholder den centrale pligt: Den, der administrerer den elektroniske opslagstavle, skal fjerne eller forhindre videre spredning af en indlagt meddelelse, hvis indholdet åbenbart er af en art som anført i angivne §'er i den svenske straffelov: Agitation, ophidselse mod folkegrupper, børnepornografi og ulovlig voldsskildring, eller hvis det er åbenbart, at der er tale om en ophavsretskrænkelse.

Efter lovens § 6 straffes overtrædelse af § 3 med bøde. Efter lovens § 7 straffes overtrædelse af § 5 - medmindre forholdet er omfattet af straffeloven eller ophavsretsloven - med bøde eller fængsel i højst 6 måneder, der i grove tilfælde kan stige til fængsel i højst 2 år, mens straffen i mindre sager kan bortfalde. Efter lovens § 8 kan udstyr, der er anvendt ved overtrædelser af § 7, konfiskeres for at forebygge yderligere kriminalitet, eller hvis der i øvrigt foreligger særlige grunde.

Den danske medieansvarslov indeholder en mulighed for, at massemedier i form af tekster, billeder og lydprogrammer, der periodisk udbredes til offentligheden, efter anmeldelse til Pressenævnet kan blive omfattet af loven, hvis de har karakter af nyhedsformidling[(29)]. Det nævnes i lovforslagets bemærkninger[(30)], at det kun er ved envejskommunikation, hvor modtageren ikke kan påvirke produktet, at der er mulighed for at begrænse ansvarsplaceringen til bestemte personer.

---

28. Lag (1998:112) om ansvar för elektroniska anslagstavlor. Loven bygger på forslaget i betænkning SOU 1996:40 om elektronisk dokumenthantering fra IT-utredningen, der i let ændret form blev fremsat som regeringens proposition 1997/98:15 af 2/10 1997.
29. Jfr. § 1, nr. 3, og § 8 i medieansvarsloven, lov nr. 348 af 6/6 1991 med senere ændringer.
30. FT 1990/91 A 3047

Det fremgår i øvrigt af lovforslaget, at medieansvarudvalgets flertal havde foreslået, at der indførtes en bestemmelse om objektivt bødeansvar for selve medieforetagendet ved visse grove freds og ærekrænkelser. Mindretallet fandt derimod bl.a., at der var grund til at frygte, at en ændret ansvarsordning ville påvirke den redaktionelle frihed. Justitsministeriet tilsluttede sig mindretallet bl.a. under henvisning til, at det ville indebære en latent risiko for en langt videregående afsmittende virkning for informationsfriheden her i landet.

Medieudvalget har senere behandlet Internetspørgsmålet i en betænkning fra 1996[(31)]. Det siges[(32)] om indholdet af Internet indledningsvis, at "der er tale om et område, hvor hovedparten af udviklingen hverken kan styres eller reguleres". Det anføres, at man kan diskutere, om der er behov for ansvarsregler for indholdet af Internet i lighed med medieansvarslovens regler, og at en sådan ansvarsregulering i givet fald burde fokusere på den personkreds, der i relation til massemedierne betragtes som "den ansvarshavende redaktør".

Medieudvalget anbefaler[(33)], at Internetudgivelser, som kan sammenlignes med traditionelle massemedier, gennem anmeldelse til Pressenævnet lader sig omfatte af medieansvarsloven. Udvalget finder derimod ikke, at der er grund til at ændre på den gældende retstilstand med hensyn til indholdsmæssig regulering af Internet. Udvalget henviser dels til, at dette ville have censurlignende karakter, og dels til de administrationsmæssige vanskeligheder.

---

31. Betænkning nr. 1320/1996 om medierne i demokratiet.

32. Betænkningen s. 432 ff.
33. Betænkningen s. 438 f.

Udvalget har drøftet behovet og mulighederne for regulering af ansvaret for indholdet af informationssystemer. I det omfang udbredelsen i en videre kreds (f.eks. via Internettet) sidestilles med erhvervsmæssig udbredelse i straffebestemmelser herom - jfr. afsnit 2.4.1 - vil dette dække en del af reguleringsbehovet. Disse lovændringer får imidlertid ikke betydning for udbredelse af oplysninger, hvor udbredelsen ikke i dag er strafbar. Det gælder f.eks. opskrifter på bomber og syntetisk narkotika. Og lovændringerne indebærer ikke i sig selv nogen pligt for administrator til at undersøge, hvad der er lagret af information.

Udvalget finder imidlertid, at den i afsnit 2.4.1 beskrevne regulering (jfr. herved som eksempel afsnit 4.4.2 om børnepornografi) dækker den væsentligste del af det område, hvor en regulering kan komme på tale. Uanset at det i særlige sammenhænge kan være ønskeligt, finder udvalget ikke anledning til at foreslå lovændringer vedrørende udbredelse af oplysninger om kemiske processer eller andre oplysninger, som det i dag ikke er ulovligt at udbrede, selv om de vil kunne have skadelig virkning i kraft af modtagerens anvendelse af oplysningerne. Det vil bl.a. være vanskeligt at afgrænse, under hvilke omstændigheder udbredelse af oplysningerne burde være lovlig, f.eks. i forskningsmæssige sammenhænge.

Med hensyn til at etablere en registreringsordning og en særlig undersøgelsespligt med hensyn til, hvad der uploades, finder udvalget, at man med den nuværende IT-struktur næppe kan opnå det ønskede formål i et bare rimeligt omfang med en sådan regulering. Det ville formentlig kun betyde, at man distribuerede uden for dansk jurisdiktion ved at up og downloade fra en fremmed homepage. En sådan regulering ville endvidere være i klar strid med de principper, der traditionelt har ligget til grund for reglerne om, at post og telefonvæsen ikke er ansvarlige for indholdet af de meddelelser, der formidles via disse systemer, og at indholdet af det formidlede ikke overvåges.

Sammenfattende finder udvalget, at reguleringen bør begrænses til det i afsnit 2.4.1 skitserede, der - hvis den nødvendige tilregnelse i form af forsæt eller uagtsomhed kan bevises - regulerer den væsentligste del af området[(34)] [(35)].

---

34. Spørgsmålet om ansvar for Internetudbydere behandles i et direktivforslag af 23/12 1998 (KOM(1998) 586 endelig udg. (EFT 1999 C 30/4)) om visse retlige aspekter af elektronisk handel i det indre marked. Efter artiklerne 1214 i dette forslag skal alle typer af Internetudbydere, jfr. afsnit 2.1, som hovedregel være anvarsfri i relation til transmissioner, de ikke har indflydelse på. For så vidt angår hosts er det dog en forudsætning, at hosten ikke har viden om ulovlig aktivitet uden at reagere derpå. Det foreslås i artikel 15, at medlemsstaterne ikke generelt må forpligte Internetudbyderne til at overvåge den information, de formidler
35. Arbejdsgruppen vedrørede datakriminalitet fandt ligeledes, at der ikke var behov for en mere vidtgående regulering.

KAPITEL 4 - STRAFFELOVENS 235 OM BØRNEPORNOGRAFI

4.1. Bestemmelsens forhistorie

Frem til 1969, hvor straffen for billedpornografi blev ophævet[(36)], var børnepornografi strafbar på lige fod med anden billedpornografi. Ved ophævelsen af pornografibestemmelsen i straffelovens § 234, der bl.a. vedrørte offentliggørelse eller udbredelse af utugtige billeder, forsvandt ligeledes hjemlen til at straffe offentliggørelse og udbredelse af børnepornografiske billeder.

Derimod har produktionen af børnepornografiske billeder m.m. til stadighed været kriminaliseret. Der vil i disse tilfælde altid ske overtrædelse af en eller flere bestemmelser i straffelovens kapitel 24, i det mindste af straffelovens

§ 232 om blufærdighedskrænkelse, herunder for medvirken. Såfremt eksisterende optagelser, der ikke selvstændigt opfylder kravene, sammenkædes på en måde, så helhedsresultatet bliver pornografisk, vil straffelovens § 264 d kunne anvendes.

I 1980[(37)] indsattes en bestemmelse, der indholdsmæssigt svarede til den nugældende § 235, stk. 1, men kun gav mulighed for bødestraf. Begrundelsen for bestemmelsen[(38)] var, at det i praksis var vanskeligt at gennemføre en straffesag for optagelsen, hvis billederne var optaget i udlandet. En del af de hørte myndigheder m.m. vendte sig direkte mod en kriminalisering af denne art. Der pegedes blandt andet på de fra de tidligere bestemmelser velkendte afgrænsningsproblemer. Der var også uenighed om strafferammen[(39)]. Flere statsadvokater udtalte sig til fordel for en bødebestemmelse; rigsadvokaten, statsadvokaten i København og politidirektøren gik ind for et strafmaksimum på 6 måneders fængsel. Straffelovrådet pegede på, at en viden om pornografiske billeders kriminalitetshæmmende virkning må medinddrages i overvejelserne om en nykriminalisering kunne begrundes.

---

36. Ved lov nr. 224 af 4/6 1969.

37. Ved lov nr. 252 af 16/6 1980.

38. Jfr. lovforslaget, FT 1979/80, 2. samling, A 1761.

39. Det lovudkast, der var udsendt til høring, lød således: "§ 235. Den, som offentliggør, sælger eller på anden måde udbreder eller i sådan hensigt fremstiller eller skaffer sig utugtige billeder af børn, straffes med bøde (hæfte eller fængsel indtil 6 måneder)."

Straffelovrådet indhentede en redegørelse fra Berl Kutchinsky. Hans konklusion på en indgående analyse var:

- "Det må siges ganske utvetydigt, at vi ikke med sikkerhed kan fastslå, at der er en præcis og direkte årsagssammenhæng mellem pornografi og seksuelle overgreb mod børn. ¿ Men der findes et stort antal indicier på, at en sådan sammenhæng [mellem udbudet af børnepornografi og et fald i antallet af sædelighedsforbrydelser mod børn] eksisterer."

Han skønnede, at man måske forhindrede ca. 50 kriminelle overgreb på børn i Danmark om året gennem den tilgængelige børnepornografi.

Straffelovrådets hovedsynspunkt var:

- "Det synspunkt, der kunne begrunde en straffebestemmelse om fremstilling og udbredelse af børnepornografi, må være et ønske og en forventning om, at man på denne måde kan bidrage til at forebygge, at børn benyttes til optagelser, der i sig selv udgør strafbare forhold. Et forbud mod udbredelse skal have det formål at formindske efterspørgslen efter sådanne optagelser og dermed bidrage til at modvirke forekomsten af strafbare krænkelser af børn."
- Det udtaler videre, at "nykriminalisering i almindelighed [må] forudsætte et nogenlunde solidt grundlag for at antage, at anvendelsen af strafferetlige midler vil have overvejende gavnlige virkninger. Det kan diskuteres, om en kriminalisering af børnepornografi på indeværende tidspunkt er tilstrækkeligt begrundet, ¿".

Straffelovrådet fandt, at bestemmelsen kun skulle dække det erhvervsmæssige salg og den erhvervsmæssige udbredelse, og at der kun skulle være bødestraf. Den gennemførte bestemmelse svarede til Straffelovrådets forslag:

- "*§ 235*. Den, som erhvervsmæssigt sælger eller på anden måde udbreder eller med forsæt hertil fremstiller eller skaffer sig utugtige fotografier, film eller lignende af børn, straffes med bøde."

Straffelovrådet afgav i 1987 en betænkning[(40)], der indeholdt en generel gennemgang af straffelovens strafferammer. § 235 bruges heri udtrykkeligt[(41)] som eksempel på en af de bestemmelser, hvorom det "uden videre [kan] fastslås, at de er af en så lidet alvorlig karakter, at de ikke bør kunne straffes med mere end en bøde eller allerhøjest med en kort frihedsstraf". Det nævnes videre[(42)], at den eneste grund til at anbringe § 235 i straffeloven er, "at der ikke findes nogen særlov, i hvilken straffebestemmelsen naturligt kan anbringes."

I 1989[(43)] ændredes strafferammen til bøde, hæfte eller fængsel indtil 6 måneder. Justitsministeriet skrev i

bemærkningerne til lovforslaget[(44)]:

- "Siden forbudet mod handel med børnepornografi blev optaget i straffelovens § 235 i 1980, har der kun været et begrænset antal sager om overtrædelse af forbudet. Uanset om der aktuelt kan påvises noget praktisk behov for en strafferammeskærpelse, kan man generelt rejse det spørgsmål, om en strafferamme med bøde for denne type kriminalitet fortsat kan anses for passende og tidssvarende, også med hensyn til de groveste former, som denne forbrydelse kan fremtræde i.
- Efter regeringens opfattelse er handel med børnepornografi en forbrydelse, der må ses på med større alvor, end den nugældende strafferamme med bøde er udtryk for."

---

40. Betænkning nr. 1099/1987 om strafferammer og prøveløsladelse.
41. Betænkningen s. 92.
42. Betænkningen s. 100.
43. Ved lov nr. 272 af 3/5 1989.
44. FT 1988/89 A 2858.

Lovændringen harmonerede med de internationale drøftelser om beskyttelse af børn, der samme år resulterede i artikel 34 i FNs konvention af 20/11 1989 om barnets rettigheder, hvorefter deltagerstaterne skal beskytte børn mod alle former for seksuel udnyttelse og seksuelt misbrug og med henblik herpå især tage alle passende nationale, bilaterale og multilaterale forholdsregler for at forhindre:

a) at et barn overtales eller tvinges til at deltage i nogen form for ulovlig seksuel aktivitet;

b) at børn udnyttes til prostitution eller andre former for ulovlig seksuel aktivitet;

c) at børn udnyttes i pornografiske forestillinger og materialer.

Europarådet anbefalede i rekommandation nr. R (91) 11 medlemslandene at overveje det tilrådelige i at kriminalisere besiddelse af børnepornografi, og i FNs Menneskerettighedskommissions resolution 1992/74 opfordredes medlemslandene til at kriminalisere besiddelsen af børnepornografi. Endvidere anbefalede Nordisk Råd i rekommandation 9/1994 en kriminalisering i Norden af besiddelse af børnepornografi.

I 1994[(45)] indsattes bestemmelsens stk. 2, der kriminaliserer besiddelsen af grovere former for børnepornografi:

- "Stk. 2. Den, som besidder fotografier, film eller lignende af børn, der har samleje eller anden kønslig omgængelse end samleje, straffes med bøde. På samme måde straffes den, som besidder fotografier, film eller lignende af børn, der har kønslig omgang med dyr, eller som anvender genstande på groft utugtig måde."

Begrundelsen for lovforslaget[(46)] var især:

- "På baggrund af, at produktion af børnepornografi i mange tilfælde sker ved grove alvorlige strafbare handlinger mod børn, kan det virke stødende, at besiddelsen af materialet ikke er strafbar. Et forbud mod besiddelse af børnepornografisk materiale markerer en klar afstandtagen fra seksuelt misbrug af børn, samtidig med at det bidrager til at værne børns rettigheder. Dertil kommer, at et forbud mod besiddelse muligvis vil kunne medføre en vis begrænsning af efterspørgslen efter børnepornografisk materiale og dermed også produktionen og de dertil knyttede seksuelle overgreb mod børn."

Med hensyn til afgrænsningen af det omfattede pornografiske materiale nævnes, at

- "Derved tilsigtes en afbalanceret løsning, der på den ene side rammer billeder optaget i forbindelse med, at der er begået alvorlige strafbare handlinger over for børn, mens besiddelsen af mindre grove billeder fortsat vil være tilladt og muligvis kan have en kriminalitetsdæmpende effekt."
- "Justitsministeriet foreslår endvidere, at strafferammen bliver bøde. Det indebærer, at politiet afskæres fra at foretage ransagning af en ikkesigtets bolig, rum eller gemmer med henblik på for eksempel beslaglæggelse af

børnepornografisk materiale .¿. Formålet med denne del af forslaget er i videst muligt omfang at værne den enkelte mod indgreb i privatlivets sfære. Forslaget udelukker imidlertid ikke, at der efter omstændighederne kan foretages ransagning hos en person, der er sigtet for besiddelse af børnepornografisk materiale¿"

---

45. Ved lov nr. 1100 af 21/12 1994.
46. FT 1994/95 A 467

Det nævnes i lovforslaget, at spørgsmålet om, hvornår der foreligger besiddelse, undertiden kan give anledning til tvivl, navnlig hvor materialet udbredes via elektroniske midler. Det siges herom:

- "Ved betragtning af tvudsendelser (eksempelvis sendt via satellit) eller billeder, der overføres fra en database til egen edbskærm, vil billedet ikke kunne siges at være i betragterens besiddelse. Er der derimod tale om, at billedet lagres, det være sig på videobånd, harddisk, diskette eller lign., således at den pågældende selv kan kalde billedet frem igen, må materialet anses for at være i vedkommendes besiddelse."

Bestemmelsen har herefter i dag følgende ordlyd:

- "§ 235. Den, som erhvervsmæssigt sælger eller på anden måde udbreder eller med forsæt hertil fremstiller eller skaffer sig utugtige fotografier, film eller lignende af børn, straffes med bøde, hæfte eller fængsel indtil 6 måneder.
- *Stk. 2*. Den, som besidder fotografier, film eller lignende af børn, der har samleje eller anden kønslig omgængelse end samleje, straffes med bøde. På samme måde straffes den, som besidder fotografier, film eller lignende af børn, der har kønslig omgang med dyr, eller som anvender genstande på groft utugtig måde."

Folketinget har den 19/11 1998 behandlet 3 forslag om ændring af straffelovens § 235:

- 1. Beslutningsforslag af 27/10 1998(47) opfordrer Justitsministeren til snarest at fremsætte lovforslag bl.a. om ændring af straffelovens § 235 således at:
- 1) Strafmaksimum for erhvervsmæssig udbredelse forhøjes til fængsel i 3 år.
- 2) Bytning sidestilles med erhvervsmæssig udbredelse,
- 3) Enhver besiddelse er strafbar uanset materialets grovhed.
- 1. Beslutningsforslag af 27/10 1998(48) opfordrer Justitsministeren til, at strafmaksimum i straffelovens § 235 forhøjes til fængsel i 3 år inden udgangen af folketingsåret.
- 2. Lovforslag af 12/11 1998(49) forslår, at straffelovens § 235 ændres således at:
- 1) Strafmaksimum i stk. 1 forhøjes til fængsel i 6 år.
- 2) Strafmaksimum i stk. 2 forhøjes til fængsel i 6 måneder.

- 47. B 22 (KRF), FT 1998/99 A 1618.
  48. B 24 (KF), FT 1998/99 A 1625.
  49. Nr. L 83 (DF), FT 1998/99 A 2095.

4.2. Omfanget af bestemmelsens brug

Antallet af anmeldelser vedrørende overtrædelser af straffelovens § har siden 1995 været stigende. De registrerede anmeldelsestal for perioden 19921998 har været følgende(50):

1992: 7 anmeldelser; 1993: 7 anmeldelser; 1994: 5 anmeldelser; 1995: 6 anmeldelser; 1996: 23 anmeldelser; 1997: 28 anmeldelser og 1998: 36 anmeldelser. De reelle anmeldelsestal for 1997 og 1998 er dog væsentlig større, jfr. det nedenfor oplyste om anmeldelser til Rigspolitichefen.

For nogle af anmeldelserne og de senere domme er der tale om sager i et større samlet sagskompleks, hvorfor

anmeldelsestallene ikke i alle tilfælde giver et fuldstændigt korrekt billede af mængden af sager. Tendensen vedrørende antallet af sager er dog yderst klar. Anmeldelsestallene for 1997 og 1998 skal ses i sammenhæng med en række henvendelser til Rigspolitichefens hjemmeside, jfr. nedenfor, der i denne periode ikke er blevet opdateret som anmeldelser og derfor ikke indgår i den almindelige statistik over anmeldelser. Det er nærliggende at antage, at denne stigning, i hvert fald delvist, kan forklares med en stigende brug af Internettet i samme periode.

I perioden 1992-1997 fordeler antallet af domfældelser[(51)] sig som følger:

1992: 3 domfældelser; 1993: 2 domfældelser; 1994: 1 domfældelse; 1995: 3 domfældelser; 1996: 10 domfældelser og 1997: 13 domfældelser.

---

50. Tallene stammer fra politiets kriminalregister.

51. Med under domfældelser regnes også bødeforlæg og afgørelser efter straffelovens §§ 6870.

Blandt de afgjorte sager kan som eksempler nævnes følgende:

- *Aalborg rets dom af 16/3 1993*
  Der var rejst tiltale for 4 forhold af straffelovens § 235, heraf 1 som forsøg og 2 som medvirkende. Der blev dømt for et forhold, hvor tiltalte i digitaliseret form havde lagret utugtige billeder af børn på en database, hvortil andre mod betaling kunne få adgang. Ved bevisførelsen fandtes det ikke nærmere fastlagt, i hvilket omfang der var sket salg eller anden udbredelse, udover at der var konstateret foretaget et betydelig antal træk på fotografierne og udbredelsen må antages at være sket til en større personkreds i mange lande. Tiltalte havde endvidere solgt fotografier på diskette. I de 3 andre forhold blev tiltalte frifundet. Tiltalte blev idømt en straf på 40 dages hæfte.
- *Lemvig rets dom af 14/2 1997*
  Der var rejst tiltale for overtrædelse af både § 235, stk. 1 og stk. 2. Vedrørende stk. 1 udtalte retten, at det kan lægges til grund, at tiltalte oprettede en database med det formål, at brugere via telefonnettet kunne skaffe sig adgang til databasen og se eller hente billeder mod senere vederlag. Brugere kunne kun downloade de billeder, der var angivet i fillisten. Retten lagde til grund, at filen ikke var tilgængelig for brugere, hvorfor det ikke fandtes bevist, at tiltalte havde forsøgt erhvervsmæssigt at udbrede utugtige billeder af børn. For overtrædelse af stk. 2 idømtes tiltalte 10 dagbøder à 200 kr., idet han havde været i besiddelse af et billede af børn, som var omfattet af stk. 2.
- *Københavns byrets dom af 23/9 1997*
  Der var rejst tiltale for overtrædelse af straffelovens § 235, stk. 2, (og straffelovens § 284, jfr. §§ 276 og 279 a samt § 286, jfr. § 279 a). Overtrædelsen af § 235, stk. 2, vedrørte besiddelse af 2 billeder af børn omfattet af bestemmelsen. Tiltalte blev straffet for besiddelse af det ene billede. Tiltalte blev endvidere dømt for overtrædelse af de andre anførte bestemmelser. Straffen blev fastsat til 1 års betinget fængsel.
- *Vordingborg rets dom af 24/9 1997*
  Den tiltalte var bl.a. tiltalt for gennem ca. 4 måneder med forsæt til erhvervsmæssigt salg eller anden udbredelse bl.a. via Internettet at have sat sig i besiddelse af ikke under 533 børnepornografiske fotografier og gennem 5 dage at have udbredt ca. 40 fotografier bl.a. via Internettet. Den tiltalte blev frifundet for tiltalen vedrørende straffelovens § 235, stk. 1, fordi der ikke var grundlag for at antage, at han havde noget erhvervsmæssigt sigte med udbredelsen, men blev dømt for overtrædelse af bestemmelsens stk. 2. (Den tiltalte blev idømt 14 dagbøder à 150 kr.).
- *Østre landsrets dom af 10/12 1998*
  Der var rejst tiltale for overtrædelse af straffelovens § 235, stk. 2, (og straffelovens § 210, § 216, § 222, § 224 og § 232). For så vidt angik overtrædelse af § 235, stk. 2, var der rejst tiltale for at have besiddet mange billeder/fotografier samt flere videofilm, indeholdende børnepornografi omfattet af bestemmelsen. Tiltalte erkendte forholdet. Der blev endvidere dømt for hovedparten af anklageskriftets øvrige forhold. Straffen blev fastsat til fængsel i 5 år.

Siden medio 1997 har der været mulighed for brugere af Internettet for at henvende sig til såkaldte "hotlines", hvis de får mistanke om børnepornografi over Internettet. Den første hotline blev etableret medio 1997 af Red Barnet, der efter aftale med Rigspolitichefens IT-støtteenhed videresender alle henvendelser til enheden. Der blev modtaget ca. 700 henvendelser i 1997 og 1025 i 1998. I august 1998 etablerede Rigspolitichefen på sin hjemmeside en

service, hvortil borgerne kan anmelde IT-relateret kriminalitet, herunder børnepornografi på Internettet. Der er siden da modtaget 350 henvendelser om børnepornografi (pr. 12/1 1999). Nogle få Internetudbydere har tillige iværksat hotlines, hvortil deres kunder kan henvende sig vedrørende ulovligheder. En af disse udbydere har videregivet 86 henvendelser (pr. 12/1 1999), som udbyderen har modtaget siden ordningens start i juli 1998. Efter det af Rigspolitichefens IT-støtteenhed oplyste vedrører alle henvendelserne børnepornografi, og det hører til den absolutte undtagelse, at et site med børnepornografi anmeldes flere gange.

Ifølge Rigspolitichefens IT-støtteenhed afhænger omfanget af den enkelte sag af, hvilken type persongruppe der er involveret. Hos enheden opdeler man persongrupperne i tre hovedgrupper:

- Nysgerrige der grundet omtale af problemet søger efter materiale på Internettet og opbygger en begrænset samling, som kan indgå i forbindelse med udveksling af pornografisk materiale i øvrigt på Internettet. I disse sager indgår der fra nogle ganske få billeder til nogle hundrede.
- Samlere med pædofile tilbøjeligheder, hvis hovedinteresse er rettet mod utugtigt billedmateriale, og som søger at komme ind i de lukkede egentlige pædofile globale sammenslutninger. Der er danske eksempler på, at sådanne samlere har billedsamlinger indeholdende 10.000-40.000 billeder.
- Pædofile med tilknytning til en eller flere lukkede globale sammenslutninger, hvor forudsætningen for deltagelse er at frembyde nyt billedmateriale i form af digitale fotos eller videoklip samt "liveoptagelser" vist for en større eller mindre del af sammenslutningens medlemmer.

Med hensyn til den sidstnævnte type gruppe blev der den 3/9 1998 gennemført en samlet aktion mod nogle hundrede mistænkte, hvoraf 78 blev anholdt. Myndighederne i 19 lande gennemførte i forening aktionen. Der blev ikke foretaget anholdelser i Danmark. I den gruppe, som aktionen var rettet mod, var det en forudsætning for at opretholde medlemsskabet, at man løbende skulle tilføre den samlede gruppe nye utugtige billeder, som man ikke tidligere havde set. Denne omstændighed indebar, at der til stadighed skulle produceres nyt materiale.

4.3. Andre landes regulering

4.3.1. Norsk ret

Den norske straffelov indeholder følgende bestemmelse:

- "§ 211. Med bøter eller med fengsel inntil 2 år eller med begge deler straffes:
- a) den som holder offentlig foredrag eller istandbringer offentlig forestilling eller utstilling av utuktig eller pornografisk innhold,
- b) den som utgir, frambyr til salg eller leie eller på annen måte søker å utbre, eller som med hensikt å foreta slik utbredelse innfører utuktige eller pornografiske skrifter, bilder, filmer, videogram eller lignende,
- c) den som overlater utuktige eller pornografiske skrifter, bilder, film, videogram og liknende til personer under 18 år,
- d) den som besitter eller innfører bilder, film, videogram eller lignende, hvor noen som er, må regnes å være eller fremstilles som å være under 16 år, er vist på en utuktig eller pornografisk måte.
- Med utuktige eller pornografiske skildringer menes i denne paragraf kjønnslige skildringer som virker støtende eller på annen måte er egnet til å virke menneskelig nedverdigende eller forrående, herunder kjønnslige skildringer med bruk av barn, dyr, vold, tvang og sadisme.
- Medvirkning straffes på samme måte.
- Med bøter eller fengsel inntil 6 måneder eller begge deler straffes den som av uaktsomhet foretar noen sådan handling som er nevnt i denne paragraf.
- På samme måte straffes den innehaver eller overordnede som forsettlig eller av uaktsomhet unnlater å hindre at det i en virksomhet blir foretatt handling som nevnt i denne paragraf.
- Ved straffeutmålingen legges det i skjerpende retning vekt på om de utuktige eller pornografiske skildringer omfatter bruk av barn, dyr, vold, tvang og sadisme.
- Paragrafen gjelder ikke for film eller videogram som Statens filmkontrol ved forhåndskontroll har godkjent til ervervsmessig framvisning eller omsetning."

4.3.2. Svensk ret

Den svenske brottsbalk indeholder i kapitel 16 følgende bestemmelser:

- "10 a § Den som skildrar barn i pornografisk bild med uppsåt att bilden sprids eller som sprider sådan bild av barn döms, om inte gärningen med hänsyn till omständigheterna är försvarlig, för barnpornografibrott till böter eller fängelse i högst två år."

Den svenske regering har den 8/12 1997 fremsat proposition 1997/98:43, hvor bestemmelsen foreslås ændret, jfr. neden for, ligesom der foreslås en lov om forbud mod ind og udførsel af børnepornografi. Det behandledes af Riksdagen den 13/5 1998 og henlagdes, da gennemførelsen kræver grundlovsændring.

Den foreslåede nye § 10 a lyder således:

"Den som

- 1. skildrar barn i pornografisk bild,
- 2. sprider, överlåter, upplåter, förevisar eller på annat sätt gör en sådan bild av barn tillgänglig för någon annan,
- 3. förvarvar eller bjuder ut en sådan bild av barn,
- 4. förmedlar kontakter mellan köpare och säljare av sådana bilder av barn eller vidtar någon annan liknande åtgärd som syftar till att främja handel med sådana bilder, eller
- 5. innehar en sådan bild av barn
- döms för barnpornografibrott till fängelse i högst två år eller, om brottet är ringa, till böter eller fängelse i högst sex månader.
- Med barn avses en person vars pubertetsutveckling inte är fullbordad eller som, när det framgår av bilden och omständigheterna kring den, är under 18 år.
- Den som i yrkesmässig verksamhet eller annars i förvärvssyfte av oaktsamhet sprider en sådan bild som avses i första stycket, döms som sägs där.
- Är ett brott som avses i första stycket at anse som grovt skall dömas för grovt barnpornografibrott till fängelse lägst sex månadar och högst fyra år. Vid bedömande av om brottet är grovt skall särskilt beaktas om det har begåtts yrkesmässigt eller i vinstsyfte, utgjort ett led i brottslig verksamhet som utövats systematisk eller i störra omfattning, avsett en särskilt stor mängd bilder eller avsett bilder där barn utsätts för särskilt hensynslös behandling.
- Förbuden mot skildring och innehav gäller inte den som tecknar, målar eller på något annat liknande hantverksmässigt sätt framställar en sådan bild som avses i första stycket, om bilden inte är avsedd att spridas, överlåtas, upplåtas, förevisas eller på annat sätt göras tillgänglig för andra. Även i andra fall skall en gärning inte utgöra brott, om särskilda omständigheter gör att gärningen måste anses uppenbart befogad."

4.3.3. Tysk ret

Den tyske Strafgesetzbuch indeholder i § 184 om "Verbreitung pornographischer Schriften" følgende bestemmelser om børnepornografi:

- "(3) Wer pornographische Schriften (§ 11 Abs. 3)[(52)], die Gewalttätigkeiten, den sexuellen Missbrauch von Kindern oder sexuelle Handlungen von Menschen mit Tieren zum Gegenstand haben,
- 1. verbreitet,
- 2. öffentlich ausstellt, anschlägt, vorführt oder sonst zugänglich macht oder
- 3. herstellt, bezieht, liefert, vorrätig hält, anbietet, ankündigt, anpreist, einzuführen oder auszuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Sinne der Nummern 1 oder 2 zu verwenden oder einem anderen eine solche Verwendung zu ermöglichen,
- wird, wenn die pornographischen Schriften den sexuellen Missbrauch von Kindern zum Gegenstand haben, mit Freiheitssstrafe von drei Monaten bis zu fünf Jahren, sonst mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
- (4) Haben die pornographischen Schriften (§ 11 Abs. 3) in den Fällen des Absatzes 3 den sexuellen Missbrauch von Kindern zum Gegenstand und geben sie ein tatsächliches Geschehen wieder, so ist die Strafe Freiheitsstrafe von sechs Monaten bis zu fünf Jahren, wenn der Täter gewerbsmässig oder als Mitglied einer Bande handelt, die sich zur fortgesetzen Begehung solcher Taten verbundet hat.
- (5) Wer es unternimmt, sich oder einem Dritten den Besitz von pornographischen Schriften (§ 11 Abs. 3) zu verschaffen, die den sexuellen Missbrauch von Kindern zum Gegenstand haben, wird, wenn die Schriften ein

tatsächliches Geschehen wiedergeben, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer die in Satz 1 bezeichneten Schriften besitz.

- (6) ¿Absatz 5 gilt nicht für Handlungen, die ausschliesslich der Erfüllung rechtmässiger dienstlicher oder beruflicher Pflichten dienen."

[52.] Den nævnte bestemmelse lyder således: "Den Schriften stehen Ton und Bildträger, Abbildungen und andere Darstellungen in denjenigen Vorschriften gleich, die auf diesen Absatz verweisen."

4.3.4. Fransk ret

Den franske Code Pénal indeholder følgende bestemmelse:

- "Art. 22723 Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image d'un mineur lorsque cette image présente un caractère pornographique est puni d'un an d'emprisonnement et de 300.000 F d'amende.
  Le fait de diffuser une telle image, par quelque moyen que ce soit, est puni des mêmes peines.
  Les peines sont portées à trois ans d'emprisonnement et à 500.000 F d'amende lorsqu'il s'agit d'un mineur de quinze ans."

4.4. Udvalgets overvejelser

4.4.1. Generelle overvejelser

Udvalget har generelt drøftet de hensyn, der skal afvejes mod hinanden i en regulering af området vedrørende børnepornografi. Der er enighed om, at der skal være tungtvejende grunde til, at der gribes ind over for informationsfriheden, og at ethvert indgreb skal begrænses til det nødvendige.

Hensynet bag reguleringen er beskyttelsen af børn. Ud fra dette synspunkt blev det i forbindelse med det oprindelige lovforslag i 1979 klart tilkendegivet, at tegninger ikke var omfattet af reguleringen. I forbindelse med den seneste ændring i 1994 fremhæves det i bemærkningerne, at ikke alene tegninger, men også billeder frembragt ved hjælp af edb, som ikke afbilder et virkeligt samleje eller anden kønslig omgængelse, falder uden for bestemmelsen. Især den sidste begrænsning giver anledning til bevisproblemer, idet f.eks. computergenererede billeder fremtræder som identiske med egentlige billeder.

Udvalget har drøftet, om også computergenererede fremstillinger eller andre fremstillinger, der har fuldstændig lighed med fotografier o.l., bør være omfattet af den strafferetlige regulering. Udvalget finder, at hensynet til beskyttelse af børn mod misbrug ikke nødvendiggør, at sådanne fremstillinger omfattes af reguleringen. Med hensyn til de bevisspørgsmål, der kan opstå, har Justitsministeriet i forbindelse med den sidste lovændring vedrørende computerskabte billeder givet udtryk for[(53)], at det vil påhvile tiltalte at sandsynliggøre, at billederne er frembragt ved hjælp af edb. Anfører tiltalte omstændigheder, der i et vist omfang bestyrker påstanden, må anklagemyndigheden føre modbevis f.eks. ved at godtgøre, at man på alle tænkelige måder har forsøgt at bevise tiltaltes påstand, men uden resultat. Udvalget finder på denne baggrund, at der ikke er behov for en strafferetlig regulering af sådanne fremstillinger.

Det er selvsagt også vanskeligt at håndhæve en dansk lovgivning, idet materialet kan være placeret på en server i en jurisdiktion, der ikke strafbelægger børnepornografi, og hvorfra transmissionen til Danmark sker i krypteret form. Udvalget finder imidlertid, at problemer af denne type - der ikke er specielle for børnepornografi - ikke bør afholde Danmark fra at have den ønskede strafferetlige regulering.

Under udvalgets diskussion af, om der er behov for ændringer i eller suppleringer af de nuværende regler om børnepornografi i straffelovens § 235, er der især peget på tre spørgsmål.

For det første må det overvejes, om det nuværende gerningsindhold i stk. 1 fortsat skal være begrænset til den erhvervsmæssige udbredelse[(54)]. For det andet må det undersøges, om besiddelseskriteriet i stk. 2 er egnet til at dække de relevante situationer i forbindelse med IT-udbredelse. For det tredje må der tages stilling til, om

strafferammerne fortsat må anses for de rigtige.

[53.] Justitsministeriets besvarelse af 30/11 1994 af spørgsmål nr. 13 fra Folketingets Retsudvalg vedrørende forslag til lov om ændring af straffeloven (besiddelse af børnepornografi) (L 38 - bilag 14).
[54.] Som nævnt i afsnit 4.1 blev bestemmelsen begrænset til det erhvervsmæssige salg eller den erhvervsmæssige udbredelse i overensstemmelse med Straffelovrådets forslag. I 1979 var afgrænsningsproblemstillingen i relation til private overdragelser, og udbredelsesformer som Internettet var endnu ikke aktuelle.

4.4.2. Straffelovens § 235, stk. 1

Der henvises til afsnit 2.4.1 vedrørende udvalgets generelle overvejelser. Som anført i det afsnit finder udvalget, at udviklingen på IT-området har medført, at en begrænsning til kriminalisering af - eller til en højere strafferamme for - erhvervsmæssig spredning i dag er en utilstrækkelig strafferetlig beskyttelse, og at man bør kriminalisere udbredelse i en videre kreds i samme omfang. Dette gælder også for spredning af børnepornografi.

Som straffelovens § 235 er formuleret i dag, kan spredning af utugtige fotografier, film o.l. af børn kun straffes efter den kvalificerede bestemmelse i stk. 1, hvis det kan bevises, at gerningsmanden har haft forsæt til erhvervsmæssig spredning. Er det ikke situationen, kan der alene straffes efter stk. 2 med bødestraf for gerningsmandens besiddelse af de utugtige billeder, der er omfattet af denne bestemmelse. Til belysning af problemstillingen kan nævnes Vordingborg rets dom af 24/9 1997, som er omtalt nærmere ovenfor i afsnit 4.2.

Justitsministeren har den 18/11 1997 besvaret et spørgsmål fra Folketingets Retsudvalg om, hvorvidt ministeren ville overveje at ændre straffelovens § 235 således, at udbredelse på Internettet kan straffes på samme måde som den erhvervsmæssige udbredelse. Baggrunden for spørgsmålet var ovennævnte dom fra Vordingborg ret. Ministeren henviste bl.a. til, at der var nedsat et udvalg om økonomisk kriminalitet og datakriminalitet, og at der vil være anledning til at overveje, om der er behov for ændring af § 235.

Udvalget finder, at det også i relation til børnepornografi er rimeligt, at der ikke stilles krav om "erhvervsmæssig" udbredelse, hvis udbredelsen sker i en videre kreds. Udvalget har især lagt vægt på, at adgang til børnepornografi via Internettet muliggør en meget omfattende udbredelse.

Det er utvivlsomt, at en del af denne udbredelse ikke er erhvervsmæssig, men udvalget finder, at også ikkeerhvervsmæssig udbredelse af billeder i en videre kreds kan være egnet til at understøtte produktion af børnepornografi, og at kriminalisering af sådan udbredelse dermed kan tjene til at forebygge de samme misbrug, som forbud mod den erhvervsmæssige udbredelse.

Som eksempel på en situation, hvor der tale om samme risici for udnyttelse af børn ved ikkeerhvervsmæssig udbredelse som ved den erhvervsmæssige udbredelse, kan nævnes distribution i "klubber" på Internettet vedrørende børnepornografi, hvor der er regler i klubben om, at man for at være medlem skal sende et bestemt antal billeder til alle medlemmer af klubben, hvorefter man modtager samme antal billeder, som man sender. Også sådanne ikkeerhvervsmæssige situationer bør være omfattet af reguleringen, hvis klubben har et større antal medlemmer.

En ændring af straffelovens § 235, stk. 1, vil bringe dansk ret på linie med norsk, svensk, tysk og fransk ret, der ikke stiller krav om, at udbredelsen skal være erhvervsmæssig, jfr. afsnit 4.3.

Der henvises til afsnit 7.2 vedrørende udvalget forslag.

4.4.3. Straffelovens § 235, stk. 2

Også kravet i straffelovens § 235, stk. 2, om "besiddelse" har givet udvalget anledning til overvejelser - både om, hvad der ligger i begrebet, og om, hvorvidt Internettet giver anledning til nye overvejelser omkring, hvad der bør være kriminaliseret.

Som nævnt i afsnit 4.1 er det forudsat i lovforslaget til den nugældende bestemmelse, at selve det at se på børnepornografiske billeder, der overføres fra en database til egen computerskærm, ikke etablerer en

besiddelsessituation i modsætning til en lagring, hvor den pågældende selv kan kalde billedet frem igen.

Denne afgrænsningsbeskrivelse kan give anledning til overvejelser omkring, hvorvidt Internetadgang til børnepornografiske billeder altid etablerer en besiddelsessituation.

Når oplysninger hentes fra hjemmesider, placeres alle sidens komponenter på harddisken i cachen, og skærmvisningen sker fra denne lagring. Cachen er et område til midlertidige Internetfiler, der typisk kan indeholde 25 % af pladsen på harddisken, men af brugeren kan indstilles til at indeholde en defineret procentdel (fra 1 % og op). Cachen vil således kunne indeholde alle hjemmesider, der har været besøgt, for en længere periode, og brugeren vil kunne hente alle de gemte komponenter frem fra cachen, der bl.a. registrerer komponentnavn, Internetadresse og dato for bl.a. seneste åbning. Det afhænger af system og valgte indstillinger, om det kan aflæses, at en komponent har været hentet igen i cachen.

Der er enighed i udvalget om, at besiddelseskravet i straffelovens § 235, stk. 2, skal forstås således, at der tillige indgår et subjektivt moment. Der skal være tale om en lagring, den pågældende har besluttet at foretage eller at udnytte. De lagringer, der er en del af den almindelige tekniske proces ved adgang til netsystemer, giver derfor nogle særlige problemstillinger. I det omfang det kan bevises, at den pågældende bruger cachen som lagringsplads med henblik på at genfremkalde derfra, er denne form for lagring omfattet af besiddelsesbegrebet. Dette gælder også, når beslutning herom først træffes på et senere tidspunkt end lagringen (f.eks. i forbindelse med, at den pågældende opdager, at der kan genfremkaldes fra cachen).

Hvis den pågældende har givet besked til systemet om at lagre, vil der altid være tale om besiddelse, men også i de situationer, hvor lagringen er en del af den almindelige tekniske proces, vil der således være tale om besiddelse, hvis den pågældende har udnyttet eller vil udnytte denne lagringsform til at genfremkalde cachens (eller et tilsvarende teknisk mellemlagers) indhold af børnepornografisk materiale[(55)] [(56)].

Efter det for udvalget oplyste har der i de p.t. kendte sager altovervejende været tale om, at billederne var blevet downloadet, og at bestemmelsen derfor var anvendelig uden at komme ind på cachens indhold.

I en række tilfælde vil der imidlertid ikke blive downloadet, idet den pågældende blot vil gå ind på særlige Internetområder med børnepornografi, eventuelt til et frit område, hvor brugen eventuelt kan bevises via logning.

---

55. Sidstnævnte problemstilling, hvor gerningsindholdet realiseres, når der træffes en beslutning vedrørende en allerede etableret besiddelse, svarer til, hvad der gælder for ulovlig omgang med hittegods, jfr. straffelovens § 277, og for underslæb, jfr. straffelovens § 278. Efter § 277 er det tillige strafbart, når beslutningen om tilegnelse træffes på et tidspunkt, hvor varetægtsforholdet på tilfældig måde er etableret.
56. Dette svarer til den afgrænsning af besiddelse i IT-mæssig sammenhæng, som arbejdsgruppen vedrørende datakriminalitet fandt skulle lægges til grund

---

Kriminaliseringen af besiddelse er som nævnt i afsnit 4.1 sket på baggrund af opfordringer fra bl.a. Europarådet, FN og Nordisk Råd, og udgangspunktet for disse opfordringer har været at begrænse efterspørgslen efter børnepornografi. På den baggrund kan det virke utilstrækkeligt at holde en benyttelsesform, der i dag i vidt omfang har afløst fysisk besiddelse, udenfor. Det må også indgå i overvejelserne, at man ved brug af Internettet ofte vil kunne få adgang til at se et billede, der ligger på en server i udlandet under omstændigheder, som ikke gør det muligt at retsforfølge besidderen af serveren.

Det er på den anden side klart, at hvis Internetbrugere kommer ind på de særlige områder, hvor der er fri adgang til børnepornografi, uden at de har noget ønske om at se børnepornografi eller som et enkelt nysgerrigt besøg, er der ikke tale om handlinger, hvor der er behov for at kriminalisere. Det er ikke sådanne situationer, der er egnede til at understøtte produktionen af børnepornografi.

Bevismæssigt vil det være meget vanskeligt at gennemføre sager, hvor selve det at se børnepornografi kriminaliseres, ligesom der vil være en vanskelig afgrænsning til de mere tilfældighedsprægede situationer, der efter udvalgets opfattelse i hvert fald ikke bør omfattes af en regulering.

Det må imidlertid antages, at der i et vist omfang er en erhvervsmæssigt præget produktion - hvor sælgeren eller

udbrederen er omfattet af bestemmelsen i straffelovens § 235, stk. 1 - og at brugerkredsen ved den erhvervsmæssige udnyttelse af børn i højere grad vil kunne identificeres, fordi også betalingsstrømme vil kunne indgå i bevisførelsen. Det er formentlig også den form for udnyttelse, hvor det strafferetlige system kan have den største præventive virkning.

Ved spørgsmålet om, hvorvidt man skal kriminalisere det, at en person mod vederlag retsstridigt gør sig bekendt med børnepornografi, har udvalget haft med i sine overvejelser, at det samlede omfang af børnepornografien synes at være voksende, jfr. ovenfor under afsnit 4.2. Dette betyder, at den samlede mængde af bagvedliggende krænkelser formentligt også er voksende. En del børnepornografiske ydelser leveres på en sådan vis, at der ikke hos modtageren er tale om besiddelse i straffelovens § 235, stk. 2's forstand, hvorfor det vil være relevant at kriminalisere selve det forhold mod vederlag at gøre sig bekendt med børnepornografi.

Dertil kommer, at når der betales vederlag for en børnepornografisk ydelse, vil det ud fra et synspunkt af samme art som det, der ligger bag kriminalisering af hæleri, være naturligt at kriminalisere aftageren af ydelsen. Uanset at den person, der betaler for at gøre sig bekendt med børnepornografien, ikke i straffelovens forstand kommer i besiddelse af børnepornografien, har han modtaget en egentlig ydelse, nemlig muligheden for at se den pågældende børnepornografi. Dette minder om hæleri, hvor hæleren modtager et gode fra den, der har begået førforbrydelsen. Herudover vil en kriminalisering kunne være medvirkende til at formindske efterspørgslen efter børnepornografiske ydelser og derved forhåbentligt være med til at formindske mængden af de bagvedliggende krænkelser. Dette synspunkt er endnu et moment, der ligner hælerisynspunktet, idet hovedformålet med kriminalisering af hæleri er et ønske om at forhindre førforbrydelserne.

På denne baggrund finder udvalget, at det forhold, at en person mod vederlag retsstridigt gør sig bekendt med børnepornografiske fremstillinger, bør kriminaliseres. Forslaget omfatter enhver form for modydelse, der har karakter af et vederlag, herunder at der byttes med andre ydelser. Ved en sådan regulering styrker man indsatsen mod erhvervsmæssig udnyttelse af børn, idet kundernes forhold tillige omfattes af den strafferetlige regulering. Forsæt skal foreligge på det tidspunkt, hvor betalingen sker, og det skal vedrøre adgang til børnepornografiske fremstillinger.

Udvalget har drøftet, om en kriminalisering bør vedrøre samme fremstillinger som straffelovens § 235, stk. 1, eller begrænses til de fremstillinger, der er nævnt i straffelovens § 235, stk. 2. Kriminaliseringen kan både ses som et hælerilignende supplement til stk. 1, hvad der kan gøre det naturligt, at reguleringen vedrører samme fremstillinger som stk. 1, og som et supplement til besiddelsesreglen i stk. 2, hvad der kan gøre det naturligt at reguleringen vedrører samme fremstillinger som stk. 2.

Udvalget vil ikke udelukke, at det i et vist omfang kan dæmme op for mere grov kriminalitet, at der er mulighed for at se på noget mindre groft end det, der er omfattet af stk. 2. Dertil kommer, at i alle de tilfælde, som ses omtalt fra praksis, har fremstillingerne eller en stor del af disse været af en art, der var omfattet af stk. 2. Envidere kan det give en mindre velbegrundet regulering, hvis eksempelvis en person ikke må købe et blad, men godt måtte besidde det, hvis en anden person forærer ham det.

Udvalget har på denne baggrund fundet, at reguleringen bør svare til den, der er i straffelovens § 235, stk. 2. Reguleringen kan derfor eventuelt ske som en udvidelse af den nugældende bestemmelse.

Der henvises til afsnit 7.2 vedrørende udvalgets forslag.

4.4.4. Strafferammen

Bestemmelsen i straffelovens *§ 235, stk. 1*, blev indsat i straffeloven i 1980. Dengang var der alene bøde i strafferammen. Dette var i overensstemmelse med flertallets opfattelse i Straffelovrådet[(57)]; rådet gav dog ingen explicit begrundelse herfor. I 1989 ændredes strafferammen, således at dens maksimum nu er fængsel i 6 måneder. Dette blev begrundet under henvisning til de grovest tænkelige former for handel med børnepornografiske billeder[(58)].

Denne strafferamme har i praksis vist sig tilstrækkelig ved de hidtil behandlede sager. Det er imidlertid udvalgets opfattelse, at det nugældende maksimum kan være for lavt, når det tages i betragtning, hvad beskyttelsesinteressen i § 235 er.

§ 235 skal for det første forhindre den krænkelse af privatlivets fred, der følger af udbredelser af billeder af denne art. Forholdet svarer for så vidt til straffelovens § 264 d om videregivelse af billeder af den pågældende under omstændigheder, der åbenbart kan forlanges unddraget offentligheden, og § 264 c om at skaffe sig eller uberettiget udnytte billeder, som er optaget under de i § 264 a nævnte omstændigheder. Både § 264 d og § 264 c har strafmaksima på 6 måneders fængsel ligesom § 235.

Derimod skal § 235 ikke anvendes på den direkte krænkelse af barnet under optagelsen af de pornografiske film eller billeder. I disse tilfælde anvendes de almindelige bestemmelser om voldtægt, samleje med mindreårig, anden kønslig omgængelse end samleje, kønslig omgængelse med en person af samme køn, blufærdighedskrænkelse osv., jfr. straffelovens kapitel 24. En forhandler, der bestiller billeder af denne art optaget hos en producent, kan straffes for medvirken til den pågældende sædelighedsforbrydelse.

Mellem producenten og den sluttelige køber eller besidder af det pornografiske materiale er der typisk en mellemhandler, der står for distributionen. I mange tilfælde foretages denne distribution for vindings skyld. Hvis den pornografiske film er bestilt af mellemhandleren, kan der som nævnt straffes for medvirken til sædelighedsforbrydelsen. Selv om dette ikke er tilfældet, er det naturligt at antage, at en betydelig del af de producerede film m.m. er optaget med henblik på et senere salg. I sådanne tilfælde kan man ikke straffe køberen (mellemhandleren) for den oprindelige sædelighedsforbrydelse, men alene efter § 235. § 235 skal således hindre mellemhandlerens køb af filmen m.m. og på den måde bidrage til, at den oprindelige optagelse og den oprindelige sædelighedsforbrydelse ikke gennemføres.

Ved vurderingen af strafværdigheden må det lægges til grund, at dette gør det rimeligt at anvende en noget højere strafferamme end ved de nævnte fredskrænkelser. Udvalget foreslår derfor, at strafmaksimum forhøjes fra de nuværende 6 måneder til 2 år. Dette er den nuværende højestestraf i Finland, Norge og Sverige, mens Island som Danmark har 6 måneder.

Med hensyn til *§ 235, stk. 2*, med den i afsnit 4.4.3 nævnte udvidelse er der tale om væsentligt mindre grove forhold end mellemhandlerens og distributørens. Den nuværende strafferamme - bøde - vil i den overvejende del af tilfældene være passende. Bestemmelsen i det nugældende stk. 2 blev indsat så sent som i 1994[(59)], og udvalget finder, at den nuværende begrænsning af straffen til bøde bør bevares som normalstrafferammen.

Udviklingen i anvendelsen af Internettet og distribution af børnepornografi via Internettet har imidlertid udviklet sig således, at udvalget finder, at der bør være mulighed for under skærpende omstændigheder at idømme hæfte eller fængsel indtil 6 måneder. Som eksempel på, hvad der skal betragtes som skærpende omstændighed, kan nævnes, at den pågældende betaler betydelige beløb for at modtage børnepornografisk materiale. Der vil ligeledes foreligge skærpende omstændigheder, hvis den pågældende besidder et meget stort antal børnepornografiske fremstillinger, eller et større antal fremstillinger af særlig grove forhold, f.eks. voldtægt af børn.

---

57. FT 1979/80 2. samling A sp. 1765.
58. FT 1988/89 A sp. 2858.
59. FT 1994/95 A sp. 467.

KAPITEL 5 - EFTERFORSKNING - MULIGHEDER I PRAKSIS

5.1. Krav til Internetudbydere og teleselskaber om registrering af logoplysninger og opbevaring heraf

Manglende eller mangelfulde oplysninger hos Internetudbydere udgør et efterforskningsmæssigt problem. Problemet bliver ikke mindre, når der efterforskes forhold, hvor der er anvendt en række Internetadresser til dispositionen, så alt - incl. det land, der reelt opereres fra - er skjult.

Modhensynet - der taler for få registreringer og kortvarig opbevaring af oplysningerne hos formidlerne - er især hensynet til privatlivets fred. Under drøftelserne blev dog også nævnt, at der er tale om en meget stor teknisk usikkerhed med hensyn til loggens indhold og fuldstændighed, og at krav på dette område er omkostningskrævende.

Det kan også fremhæves, at det på nogle potentielle gerningsmænd formentlig vil kunne have en vis forebyggende effekt, hvis de ved, at transaktionerne logges, og at loggen opbevares i en længere periode.

Det er klart ikke muligt at tilgodese disse modsatrettede hensyn fuldt ud. Der er heller ikke tale om et problem, der kan totalløses via dansk lovgivning, men i et vist omfang vil en dansk regulering være en god hjælp.

EU udfærdigede den 17/1 1995 en resolution om lovlig aflytning af telekommunikation(60). Bl.a. skal de retshåndhævende myndigheder have adgang til den opkaldte parts nummer ved udgående forbindelser, den opkaldende parts nummer ved indgående forbindelser, alle signaler målet har udsendt, forbindelsens begyndelses og afslutningstidspunkter samt varighed, faktiske bestemmelsesnummer og mellemliggende kaldenumre, hvis kommunikationen er blevet omstyret. Resolutionen nævner ikke spørgsmålet om opbevaringstid for oplysninger.

I G8-landenes erklæring af 10/12 1997 om hightech crime(61) nævnes i principerklæringens punkt V, at retssystemerne skal tillade bevaring og hurtig adgang til elektroniske data, og i punkt IX, at informations og telekommunikationssystemer i mulige omfang skal udformes, så det hjælper til at forhindre og opdage netværksmisbrug og letter sporing af kriminelle og indsamling af beviser.

Professor Ulrich Sieber nævner i sin rapport af 1/1 1998 til EU Kommissionen(62) Trace Back Procedures som et meget væsentligt punkt. Det siges i rapporten:

- "The study showed that one of the main problems for prosecuting computer crime is the anonymity provided by international computer networks. This anonymity must not be completely removed since privacy protection for users and anonymity (e.g. for social minority groups) is an important social value which should not be given up in international computer networks. However, on the other side, it should be possible, under welldefined legal circumstances (such as court orders) to lift anonymity in order to trace back the authors of illegal actions (such as hackers) or of illegal or harmful contents (such as paedophiles). Today such trace back procedures are often hindered or made impossible due to the features of the TCP/IP protocol of the Internet and in addition especially by the activities of anonymous remailers and the use of free access software."

IT-sikkerhedsrådet har i april 1998 udarbejdet en rapport om Privatliv på Internet(63). Det nævnes i rapporten(64) vedrørende lagring af transaktionsoplysninger, at visse Internetleverandører gemmer sådanne oplysninger i 3 måneder - bl.a. for at gøre det muligt at efterkomme editionsbegæringer - mens andre ikke har nogen fast praksis. IT-sikkerhedsrådet bemærker, at en længerevarende opbevaring hos en Internetudbyder kan medføre betydelig risiko for indgreb i brugerens privatliv. Det nævnes, at Internetudbydere kun i få tilfælde benytter disse oplysninger i forbindelse med kundeafregninger. Det siges videre:

- "Det er væsentligt, at debatten herom tager udgangspunkt i en afvejning af på den ene side berettigede efterforskningshensyn og på den anden side vigtigheden af at undgå det totale overvågningssamfund, alene fordi den nye teknologi giver mulighed herfor.
- IT-sikkerhedsrådet finder det betænkeligt, at en praksis for opbevaring af transaktionsoplysninger alene baseres på efterforskningshensyn, der ikke er understøttet af særlig lovhjemmel, f.eks. i reglerne om indgreb i meddelelseshemmeligheden. Rådet finder, at Internetudbydere, bl.a. af sikkerhedsmæssige hensyn, bør opbevare så få oplysninger som muligt i så kort tid som muligt, idet udstrækningen af denne tid bl.a. må bestemmes ud fra hensynet til at gennemføre sædvanlige backupprocedurer m.v. Rådet skal bemærke, at et sådant minimumsprincip i øvrigt er i overensstemmelse med såvel den gældende registerlovgivning som med EUdirektivet om behandling af personoplysninger. Såvel hensynet til politiets efterforskning som hensynet til brugeren selv (f.eks. i forbindelse med senere bevisførelser om indgåede aftaler m.v.) taler for, at der etableres fastere principper for denne lagring.
  Rådet er dog også opmærksomt på, at særlige regler, f.eks. om bogføringspligt, kan indebære en pligt til at opbevare transaktionsoplysninger i længere tid."

---

60. Jfr. bilag 1.
61. Jfr. bilag 1.
62. Legal Aspects of ComputerRelated Crime in the Information Society, afsnit V.C.6.
63. Rapporten findes på http://www.fsk.dk./
64. Afsnittet: "Der bør være ensartede regler om lagring af transaktionsoplysninger".

Som nævnt i afsnit 2.2 foreligger der i EU et foreløbigt udkast til fælles aktion vedrørende børnepornografi på Internettet(65). Udkastet peger bl.a. på en mulighed for at regulere Internetudbydere således, at trafikrelaterede data, hvor det er muligt, opbevares i det tidsrum, der kan være nødvendigt for at kunne sende disse data til de retsforfølgende myndigheder.

Det bemærkes, at minimumsprincippet vedrørende opbevaring af personidentificerbare oplysninger i EUdirektivet om behandling af personoplysninger(66) ikke er til hinder for, at der pålægges den registrerings og opbevaringspligt, der vurderes at være nødvendig for efterforskning af kriminalitet. Tilsvarende gælder med hensyn til de tiltag til beskyttelse af privatlivets fred, der er nævnt i EuropaParlamentet og Rådets direktiv 97/66/EF om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren(67).

Uanset hvilken opbevaringsperiode, der vurderes at være nødvendig, er det hensigtsmæssigt, at der etableres fastere principper, f.eks. i form af en lovregulering.

---

65. Gengivet i Rådets pressemeddelelse fra mødet 3.4. december 1998 (13673/98 (Presse 427)).
66. EuropaParlamentet og Rådets direktiv 95/46/EF af 24/10 1995 om beskyttelse af fysiske forbindelser i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, EFT 1995 L 281/31.
67. EFT 1998 L 24/1.

I afsnit 6 behandles spørgsmålet om retsplejelovens regler - herunder spørgsmålet om, hvornår reglerne om henholdsvis edition og indgreb i meddelelseshemmeligheden skal/bør kunne anvendes, og om der bør ske en udvidelse af området for, hvornår indgreb i meddelelseshemmeligheden kan benyttes.

I afsnit 2.4.2.1 er nævnt en sag om mulig kursmanipulation via Internettet, der illustrerer behovet for at kunne få logoplysninger. Tilsvarende gælder i en række andre sager. Som yderligere eksempel kan nævnes et anmeldelseskompleks fra december 1997, hvor en finsk virksomhed anmeldte, at der via en dansk Internetudbyder var hacket ind i deres anlæg, opnået fuld kontrol, viderehacket til andre maskiner rundt i verden og derefter rettet i logfiler og indlagt virus i processoren, så den måtte udskiftes. I Danmark anmeldte to virksomheder, at der via den finske virksomhed var hacket hos dem. Det er klart, at der er behov for logoplysninger fra den danske Internetudbyder(68) .

Med hensyn til de efterforskningsmæssige behov kan bl.a. følgende anføres:

Oplysninger om B-nummeret (det nummer, der ringes til) fastholdes i dag kun kortvarigt hos teleselskaberne, hvilket frembyder vanskeligheder for en efterfølgende efter forskning, idet der går tid til anmeldelse, visitering og opstart af efterforskning. Det vil også kunne være afgørende, at A-nummeret (det nummer, der ringes fra) og IPadressen videreføres og fastholdes i systemerne.

---

68. Arbejdsgruppen vedrørende datakriminalitet har drøftet de problemer, der kan være ved at anvende logudskrifter som bevis. Der var enighed om, at det kan være vanskeligt at føre (68)bevis for, at loggen er korrekt. Nogle af arbejdsgruppens medlemmer var af den opfattelse, at loggen generelt var et uegnet bevismiddel. Andre medlemmer anførte, at loggen i en række sager vil være egnet til at give oplysninger, så efterforskningen kan målrettes bedre, og at loggen i den endelige sag vil være understøttet af en række andre beviser. I nogle sager vil loggen være den eneste efterforskningsmulighed.

Ud fra et efterforskningsmæssigt synspunkt har det stor betydning, at Anummeret logges, uanset om den pågældende har benyttet muligheden for at blokere for visning af Anummeret hos den, der ringes til. Denne særlige mulighed må antages primært at skulle beskytte imod, at nummeret kan vises hos modtageren (indehaveren/brugeren af Bnummeret) og ikke at tage sigte på de registreringer, der kan være behov for i telekæden.

Det bemærkes, at i hvert fald én af de større Internetudbydere kun tilslutter til Internettet, hvis Anummeret samtidig registreres (hvilket sker, uanset om det er visningsbeskyttet eller ej).

Der er ud fra et efterforskningsmæssigt synspunkt ikke alene behov for at A og Bnummer samt IPadresse logges, men også for, at disse logoplysninger opbevares i et længere tidsrum, og endvidere for, at udbyderen logger, hvornår kunden har logget på og af.

I praksis har det under efterforskning vist sig, at teleselskabers og Internetudbyderes tidsangivelser i loggen har været upræcise. Det vil derfor set fra et efterforskningsmæssigt synspunkt være hensigtsmæssigt, hvis der stilles krav om, at der etableres et system med korrekt dansk realtid, f.eks. ved at serveren jævnligt synkroniseres med realtid. Hvis tidsregistreringer i logninger, der indgår i en efterforskning, ikke er korrekte, risikerer politiet at målrette efterforskningen mod forkerte personer.

Nogle sager har måttet opgives, fordi logningsinformationerne var mangelfulde, og der har været sager, der har været efterforsket mod forkerte sigtede (der i nogle tilfælde har været anholdt). Problemet har typisk været, at Anummeret manglede, og at tidsangivelsen var behæftet med for store usikkerhedsmarginer.

Spørgsmålet er, ikke mindst set i lyset af, at alle kan etablere sig som Internetudbydere, om der bør være mulighed for at straffe for manglende overholdelse af reglerne. Dette gælder f.eks. også i relation til hvidvasklovens krav til finanssektoren om ID-oplysninger og opbevaring af disse og af transaktionsoplysninger.

Det er endvidere efterforskningsmæssigt et problem, at almindeligt tilgængelige PCer (biblioteker, Internetcaféer m.v.) kan benyttes til at opnå anonymitet ved Internetanvendelsen. Det kunne derfor ud fra et efterforskningsmæssigt synspunkt være hensigtsmæssigt, hvis der ved benyttelse af almindeligt tilgængelige PCer blev stillet krav om identitetsregistrering og opbevaring heraf samt opbevaring af logoplysninger og om, hvem der har været på systemet hvornår.

Et tilsvarende efterforskningsmæssigt problem opstår, hvis en arbejdsgiver ikke logger oplysninger om virksomhedens datatrafik, herunder brugeroplysninger, samt ved anvendelse af PCer på skoler, universiteter m.v.

Udvalget finder imidlertid, at det vil være urealistisk at tro, at det er muligt at gennemføre en effektiv regulering på disse områder[(69)]. Hvis efterforskningen viser, at en af disse PCer er blevet benyttet, og der ikke findes oplysninger om brugeren, må det i stedet forsøges via afhøringer at afgrænse den mulige brugerkreds. I disse situationer kan politiet i det mindste få indkredset, hvor en mere traditionel efterforskning skal sættes ind. Udvalget stiller derfor kun forslag om en regulering vedrørende udbydere, da oplysninger fra disse i mange tilfælde vil være den eneste mulighed for at udfinde det sted, der er handlet fra.

Udvalget finder, at der af efterforskningsmæssige grunde bør stilles krav om, at Internetudbydere og teleselskaber skal logge både A- og B-nummeret - for A-nummerets vedkommende uanset om den pågældende har benyttet muligheden for, at der ikke sker visning af A-nummeret. Endvidere bør udbyderen logge IPadresse for den, der ringer op, brugertid, tidspunkt for opkobling/nedkobling, opkoblingens længde og sessionstype (FTP/Telnet)[(70)]. Der bør tillige stilles krav om opbevaringsformat (læsbarhed). Derudover bør eventuelle kontooplysninger opbevares. Opbevaring af oplysninger skal ske i Danmark, hvis udbyderen er i Danmark, uanset om udbyderen er selvstændig eller filial af en udenlandsk virksomhed[(71)]

---

69. Arbejdsgruppen vedrørende datakriminalitet fandt ligeledes, at områderne ikke kunne reguleres effektivt.

70. Dette gælder, selv om udvalget er opmærksom på, at man remote kan anvende FTP/Telnet, dvs. fra en anden server end éns udbyders (så efterforskning vanskeliggøres eller umuliggøres på grund af indskydelse af en række udbydere), således at dette mest vil være en hjælp ved de mindre professionelle kriminelle.

71. Flere medlemmer af arbejdsgruppen vedrørende datakriminalitet har peget på, at der ved udvidede registrerings og opbevaringsregler samtidig bør stilles krav om foranstaltninger til beskyttelse mod uautoriseret adgang og manipulation.

Endvidere bør det tilstræbes, at det sikres, at korrekt dansk realtid registreres.

Opbevaringstiden for disse oplysninger bør set fra et efterforskningsmæssigt synspunkt ideelt være 5 år, svarende til bogføringsloven og hvidvaskloven, men da dette af praktiske grunde formentlig er for vidtgående så i hvert fald en periode, der muliggør efterforskning i de fleste sager, hvor der er behov for disse oplysninger.

Efter de for udvalget foreliggende oplysninger opbevares loggen vedrørende emails ofte i 6 måneder, mens der ikke i øvrigt er nogen fast praksis.

Udvalget har nærmere drøftet de forskellige hensyn, der kan tale for henholdsvis en længere og en kortere opbevaringstid. Efterforskningsmæssige hensyn taler for en frist på ikke under 1 år.

Ikke mindst i sager med ekstremt store datamæng der eller i sager, der efterforskningsmæssigt starter i et andet land, der derefter konstaterer, at der skal efterforskes også i Danmark, vil en kortere frist kunne betyde, at videre efterforskning umuliggøres. For langt de fleste sagers vedkommende vil en frist på 6 måneder imidlertid være tilstrækkelig.

Ved valg af en kortere frist tages et større hensyn til både privatlivets fred og de omkostninger,der påføres udbyderne. Særligt vedrørende hensynet til privatlivets fred tilsiger dette hensyn, at der logges mindst muligt, og at loggen opbevares i så kort tid som muligt, idet risikoen for, at oplysninger kommer på forkerte hænder, er større, jo længere opbevaringsperioden er.

Med hensyn til *retten* til at opbevare oplysninger kan det oplyses, at lovforslaget om behandling af personoplysninger (L 44 i folketingsåret 199899) indeholder regler herom. Lovforslaget har navnlig til formål at gennemføre direktivet om behandling af personoplysninger (95/46/EF). Lovforslaget blev ikke vedtaget i folketingssamlingen 199899, men agtes genfremsat i den kommende folketingssamling.

Det følger af lovforslagets § 5, stk. 5 (der har sin baggrund i direktivets artikel 6, stk. 1, litra e), at indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidspunkt end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles. Den dataansvarlige skal efter lovforslagets anmeldelsesordning (lovforslagets kapitel 13) angive sletningsfristen i sin anmeldelse til Datatilsynet eller (hvis der ikke skal ske anmeldelse til Datatilsynet) opbevare dokumentation herfor.

Udvalget har på baggrund af drøftelserne valgt at anbefale en opbevaringsfrist på 6 måneder. Spørgsmålet om, hvorvidt udbyderen har ret til at opbevare logoplysninger ud over den pligtmæssige opbevaring i 6 måneder, må afgøres på grundlag af de ovenfor nævnte almindelige regler i registerlovgivningen(72).

Med hensyn til formen for reguleringen har udvalget indgående drøftet, om de ønskede registreringer og opbevaringen heraf ville kunne gennemføres ved en selvregulering.

Nogle medlemmer har henvist til, at der ikke er tale om en branche med etablerede traditioner med hensyn til selvregulering, eller med egne sanktionssystemer, ligesom der end ikke findes en registrering af Internetleverandører. Dette kan i sig selv tale mod en løsning med selvregulering, men dertil kommer, at der er tale om tiltag, der alene har efterforskningsmæssig interesse, og at efterforskningsmulighederne bør sikres gennem lovgivning herom. Dette svarer også til, at det f.eks. i § 3 h i lov om visse forhold på telekommunikationsområdet er fastsat, at udbydere af offentlige telenet og teletjenester uden udgift for staten skal sikre, at telecentralerne er indrettet således, at politiet kan få adgang til at foretage indgreb i meddelelseshemmeligheden.

---

72. Et flertal i arbejdsgruppen vedrørende datakriminalitet (Kim Aarenstrup, Mads Bryde Andersen, Jan Friis, Hans Jakob Paldam Folker, Michael Geskjær, Carsten Heilbuth, Ulla Høg, Helle Jahn, Jens Kruse Mikkelsen, Ronald Pedersen, Ole Stampe Rasmussen, Henrik OftebroSvendsen,) har på baggrund af arbejdsgruppens drøftelser fundet, at arbejdsgruppen skulle anbefale en opbevaringsfrist på 6 måneder. Et mindretal (Jan Carlsen) fandt, at der

maksimalt skulle opbevares i 3 måneder med tvungen sletning efter udløbet af perioden.

Andre medlemmer har henvist til, at forpligtelsen bør kunne gennemføres ved selvregulering. Disse medlemmer mener ikke, at reglerne i lov om visse forhold på telekommunikationsområdet er egnede som retsgrundlag for den uoverskuelige mængde af Internetleverandører, for hvilke en forpligtelse af denne art får betydning.

Disse medlemmer har peget på, at der for tiden pågår intense bestræbelser på at gennemføre selvregulering indenfor Internetbranchen i en række henseender, og at man i tråd med den almindelige tendens i retning mod selvregulering bør give branchen mulighed for selv at tilvejebringe denne regulering, samtidig med at branchen alligevel skal tage stilling til spørgsmålet om, hvor længe man har *ret* til at opbevare sådanne logoplysninger. Når man vurderer udsigten til at gennemføre ønsket om opbevaring af logoplysninger i 6 måneder gennem selvregulering, må det i øvrigt tages i betragtning, at Internetleverandørerne kan have en økonomisk interesse i at følge en sådan praksis, eftersom udleveringen af de pågældende oplysninger sker mod betaling.

Et flertal i udvalget (Preben Bialas, Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Michael Clan, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Lau Kramer, Kirsten Mandrup, Annemette Møller, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder, at reguleringen skal ske ved lov[(73)].

Et mindretal i udvalget (Mads Bryde Andersen, Vagn Greve, Jesper Koefoed, Lars Bo Langsted) finder, at spørgsmålet så vidt muligt skal løses ved en selvregulering i branchen. Disse medlemmer er dog enige i en lovgivningsmæssig løsning, såfremt det viser sig, at reguleringsbestræbelserne ikke bærer frugt[(74)].

Der henvises til afsnit 7.3 vedrørende udvalgets forslag

[73.] I arbejdsgruppen vedrørende datakriminalitet fandt flertallet (Kim Aarenstrup, Jan Friis, Hans Jakob Paldam Folker, Michael Goeskjær, Ulla Høg, Helle Jahn, Jens Kruse Mikkelsen, Ronald Pedersen, Ole Stampe Rasmussen, Henrik OftebroSvendsen) ligeledes, at reguleringen burde ske ved lov.
[74.] I arbejdsgruppen vedrørende datakriminalitet fandt et mindretal (Mads Bryde Andersen, Jan Carlsen og Carsten Heilbuth) ligeledes, at selvregulering skulle anvendes. To af disse medlemmer (Mads Bryde Andersen og Carsten Heilbuth) var enige i en lovgivningsmæssig løsning, såfremt selvregulering viste sig ikke at være tilstrækkeligt.

5.2. Kryptering

Et særligt spørgsmål er, hvordan - og om - man kan sikre sig, at den teknologiske udvikling ikke sker på en måde, der reelt udelukker politiets efterforskning eller dog udelukker anvendelsen af visse særligt egnede metoder. Dette vanskelige spørgsmål er bl.a. behandlet af Mads Bryde Andersen og Peter Landrock i en artikel om "Kryptering og efterforskning"[(75)].

Den i afsnit 6.4 nævnte sendemastproblemstilling er for så vidt et eksempel herpå, men er dog primært et eksempel på, at lovgivningen ikke er tilpasset de faktiske situationer.

Et særligt vanskeligt og både nationalt og internationalt omdiskuteret område er anvendelsen af kryptering. Kryptering er på den ene side et uhyre velegnet middel til at beskytte informationer, og dermed også et meget velegnet middel til at forhindre kriminalitet. Samtidig kan en effektiv kryptering betyde, at politiet ikke reelt har mulighed for at efterforske. Forskellige lande har overvejet en række løsninger - fra forbud mod kryptering til kun at tillade bestemte krypteringsformer - men ingen har fundet på en velegnet løsning.

Spørgsmålet er også behandlet i flere rapporter fra regeringens ekspertudvalg om kryptering[(76)]. Dette udvalg behandler spørgsmålene om, hvorvidt det er muligt ved lovregulering eller på frivillig basis at nå frem til en anvendelse af kryptering, der sikrer en hensigtsmæssig balance mellem behovet for at anvende kryptering og behovet for at efterforske kriminalitet.

Udvalget vil pege på, at hvis det i en sag er sandsynligt, at væsentlige beviser kun forefindes i krypteret form, vil

sagens øvrige bevisligheder - herunder indiciebeviser - formentlig blive tillagt relativt større vægt.

---

75. Juristen 1995, s. 306 ff.
76. Rapporterne er udgivet af Forskningsministeriet og findes på adressen http://fsk.dk.

KAPITEL 6 - EFTERFORSKNING - RETSPLEJELOVENS REGLER

Spørgsmålene i dette afsnit vedrører især følgende problemstillinger:

a) Hvornår kan editionsreglerne anvendes?

b) Skal dele af det område, der i dag reguleres af reglerne om indgreb i meddelelseshemmeligheden, overflyttes til editionsområdet?

c) Hvem kan som indehaver af en telefon give samtykke til teleoplysninger?

d) Er der former for indgreb i meddelelseshemmeligheden, der ikke kan foretages efter de gældende regler, og skal der i givet fald skabes fornøden lovhjemmel?

e) Er der behov for at udvide området for, hvornår der kan gøres indgreb i meddelelseshemmeligheden?

Spørgsmål a) behandles i afsnit 6.1 om adgang til digitale meddelelser.

Spørgsmål b) behandles i afsnit 6.2 om lagrede teleoplysninger.

Spørgsmål c) behandles i afsnit 6.3 om teleoplysninger i henhold til samtykke.

Spørgsmål d) behandles i afsnit 6.4 om sendemaster.

Spørgsmål e) behandles i afsnit 6.5 om indgreb i meddelelseshemmeligheden i øvrigt.

De bestemmelser i retsplejeloven, der er relevante i denne forbindelse, er reglerne om edition og indgreb i meddelelseshemmeligheden. Disse regler er gengivet i uddrag i bilag 2.

Udvalget har drøftet, om der er - eller nødvendigvis er - forskel på reglerne om edition og reglerne om indgreb i meddelelseshemmeligheden med hensyn til, hvornår den sigtede bliver underrettet om et indgreb.

Som det fremgår, skal der ved indgreb i meddelelseshemmeligheden beskikkes en advokat, før retten træffer afgørelse. Efter retsplejelovens § 788 underrettes den, indgrebet er rettet mod, når indgrebet er afsluttet, men politiet har en frist på yderligere 14 dage til at anmode om, at underretning undlades eller udsættes. Underretning skal ikke gives til den sigtede, medmindre den sigtede er indehaver af telefonen eller lokaliteten eller direkte berørt af indgrebet.

Ved et retsmøde om en editionskendelse skal den sigtede ikke underrettes[(77)], men en eventuel forsvarer skal som hovedregel underrettes om retsmødet og er berettiget til at overvære det. Forsvareren må ikke uden rettens samtykke videregive oplysninger fra retsmødet.[(78)] Retsbogen, kendelsen og politirapporten om editionens gennemførelse indgår som almindelige bilag i straffesagen, og der kan kun i særlige situationer (hvis det undtagelsesvis er påkrævet på grund af hensynet til fremmede magter, til statens sikkerhed eller til sagens opklaring eller tredjemand) gives pålæg om, at oplysningerne ikke må videregives til den sigtede.[(79)]

Den, der skal pålægges edition, skal have lejlighed til at udtale sig før afgørelsen. Den pågældende kan underrette den sigtede om indgrebet, medmindre der i særlige tilfælde gives pålæg efter retsplejelovens § 189 (hvorefter der

kan pålægges et vidne tavshedspligt af hensyn til fremmede magter, til statens sikkerhed eller til opklaring af alvorlige forbrydelser). Bestemmelsen har i praksis også fundet anvendelse på selve editionshandlingen.

Ved den ændring af retsplejeloven, der er trådt i kraft 1/7 1999[(80)], er der ikke sket en ændring i retstilstanden omkring edition, men der er i § 804, stk. 2, jfr. § 803, stk. 1, indsat en klar henvisning til, at § 189 finder tilsvarende anvendelse.

---

77. Jfr. retsplejelovens § 748, stk. 1.
78. Jfr. retsplejelovens § 748, stk. 2.
79. Jfr. retsplejelovens § 745, stk. 4.
80. Lov nr. 229 af 21/4 1999 om ændring af retsplejeloven (Beslaglæggelse, edition m.v.).

6.1. Adgang til indholdet af digitale meddelelser

Digitale meddelelser kan teknisk sendes på forskellige måder, hvoraf den mest almindelige i dag er email. De nedenfor behandlede spørgsmål om email gælder tilsvarende for andre former for digitale meddelelser.

De behandlede spørgsmål vedrører alene, hvilket retsskridt der skal anvendes ved adgang til selve den digitale meddelelse. Oplysning om, hvem der er indehaver af en kendt email adresse, reguleres af reglerne om edition (på samme måde som adgangen til at få oplyst, hvem der er abonnent til et hemmeligt telefonnummer).

Spørgsmålet om adgang til email oplysninger opstår i flere situationer:

1) I relation til læst email, der forefindes på en PC ved ransagning.

2) I relation til ikke læst email, der kan indhentes via en PC i forbindelse med en ransagning, der omfatter denne.

3) I relation til adgang til læst email hos Internetudbyderen.

4) I relation til adgang til ikke læst email hos Internetudbyderen.

I *situation 1* er der ikke tvivl om, at de almindelige regler om ransagning og beslaglæggelse finder anvendelse.

I *situation 2* vil man i praksis sidestille situationen med den situation, hvor der ved ransagning findes et uåbnet brev. Her finder de almindelige regler om ransagning og beslaglæggelse ligeledes anvendelse, fordi brevet ikke er i et forsendelsesforløb, jfr. nedenfor og UfR 1992.373 V, der vedrørte et brev, der ikke var overgivet til forsendelse.

I Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter nævnes[(81)], at indgreb, der gennemføres inden kommunikationens påbegyndelse eller efter dens afslutning, bør bedømmes efter reglerne om ransagning og beslaglæggelse. Det siges videre:

- "Dette vil f.eks. gælde et brev eller anden forsendelse inden afsendelsen eller efter fremkomsten til adressaten, eller en båndoptagelse af en stedfunden samtale (eller et notat om samtalen), fundet hos en deltager. Det vil også gælde en kassette, som politiet ved en husundersøgelse finder i en automatisk telefonsvarer, og hvorpå personer, der har ringet til den pågældende telefon, har indtalt meddelelser, ligesom det vil gælde en telexstrimmel, som politiet finder siddende i en telexmaskine om morgenen, og hvorpå der til indehaveren af telexmaskinen i nattens løb er udskrevet meddelelser fra andre telexbrugere. Breve, der på posthuset er lagt i modtagerens postboks, men endnu ikke er afhentet af denne, er formentlig omfattet af reglerne om brevåbning, såfremt politiet ønsker med postvæsenets hjælp - og uden at modtageren gøres bekendt med indgrebet - at læse brevene. Hvis politiet derimod - f.eks. ved brug af en i bevaring taget boksnøgle - kan låse sig ind i postboksen, er man uden for reglerne om brevåbning, og politiet kan gå frem efter reglerne om beslaglæggelse. Virkningen af, at indgrebet bedømmes efter reglerne om ransagning og beslaglæggelse, er dels, at betingelserne for indgrebets foretagelse er anderledes (og lempeligere), dels, at indgrebet ikke kan gennemføres hemmeligt."

En overførsel af disse regler på email vil betyde, at man er uden for området for indgreb i meddelelseshemmeligheden, når emailen er nået frem til adressatens adresse, hvilket må svare til, at der er adgang til emailen fra adressatens terminal.

I *situation 3 og 4* bliver spørgsmålet, om indgrebet får en anden karakter, hvis det gennemføres hos Internetudbyderen, således at oplysningerne ikke kan indhentes ved edition (der er det normale retsmiddel at bruge - i stedet for ransagning - hos helt uden for stående personer), men skal følge reglerne om indgreb i meddelelseshemmeligheden (telefonaflytning)[(82)].

Der er ved edition som ved indgreb i meddelelseshemmeligheden mulighed for, såfremt der er et særligt efterforskningsmæssigt behov, at den sigtede først på et senere tidspunkt underrettes om retsskridtet. Desuden kan der ved alvorlige forbrydelser pålægges den, mod hvem editionen er rettet, en strafbelagt tavshedspligt efter retsplejelovens § 189.

I den typiske situation vil den sigtede være bekendt med politiets efterforskning[(83)], idet formålet med editionen vil være at finde email, den sigtede har slettet, men som måske fortsat i et vist omfang kan fremfindes hos Internetudbyderen. Der vil således typisk være tale om læst email.

Der er enighed i udvalget om, at hvis der er tale om et fremadrettet indgreb, der har karakter af overvågning af korrespondancen, bør det være omfattet af regler om indgreb i meddelelseshemmeligheden. Dette er også lagt til grund i UfR 1999.178 VLK, hvor en kendelse om oplysninger om indgående email blev anset for omfattet af retsplejelovens § 780, stk. 1, nr. 1, om telefonaflytning.

Udvalget har delt sig i spørgsmålet om, hvorvidt dette også bør gælde for indgreb, der er bagudrettede.

Et flertal i udvalget (Mads Bryde Andersen, Preben Bialas, Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Vagn Greve, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Lars Bo Langsted, Kirsten Mandrup, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder ikke anledning til at foreslå ændringer i retsplejelovens regler om indgreb i meddelelseshemmeligheden.[(84)] Disse medlemmer finder således, at elektronisk post (e-post eller e-mail) ikke adskiller sig grundlæggende fra andre kommunikationsformer, der er omfattet af reglerne om indgreb i meddelelseshemmeligheden, og at der derfor ikke er grund til at give politiet en videre adgang til at foretage indgreb i kommunikation i form af elektronisk post.

---

81. S. 55.

82. Ifølge Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, s. 57, skal telekommunikation sidestilles med telefonsamtaler og ikke med postforsendelser

83. Medmindre de helt specielle regler om hemmelige ransagninger har fundet anvendelse, jfr. retsplejelovens § 799.84. Et flertal i arbejdsgruppen vedrørende datakriminalitet (Mads Bryde Andersen, Jan Carlsen, Hans Jakob Paldam Folker, Carsten Heilbuth, Helle Jahn, Jens Kruse Mikkelsen, Ole Stampe Rasmussen) var af samme opfattelse som udvalgets flertal.

Efter disse medlemmers opfattelse må elektroniske breve sidestilles med traditionelle (fysiske) breve, jfr. retsplejelovens § 780, stk. 1, nr. 4 og 5. En sammenligning af kommunikationsforløbene ved henholdsvis traditionelle brevforsendelser og elektronisk post må efter disse medlemmers opfattelse føre til, at elektronisk post, der beror hos en Internetudbyder, må sidestilles med breve i en postboks, jfr. de ovenfor citerede forarbejder til de gældende bestemmelser.

Det er forudsat, at reglerne om indgreb i meddelelseshemmeligheden ikke omfatter indgreb, der gennemføres inden kommunikationens begyndelse eller efter dens afslutning. Reglerne finder således ikke anvendelse, hvis politiet kan skaffe sig meddelelsen ved et straffeprocessuelt tvangsindgreb mod afsender eller modtager af meddelelsen (jfr. reglerne om ransagning og beslaglæggelse). Hvis politiet derimod ønsker at skaffe sig meddelelsen med bistand fra en kommunikationsformidler, må dette ske efter reglerne om indgreb i meddelelseshemmeligheden. Dette må gælde, uanset om kommunikationsformidleren er et telefonselskab, en postvirksomhed eller en udbyder af

elektronisk kommunikation (herunder en Internetudbyder).

Kommunikationen kan efter de principper, der er lagt til grund ved udformningen af reglerne om indgreb i meddelelseshemmeligheden, kun siges at være afsluttet, når meddelelsen er kommet modtageren i hænde på en sådan måde, at politiet kan skaffe sig adgang til meddelelsen under en ransagning på modtagerens (fysiske) adresse eller ved anvendelse af midler beslaglagt under en sådan ransagning (en postboksnøgle eller en adgangskode til en elektronisk postkasse). Adgangskoden kan f.eks. være fast indkodet i Internetkommunikationsprogrammet (browseren) på den mistænktes computer, således at der ved opstart af programmet automatisk etableres forbindelse til den elektroniske postkasse hos Internetudbyderen. I denne situation vil det ikke være nødvendigt for politiet at gå frem efter reglerne om indgreb i meddelelseshemmeligheden.

Et mindretal i udvalget (Michael Clan, Annemette Møller) finder, at reglerne om edition bør anvendes, og at der ikke bør stilles de særlige krav, der gælder for indgreb i meddelelseshemmeligheden[(85)]

Der er tale om et indgreb, hvor oplysningerne - hvis de fortsat lå hos den sigtede - kunne tilvejebringes i medfør af de almindelige ransagningsregler. De henviser herudover til, at der ved den oprindelige stillingtagen i 1984 til datakommunikation er tænkt på en igang værende kommunikationsstrøm, hvor kommunikationen ikke er nået fysisk frem til den pågældende, og ikke på den særlige email struktur.

Disse medlemmer finder i øvrigt, at der altid bør beskikkes forsvarer i disse situationer, hvis det ikke allerede er sket.

Disse medlemmer lægger også vægt på, at den sigtede selv har valgt, at kommunikationen kan ske via kommunikationskanaler, hvor en tredjemand indgår i forløbet og besidder, hvad der kan sidestilles med en brevkopi. Situationen er meget atypisk i forhold til traditionelle postforsendelser, fordi Internetudbyderen straks har gjort forsendelsen tilgængelig for adressaten på dennes adresse. Der er således efter de principper, der gælder for f.eks. postforsendelser, telexkommunikation og meddelelser til telefonsvarere, ikke tale om et igangværende kommunikationsforløb. Når oplysningerne findes hos Internetudbyderen, er kommunikationen afsluttet. Ønsker man at føre særlig sikret korrespondance, må det ske ved sædvanlige lukkede forsendelser, der ikke er tilgængelige i andre systemer, eller der må anvendes særligt sikre krypteringsteknikker.

Det er også den fortolkning, der anlægges i retspraksis. F.eks. blev der i en sag om piratkopiering afsagt editionskendelse vedrørende email fra den sigtedes kendte email adresse og eventuelle andre adresser tilhørende ham, jfr. UfR 1998.1613 ØLK. Forsvareren gjorde både for byretten oglandsretten gældende, at der var tale om indgreb i meddelelseshemmeligheden, og at der derfor ikke kunne afsiges editionskendelse[(86)]. Byretten afsagde editionskendelse og anførte, at den hos Internetudbyderen beroende post ikke fandtes at være under forsendelse, men måtte ligestilles med post, der var kommet frem til den sigtedes bopæl. Østre landsret stadfæstede kendelsen af de af byretten anførte grunde.

Flertallets forslag er reelt ikke et forslag om ikke at ændre retstilstanden, men er et forslag om at begrænse de efterforskningsmuligheder, der, jfr. Østre landsrets kendelse, må antages at være i dag. Mindretallet finder mere principielt, at det ikke er acceptabelt at foreslå løsninger, der begrænser politiets nuværende muligheder for at efterforske og dermed begrænser mulighederne for at bekæmpe kriminalitet.

Der henvises til afsnit 7.4.

---

85. Et mindretal i arbejdsgruppen vedrørende datakriminalitet (Kim Aarenstrup, Jan Friis, Michael Goeskjær, Ulla Høg, Gunnar Kappel, Henrik OftebroSvendsen, Ronald Pedersen) var af samme opfattelse som udvalgets mindretal. De fandt dog, at forudsætningen for at anvende editionsreglerne må være, at der beskikkes en forsvarer i disse situationer, hvis det ikke allerede er sket.

86. Der ville på grund af sagstypen ikke have kunnet afsiges kendelse om indgreb i meddelelseshemmeligheden, idet piratkopiering ikke er en af de kriminalitetstyper, hvor der kan foretages sådanne indgreb, jfr. retsplejelovens § 781.

6.2. Teleoplysninger

Den første lovregulering af området skete ved lov nr. 202 af 11/6 1954, hvor der indsattes følgende bestemmelse som retsplejelovens § 750 a. Bestemmelsen blev ved lov nr. 243 af 8/6 1978 flyttet uændret til § 788:

- "*§ 788*. Det kan endvidere ved rettens kendelse bestemmes, at vedkommende telefonadministration skal meddele politiet oplysninger om, hvilke telefoner der i et bestemt tidsrum sættes eller har været sat i forbindelse med en bestemt telefon, når
- 1) der er påviselig grund til at antage, at de ønskede oplysninger vil være af betydning for opklaring af en af de i § 787, stk. 1, omhandlede forbrydelser[87], eller
- 2) det skønnes sandsynligt, at opklaring af en forbrydelse kun vil være mulig gennem de ønskede oplysninger, og foranstaltningen står i rimeligt forhold til forbrydelsens karakter, eller
- 3) det må antages, at det kun ved hjælp af de ønskede oplysninger er muligt at finde frem til den, der gør sig skyldig i gentagne fredskrænkelser som omhandlet i straffelovens § 265.
- *Stk. 2*. I påtrængende tilfælde kan politiet uden forudgående retskendelse træffe bestemmelse som i stk. 1 nævnt. § 787, stk. 3,[88] finder da tilsvarende anvendelse."

I Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter foreslog udvalget[89], at de dagældende regler blev ændret således, at der ved alle former for kriminalitet kunne gives teleoplysninger, hvis indehaveren samtykkede (den nugældende § 786, stk. 2, i retsplejeloven). Det nævntes endvidere[90], at teleoplysning hidtil kun havde været anvendt i beskedent omfang, og antagelig overvejende med indehaverens samtykke, men kunne tænkes at tiltrække sig større opmærksomhed i fremtiden også uden for samtykkesituationen.

Det fremgår af betænkningen[91], at udvalget foreslog et fælles kriminalitetskrav for alle indgreb i meddelelseshemmeligheden, hvilket for nogle af indgrebenes vedkommende betød strengere krav og for andre mildere krav, og at den særlige regel om fredskrænkelser ønskedes opretholdt i relation til teleoplysninger. For teleoplysningers vedkommende betød det fælles kriminalitetskrav, at den særlige mulighed for at få teleoplysninger, når det skønnedes sandsynligt, at opklaring af en forbrydelse kun ville være mulig gennem de ønskede oplysninger, og foranstaltningen stod i rimeligt forhold til forbrydelsens karakter, bortfaldt.

---

87. En række særligt opremsede forbrydelser samt forbrydelser med et strafmaksimum på 8 år eller derover.
88. Om underretning til retten med henblik på rettens godkendelse.
89. Betænkningen s. 61 f.
90. Betænkningen s. 63.
91. Betænkningen. s. 89 f.

Der opstod efterfølgende tvivl om, hvorvidt lagrede teleoplysninger skulle behandles efter reglerne om edition eller efter reglerne om indgreb i meddelelseshemmeligheden[92]. Østre landsret afsagde den 22/2 1991 kendelse om, at det var editionsreglerne, der skulle anvendes ved lagrede teleoplysninger. Vestre landsret anvendte i UfR 1992.638 VLK reglerne om teleoplysninger[93]. Dette er også lagt til grund i de i afsnit 6.4 omtalte sendemastkendelser.

Domstolene stiller i dag krav om, at både editionsreglerne og reglerne om indgreb i meddelelseshemmeligheden skal være opfyldt, før der kan afsiges kendelse vedrørende lagrede teleoplysninger[94].

Et flertal i udvalget (Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Vagn Greve, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Lars Bo Langsted, Kirsten Mandrup, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder ikke anledning til at foreslå ændringer af retsplejelovens regler om indgreb i meddelelseshemmeligheden i form af teleoplysning[95].

Regler om indgreb i meddelelseshemmeligheden er udtryk for en afvejning af på den ene side hensynet til en effektiv kriminalitetsbekæmpelse og på den anden side hensynet til borgernes privatliv.

92.

Strafferetsplejeudvalget havde dog anført, betænkningen s. 210, at der ikke ved udeladelsen af ordene "eller har været sat", der fandtes i den gældende § 788, var tilsigtet nogen realitetsændring.

93. I UfR 1989.870 VLK havde landsretten tidligere fundet, at der ikke var hjemmel i retsplejelovens § 780, stk. 1, nr. 3, til at give bagudrettede teleoplysninger.

94. Jfr. UfR 1993.1 HKK og UfR 1995.374 HKK. Det nævnes i lovforslag L 41 199899 om beslaglæggelse, edition m.v., FT 1997/98 A 828, i bemærkningerne til § 801, at der ikke med lovforslaget tilsigtes ændringer i denne retstilstand. Dette er også lagt til grund i lovforslag nr. L 202 199596 om datakriminalitet, FT 1995/96 A 4068, jfr. lovforslagets pkt. 5.3 og 5.4 og den nugældende bestemmelse i retsplejelovens § 781, stk. 3.

95. Et mindretal i arbejdsgruppen vedrørende datakriminalitet (Jan Carlsen, Hans Jakob Paldam Folker, Helle Jahn, Jens Kruse Mikkelsen, Ole Stampe Rasmussen) var af samme opfattelse som udvalgets flertal.

Efter flertallets opfattelse tilsiger hensynet til beskyttelse af borgernes fortrolige kommunikation med andre også en beskyttelse af oplysninger om, *hvem* der er kommunikeret med. Dette er også lagt til grund i Strafferetsplejeudvalgets betænkning nr. 1024/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter.

Uanset et indgreb i form af indhentning af teleoplysninger kan siges at indebære en vis mindre grad af integritetskrænkelse end de øvrige indgreb i meddelelseshemmeligheden, herunder telefonaflytning, bør der efter disse medlemmers opfattelse - henset til de ovenfor beskrevne modhensyn - ikke gives politiet adgang til teleoplysninger efter (de væsentlig lempeligere) regler om edition.

En anvendelse af reglerne om edition vil således bl.a. indebære, at indgrebet som udgangspunkt kan anvendes ved alle former for kriminalitet. En begrænsning vil alene følge af en proportionalitetsafvejning i den konkrete sag, dvs. om indgrebet står i misforhold til sagens betydning og den ulempe, som indgrebet kan antages at medføre. Efter reglerne om indgreb i meddelelseshemmeligheden kan indgrebet - bortset fra enkelte i loven særligt opregnede lovovertrædelser - kun anvendes ved efterforskning af lovovertrædelser, der efter loven kan straffes med fængsel i 6 år eller derover.

For så vidt angår spørgsmålet om en udvidelse af reglerne om indgreb i meddelelseshemmeligheden - en udvidelse der i givet fald også vil få betydning for teleoplysninger - henvises til afsnit 6.5 nedenfor.

Mindretallets forslag (omtalt nedenfor) indebærer, at også pålæg til teleselskabet om registrering af teleoplysninger i en periode frem i tiden skal behandles efter reglerne om edition. Disse regler indeholder - i modsætning til reglerne om indgreb i meddelelseshemmeligheden - ikke bestemmelser om frister for sådanne indgreb, idet editionsregler i alt væsentligt er tænkt anvendt på allerede eksisterende oplysninger. Editionsreglerne indeholder heller ikke regler om beskikkelse af advokat for indehaveren af pågældende telefon og foreslås af mindretallet kun ændret således, at der skal ske forsvarerbeskikkelse for den sigtede, der ikke behøver at være identisk med indehaveren af telefonen. Mindretallets forslag indebærer således på flere punkter en svækkelse af de retsgarantier, som de gældende regler er udtryk for.

Et mindretal i udvalget (Mads Bryde Andersen, Preben Bialas, Michael Clan, Annemette Møller) finder, at det ved teleoplysninger, der allerede lagres i anden sammenhæng, bør være en tilstrækkelig garanti, at der skal afsiges editionskendelse[(96)]. Oplysningerne er ikke mere følsomme end en række andre oplysninger, der kan udleveres efter editionsreglerne, og det kræver i dag ikke et særligt indgreb fra teleselskabernes side at fremskaffe oplysningerne.

---

96. Et flertal i arbejdsgruppen vedrørende datakriminalitet (Kim Aarenstrup, Mads Bryde Andersen, Jan Friis, Michael Goeskjær, Carsten Heilbuth, Ulla Høg, Gunnar Kappel, Henrik OftebroSvendsen, Ronald Pedersen) var af samme opfattelse som mindretallet.

Disse medlemmer er enige om, at forudsætningen for at anvende editionsreglerne skal være, at der beskikkes en forsvarer i disse situationer, hvis det ikke allerede er sket.

Mindretallet vil pege på, at teleoplysninger er det mindst indgribende af de indgreb, der reguleres af reglerne om

indgreb i meddelelseshemmeligheden. Ved indgrebet får politiet ikke kendskab til indholdet af kommunikationen, ligesom kommunikationen ikke unddrages modtageren.

Betydningen af at kunne få teleoplysninger er endvidere betydelig større ved den kriminalitet, der kendes i dag, end den var, da strafferetsplejerådet foreslog den ensartede regulering af området. Dette har også efterfølgende medført behov for, at der blev skabt en særlig hjemmel i retsplejelovens § 781, stk. 2 og stk. 3, til at indhente teleoplysninger i hackersager og telefonmisbrugssager. Også for så vidt angår sager om børnepornografi er der i dag behov derfor, ligesom der i øvrigt vil kunne være behov i sagstyper, hvor Internettet indgår, f.eks. i sager om piratkopiering eller kursmanipulation. Også på områder uden for den IT-relaterede kriminalitet - f.eks. i sager om EUsvig eller afgiftssvig i øvrigt - er der på grund af mange personers samvirke og indbyrdes kommunikation et større behov end tidligere for at få oplysninger af denne type.

Området for teleoplysninger, der tidligere blev registreret i forbindelse med teleselskabernes kontrol eller i forbindelse med efterforskning, har ændret sig væsentligt gennem de senere år. Der sker i dag automatisk en omfattende registrering, og kunder kan vælge at få alle samtaler specificeret (i hvilket tilfælde oplysningerne vil kunne findes ved en ransagning). Der er således i vidt omfang ikke tale om, at teleoplysninger indhentes i specielt øjemed, men alene om almindelig adgang til data, teleselskabet allerede besidder.

Det fremgår af Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, s. 62, jfr. s. 254 ff., at udgangspunktet var, at teleoplysninger forudsatte, at der blev etableret en fastholdeanordning. Teleoplysninger havde således en anden karakter, end tilfældet er i dag, idet oplysningerne som udgangspunkt ikke forelå, men kunne tilvejebringes ved særlige tekniske indgreb. I modsætning til i dag kunne alle derfor forvente, at teleoplysninger ikke fandtes, medmindre der blev foretaget et særligt indgreb, mens det i dag er almindelig viden, at oplysningerne altid registreres hos teleselskabet.

Teleoplysninger, der alene angiver, hvilke telefonnumre m.v. der har været forbindelse til, adskiller sig indgrebsmæssigt markant fra de mere indgribende tiltag som telefonaflytning m.v. Det kan derfor være nærliggende at overveje, om adgangen til sådanne oplysninger i de tilfælde, hvor de allerede

registreres i andet øjemed, skal flyttes fra reglerne om indgreb i meddelelseshemmeligheden, således at alene editionsreglerne finder anvendelse.

Konsekvensen af at benytte editionsreglerne er, at de særlige krav i retsplejelovens § 781 til kriminalitetens art og indgrebets afgørende betydning for efterforskningen ikke finder anvendelse.

Det bemærkes i den forbindelse, at domstolene også ved edition vurderer, om indgrebet konkret er nødvendigt, og at disse regler også finder anvendelse på andre følsomme oplysninger - f.eks. oplysninger, der skal indhentes fra den sigtedes pengeinstitut eller revisor[(97)].

Editionsreglerne anvendes normalt ved alle oplysninger, uanset hvor følsomme de er, når oplysningerne er tilgængelige hos den, editionen rettes mod, uden særlige tiltag. Domstolene er derfor også ved edition vant til, at der er forskel på følsomheden af de ønskede oplysninger, og at dette kan have betydning for, hvornår og i hvilket omfang en begæring om edition - f.eks. i et pengeinstitut, hos en revisor eller hos en advokat - skal imødekommes.

---

97. Ved lov nr. 229 af 21/4 1999 om ændring af retsplejeloven (Beslaglæggelse, edition m.v.) er den almindelige proportionalitetsgrundsætning blevet lovfæstet bl.a. ved, at den nye § 805, stk. 1, har fået følgende formulering: "Beslaglæggelse må ikke foretages, og pålæg om edition må ikke meddeles, såfremt indgrebet står i misforhold til sagens betydning og det tab eller den ulempe, som indgrebet kan antages at medføre."

De særlige regler om teleoplysninger afviger således i dag - hvor der ikke skal foretages særlige indgreb for at fremskaffe dem - fra de regler der i øvrigt gælder for selv meget følsomme oplysninger, som personer eller selskaber besidder som et almindeligt led i deres virksomhed.

Disse medlemmer vil i den forbindelse også pege på, at en vis overvågning af en mistænkts adfærd også helt uden retskendelse er tilladt i visse tilfælde. Det gælder for almindelig skygning og vil efter lovforslaget om beslaglæggelse, edition m.v. også efter lovreguleringen af observation[(98)] gælde for fotografering, iagttagelse med

kikkert o.l. af personer, der befinder sig på et ikke frit tilgængeligt sted, hvis indgrebet må antages at være af væsentlig betydning for efterforskningen og den aktuelle lovovertrædelse kan medføre frihedsstraf. Mere indgribende observationsformer (fjernbetjente eller automatisk virkende overvågningsapparater) stilles der større krav til, herunder krav om kendelse, og sker denne observation i bolig eller andre husrum svarer kravene til de almindelige krav ved indgreb i meddelelseshemmeligheden.

---

98. Lovforslagets § 791 a.

Justitsministeriet har i lovforslaget taget stilling til, om pejling skulle lovreguleres. Det siges herom:

- "Ved *pejling* forstås, at politiet monterer pejleudstyr på en genstand, f.eks. en bil, som politiet formoder kan være lastet med narkotika, med henblik på at kunne følge genstandens bevægelser på afstand. For en umiddelbar betragtning har pejling visse lighedspunkter med observation og aflytning. Ved hjælp af teknisk udstyr opnår politiet en viden, som normalt forudsætter, at man fysisk er til stede.
- Pejling giver imidlertid ikke mulighed for at optage billeder eller aflytte samtaler. Pejling har nærmest karakter af en "skygning" under anvendelse af tekniske hjælpemidler. Indgrebet ses derfor ikke at være af så væsentlig og indgribende karakter, at det bør sidestilles med andre efterforskningsmidler, der er reguleret i retsplejeloven.
- På den baggrund finder Justitsministeriet ikke anledning til at foreslå en lovregulering af politiets anvendelse af pejling.
- Det bemærkes, at Vestre Landsret den 16. september 1996 har afsagt kendelse om pejling (gengivet i *Ugeskrift for Retsvæsen 1996, s. 1496*). Landsretten fandt, at monteringen og anvendelsen af elektronisk sporingsudstyr på en mistænkts bil (pejling) ikke var et straffeprocessuelt tvangsindgreb. Efter landsrettens opfattelse var der tale om skygning under anvendelse af tekniske hjælpemidler, og et sådant efterforskningsskridt krævede ikke lovhjemmel og dermed heller ikke forudgående indhentelse af rettens kendelse."

Mindretallet vil særligt fremhæve, at der bl.a. ved afgørelsen af, hvor indgribende et indgreb pejling er, lægges vægt på, at der ikke er mulighed for at optage billeder eller aflytte samtaler. Teleoplysninger - der også efter disse medlemmers forslag fortsat vil kræve retskendelse - er ligeledes karakteriseret ved, at man kan følge den mistænktes bevægelser (ikke som ved peling fysiske bevægelser, men bevægelser på telekommunikationsnet), men ikke får andre personlige oplysninger i forbindelse med indgrebet.

Der henvises til afsnit 7.5 vedrørende udvalgets forslag.

6.3. Teleoplysninger i henhold til samtykke m.v.

Efter retsplejelovens § 786, stk. 2, kan der i alle sagstyper gives teleoplysninger i henhold til retskendelse, hvis indehaveren af apparatet meddeler samtykke.

I UfR 1996.18 VLK fandt Vestre landsret det efter forarbejderne til bestemmelsen betænkeligt at antage, at bestemmelsen havde haft tilfælde for øje, hvor der var tale om en offentlig telefon. De to teleselskaber kunne derfor ikke give samtykke til at udlevere udskrifter over de telefonnumre, der var blevet kontaktet ved hjælp af et telekort.

- Sagen vedrørte indbrudstyverier, og der var under ransagning hos den sigtede fundet et telekort. Et vidne havde oplyst, at han havde set den sigtede telefonere fra en korttelefonboks og set, at der umiddelbart efter var ankommet en varebil til den sigtedes bopæl, hvor bilen blev læsset med nogle papkasser. Anklageren henviste til, at der var bestemte grunde til at antage, at der med telekortet var blevet kontaktet personer, som kunne mistænkes for hæleri. (Betingelserne for indgreb i meddelelseshemmeligheden var ikke opfyldt, idet sagen vedrørte tyveri, der dengang ikke gav mulighed for teleoplysninger, og mistanke om hæleri, hvis omfang der ikke kunne siges noget om).

Såfremt teleoplysninger helt eller overvejende bliver omfattet af editionsreglerne, vil en editionskendelse i denne situation rette sig til teleselskaberne.

Et flertal i udvalget (Preben Bialas, Susan Bramsen, Bent Carlsen, Vagn Greve, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Kirsten Mandrup, Lene Nielsen, Henrik Rothe) finder ikke, at teleselskaberne skal kunne meddele samtykke ved offentlige telefoner[(99)].

---

99. Et mindretal i arbejdsgruppen vedrørende datakriminalitet (Hans Jakob Paldam Folker, Helle Jahn, Jens Kruse Mikkelsen, Ole Stampe Rasmussen) var af samme opfattelse.

Bestemmelsen i retsplejelovens § 786, stk. 2, bygger på det synspunkt, at en telefonabonnent ikke i forhold til telefonselskabernes tavshedspligt kan anses for "uvedkommende" med hensyn til oplysninger om, hvem der ringer til abonnenten, og at der ikke er en sådan beskyttelsesværdig interesse i hemmeligholdelse hos personer, der kalder et andet telefonnummer, at udlevering af disse oplysninger til politiet med samtykke fra indehaveren af denne telefon bør omfattes af reglerne om indgreb i meddelelseshemmeligheden, jfr. Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, s. 62. I retspraksis er det fastslået, at bestemmelsen også finder anvendelse på oplysninger om udgående opkald fra en bestemt telefon, jfr. UfR 1996.169 ØLK.

Efter disse medlemmers opfattelse kan et telefonselskab ikke siges at have rådighed over en offentlig telefon på samme måde som en privat telefonabonnent har rådighed over sin telefon. Der er derfor ikke samme anledning til at give telefonselskabet adgang til med sit samtykke at fravige reglerne om indgreb i meddelelseshemmeligheden. Hvis man låner en privat telefon (eller stjæler en mobiltelefon) må man være indstillet på, at den pågældende telefonabonnent modtager udførlige samtalespecifikationer i forbindelse med telefonregningen. Benyttelsen af en offentlig telefon kan nærmest betragtes som et "ad hocabonnement", hvor man mod vederlag får (en begrænset) adgang til at benytte telefonnettet. Et indgreb mod en bruger af en offentlig telefon bør derfor sidestilles med et indgreb imod en privat telefonabonnent. De særlige hensyn, der i sin tid begrundede bestemmelsen i § 786, stk. 2, kan efter disse medlemmers opfattelse ikke udstrækkes til også at begrunde en lignende regel for offentlige telefoner.

Udvalget finder i øvrigt, at formuleringen i retsplejelovens § 786, stk. 1, bør tilpasses den terminologi, der anvendes i dag vedrørende post og televirksomhed.

Et mindretal i udvalget (Mads Bryde Andersen, Hans Henrik Brydensholt, Jørgen Christiansen, Michael Clan, Alexander Houen, Lars Bo Langsted, Annemette Møller) finder, at teleselskaberne - uanset hvilket regelsæt der finder anvendelse - skal kunne meddele samtykket, når der er tale om offentlige telefoner. Der er enighed om, at der skal beskikkes en forsvarer i disse situationer, hvis det ikke allerede er sket[(100)].

Disse medlemmer har i den forbindelse lagt vægt på, at der ikke kan være nogen berettiget forventning om, at indehaveren af en telefon ikke kan give politiet (adgang til) oplysning om, hvilken brug der har været gjort af telefonen. Med den retstilstand, der er i dag vedrørende indgreb i meddelelseshemmeligheden, betyder det, at der ved en lang række kriminalitetsformer ikke er mulighed for at få adgang til disse allerede registrerede oplysninger, hvis en offentlig telefon er benyttet (i modsætning til f.eks. en telefon, der ejes af en restaurant).

Spørgsmålet om samtykke ved offentlige telefoner er opstået som en konsekvens af, at oplysningerne i dag registreres. Det er af samme grund ikke behandlet i Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, der, jfr. betænkningens s. 61 ff., især tager udgangspunkt i, at hovedområdet for teleoplysninger er truende, injurierende eller på andre måder generende telefonopkald til en privat abonnent. Udvalgets forventninger til, at indgrebet i fremtiden vil tiltrække sig større opmærksomhed, er især knyttet til, at telefonaflytninger er ressourcekrævende, og at det i en del sager kunne være af betydning for politiet at få oplyst, om bestemte telefoner, til hvis indehavere man har mistanke i sagskomplekset, bliver sat i forbindelse med hinanden.

I den ovenfor nævnte kendelse (UfR 1996.169 ØLK) blev det lagt til grund, at indehaveren af en stjålen mobiltelefon kunne meddele samtykke efter retsplejelovens § 786, stk. 2. Denne kendelse understøtter efter disse medlemmers opfattelse det synspunkt, at det formelle ejerskab er tilstrækkeligt til, at man er samtykkeberettiget, også når samtalerne utvivlsomt er abonnenten helt uvedkommende.

Et af udvalgets medlemmer (Erik Overgaard) har ikke taget stilling til, hvilken løsning der skal vælges.

Der henvises til afsnit 7.6 vedrørende udvalgets forslag.

---

100. Et flertal i arbejdsgruppen vedrørende datakriminalitet (Kim Aarenstrup, Mads Bryde Andersen, Jan Carlsen, Jan Friis, Michael Goeskjær, Carsten Heilbuth, Ulla Høg, Gunnar Kappel, Henrik OftebroSvendsen, Ronald Pedersen) var af samme opfattelse.

6.4. Særligt om sendemaster

En særlig variant af teleoplysninger er de såkaldte "masteoplysninger". Hvor den typiske situation ved teleoplysninger er, at der ønskes oplysninger vedrørende bestemte telefonnumre, er situationen ved masteoplysninger den, at der ønskes oplysninger om alle telefoner, der i et givet tidsrum har benyttet en bestemt sendemast.

Indgrebet er primært relevant i store sager om grove kriminalitetsformer, f.eks. sager om rockerdrab, ildspåsættelser o.l. Som et eksempel, hvor der kan være behov for indgreb af denne type, kan også nævnes en ny sag, hvor falske politifolk bortførte en chauffør og en lastbil med 7 mio. cigaretter.

I udtalelser i anledning af nedenfor nævnte afgørelse i UfR 1997.1021 H om behovet for at kunne få sendemastoplysninger er også peget på, at der kan være behov for masteoplysninger i forbindelse med terrorattentater eller igangværende gidselsituationer.

Udgangspunktet i de sager, hvor der er behov for indgrebet, er således, at et antal ukendte personer, der har begået en alvorlig forbrydelse, vurderes nødvendigvis at måtte have kommunikeret med hinanden umiddelbart før og efter gerningen, muligvis via mobiltelefoner. En mulighed, måske den eneste, for at komme opklaringen nærmere er at få en logudskrift fra sendemasten nærmest gerningsstedet for et tidsrum eksempelvis fra 1 time før til ½ time efter forbrydelsen for at kunne se, hvilke telefoner der har kommunikeret via masten i det relevante tidsrum.

Masteoplysninger er ikke selvstændigt reguleret i retsplejelovens § 780, men de udgør en særlig form for teleoplysninger, idet det alene er et spørgsmål om at få oplysninger om teleforbindelser og ikke om indholdet af kommunikationen.

Som eksempler på sendemastkendelser kan nævnes følgende, hvoraf 3 har været behandlet af Højesteret:

- *Højesterets kendelse af 28/6 1994*[(101)]
  Sagen vedrørte efterforskning i forbindelse med mistanke om grov narkotikakriminalitet og omfattende hæleri. Der blev i den forbindelse anmodet om kendelse om aflytning af samtaler, der foregik via mobiltelefon fra en bestemt ejendom, samt teleoplysninger vedrørende kommunikation med de pågældende mobiltelefoner.
  Byretten afsagde kendelse herom under henvisning til retsplejelovens § 780, stk. 1, nr. 1, nr. 2 og nr. 3.
  Østre Landsret ophævede kendelsen under henvisning til, at der ikke var hjemmel til at foretage telefonaflytning af ikke nærmere angivne mobiltelefoner eller til at foretage aflytning af telefoner inden for et angivet afgrænset område.
  Højesteret stadfæstede byrettens afgørelse med følgende begrundelse: "Højesteret finder, at bestemmelserne i retsplejelovens § 780, stk. 1, nr. 1, nr. 2 og nr. 3, efter deres ordlyd omfatter de her omhandlede indgreb. Indgrebene kan ikke anses for mere vidtgående end de tilfælde af aflytning, der traditionelt henføres under bestemmelserne, og der findes ikke grundlag for gennem en indskrænkende fortolkning at afskære anvendelsen af disse efterforskningsskridt. Idet betingelserne efter retsplejelovens § 781, stk. 1, efter det oplyste er opfyldt, tager Højesteret derfor anklagemyndighedens påstand til følge."

---

101. Kendelsen er ikke trykt i UfR, men Højesterets afgørelse er gengivet i note 1 til UfR 1996.1339 HKK.

UfR 1996.1339 HKK

Der blev anmodet om kendelse bl.a. om oplysning om, hvilke kommunikationsapparater der fra en dag kl. 22.00 til næste dag kl. 06.00 havde været sat i forbindelse med hinanden under aktivering af sendemaster, der geografisk dækkede en bestemt adresse og en radius på 1 km. herfra.
Byretten afsagde kendelse herom.
Vestre landsret ophævede kendelsen herom med følgende begrundelse: "Således som begæringen er udformet, vil indgrebet omfatte ikke telefoner m.v., der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat, men telefoner m.v., der sættes i forbindelse med en helt ubestemt kreds af telefoner eller andre kommunikationsapparater i et større område. Da et sådant indgreb ikke har hjemmel i retsplejelovens § 780, stk. 1, nr. 3, kan begæringen ikke tages til følge, og den påkærede kendelse om udlevering af de anførte optegnelser ophæves derfor."
Højesteret stadfæstede byrettens afgørelse bl.a. under henvisning til Højesterets kendelse af 28/6 1994.

Byretskendelse af 29/11 1996

- Sagen vedrørte efterforskning af drabsforsøg i forbindelse med skud mod 2 rockere. Der blev i den forbindelse anmodet om kendelse om oplysning om, hvilke kommunikationsapparater der den aktuelle dag mellem kl. 00.01 og 06.00 havde været sat i forbindelse med hinanden under aktivering af sendemaster, der geografisk dækkede den gade, hvor der var skudt, og en radius på 2 km. herfra. Byretten afsagde kendelse om dette indgreb, men begrænsede radius til 1 km.

Vestre landsrets kendelse af 21/12 1996

- Sagen vedrørte efterforskning af brandstiftelse. Der blev i den forbindelse anmodet om kendelse om oplysning om, hvilke kommunikationsapparater der en dag fra kl. 23.00 til næste dag kl. 01.00 og en anden dag fra kl. 01.00 til kl. 03.00 havde været sat i forbindelse med hinanden under aktivering af sendemaster, der geografisk dækkede et område, der var afgrænset af 3 gader.
  Byretten afsagde kendelse om det ønskede indgreb, og Vestre landsret stadfæstede kendelsen.

UfR 1997.1021 H

- Sagen vedrørte efterforskning i forbindelse med en bombe, der var placeret i en gade. Der blev anmodet om kendelse om oplysning om, hvilke kommunikationsapparater der fra en dag kl. 18.00 til næste dag kl. 06.00 havde været sat i forbindelse med hinanden under aktivering af sendemaster, der geografisk dækkede en bestemt adresse og en radius på 1 km. herfra.
  Byretten afslog med følgende begrundelse: "Da det ønskede indgreb vedrører et meget vidt og ubestemt antal telefoner, findes der ikke bestemte grunde til at antage, at der fra de pågældende telefoner er givet meddelelse af betydning for efterforskningen til eller fra mistænkte for forsøg på manddrab. Som følge heraf findes betingelserne i retsplejelovens § 781, stk. 1, nr. 1 og nr. 2, ikke opfyldt."
  Østre landsret afsagde den ønskede kendelse under henvisning til Højesterets afgørelser fra 1994 og 1996.
  For Højesteret blev det oplyst, at indgrebet ifølge teleselskaberne ville omfatte 25.00030.000 samtaler.
  Højesteret stadfæstede byrettens kendelse under henvisning til de nu foreliggende oplysninger om den manglende mulighed for nærmere afgrænsning af samtaleregistreringer vedrørende mobiltelefoner.[(102)](#) [(103)](#)

Afgørelsen fra 1997, der var en ændring af Højesterets tidligere praksis, har betydning både i relation til telefoner og i relation til trådløs datatransmission.

[102.] I note 1 til kendelsen henvises til en artikel af Ole Unmack Larsen i Juristen 1997 s. 35 ff. "Mobiltelefoner og retsplejelovens § 780, stk. 1, nr. 1, nr. 2 og nr. 3". I artiklen er bl.a. en beskrivelse af antallet af radioceller, daglige samtaler pr. celle og masternes rækkevidde.
[103.] Rigsadvokaten henviste i sit kæreskrift bl.a. til, at aflytning af en offentlig telefon i en lufthavn eller på en banegård ligeledes vil kunne omfatte en større personkreds og tillige vil være mere indgribende, idet politiet får kendskab til samtalens indhold

---

Rigsadvokaten har på baggrund af denne kendelse anbefalet over for Justitsministeriet, at der skabes lovhjemmel til at indhente sådanne teleoplysninger. Rigsadvokaten har i forbindelse hermed fremhævet, at masteoplysninger er et vigtigt efterforskningsmiddel, og at den utilsigtede krænkelse af en større personkreds, der af tekniske årsager kan

blive omfattet, er af relativ beskeden karakter, ligesom der er pligt til snarest at destruere oplysninger, der er uden efterforskningsmæssig betydning. Endvidere kan indgrebet kun foretages under retlig kontrol og under iagttagelse af de almindelige proportionalitetsregler.

Det fremgår af Justitsministeriets lovforslag om beslaglæggelse, edition m.v.[(104)], at Justitsministeriet har overvejet i forbindelse med dette lovforslag at medtage et forslag, der skaber hjemmel til indhente de teleoplysninger, der er omtalt i Højesterets 1997kendelse, men at Justitsministeriet finder, der er behov for nærmere overvejelser navnlig om, hvordan en sådan hjemmel skal udformes for at tage højde for den teknologiske udvikling. Justitsministeriet har derfor fundet det rigtigst, at spørgsmålet indgår i overvejelserne i udvalget om økonomisk kriminalitet og datakriminalitet.

Østre landsret har ved en kendelse af 13/11 1998, jfr. UfR 1999.320 Ø, stadfæstet en kendelse om, at der kunne indhentes masteoplysninger i en sag om forsøg på manddrab. Landsretten lagde vægt på, at situationen adskilte sig fra den situation, der var aktuel ved Højesterets kendelse i 1997, idet der forelå oplysninger om én kortvarig telemeddelelse modtaget på en bestemt lokalitet, således at denne meddelelse skulle afgrænses over for et forholdsvis begrænset antal meddelelser eller samtaler. (Det drejede sig om 998 opkald over en periode på 50 minutter).

Som nævnt i afsnit 2.2 udfærdigede EU den 17/1 1995 en resolution om lovlig aflytning af telekommunikation[(105)]. Bl.a. bør de retshåndhævende myndigheder have mulighed for at kunne få så nøjagtig oplysning som mulig om mobile abonnenters geografiske placering inden for nettet.

Udvalget er enig i Rigsadvokatens betragtninger. Udvalget finder derfor, at der bør tilvejebringes en klar hjemmel til indgreb af denne type. For at sikre, at der tages højde for den teknologiske udvikling, bør formuleringen ikke specifikt vedrøre masteoplysninger, men vedrøre teleoplysninger, der ikke kan specificeres på kendelsestidspunktet.

De medlemmer af udvalget, der i øvrigt finder, at editionsreglerne frembyder tilstrækkelig garanti ved lagrede teleoplysninger, er enige med de øvrige medlemmer i, at masteoplysninger og tilsvarende oplysninger skal behandles efterindgreb i meddelelseshemmeligheden, da der er tale om meget bredere indgreb.

Udvalget finder herudover, at reglerne skal opfylde kravene til særligt kvalificere indgreb i meddelelseshemmeligheden[(106)].

Der henvises til afsnit 7.5 vedrørende udvalgets forslag.

---

104. FT 1998/99 A 828.
105. Jfr. bilag 1.
106. Der var også enighed i arbejdsgruppen vedrørende datakriminalitet om en regulering som den af udvalget foreslåede.

6.5. Indgreb i meddelelseshemmeligheden i øvrigt

Som nævnt i afsnit 2.1 ændredes retsplejelovens § 781 i 1996[(107)] således, at der blev adgang til telefonaflytning og teleoplysninger i hackersager[(108)] og adgang til teleoplysninger i sager om overtrædelse af straffelovens § 279 a eller § 293, stk. 1, begået ved anvendelse af en telekommunikationstjeneste.

- Det siges i lovforslaget[(109)] om baggrunden for denne ændring bl.a.:
- "For så vidt angår spørgsmålet om *indgreb i meddelelseshemmeligheden* kan Justitsministeriet tilslutte sig Strafferetsplejeudvalgets principielle synspunkt (jf. bet. 1023/1984, s. 5152), hvorefter der generelt bør sættes snævre grænser for politiets indgreb i meddelelseshemmeligheden.
- Som også fremhævet af Strafferetsplejeudvalget er der imidlertid nye kriminalitetsformer, hvor sædvanlige efterforskningsmetoder ikke rækker til.
- Der må derfor foretages en afvejning mellem på den ene side den ulempe eller skade, som indgrebet er forbundet med for samfundet og for den enkelte, som indgrebet rammer, og på den anden side den betydning,

indgrebet har som middel til opklaring og bekæmpelse af kriminalitet, samt kriminalitetens art og grovhed.

- Efter Justitsministeriets opfattelse har udviklingen siden 1985 - hvor Folketinget senest drøftede spørgsmålet om indgreb i meddelelseshemmeligheden over for "hackerkriminalitet" - vist behov for at anvende dette efterforskningsmiddel over for kriminalitet, der begås ad elektronisk vej, og hvor mere traditionelle efterforskningsmetoder derfor ikke er anvendelige. "Hackerkriminalitet" begås således typisk ved, at gerningsmanden fra sin egen pc'er og gennem et modem kobler sig på det offentlige telefonnet eller eventuelt et datanet og derfra gennem forurettedes modem eller en tilsvarende "indgang" skaffer sig adgang til forurettedes dataanlæg.
- Ganske vist er det som nævnt ovenfor i pkt. 4.2.2. muligt at foretage teleoplysning med samtykke fra en forurettet, jf. retsplejelovens § 786, stk. 2. Den fremgangsmåde er imidlertid langt fra altid tilstrækkelig. Der kan således være forurettede, der modsætter sig politiets indblanding, jf. herved ovenfor pkt. 4.1. om påtalespørgsmålet. Langt vigtigere er det imidlertid, at politiet når det f.eks. med samtykke fra en forurettet er lykkedes at finde en mistænkt ofte vil have behov for at foretage teleoplysninger med udgangspunkt i den mistænktes telefon m.v. for at belyse omfanget af hans mulige kriminelle aktivitet over for andre ofre. Hertil kommer yderligere, at der kan være behov for telefonaflytning; ikke så meget med hensyn til samtaler som med hensyn til datakommunikation for derigennem at klarlægge den nærmere karakter af den strafbare handling, dvs. hvad den mistænkte foretager sig med hensyn til fremmede dataanlæg.
- Det er på den baggrund Justitsministeriets opfattelse, at der i sager om overtrædelse af straffelovens § 263, stk. 2, og § 263, stk. 3, jfr. stk. 2, bør være mulighed for at foretage telefonaflytning og teleoplysning, uanset kriminalitetskravet ikke er opfyldt. Derimod ses der ikke at være anledning til at give mulighed for at foretage anden aflytning, brevåbning eller brevstandsning.

¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿

¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿

¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿

[107.] Ved lov nr. 388 af 22/5 1996.
[108.] Straffelovens § 263, stk. 2 og 3.
[109.] FT 1995/96 A 4068.

- På lignende måde som ved "hackerkriminalitet" begås også "tyveri af telefontid" ved hjælp af telefon eller anden telekommunikationstjeneste. Derfor er de mere traditionelle efterforskningsmetoder ikke anvendelige. For at opklare disse lovovertrædelser er der således behov for at foretage teleoplysning, ikke blot med udgangspunkt i en forurettets telefon m.v., jf. retsplejelovens § 786, stk. 2, (omtalt ovenfor i pkt. 4.2.2. og 4.3.), men også med udgangspunkt i den mistænktes telefon m.v.
- Det er på den baggrund Justitsministeriets opfattelse, at der i de omhandlede sager bør være mulighed for at foretage teleoplysning, uanset at kriminalitetskravet ikke er opfyldt. De almindelige regler om mistankekrav, indikationskrav og proportionalitetskrav vil fortsat finde anvendelse. ¿."

Bestemmelsen blev yderligere udvidet i 1997[(110)], så også grov vold, fareforvoldelse efter straffelovens § 252, stk. 1, grove tyverier og menneskesmugling (udlændingelovens § 59, stk. 3) blev omfattet.

Det siges i lovforslaget[(111)] om baggrunden for denne ændring bl.a.:

- "Justitsministeriet kan tilslutte sig det principielle synspunkt, som både af Strafferetsplejeudvalget og Folketinget blev lagt til grund ved udformningen af de nugældende regler om indgreb i meddelelseshemmeligheden, og hvorefter der generelt bør sættes snævre grænser for politiets indgreb i meddelelseshemmeligheden.
- Reglerne om politiets efterforskningsmidler må imidlertid også ses i lyset af de samfundsmæssige forhold og den udvikling, som sker med hensyn til kriminalitetens karakter.
- Der må derfor - når nye kriminalitetsformer og omfanget af disse giver anledning til det - foretages en afvejning mellem på den ene side den ulempe eller skade, som indgrebet er forbundet med for den, der udsættes for indgrebet, og på den anden side den betydning, indgrebet har som middel til opklaring og

bekæmpelse af kriminalitet, og kriminalitetens art og grovhed.

- Ved denne afvejning indgår det således bl.a., om kriminaliteten har en karakter, som er egnet til at blive afdækket af politiet ved hjælp af indgreb i meddelelseshemmeligheden.
- Det er Justitsministeriets opfattelse, at indgreb i meddelelseshemmeligheden i mange tilfælde vil være et relevant efterforskningsmiddel i forhold til kriminalitet, som er kendetegnet ved, at den begås af flere personer i forening.
- Justitsministeriet finder på den baggrund, at der bør være adgang til indgreb i meddelelseshemmeligheden for kriminalitetsformer, der ofte begås af en flerhed af personer, i det omfang, der er tale om kriminalitet af en så alvorlig karakter, at sådanne indgreb er velbegrundede."

---

110. Ved lov nr. 411 af 6/10 1997.

111. FT 1996/97 A 2475

Ved samme lovændring indsattes bestemmelsen i retsplejelovens § 789, stk. 3, der brød med det hidtidige princip i bestemmelsens stk. 2 om, at tilfældighedsfund i forbindelse med indgreb i meddelelseshemmeligheden ikke måtte anvendes som bevis i retten vedrørende kriminalitet, der ikke ville have kunnet danne grundlag for det pågældende indgreb. Efter den nye bestemmelse kan retten tillade, at beviset anvendes, hvis andre efterforskningsskridt ikke er egnede til at sikre bevis i sagen, og sagen angår en lovovertrædelse, der kan medføre fængsel i 1 år og 6 måneder eller derover.

Det kan mere generelt overvejes, om disse efterhånden mange undtagelser fra hovedreglen om, at der skal være mulighed for fængsel i 6 år, er udtryk for, at bestemmelsen ikke længere er tidssvarende.

Særlig for IT-relateret kriminalitet er der i dag et efterforskningsmæssigt behov for en yderligere udvidelse af området med henblik på bekæmpelse af kriminalitet via Internettet, BBS'er o.l.

Det kan bl.a. fremhæves, at ved groft bedrageri, der f.eks. begås via Internetkommunikation, er der hjemmel til indgreb i meddelelseshemmeligheden. Det er imidlertid ikke sikkert, at man i den indledende efterforskningsfase kan give et rimeligt kvalificeret skøn over omfanget, hvilket efter omstændighederne betyder, at sådanne indgreb ikke kan anvendes. Dette er også baggrunden for, at telefonmisbrug, der omfattes af databedrageribestemmelsen i straffelovens § 279 a, i 1996 fik selvstændig hjemmel til teleoplysninger(112), uanset groft databedrageri opfylder kriminalitetskravet i retsplejelovens § 781, stk. 1.

F.eks. kan sager vedrørende overtrædelse af straffelovens § 235 om børnepornografi ikke efterforskes effektivt med de nugældende regler. Tilsvarende gælder for en række andre sager, f.eks. sager om insiderhandel, kursmanipulation og piratkopiering. Det gælder også industrispionage i forbindelse med husfredskrænkelser, der ellers var omfattet af forslaget i Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter og var medtaget i lovforslaget(113).

Udvalget finder at der i det omfang, hvor der er særligt behov herfor, bør skabes adgang til indgreb i meddelelseshemmeligheden ved IT-relateret kriminalitet. En bestemmelse herom bør dog begrænses til de efterforskningssituationer, hvor der reelt -som ved hacking og telefonmisbrug (hvor andres abonnementer belastes med samtaleafgiften) - ikke er andre effektive efterforskningsmuligheder, herunder efterforskning af kriminalitet, der begås via netværk.

Et flertal i udvalget (Mads Bryde Andersen, Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Vagn Greve, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Lars Bo Langsted, Kirsten Mandrup, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder i overensstemmelse med Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, s. 5152, at der generelt bør sættes snævre grænser for politiets indgreb i meddelelseshemmeligheden, men at der dog - som anført af Strafferetsplejeudvalget og lagt til grund af Folketinget ved senere ændringer af bestemmelserne - kan være særlige kriminalitetsformer, hvor sædvanlige efterforskningsmetoder ikke rækker til. Disse medlemmer finder således, at der løbende på baggrund af udviklingen i kriminalitetsformerne må tages stilling til, om der er behov for at udvide adgangen til indgreb i meddelelseshemmeligheden til flere straffebestemmelser. Der må i den forbindelse foretages en overordnet afvejning mellem på den ene side hensynet til en effektiv kriminalitetsbekæmpelse og på den anden side hensynet

til borgernes privatliv[(114)].

Ved den nedenfor af mindretallet foreslåede bestemmelse vil efterforskning af en betydelig videre kreds af lovovertrædelser end i dag kunne danne grundlag for indgreb i meddelelseshemmeligheden, forudsat at andre efterforskningsmetoder ikke er egnede til at sikre bevis i sagen.

Disse medlemmer kan ikke støtte en sådan generel, væsentlig lempelse af kriminalitetskravet ved indgreb i meddelelseshemmeligheden.

---

112. Jfr. retsplejelovens § 781, stk. 3.

113. Lovforslag nr. L 164 (198485).

114. Et mindretal i arbejdsgruppen vedrørende datakriminalitet (Mads Bryde Andersen, Hans Jakob Paldam Folker, Michael Goeskjær, Helle Jahn, Jens Kruse Mikkelsen) var enig i de betragtninger, udvalgets flertal har på dette område

---

Flertallet finder i denne sammenhæng på det foreliggende grundlag kun anledning til at overveje, om der bør være adgang til at foretage indgreb i meddelelseshemmeligheden ved efterforskning af sager om udbredelse og besiddelse af børnepornografi, jfr. straffelovens § 235. Da denne kriminalitet - på samme måde som "hackerkriminalitet" - i dag i høj grad begås ad elektronisk vej, hvor mere traditionelle efterforskningsmetoder ikke er anvendelige, foreslår disse medlemmer, at der i sager af denne karakter bliver mulighed for indgreb i meddelelseshemmeligheden, uanset det sædvanlige kriminalitetskrav (6 års fængsel i strafferammen) ikke er opfyldt.

Et af flertallets medlemmer (Kirsten Mandrup) finder endvidere, at det tillige bør overvejes at skabe mulighed for indgreb i meddelelseshemmeligheden for så vidt angår efterforskning af sager om misbrug af intern viden og kursmanipulation efter lov om værdipapirhandel m.v. Dette medlem peger på, at det på dette område, hvor kriminalitetskravet på 6 års fængsel ikke er opfyldt, i praksis har vist sig, at traditionelle efterforskningsmetoder ikke i fuldt tilstrækkeligt omfang er egnet til at imødegå denne form for kriminalitet.

Flertallet er enig i, at dette er et område, hvor der kan være anledning til at overveje yderligere udvidelser. Flertallet vil heller ikke udelukke, at en nærmere analyse af andre områder kan vise, at der er behov for en regulering ud over den foreslåede. Der er på den baggrund enighed om, at det indgår i udvalgets videre arbejde, om der kan påpeges behov for yderligere reguleringer.

Et mindretal i udvalget (Preben Bialas, Michael Clan, Annemette Møller) finder, at den regulering, der kan være behov for ved IT-relateret kriminalitet, ikke skal bestå i, at der indsættes en henvisning til endnu flere paragraffer, hvor sådanne indgreb er mulige, uanset hvordan kriminaliteten konkret er gennemført, men derimod skal være en regulering, der begrænses til mere specielle tilfælde og samtidig har en mere fremtidssikret formulering, således at indgreb i meddelelseshemmeligheden muliggøres i de situationer, hvor der i den konkrete sag er et meget stort behov for det, for at kunne opklare kriminaliteten, men ikke udvides herudover[(115)].

Retsplejelovens § 754 a om agenter har som et af kriterierne, at "andre efterforskningsskridt ikke vil være egnede til at sikre bevis i sagen" og retsplejelovens § 781 om indgreb i meddelelseshemmeligheden har som et af kriterierne, at "indgrebet må antages at være af afgørende betydning for efterforskningen". Ved siden af disse krav opstilles de særlige krav til kriminalitetens art.

Særligt vedrørende teleoplysninger henvises til afsnit 6.2. Som det fremgår, var det fra 1954 til 1985[(116)] muligt at få teleoplysninger, dels når oplysningerne ville være af betydning for opklaring af forbrydelser, der påtaltes af statsadvokaterne, og endvidere i alle andre sager, såfremt det skønnedes "sandsynligt, at opklaring af en forbrydelse kun vil være mulig gennem de ønskede oplysninger, og foranstaltningen står i rimeligt forhold til forbrydelsens karakter"[(117)].

Der er ikke i betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter anført nogen særlig begrundelse for den foreslåede begrænsning af området. Justitsministeriets strafferetsplejeudvalg anfører dog mere generelt[(118)], at der er enighed om, at der generelt set bør sættes snævre

grænser for politiets indgreb i meddelelseshemmeligheden. Det siges endvidere:

- "Opgaven ved reglernes udformning må derfor bestå i på den ene side ikke urimeligt at beskære politiets mulighed for at opklare og dermed bekæmpe alvorlig kriminalitet, herunder narkotikakriminalitet, men på den anden side at stille sådanne begrænsninger op for anvendelsen af indgrebene, at de hastigt voksende tekniske muligheder ikke fører til en overhåndtagende offentlig aflytning af borgerne."

---

115. Et flertal i arbejdsgruppen vedrørende datakriminalitet (Kim Aarenstrup, Jan Carlsen, Jan Friis, Carsten Heilbuth, Ulla Høg, Gunnar Kappel, Henrik OftebroSvendsen, Ronald Pedersen, Ole Stampe Rasmussen) er enig i mindretallets forslag.

116. De nye regler blev indført ved lov nr. 227 af 6/6 1985.

117. Det siges i lovforslaget, FT 1953/54 A 2145, vedrørende denne bestemmelse, at da indgrebet er af væsentlig mindre betydning end egentlig aflytning, har man ikke fundet det nødvendigt at drage så snævre grænser for dette som for aflytning.

118. Betænkningen s. 51 og 54

Disse medlemmer finder, at indgreb i meddelelseshemmeligheden fortsat skal have karakter af indgreb, der kun foretages i nødvendigt omfang. De er imidlertid betænkelige ved, at de moderne kommunikationsformer i nogle tilfælde betyder, at kriminalitet ikke kan efterforskes. Situationen er her ikke den, at borgeren skal beskyttes mod politiets muligheder i det moderne samfund, men derimod den, at borgeren skal beskyttes mod de kriminelles muligheder i det moderne samfund.

De ændringer, der i de senere år er foretaget i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden, viser, hvor hurtigt bestemmelserne bliver utidssvarende i forhold til efterforskningsbehovet. De viser også, hvor relativt lang tid der går, fra efterforskningsbehovet konstateres (f.eks. ved hacking og telefonmisbrug), til der skabes fornøden lovhjemmel.

Den form, der anvendes i dag i retsplejelovens § 781, hvor der indsættes stadig flere undtagelser fra kravet om, at der skal kunne straffes med fængsel i 6 år, er ikke hensigtsmæssig i et samfund, hvor IT-anvendelsen er i konstant udvikling. Behovet for at kunne få masteoplysninger og for at kunne bekæmpe kriminalitet, der begås via Internettet, er ting, der ikke var anledning til at tage nærmere stilling til, da Justitsministeriets strafferetsplejeudvalg afgav betænkning i 1984, men mindre end 10 år efter var det aktuelle problemstillinger.

Disse medlemmer finder, at der på baggrund af den konstaterede udvikling i dag bør åbnes mulighed for, at domstolene kan afsige kendelse om indgreb i meddelelseshemmeligheden i alle situationer, hvor der reelt ikke er andre efterforskningsmuligheder. De finder dog, at denne mere generelle adgang bør være forbeholdt for kriminalitet, der kan straffes med fængsel i 1 år og 6 måneder eller derover. I det omfang sådanne indgreb ønskes foretaget over for kriminalitet med et lavere strafmaksimum - som f.eks. børnepornografibestemmelsen i sin nuværende affattelse - må den eller de aktuelle bestemmelser fortsat nævnes særskilt.

Derudover finder disse medlemmer, at den model, der anvendes i dag, hvor der baseret på et konstateret behov indsættes henvisninger til flere straffebestemmelser, kun er velegnet i tilfælde, hvor der ønskes skabt mulighed for, at der altid kan foretages indgreb i meddelelseshemmeligheden ved den type lovovertrædelser. Derimod kan det være betænkeligt at udvide efter denne model, hvis behovet for indgreb i meddelelseshemmeligheden reelt kun er meget stort i de af sagerne, hvor f.eks. Internettet er benyttet. F.eks. vil en udvidelse til indgreb i meddelelseshemmeligheden ved børnepornografi - en udvidelse der er behov for i dag netop på grund af distributionen via Internettet - med den gældende model betyde, at indgreb (f.eks. poststandsning og telefonaflytning) kan ske også i sager, der ikke er IT-relaterede. Mindretallet tager ikke afstand fra, at der kan være behov for en sådan regulering, men vil alene fremhæve, at denne reguleringsform er mere indgribende i relation til de kriminalitetsformer, der nævnes, end den af mindretallet foreslåede.

Eksempelvis kan også nævnes, at mindretallet ikke finder, at der generelt er stort behov for, at der kan foretages indgreb i meddelelseshemmeligheden i sager om ophavsretslovskrænkelser i form af piratkopiering. Der vil derimod kunne være det i sager, hvor programmer distribueres via Internettet, ikke mindst hvis det er den eneste indgang til sagen. Såfremt flertallets indstilling vedrørende digitale meddelelser følges, jfr. afsnit 6.1, vil det f.eks. heller ikke længere være muligt at få oplysninger fra Internetudbyderen i sådanne sager, således som det blev tilladt

i UfR 1998.1613 ØLK.

Tilsvarende gælder for de i afsnit 2.4.2.1 nævnte sager om kursmanipulation og insiderviden. I nogle sager, især de, der foregår via Internettet, vil indgreb i meddelelseshemmeligheden være en forudsætning for, at gerningsmanden kan findes. I andre sager har der ikke i praksis været et så stort behov derfor, at der har været anledning til at foreslå, at sådanne indgreb kunne foretages.

Problemet kan også opstå i de i 2.4.2.2 nævnte sager om markedsføring på eller via Internettet. Det vil kunne være vanskeligt i nogle sager - uanset om de i visse grovere tilfælde opfylder kriminalitetskravet - at vide ved efterforskningens start, om de vil blive omfattet.

Der henvises til afsnit 7.7 udvalgets forslag.

KAPITEL 7 - UDVALGETS FORSLAG MED BEMÆRKNINGER

7.1. Dansk straffemyndighed ved salg og udbredelse via Internettet

Der henvises til afsnit 2.3 vedrørende de danske regler om straffemyndighed og udvalgets overvejelser.

Udvalget har særligt vurderet de danske regler om straffemyndighed i relation til salg og udbredelse af børnepornografi via Internettet.

Det er udvalgets umiddelbare opfattelse, at den retstilstand, som de gældende jurisdiktionsbestemmelser må antages at indebære i forhold til salg og udbredelse af børnepornografi, er tilfredsstillende. Udvalget finder derfor ikke på det foreliggende grundlag behov for lovændringer på området.

Da retspraksis af betydning for de her behandlede spørgsmål imidlertid indtil nu har været sparsom, og da udviklingen hele tiden åbner nye tekniske muligheder, som stiller lovgivningen og retsanvendelsen over for nye udfordringer, kan det ikke udelukkes, at der i fremtiden kan forekomme tilfælde, der vil afsløre mangler ved de gældende jurisdiktionsregler. Der kan derfor være grund til løbende at følge udviklingen nøje for at sikre, at straffelovens regler om straffemyndighed til stadighed er tidssvarende i forhold til den teknologiske udvikling.

7.2. Straffelovens § 235

Der henvises til afsnit 4.4 vedrørende udvalgets overvejelser.

Udvalget foreslår, at bestemmelsen i straffelovens § 235, stk. 1, om udbredelse af børnepornografi ændres således, at ikke kun den erhvervsmæssige udbredelse, men også udbredelse i en videre kreds er omfattet. En sådan ændring vil bl.a. betyde, at udbredelse via netværker, herunder Internettet, bliver omfattet også i tilfælde, hvor udbredelsen ikke er erhvervsmæssig, ligesom den vil være anvendelig i tilfælde, hvor der ikke kan føres det fornødne bevis for, at udbredelsen er erhvervsmæssig.

Udvalget foreslår endvidere, at strafmaksimum hæves til fængsel i 2 år, jfr. udvalgets vurderinger i afsnit 4.4.4.

Udvalget foreslår endvidere, at § 235, stk. 2, om besiddelse udvides til også at omfatte den, der mod vederlag retsstridigt gør sig bekendt med børnepornografiske fremstillinger. Udvalget har herved lagt vægt på, at en del børnepornografiske ydelser leveres på en sådan vis, at der ikke er tale om besiddelse i straffelovens § 235, stk. 2's forstand. Sådanne tilfælde bør efter udvalgets vurdering kriminaliseres ud fra de samme beskyttelseshensyn, der i øvrigt ligger til grund for § 235.

Med hensyn til bestemmelsen i stk. 2 finder udvalget, at den nuværende strafferamme - bøde - i den overvejende del af tilfældene vil være passende, og at den nuværende begrænsning af straffen til bøde bør bevares som normalstrafferammen.

Udviklingen i anvendelsen af Internettet og distribution af børnepornografi via Internettet har imidlertid udviklet sig således, at udvalget finder, at der bør være mulighed for under skærpende omstændigheder at idømme hæfte eller fængsel indtil 6 måneder. Som eksempel på, hvad der skal betragtes som skærpende omstændighed, kan nævnes, at den pågældende betaler betydelige beløb for at modtage børnepornografisk materiale. Der vil ligeledes foreligge skærpende omstændigheder, hvis den pågældende besidder et meget stort antal børnepornografiske fremstillinger, eller et større antal fremstillinger af særlig grove forhold, f.eks. voldtægt af børn.

Straffelovens § 235 foreslås herefter affattet således:

"*§ 235*. Den, som erhvervsmæssigt sælger eller på anden måde udbreder utugtige fotografier, film eller lignende af børn, straffes med bøde, hæfte eller fængsel indtil 2 år. På samme måde straffes den, som i en videre kreds udbreder sådanne fremstillinger.

Stk. 2. Den, som retsstridigt besidder eller mod vederlag gør sig bekendt med fotografier, film eller lignende af børn, der

1) har samleje eller anden kønslig omgængelse end samleje eller

2) har kønslig omgang med dyr eller

3) anvender genstande på groft utugtig måde,

straffes med bøde eller under skærpende omstændigheder med hæfte eller fængsel indtil 6 måneder."

Stk. 1, 1. pkt., svarer til det nugældende stk. 1 med den ændring, at det ikke længere nævnes, at det at fremstille eller skaffe sig det nævnte materiale med forsæt til at overtræde bestemmelsen er strafbart. At dette tidligere var nævnt var begrundet i, at der oprindelig var tale om en bødebestemmelse, og at det derfor ikke uden en særlig bestemmelse herom var muligt at straffe for forsøg, jfr. straffelovens § 21, stk. 3. Da de almindelige forsøgsregler finder anvendelse, er der ikke behov for at nævne særlige forsøgssituationer.

Endvidere foreslås strafmaksimum forhøjet til 2 år.

Stk. 1, 2. pkt., indeholder den af udvalget foreslåede udvidelse, således at ikke alene den erhvervsmæssige udbredelse, men også udbredelse i en videre kreds, er dækket af bestemmelsen.

Bestemmelsen i stk. 2 er i forhold til den nugældende bestemmelse udvidet med, at en person uden at etablere en besiddelsessituation mod vederlag gør sig bekendt med de særlige former for børnepornografisk materiale. Det nævnte "vederlag" omfatter enhver form for modydelse, herunder at der byttes med andre ydelser. Kravet om retsstridighed betyder, at f.eks. adgang, der er efterforskningsmæssigt begrundet, herunder en adgang, der har til formål at finde billeder af forsvundne børn, ikke omfattes af bestemmelsen. Retsstridighedskravet svarer til, hvad der formuleres direkte i det svenske lovforslag, jfr. afsnit. 4.3.2, hvorefter bestemmelsen ikke gælder tilfælde, hvor særlige omstændigheder gør, at handlingen må anses for åbenbart beføjet.

Endvidere foreslås strafmaksimum forhøjet til 6 måneder.

7.3. Krav til Internetudbydere, teleselskaber m.v.

Der henvises til afsnit 5.1 vedrørende udvalgets overvejelser.

Som nævnt finder udvalget, at der bør stilles krav om, at Internetudbydere og teleselskaber skal logge både A og B-nummeret - for A-nummerets vedkommende uanset om den pågældende har benyttet muligheden for, at der ikke sker visning af Anummeret. Endvidere bør udbyderen logge IPadresse for den, der ringer op, brugertid, tidspunkt for opkobling/nedkobling, opkoblingens længde og sessionstype (FTP/Telnet). Der bør tillige stilles krav om opbevaringsformat (læsbarhed) og foranstaltninger til beskyttelse mod uautoriseret adgang og manipulation. Derudover bør eventuelle kontooplysninger opbevares. Opbevaring af oplysninger skal ske i Danmark, hvis udbyderen er i Danmark, uanset om udbyderen er selvstændig eller filial af en udenlandsk virksomhed.

Endvidere bør det tilstræbes, at det sikres, at korrekt dansk realtid registreres.

Udvalget har nærmere drøftet de forskellige hensyn, der kan tale for henholdsvis en længere og en kortere opbevaringstid.

Udvalget har på baggrund af drøftelserne valgt at anbefale en opbevaringsfrist på 6 måneder. Spørgsmålet om, hvorvidt udbyderen har *ret* til at opbevare logoplysninger ud over den pligtmæssige opbevaring i 6 måneder, må afgøres på grundlag af de almindelige regler i registerlovgivningen.

Med hensyn til formen for reguleringen har udvalget indgående drøftet, om de ønskede registreringer og opbevaringen heraf ville kunne gennemføres ved en selvregulering.

Nogle medlemmer har henvist til, at der ikke er tale om en branche med etablerede traditioner med hensyn til selvregulering, eller med egne sanktionssystemer, ligesom der end ikke findes en registrering af Internetleverandører. Dette kan i sig selv tale mod en løsning med selvregulering, men dertil kommer, at der er tale om tiltag, der alene har efterforskningsmæssig interesse, og at efterforskningsmulighederne bør sikres gennem lovgivning herom. Dette svarer også til, at det f.eks. i § 3 h i lov om visse forhold på telekommunikationsområdet er fastsat, at udbydere af offentlige telenet og teletjenester uden udgift for staten skal sikre, at telecentralerne er indrettet således, at politiet kan få adgang til at foretage indgreb i meddelelseshemmeligheden.

Andre medlemmer har henvist til, at forpligtelsen bør kunne gennemføres ved selvregulering. Disse medlemmer mener ikke, at reglerne i lov om visse forhold på telekommunikationsområdet er egnede som retsgrundlag for den uoverskuelige mængde af Internetleverandører, for hvilke en forpligtelse af denne art får betydning.

Disse medlemmer har peget på, at der for tiden pågår intense bestræbelser på at gennemføre selvregulering indenfor Internetbranchen i en række henseender, og at man i tråd med den almindelige tendens i retning mod selvregulering bør give branchen mulighed for selv at tilvejebringe denne regulering, samtidig med at branchen alligevel skal tage stilling til spørgsmålet om, hvor længe man har *ret* til at opbevare sådanne logoplysninger. Når man vurderer udsigten til at gennemføre ønsket om opbevaring af logoplysninger i 6 måneder gennem selvregulering, må det i øvrigt tages i betragtning, at Internetleverandørerne kan have en økonomisk interesse i at følge en sådan praksis, eftersom udleveringen af de pågældende oplysninger sker mod betaling.

Et flertal i udvalget (Preben Bialas, Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Michael Clan, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Lau Kramer, Kirsten Mandrup, Annemette Møller, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder, at reguleringen skal ske ved lov.

Et mindretal i udvalget (Mads Bryde Andersen, Vagn Greve, Jesper Koefoed, Lars Bo Langsted) finder, at spørgsmålet så vidt muligt skal løses ved en selvregulering i branchen, Disse medlemmer er dog enige i en lovgivningsmæssig løsning, såfremt det viser sig, at reguleringsbestræbelserne ikke bærer frugt.

7.4. Adgang til indholdet af digitale meddelelser

Der henvises til afsnit 6.1 vedrørende udvalgets overvejelser.

Udvalget har nærmere drøftet, om adgang til email (eller andre digitale meddelelser) hos udbyderen skal behandles efter retsplejelovens regler om edition eller om dens regler om indgreb i meddelelseshemmeligheden.

Der er enighed i udvalget om, at hvis der er tale om et fremadrettet indgreb, der har karakter af overvågning af indholdet af korrespondancen, bør det være omfattet af regler om indgreb i meddelelseshemmeligheden.

Udvalgets medlemmer har delt sig i spørgsmålet om, hvorvidt dette også bør gælde for indgreb, der er bagudrettede.

Et flertal i udvalget (Mads Bryde Andersen, Preben Bialas, Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Vagn Greve, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Lars Bo Langsted, Kirsten Mandrup, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder ikke anledning til at foreslå ændringer i retsplejelovens regler om indgreb i meddelelseshemmeligheden. Disse medlemmer finder således, at elektronisk post (epost eller email) ikke adskiller sig grundlæggende fra andre kommunikationsformer, der er omfattet af reglerne om indgreb i meddelelseshemmeligheden, og at der derfor ikke er grund til at give politiet en videre adgang til at foretage indgreb i kommunikation i form af elektronisk post.

Efter disse medlemmers opfattelse må elektroniske breve sidestilles med traditionelle (fysiske) breve, jfr. retsplejelovens § 780, stk. 1, nr. 4 og 5. En sammenligning af kommunikationsforløbene ved henholdsvis traditionelle brevforsendelser og elektronisk post må efter disse medlemmers opfattelse føre til, at elektronisk post, der beror hos en Internetudbyder, må sidestilles med breve i en postboks, jfr. de ovenfor citerede forarbejder til de gældende bestemmelser.

Det er forudsat, at reglerne om indgreb i meddelelseshemmeligheden ikke omfatter indgreb, der gennemføres inden kommunikationens begyndelse eller efter dens afslutning. Reglerne finder således ikke anvendelse, hvis politiet kan skaffe sig meddelelsen ved et straffeprocessuelt tvangsindgreb mod afsender eller modtager af meddelelsen (jfr. reglerne om ransagning og beslaglæggelse). Hvis politiet derimod ønsker at skaffe sig meddelelsen med bistand fra en kommunikationsformidler, må dette ske efter reglerne om indgreb i meddelelseshemmeligheden. Dette må gælde, uanset om kommunikationsformidleren er et telefonselskab, en postvirksomhed eller en udbyder af elektronisk kommunikation (herunder en Internetudbyder).

Kommunikationen kan efter de principper, der er lagt til grund ved udformningen af reglerne om indgreb i meddelelseshemmeligheden, kun siges at være afsluttet, når meddelelsen er kommet modtageren i hænde på en sådan måde, at politiet kan skaffe sig adgang til meddelelsen under en ransagning på modtagerens (fysiske) adresse eller ved anvendelse af midler beslaglagt under en sådan ransagning (en postboksnøgle eller en adgangskode til en elektronisk postkasse). Adgangskoden kan f.eks. være fast indkodet i Internetkommunikationsprogrammet (browseren) på den mistænktes computer, således at der ved opstart af programmet automatisk etableres forbindelse til den elektroniske postkasse hos Internetudbyderen. I denne situation vil det ikke være nødvendigt for politiet at gå frem efter reglerne om indgreb i meddelelseshemmeligheden.

Et mindretal i udvalget (Michael Clan, Annemette Møller) finder, at reglerne om edition bør anvendes, og at der ikke bør stilles de særlige krav, der gælder for indgreb i meddelelseshemmeligheden. Der er tale om et indgreb, hvor oplysningerne - hvis de fortsat lå hos den sigtede - kunne tilvejebringes i medfør af de almindelige ransagningsregler. De henviser herudover til, at der ved den oprindelige stillingtagen i 1984 til datakommunikation er tænkt på en igangværende kommunikationsstrøm, hvor kommunikationen ikke er nået fysisk frem til den pågældende, og ikke på den særlige email struktur.

Disse medlemmer finder i øvrigt, at der altid bør beskikkes forsvarer i disse situationer, hvis det ikke allerede er sket.

Disse medlemmer lægger også vægt på, at den sigtede selv har valgt, at kommunikationen kan ske via kommunikationskanaler, hvor en tredjemand indgår i forløbet og besidder, hvad der kan sidestilles med en brevkopi. Situationen er meget atypisk i forhold til traditionelle postforsendelser, fordi Internetudbyderen straks har gjort forsendelsen tilgængelig for adressaten på dennes adresse. Der er således efter de principper, der gælder for f.eks. postforsendelser, telexkommunikation og meddelelser til telefonsvarere, ikke tale om et igangværende kommunikationsforløb. Når oplysningerne findes hos Internetudbyderen, er kommunikationen afsluttet. Ønsker man at føre særlig sikret korrespondance, må det ske ved sædvanlige lukkede forsendelser, der ikke er tilgængelige i andre systemer, eller der må anvendes særligt sikre krypteringsteknikker.

Det er også den fortolkning, der anlægges i retspraksis. F.eks. blev der i en sag om piratkopiering afsagt editionskendelse vedrørende email fra den sigtedes kendte email adresse og eventuelle andre adresser tilhørende ham, jfr. UfR 1998.1613 ØLK. Forsvareren gjorde både for byretten og landsretten gældende, at der var tale om indgreb i meddelelseshemmeligheden, og at der derfor ikke kunne afsiges editionskendelse[(119)]. Byretten afsagde editionskendelse og anførte, at den hos Internetudbyderen beroende post ikke fandtes at være under forsendelse, men måtte ligestilles med post, der var kommet frem til den sigtedes bopæl. Østre landsret stadfæstede kendelsen af de af byretten anførte grunde.

Flertallets forslag er reelt ikke et forslag om ikke at ændre retstilstanden, men er et forslag om at begrænse de efterforskningsmuligheder, der, jfr. Østre landsrets kendelse, må antages at være i dag. Mindretallet finder mere principielt, at det ikke er acceptabelt at foreslå løsninger, der begrænser politiets nuværende muligheder for at efterforske og dermed begrænser mulighederne for at bekæmpe kriminalitet.

---

119. Der ville på grund af sagstypen ikke have kunnet afsiges kendelse om indgreb i meddelelseshemmeligheden,

idet piratkopiering ikke er en af de kriminalitetstyper, hvor der kan foretages sådanne indgreb, jfr. retsplejelovens § 781.

7.5. Teleoplysninger (incl. sendemaster)

Der henvises til afsnit 6.2 og 6.4 vedrørende udvalgets overvejelser.

Et flertal i udvalget (Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Vagn Greve, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Lars Bo Langsted, Kirsten Mandrup, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder ikke anledning til at foreslå ændringer af retsplejelovens regler om indgreb i meddelelseshemmeligheden i form af teleoplysning.

Regler om indgreb i meddelelseshemmeligheden er udtryk for en afvejning af på den ene side hensynet til en effektiv kriminalitetsbekæmpelse og på den anden side hensynet til borgernes privatliv.

Efter flertallets opfattelse tilsiger hensynet til beskyttelse af borgernes fortrolige kommunikation med andre også en beskyttelse af oplysninger om, *hvem* der er kommunikeret med. Dette er også lagt til grund i Strafferetsplejeudvalgets betænkning nr. 1024/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter.

Uanset et indgreb i form af indhentning af teleoplysninger kan siges at indebære en vis mindre grad af integritetskrænkelse end de øvrige indgreb i meddelelseshemmeligheden, herunder telefonaflytning, bør der efter disse medlemmers opfattelse - henset til de ovenfor beskrevne modhensyn - ikke gives politiet adgang til teleoplysninger efter (de væsentlig lempeligere) regler om edition.

En anvendelse af reglerne om edition vil således bl.a. indebære, at indgrebet som udgangspunkt kan anvendes ved alle former for kriminalitet. En begrænsning vil alene følge af en proportionalitetsafvejning i den konkrete sag, dvs. om indgrebet står i misforhold til sagens betydning og den ulempe, som indgrebet kan antages at medføre. Efter reglerne om indgreb i meddelelseshemmeligheden kan indgrebet - bortset fra enkelte i loven særligt opregnede lovovertrædelser - kun anvendes ved efterforskning af lovovertrædelser, der efter loven kan straffes med fængsel i 6 år eller derover.

For så vidt angår spørgsmålet om en udvidelse af reglerne om indgreb i meddelelseshemmeligheden - en udvidelse der i givet fald også vil få betydning for teleoplysninger - henvises til afsnit 7.7 nedenfor.

Mindretallets forslag (jfr. nedenfor) indebærer, at også pålæg til teleselskabet om registrering af teleoplysninger i en periode frem i tiden skal behandles efter reglerne om edition. Disse regler indeholder - i modsætning til reglerne om indgreb i meddelelseshemmeligheden - ikke bestemmelser om frister for sådanne indgreb, idet editionsregler i alt væsentligt er tænkt anvendt på allerede eksisterende oplysninger. Editionsreglerne indeholder heller ikke regler om beskikkelse af advokat for indehaveren af pågældende telefon og foreslås af mindretallet kun ændret således, at der skal ske forsvarerbeskikkelse for den sigtede, der ikke behøver at være identisk med indehaveren af telefonen. Mindretallets forslag indebærer således på flere punkter en svækkelse af de retsgarantier, som de gældende regler er udtryk for.

Et mindretal i udvalget (Mads Bryde Andersen, Preben Bialas, Michael Clan, Annemette Møller) finder, at det ved teleoplysninger, der allerede lagres i anden sammenhæng, bør være en tilstrækkelig garanti, at der skal afsiges editionskendelse. Oplysningerne er ikke mere følsomme end en række andre oplysninger, der kan udleveres efter editionsreglerne, og det kræver i dag ikke et særligt indgreb fra teleselskabernes side at fremskaffe oplysningerne.

Mindretallet vil pege på, at teleoplysninger er det mindst indgribende af de indgreb, der reguleres af reglerne om indgreb i meddelelseshemmeligheden. Ved indgrebet får politiet ikke kendskab til indholdet af kommunikationen, ligesom kommunikationen ikke unddrages modtageren.

Betydningen af at kunne få teleoplysninger er endvidere betydelig større ved den kriminalitet, der kendes i dag, end den var, da strafferetsplejerådet foreslog den ensartede regulering af området. Dette har også efterfølgende medført behov for, at der blev skabt en særlig hjemmel i retsplejelovens § 781, stk. 2 og stk. 3, til at indhente teleoplysninger i hackersager og telefonmisbrugssager. Også for så vidt angår sager om børnepornografi er der i

dag behov derfor, ligesom der i øvrigt vil kunne være behov i sagstyper, hvor Internettet indgår, f.eks. i sager om piratkopiering eller kursmanipulation. Også på områder uden for den IT-relaterede kriminalitet - f.eks. i sager om EUsvig eller afgiftssvig i øvrigt - er der på grund af mange personers samvirke et større behov end tidligere for at få oplysninger af denne type.

Disse medlemmer er enige om, at forudsætningen for at anvende editionsreglerne skal være, at der beskikkes en forsvarer i disse situationer, hvis det ikke allerede er sket.

Editionsreglerne anvendes normalt ved alle oplysninger, uanset hvor følsomme de er, når oplysningerne er tilgængelige hos den, editionen rettes mod, uden særlige tiltag. Domstolene er derfor også ved edition vant til, at der er forskel på følsomheden af de ønskede oplysninger, og at dette kan have betydning for, hvornår og i hvilket omfang en begæring om edition - f.eks. i et pengeinstitut, hos en revisor eller hos en advokat - skal imødekommes.

De særlige regler om teleoplysninger afviger således i dag - hvor der ikke skal foretages særlige indgreb for at fremskaffe dem - fra de regler, der i øvrigt gælder for selv meget følsomme oplysninger, som personer eller selskaber besidder som et almindeligt led i deres virksomhed.

Disse medlemmer foreslår, at retsplejelovens § 780, stk. 1, nr. 3, ændres således, at bestemmelsen alene omfatter masteoplysninger og tilsvarende oplysninger (udvidet teleoplysning).

For så vidt angår lagrede teleoplysninger, vil de herefter blive indhentet efter reglerne om edition, jfr. retsplejelovens § 827. Ved afgørelse om edition skal retten tage stilling til, om indgrebet står i misforhold til sagens betydning (hvilket efter seneste lovændring[(120)] er formuleret udtrykkeligt i § 805, stk. 1). Dette bør være en tilstrækkelig garanti for, at der kun gives teleoplysninger i sager, hvor retten har afvejet indgrebet mod sagens betydning.

---

120. Lov nr. 229 af 21/4 1999 om ændring af retsplejeloven (Beslaglæggelse, edition m.v.).

Særligt om masteoplysninger

Udvalget finder, at der bør tilvejebringes en klar hjemmel til indgreb i form af masteoplysninger o.l. De medlemmer af udvalget, der i øvrigt finder, at editionsreglerne frembyder tilstrækkelig garanti ved lagrede teleoplysninger, er enige med de øvrige medlemmer i, at masteoplysninger og tilsvarende oplysninger skal behandles efter reglerne om indgreb i meddelelseshemmeligheden, da der er tale om meget bredere indgreb. Udvalget finder herudover, at reglerne skal opfylde kravene til særligt kvalificerede indgreb i meddelelseshemmeligheden.

Udvalget foreslår, at sendemaster reguleres i retsplejelovens § 780, stk. 1, nr. 3 (hvis den nugældende nr. 3 ophæves) eller nr. 4, med følgende ordlyd:

"4) indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater inden for et nærmere angivet område der sættes i forbindelse med andre telefoner eller kommunikationsapparater (udvidet teleoplysning),"

Udvalget foreslår endvidere, at der kun skal være adgang til udvidet teleoplysning under de betingelser (mistanke om en forbrydelse, som har medført eller som kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier), der gælder for anden aflytning end telefonaflytning.

Det foreslås derfor, at der i § 781, stk. 5, efter "Aflytning efter § 780, stk. 1, nr. 2, indsættes "og udvidet teleoplysning efter § 780, stk. 1, [nr. 3] [nr. 4]".

7.6. Teleoplysninger i henhold til samtykke m.v.

Der henvises til afsnit 6.3 vedrørende udvalgets overvejelser.

Med hensyn til retsplejelovens § 786, stk. 1, foreslår udvalget, at "post og telegrafvæsenet, telefonselskaberne og

andre tilsvarende offentlige og private virksomheder" ændres til "postvirksomheder og udbydere af offentlige telenet eller teletjenester". Ændringen bringer terminologien i overensstemmelse med lov nr. 89 af 8/2 1995 om postvirksomhed og med den nyere telelovgivning, jfr. herved f.eks. § 1, stk. 5, i lov om konkurrenceforhold og samtrafik i telesektoren, jfr. lovbekendtgørelse nr. 860 af 4/12 1998.

Med hensyn til samtykkereglen i retsplejelovens § 786, stk. 2, har udvalget delt sig i spørgsmålet om, hvorvidt teleselskaberne skal kunne meddele dette samtykke ved offentlige telefoner.

Et flertal i udvalget (Preben Bialas, Susan Bramsen, Bent Carlsen, Vagn Greve, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Kirsten Mandrup, Lene Nielsen, Henrik Rothe) finder ikke, at teleselskaberne skal kunne meddele samtykke ved offentlige telefoner.

Bestemmelsen i retsplejelovens § 786, stk. 2, bygger på det synspunkt, at en telefonabonnent ikke i forhold til telefonselskabernes tavshedspligt kan anses for "uvedkommende" med hensyn til oplysninger om, hvem der ringer til abonnenten, og at der ikke er en sådan beskyttelsesværdig interesse i hemmeligholdelse hos personer, der kalder et andet telefonnummer, at udlevering af disse oplysninger til politiet med samtykke fra indehaveren af denne telefon bør omfattes af reglerne om indgreb i meddelelseshemmeligheden, jfr. Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, s. 62. I retspraksis er det fastslået, at bestemmelsen også finder anvendelse på oplysninger om udgående opkald fra en bestemt telefon, jfr. UfR 1996.169 ØLK.

Efter disse medlemmers opfattelse kan et telefonselskab ikke siges at have rådighed over en offentlig telefon på samme måde som en privat telefonabonnent har rådighed over sin telefon. Der er derfor ikke samme anledning til at give telefonselskabet adgang til med sit samtykke at fravige reglerne om indgreb i meddelelseshemmeligheden. Hvis man låner en privat telefon (eller stjæler en mobiltelefon) må man være indstillet på, at den pågældende telefonabonnent modtager udførlige samtalespecifikationer i forbindelse med telefonregningen. Benyttelsen af en offentlig telefon kan nærmest betragtes som et "ad hocabonnement", hvor man mod vederlag får (en begrænset) adgang til at benytte telefonnettet. Et indgreb mod en bruger af en offentlig telefon bør derfor sidestilles med et indgreb imod en privat telefonabonnent. De særlige hensyn, der i sin tid begrundede bestemmelsen i § 786, stk. 2, kan efter disse medlemmers opfattelse ikke udstrækkes til også at begrunde en lignende regel for offentlige telefoner.

Et mindretal i udvalget (Mads Bryde Andersen, Hans Henrik Brydensholt, Jørgen Christiansen, Michael Clan, Alexander Houen, Lars Bo Langsted, Annemette Møller) finder, at teleselskaberne - uanset hvilket regelsæt der finder anvendelse - skal kunne meddele samtykket, når der er tale om offentlige telefoner. Der er enighed om, at der skal beskikkes en forsvarer i disse situationer, hvis det ikke allerede er sket.

Disse medlemmer har i den forbindelse lagt vægt på, at der ikke kan være nogen berettiget forventning om, at indehaveren af en telefon ikke kan give politiet (adgang til) oplysning om, hvilken brug der har været gjort af telefonen. Med den retstilstand, der er i dag vedrørende indgreb i meddelelseshemmeligheden, betyder det, at der ved en lang række kriminalitetsformer ikke er mulighed for at få adgang til disse allerede registrerede oplysninger, hvis en offentlig telefon er benyttet (i modsætning til f.eks. en telefon, der ejes af en restaurant).

Spørgsmålet om samtykke ved offentlige telefoner er opstået som en konsekvens af, at oplysningerne i dag registreres. Det er af samme grund ikke behandlet i Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, der, jfr. betænkningens s. 61 ff, især tager udgangspunkt i, at hovedområdet for teleoplysninger er truende, injurierende eller på andre måder generende telefonopkald til en privat abonnent. Udvalgets forventninger til, at indgrebet i fremtiden vil tiltrække sig større opmærksomhed, er især knyttet til, at telefonaflytninger er ressourcekrævende, og at det i en del sager kunne være af betydning for politiet at få oplyst, om bestemte telefoner, til hvis indehavere man har mistanke i sagskomplekset, bliver sat i forbindelse med hinanden.

I den ovenfor nævnte kendelse (UfR 1996.169 ØLK) blev det lagt til grund, at indehaveren af en stjålen mobiltelefon kunne meddele samtykke efter retsplejelovens § 786, stk. 2. Denne kendelse understøtter efter disse medlemmers opfattelse det synspunkt, at det formelle ejerskab er tilstrækkeligt til, at man er samtykkeberettiget, også når samtalerne utvivlsomt er abonnenten helt uvedkommende.

Et medlem af udvalget (Erik Overgaard) har ikke taget stilling til, hvilken løsning der skal vælges.

7.7. Indgreb i meddelelseshemmeligheden i øvrigt

Der henvises til afsnit 6.5 vedrørende udvalgets overvejelser.

Udvalget finder, at der i det omfang, hvor der er særligt behov herfor, bør skabes adgang til indgreb i meddelelseshemmeligheden ved IT-relateret kriminalitet. En bestemmelse herom bør dog begrænses til de efterforskningssituationer, hvor der reelt - som ved hacking og telefonmisbrug (hvor andres abonnementer belastes med samtaleafgiften) - ikke er andre effektive efterforskningsmuligheder, herunder efterforskning af kriminalitet, der begås via netværk.

Et flertal i udvalget (Mads Bryde Andersen, Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Vagn Greve, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Lars Bo Langsted, Kirsten Mandrup, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder i overensstemmelse med Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, s. 5152, at der generelt bør sættes snævre grænser for politiets indgreb i meddelelseshemmeligheden, men at der dog - som anført af Strafferetsplejeudvalget og lagt til grund af Folketinget ved senere ændringer af bestemmelserne - kan være særlige kriminalitetsformer, hvor sædvanlige efterforskningsmetoder ikke rækker til. Disse medlemmer finder således, at der løbende på baggrund af udviklingen i kriminalitetsformerne må tages stilling til, om der er behov for at udvide adgangen til indgreb i meddelelseshemmeligheden til flere straffebestemmelser. Der må i den forbindelse foretages en overordnet afvejning mellem på den ene side hensynet til en effektiv kriminalitetsbekæmpelse og på den anden side hensynet til borgernes privatliv.

Ved den nedenfor af mindretallet foreslåede bestemmelse vil efterforskning af en betydelig videre kreds af lovovertrædelser end i dag kunne danne grundlag for indgreb i meddelelseshemmeligheden, forudsat at andre efterforskningsmetoder ikke er egnede til at sikre bevis i sagen.

Disse medlemmer kan ikke støtte en sådan generel, væsentlig lempelse af kriminalitetskravet ved indgreb i meddelelseshemmeligheden.

Flertallet finder i denne sammenhæng på det foreliggende grundlag kun anledning til at overveje, om der bør være adgang til at foretage indgreb i meddelelseshemmeligheden ved efterforskning af sager om udbredelse og besiddelse af børnepornografi, jfr. straffelovens § 235. Da denne kriminalitet - på samme måde som "hackerkriminalitet" - i dag i høj grad begås ad elektronisk vej, hvor mere traditionelle efterforskningsmetoder ikke er anvendelige, foreslår disse medlemmer, at der i sager af denne karakter bliver mulighed for indgreb i meddelelseshemmeligheden, uanset det sædvanlige kriminalitetskrav (6 års fængsel i strafferammen) ikke er opfyldt.

Et af flertallets medlemmer (Kirsten Mandrup) finder endvidere, at det tillige bør overvejes at skabe mulighed for indgreb i meddelelseshemmeligheden for så vidt angår efterforskning af sager om misbrug af intern viden og kursmanipulation efter lov om værdipapirhandel m.v. Dette medlem peger på, at det på dette område, hvor kriminalitetskravet på 6 års fængsel ikke er opfyldt, i praksis har vist sig, at traditionelle efterforskningsmetoder ikke i fuldt tilstrækkeligt omfang er egnet til at imødegå denne form for kriminalitet.

Flertallet er enig i, at dette er et område, hvor der kan være anledning til at overveje yderligere udvidelser. Flertallet vil heller ikke udelukke, at en nærmere analyse af andre områder kan vise, at der er behov for en regulering ud over den foreslåede. Der er på den baggrund enighed om, at det indgår i udvalgets videre arbejde, om der kan påpeges behov for yderligere reguleringer.

Et mindretal i udvalget (Preben Bialas, Michael Clan, Annemette Møller) finder, at den regulering, der kan være behov for ved IT-relateret kriminalitet, ikke skal bestå i, at der indsættes en henvisning til endnu flere paragraffer, hvor sådanne indgreb er mulige, uanset hvordan kriminaliteten konkret er gennemført, men derimod skal være en regulering, der begrænses til mere specielle tilfælde og samtidig har en mere fremtidssikret formulering, således at indgreb i meddelelseshemmeligheden muliggøres i de situationer, hvor der i den konkrete sag er et meget stort behov for det, for at kunne opklare kriminaliteten, men ikke udvides herudover.

Retsplejelovens § 754 a om agenter har som et af kriterierne, at "andre efterforskningsskridt ikke vil være egnede

til at sikre bevis i sagen" og retsplejelovens § 781 om indgreb i meddelelseshemmeligheden har som et af kriterierne, at "indgrebet må antages at være af afgørende betydning for efterforskningen". Ved siden af disse krav opstilles de særlige krav til kriminalitetens art.

Særligt vedrørende teleoplysninger henvises til afsnit 6.2. Som det fremgår, var det fra 1954 til 1985[(121)] muligt at få teleoplysninger, dels når oplysningerne ville være af betydning for opklaring af forbrydelser, der påtaltes af statsadvokaterne, og endvidere i alle andre sager, såfremt det skønnedes "sandsynligt, at opklaring af en forbrydelse kun vil være mulig gennem de ønskede oplysninger, og foranstaltningen står i rimeligt forhold til forbrydelsens karakter"[(122)].

Der er ikke i betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter anført nogen særlig begrundelse for den foreslåede begrænsning af området. Justitsministeriets strafferetsplejeudvalg anfører dog mere generelt[(123)], at der er enighed om, at der generelt set bør sættes snævre grænser for politiets indgreb i meddelelseshemmeligheden. Det siges endvidere:

- "Opgaven ved reglernes udformning må derfor bestå i på den ene side ikke urimeligt at beskære politiets mulighed for at opklare og dermed bekæmpe alvorlig kriminalitet, herunder narkotikakriminalitet, men på den anden side at stille sådanne begrænsninger op for anvendelsen af indgrebene, at de hastigt voksende tekniske muligheder ikke fører til en overhåndtagende offentlig aflytning af borgerne."

---

121. De nye regler blev indført ved lov nr. 227 af 6/6 1985.
122. Det siges i lovforslaget, FT 1953/54 A 2145, vedrørende denne bestemmelse, at da indgrebet er af væsentlig mindre betydning end egentlig aflytning, har man ikke fundet det nødvendigt at drage så snævre grænser for dette som for aflytning.
123. Betænkningen s. 51 og 54.

Disse medlemmer finder, at indgreb i meddelelseshemmeligheden fortsat skal have karakter af indgreb, der kun foretages i nødvendigt omfang. De er imidlertid betænkelige ved, at de moderne kommunikationsformer i nogle tilfælde betyder, at kriminalitet ikke kan efterforskes. Situationen er her ikke den, at borgeren skal beskyttes mod politiets muligheder i det moderne samfund, men derimod den, at borgeren skal beskyttes mod de kriminelles muligheder i det moderne samfund.

De ændringer, der i de senere år er foretaget i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden, viser, hvor hurtigt bestemmelserne bliver utidssvarende i forhold til efterforskningsbehovet. De viser også, hvor relativt lang tid der går, fra efterforskningsbehovet konstateres (f.eks. ved hacking og telefonmisbrug), til der skabes fornøden lovhjemmel.

Den form, der anvendes i dag i retsplejelovens § 781, hvor der indsættes stadig flere undtagelser fra kravet om, at der skal kunne straffes med fængsel i 6 år, er ikke hensigtsmæssig i et samfund, hvor IT-anvendelsen er i konstant udvikling. Behovet for at kunne få masteoplysninger og for at kunne bekæmpe kriminalitet, der begås via Internettet, er ting, der ikke var anledning til at tage nærmere stilling til, da Justitsministeriets strafferetsplejeudvalg afgav betænkning i 1984, men mindre end 10 år efter var det aktuelle problemstillinger.

Disse medlemmer finder, at der på baggrund af den konstaterede udvikling i dag bør åbnes mulighed for, at domstolene kan afsige kendelse om indgreb i meddelelseshemmeligheden i alle situationer, hvor der reelt ikke er andre efterforskningsmuligheder. De finder dog, at denne mere generelle adgang bør være forbeholdt for kriminalitet, der kan straffes med fængsel i 1 år og 6 måneder eller derover. I det omfang sådanne indgreb ønskes foretaget over for kriminalitet med et lavere strafmaksimum - som f.eks. børnepornografibestemmelsen i sin nuværende affattelse - må den eller de aktuelle bestemmelser fortsat nævnes særskilt.

Derudover finder disse medlemmer, at den model, der anvendes i dag, hvor der baseret på et konstateret behov indsættes henvisninger til flere straffebestemmelser, kun er velegnet i tilfælde, hvor der ønskes skabt mulighed for, at der altid kan foretages indgreb i meddelelseshemmeligheden ved den type lovovertrædelser. Derimod kan det være betænkeligt at udvide efter denne model, hvis behovet for indgreb i meddelelseshemmeligheden reelt kun er meget stort i de af sagerne, hvor f.eks. Internettet er benyttet. F.eks. vil en udvidelse til indgreb i

meddelelseshemmeligheden ved børnepornografi - en udvidelse der er behov for i dag netop på grund af distributionen via Internettet - med den gældende model betyde, at indgreb (f.eks. poststandsning og telefonaflytning) kan ske også i sager, der ikke er IT-relaterede. Mindretallet tager ikke afstand fra, at der kan være behov for en sådan regulering, men vil alene fremhæve, at denne reguleringsform er mere indgribende i relation til de kriminalitetsformer, der nævnes, end den af mindretallet foreslåede.

Eksempelvis kan også nævnes, at mindretallet ikke finder, at der generelt er stort behov for, at der kan foretages indgreb i meddelelseshemmeligheden i sager om ophavsretslovskrænkelser i form af piratkopiering. Der vil derimod kunne være det i sager, hvor programmer distribueres via Internettet, ikke mindst hvis det er den eneste indgang til sagen. Såfremt flertallets indstilling vedrørende digitale meddelelser følges, jfr. afsnit 6.1, vil det f.eks. heller ikke længere være muligt at få oplysninger fra Internetudbyderen i sådanne sager, således som det blev tilladt i UfR 1998.1613 ØLK.

Tilsvarende gælder for de i afsnit 2.4.2.1 nævnte sager om kursmanipulation og insiderviden. I nogle sager, især de, der foregår via Internettet, vil indgreb i meddelelseshemmeligheden være en forudsætning for, at gerningsmanden kan findes. I andre sager har der ikke i praksis været et så stort behov derfor, at der har været anledning til at foreslå, at sådanne indgreb kunne foretages.

Problemet kan også opstå i de i 2.4.2.2 nævnte sager om markedsføring på eller via Internettet. Det vil kunne være vanskeligt i nogle sager - uanset om de i visse grovere tilfælde opfylder kriminalitetskravet - at vide ved efterforskningens start, om de vil blive omfattet.

BILAG 1 - Internationale rekommandationer m.v.

OECDs 1986-rekommandationer

OECD påbegyndte i 1984 en analyse af medlemsstaternes lovgivning vedrørende computerrelateret kriminalitet. Resultatet blev publiceret i 1986[(124)]. Det konkluderes i rapporten, at det anbefaledes, at medlemsstaterne overvejede en eventuel straffelovgivning vedrørende:

a) The input, alteration, erasure and/or suppression of computer data and/or computer programmes made wilfully with the intent to commit an illegal transfer of funds or of another thing of value;

b) The input, alteration erasure and/or suppression of computer data and/or computer programmes made wilfully with the intent to commit a forgery;

c) The input, alteration erasure and/or suppression of computer data and/or computer programmes, or other interference with computer systems, made wilfully with the intent to hinder the functioning of a computer and/or telecommunication system;

d) The infringement of the exclusive right of the owner of a protected computer programme with the intent to exploit commercially the programme and put it on the market;

e) The access to or interception of a computer and/or telecommunication system made knowingly and without the authorisation of the person responsible for the system, either (i) by the infringement of security measures or (ii) for other dishonest or harmfull intentions.

---

124. OECD rapport ICCP nr. 10, Computerrelated crime : Analysis of legal policy.

Europarådets rekommandation nr. R(89)9

Europarådet inkluderede fra 1985-86 computerrelateret kriminalitet i CDCPs[(125)] arbejdsprogram. Arbejdet tog bl.a. udgangspunkt i OECDs ovennævnte rapport, og der udfærdigedes i 1989 guidelines - delt i en "minimum list" og en "optional list" - bl.a. med henblik på at opnå en vis harmonisering af lovgivningen, da der ofte var tale om grænseoverskridende kriminalitet. I 1989 vedtoges rekommandation nr. R(89)9, der anbefalede, at medlemsstaterne

bl.a. tog hensyn til disse guidelines i deres lovgivning[(126)].

Indholdet af de foreslåede guidelines er følgende:
I. Minimum list of offences necessary for a uniform criminal policy on legislation concerning computerrelated crimea.

a. Computerrelated fraud
The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for himself or for another person.

---

125. The European Committee on Crime Problems
126. Rekommandationen, rapporten og guidelines er trykt af Europarådet i 1990 (Computerrelated Crime). v

---

b. Computer forgery
The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, in a manner or under such conditions as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence.

c. Damage to computer data or programs
The erasure, damaging, deterioration or suppression of computer data or computer programs without right.

d. Computer sabotage
The input, alteration, erasure or suppression of computer data or computer programs, or interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunication system.

e. Unauthorised access
The access without right to a computer system or network by infringing security measures.

f. Unauthorised interception
The interception, made without right by technical means, of communication to, from and within a computer system or network.

g. Unauthorised reproduction of a protected computer program
The reproduction, distribution or communication to the public without right of a computer program, which is protected by law.

h. Unauthorised reproduction of a topography
The reproduction without right of a topography, protected by law, of a semi conductor product, of the commercial exploitation or the importation for thar purpose, done without right, of a topography or of a semi conductor product, manufactured by using the topography.

II. Optional list
a. Alteration of computer data or computer programs
The alteration of computer data or computer programs without right.

b. Computer espionage
The acquisition by improper means or the disclosure, transfer or use of a trade or commercial secret without right or any other legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third person.

c. Unauthorised use of a computer
The use of a computer system or network without right, that either:
i. is made with the acceptance of a significant risk of loss being caused to the person entitled to use the system or harm to the system or its functioning, or

ii. is made with the intent to cause loss to the person entitled to use the system or harm to the system or its functioning, or

iii. causes loss to the person entitled to use the system or harm to the system or its functioning.

d. Unauthorised use of a protected computer program
The use without right of a computer program which is protected by law and which has been reproduced without right, with the intent either to procure an unlawful economic gain for oneself or for another person, or to cause harm to the holder of the right.

Europarådets rekommandation nr. R(95)13

Europarådet nedsatte i 1991 "Committee of Experts on Procedural Law Problems connected with Computerrelated Crime" (PCPC). I 1995 vedtoges rekommandation R(95)13 vedrørende efterforskning, internationalt samarbejde m.v., der anbefalede, at medlemsstaterne tog hensyn til følgende principper:

I. Search and seizure

1. The legal distinction between searching computer systems and seizing data stored therin and intercepting data in the course of transmission should be clearly delineated and applied.

2. Criminal procedural laws should permit investigating authorities to search computer systems and seize data under similar conditions as under traditional powers of search and seizure. The person in charge of the system should be informed that the system has been searched and of the kind of data that has been seized. The legal remedies that are provided for in general against search and seizure should be equally applicable in case of search in computer systems and in case of seizure of data therin.

3. During the execution of a search, investigating authorities should have the power, subject to appropriate safeguards, to extend the search to other computer systems within their jurisdiction which are connected by means of a network and to seize the data therin, provided that immediate action is required.

4. Where automatically processed data is functionally equivalent to a traditional document, provisions in the criminal procedural law relating to search and seizure of documents should apply equally to it.

II. Technical surveillance

5. In view of the convergence of information technology and telecommunication, laws pertaining to technical surveillance for the purposes of criminal investigations, such as interception of telecommunication, should be reviewed and amended, where necessary, to ensure their applicability.

6. The law should permit investigating authorities to avail themselves of all necessary technical measures that enable the collection of traffic data in the investigation of crimes.

7. When collected in the course of a criminal investigation and in particular when obtained by means of intercepting telecommunication, data which is the object of legal protection and processed by a computer system should be secured in an appropriate manner.

8. Criminal procedural laws should be reviewed with at view to making possible the interception of telecommunications and the collection of traffic data in the investigation of serious offences against the confidentiality, integrity and availability of telecommunication or computer systems.

III. Obligations to cooperate with the investigating authorities

9. Subject to legal privileges or protection, most legal systems permit investigating authorities to order persons to hand over objects under their control that are required to serve as evidence. In a parallel fashion, provisions should be made for the power to order persons to submit any specified data under their control in a computer system in the form required by the investigating authority.

10. Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under their control to provide all necessary information to enable access to a computer system and the data therin. Criminal procedural law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure data therin.

11. Specific obligations should be imposed on operators of public and private networks that offer telecommunication services to the public to avail themselves of all necessary technical measures that enable the interception of telecommunication by the investigating authorities.

12. Specific obligations should be imposed on serviceproviders who offer telecommuncation services to the public, either through public or private networks, to provide information to identify the user, when so ordered by the competent investigating authority.

IV. Electronic evidence

13. The common need to collect, preserve and present electronic evidence in ways that best ensure and reflect their integrity and irrefutable authenticity, both for the purposes of domestic prosecution and international cooperation, should be recognised. Therefore, procedures and technical methods for handling electronic evidence should be further developed, and particularly in such a way as to ensure their compatibility between states. Criminal procedural law provisions on evidence relating to traditional documents should similarly apply to data stored in a computer system.

V. Use of encryption

14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary.VI. Research, statistics and training

15. The risks involved in the development and application of information technology with regard to commission of criminal offences should be assessed continuously. In order to enable the competent authorities to keep abreast of new phenomena in the field of computerrelated offences and to develop appropriate countermeasures, the collection and analysis of data on these offences, including the modus operandi and technical aspects, should be furthered.

16. The establishment of specialised units for the investigation of offences, the combating of which requires special expertise in information technology, should be considered. Training programmes enabling criminal justice personnel to avail themselves of expertise in this field should be furthered.

VII. International cooperation

17. The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignity or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.

18. Expedited and adequate procedures as well as a system of liaison should be available according to which the investigating authorities may request the foreign authorities to promptly collect evidence. For that purpose the requested authorities should be authorised to search a computer system and seize data with a view to its subsequent transfer. The requested authorities should also be authorised to provide trafficking data related to a specific telecommunication, intercept a specific telecommunication or identify its source. For that purpose, the existing mutual legal assistance instruments need to be supplemented.

EUs rekommandation af 17/1 1995 om aflytning af telekommunikation[(127)]

Rådet anbefalede, at medlemsstaterne tog hensyn til følgende krav:

1. Law enforcement agencies require access to the entire telecommunications transmitted, or caused to be

transmitted, to and from the number or other identifier of the target service used by the interception subject. Law enforcement agencies also require access to the callassociated data that are generated to process the call.

2. Law enforcement agencies require a realtime, fulltime monitoring capability for the interception of telecommunications. Call associated data should also be provided in realtime. If call associated data cannot be made available in real time, law enforcement agencies require the data to be available as soon as possible upon call termination.

3. Law enforcement agencies require network operators/service providers to provide one or several interfaces from which the intercepted communications can be transmitted to the law enforcement monitoring facility. These interfaces have to be commonly agreed on by the interception authorities and the network operators/service providers. Other issues associated with these interfaces will be handled according to accepted practices in individual countries.

4. Law enforcement agencies require interceptions to be implemented so that neither the interception target nor any other unauthorised person is aware of any changes made to fulfil the interception order. In particular, the operation of the target service must appear unchanged to the interception subject.

5. Law enforcement agencies require the interception to be designed and implemented to preclude unauthorised or improper use and to safeguard the information related to the interception.

6. Based on a lawful enquiry and before implementation of the interception, law enforcement agencies require (1) the interception subject's identity, service number or other distinctive identifier, (2) information on the services and features of the telecommunications system used by the interception subject and delivered by network operators/service providers, and (3) information on the technical parameters of the transmission to the law enforcement monitoring facility.

7. During the interception, law enforcement agencies may require information and/or assistance from the network operators/service providers to ensure that the communications acquired at the interception interface are those communications associated with the target service. The type of information and/or assistance required will vary according to the accepted practices in individual countries.

8. Law enforcement agencies require network operators/service providers to make provisions for implementing a number of simultaneous incepts. Multiple interceptions may be required for a single target service to allow monitoring by more than one law enforcement agency. In this case, network operators/service providers should take precautions to safeguard the identities of the monitoring agencies and ensure the confidentiality of the investigations. The maximum number of simultaneous interceptions for a given subscriber population will be in accordance with national requirements.

9. Law enforcement agencies require network operators/service providers to implement interceptions as quickly as possible (in urgent cases within a few hours or minutes). The response requirements of law enforcement agencies will vary by country and by the type of target service to be intercepted.

10. For the duration of the interception, law enforcement agencies require that the reliability of the services supporting interceptions at least equals the reliability of the target services provided to the interception subject. Law enforcement require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the network operators/service providers.

---

127. Udarbejdet på grundlag af artikel K.1 og K.2 i traktaten om Den Europæiske Union.

G8landenes[(128)] erklæring af 8/12 1997 om hightech crime

G8landenes justits og indenrigsministre vedtog på mødet i december 1997 følgende:

Statement of Principles

I. There must be no save havens for those who abuse information technologies.

II. Investigation and prosecution of international hightech crimes must be coordinated among all concerned States, regardless of where harm has occurred.

III. Law enforcement personnel must be trained and equipped to address hightech crimes.

IV. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.

V. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.

VI. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international hightech crime.

VII. Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides.

VIII. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.

IX. To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.

X. Work in this area should be coordinated with the work of other relevant international fora to ensure against duplication of efforts.

---

128. *Canada, Frankrig, Italien, Japan, Rusland, Storbritannien, Tyskland og USA.*

Action Plan

1. Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational hightech cases and designate a pointofcontact who is available on a twentyfour hour basis.

2. Take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating hightech crime and assisting law enforcement agencies of other States.

3. Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of hightech crimes.

4. Consider issues raised by hightech crimes, where relevant, when negotiating mutual assistance agreements or arrangements.

5. Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; transborder searches of data where the location of that data is unknown.

6. Develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally.

7. Work jointly with industry to ensure that new technologies facilitate our effort to combat hightech crime

8. Ensure that we can, in urgent and appropriate cases, accept and respond to mutual assistance requests relating to hightech crime by expedited but reliable means of communications, including voice, fax, or email, with written confirmation to follow where required.

9. Encourage internationally recognized standardsmaking bodies in the fields of telecommunications and information technologies to continue providing the public and private sectors with standards for reliable and secure telecommunications and data processing technologies.

10. Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions.

EU's udkast til Fælles Aktion om bekæmpelse af børnepornografi på Internettet (3/412 1998)

The Council agreed on this Joint Action which it will adopt formally at a forthcoming session:

"THE COUNCIL OF THE EUROPEAN UNION,

HAVING REGARD TO the Treaty on European Union, and in particular Article K.3 thereof,

HAVING REGARD TO the initiative of Austria,

TAKING ACCOUNT OF the Resolution adopted by the European Parliament on 19 September 1996 on minors, who are victims of violence,

BEARING IN MIND the Declaration and Agenda for Action, unanimously accepted by delegates at the World Congress against commercial sexual exploitation of children, held in Stockholm in August 1996, and the conclusions and recommendations of the European followup conference to the World Congress, held in Strasbourg in April 1998,

BEARING IN MIND, the European Convention on Human Rights, and in particular Article 10(2), thereof,

RECALLING Article 34 of the Convention on the Rights of the Child of 20 November 1989,

BEARING IN MIND the Joint Action of 24 February 1997 adopted by the Council on the basis of Article K.3 of the Treaty on European Union concerning action to combat trafficking in human beings and sexual exploitation of children[(129)],

TAKING ACCOUNT OF the Council Resolution of 17 January 1995 on the lawful interception of telecommunications[(130)],

BEARING IN MIND the Council Resolution of 20 December 1996 on individuals who cooperate with the judicial process in the fight against international organized crime [(131)],

BEARING IN MIND the Council decision of 18 December 1996 to extend the mandate of the EDU to include the area of trafficking in human beings,

WHEREAS, at its meeting on 5 and 6 December 1997, the Council provided for an extension of the term of "traffic in human beings", in the Annex regarding Article 2 (2) of the EUROPOL Convention to the effect that traffic in human beings and the exploitation of minors also includes the production, sale or distribution of child pornographic materials, and having regard to the Declaration of 5 and 6 December 1997 approved by the Council;

BEARING IN MIND the Council Resolution of 28 November 1996[(132)] on illegal and harmful content on the Internet, adopted at the Council meeting,

TAKING INTO ACCOUNT the Recommendation adopted by the Council of the European Union on 28 September 1998[(133)] on the development of the competitiveness of the European audiovisuals and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity,

BEARING IN MIND the Commission communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on the "action plan on promoting safe use of the Internet",

RECALLING the European Union's action plan to combat organised crime, approved by the Amsterdam European Council in June 1997[(134)], and the 10 principles of the G8 regarding hightech crime taken note of at the Justice and Home Affairs Council meeting in 19 March 1998.

[129.] *OJ L 63, 4.3.1997, p. 2.*
[130.] *OJ C 329, 4.11.1996, p. 1.*
[131.] *OJ C 10, 11.1.1997, p. 1.*
[132.] *OJ C 70, 6.3.1997, p. 1.*
[133.] *OJ L 270, 7.10.1998, p. 48*
[134.] *OJ C 251, 15.8.1997, p.1.*

WHEREAS the traffic in human beings and the sexual exploitation of children constitute a serious infringement of fundamental human rights and in particular of human dignity;

AWARE of the fact that the sexual abuse of children and the production, processing, possession and distribution of child pornography may constitute an important form of international organized crime, the extent of which within the European Union gives cause for ever increasing concern,

CONVINCED that a high value must be placed on the physical and emotional integrity of children and the protection of victims of sexual crimes,

AWARE OF THE NEED for further measures by the Union for promoting the safe use of the Internet,

IN ORDER TO prevent and combat the sexual abuse of children and in particular the production, processing, distribution and possession of child pornography through the Internet,

HAS ADOPTED THIS JOINT ACTION:

Article 1

1. In order to intensify measures to prevent and combat the production, processing, distribution and possession of child pornography and to promote the effective investigation and prosecution of offences in this area, the Member States will take the necessary measures to encourage Internet users to inform law enforcement authorities, either directly or indirectly, on suspected distribution of child pornography material on the Internet, if they come across such material. Internet users shall be made aware of ways to make contract with law enforcement authorities or entities which have privileged links with law enforcement authorities, to enable such authorities to fulfil their task of preventing and combating child pornography in the Internet.

2. Where necessary, and taking account of the administrative structure of each Member State, measures for the promotion of effective investigation and prosecution of offences in this area could be the setting up of specialised units within law enforcement with the necessary expertise and resources to be able to deal swiftly with information on suspected production, processing, distribution and possession of child pornography.

3. The Member States shall ensure that the law enforcement authorities act swiftly when they have received information on suspected production, processing, distribution and possession of child pornography.

Article 2

1. The Member States undertake to ensure the widest possible cooperation to facilitate an effective investigation and prosecution of offences concerning child pornography on the Internet in accordance with existing arrangements and agreements.

2. Existing channels for communication, such as Interpol, shall be used. To the extent that points of contact consisting of knowledgeable personnel have been set up already on a 24hour basis to ensure a timely, effective response to these offences, such points of contact shall be used for exchange of information and further contacts between Member States with a view to taking efficient action against offences involving child pornography.

3. Member States shall ensure that Europol, within the limits of its mandate, is informed of suspected cases of child pornography.

4. The Member States, in appropriate cooperation with Europol, shall examine the possibility of organising regular meetings of competent authorities specialising in fight against child pornography on the Internet with a view to promoting general information exchanges, analyses of the situation and tactical coordination.

5. Member States shall notify the General Secretariat of the Council of the organizational unit of units acting as contact points under paragraph 2. The General Secretariat shall notify all Member States of these contact points.

Article 3

While engaging in a constructive dialogue with industry, Member States shall examine appropriate measures, of a voluntary or a legally binding nature, to eliminate child pornography on the Internet. In particular, the Member States shall exchange experiences on the effectiveness of any measures they have taken to eliminate child pornography on the Internet. They may, for instance, in this context examine one or several of the following measures prompting Internet providers:

1. to advice the competent entities mentioned in article 1, paragraph 1 or the units mentioned in article 1, paragraph 2 of child pornography material of which they have been informed or of which they are aware and which is distributed through them;

2. to withdraw from circulation child pornography material of which they have been informed or of which they are aware and which are distributed through them unless otherwise specified by the competent authorities;

3. in accordance with the Council Resolution of 17 January 1995 in the lawful interception of telecommunications to retain traffic related data, where applicable and technically feasible - in particular for criminal prosecution purposes in cases of suspected sexual abuse of children, production, processing and distribution of child pornography - for such time as may be specified under the applicable national law to allow the data to be made available for inspection by the criminal prosecution authorities in accordance with the applicable rules of procedure;

4. to set up their own control systems for combating the production, processing, distribution and possession of child pornography.

Article 4

Member States shall regularly verify whether technological developments require, in order to maintain the efficiency of the fight against child pornography on the Internet, changes to criminal procedural law, while respecting the fundamental principles thereof and, where necessary, shall make appropriate proposals to their competent authorities to that end.

Article 5

Member States, in contact with the industry, shall cooperate by sharing their experiences and encouraging, if possible, the production of filters and other technical means to prevent and detect the distribution of child pornography material.

Article 6

1. The Council shall examine the extent to which Member States have fulfilled their obligations arising out of the Joint Action of 24 February 1997 adopted by the Council on the basis of Article K.3 of the Treaty on European Union concerning action to combat trafficking in human beings and sexual exploitation of children, and the extent to which the measures proposed in the present joint action have proved effective.

2. This examination may be carried out, with the exceptions mentioned under a) and b) below, under the Joint Action of 5 December 1997 establishing a mechanism for evaluating the application and implementation at national level of international undertakings in the fight against organized crime[(135)]. In this context, the Council shall also examine the extent to which Member States have implemented the Council Resolution of 17 January 1995 on the lawful interception of telecommunications into national law. The exceptions are:

a) evaluation teams shall consist of two experts;

b) onthespot evaluation shall be made so as to avoid cumbersome procedures.

1. The assessment specified in Title IV B of the Joint Action of 24 February 1997, shall not be carried out. It shall be replaced by the assessment referred to in paragraph 2.

2. On the basis of the information received in the course of this assessment, the Council shall examine any further measure it may wish to take in order to make fight against child pornography and sexual exploitation of children more effective.

Article 7

This joint action shall be published in the Official Journal; it shall enter into force on the day of its publication in the Official Journal."

---

135. OJ L 344, 15.12.97, p.7.

BILAG 2 - Edition og indgreb i meddelelseshemmeligheden

Edition (§ 827, stk. 1)

"Retten kan pålægge den person eller offentlige myndighed, der har rådighed over dokumenter eller andre ting af den i § 824 nævnte art[(136)], at forevise eller udlevere dem, medmindre der derved vil fremkomme oplysning om forhold, som vedkommende ville være udelukket fra eller fritaget for at afgive forklaring om som vidne, jf. §§ 169172." [(137)]

Kapitel 71. Indgreb i meddelelseshemmeligheden

§ 780. Politiet kan efter reglerne i dette kapitel foretage indgreb i meddelelseshemmeligheden ved at

1) aflytte telefonsamtaler eller anden tilsvarende telekommunikation (telefonaflytning),
2) aflytte andre samtaler eller udtalelser ved hjælp af et apparat (anden aflytning),
3) indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat, selv om indehaveren af dette ikke har meddelt tilladelse hertil (teleoplysning),
4) tilbageholde, åbne og gøre sig bekendt med indholdet af breve, telegrammer og andre forsendelser (brevåbning) og
5) standse den videre befordring af forsendelser som nævnt i nr. 4 (brevstandsning).
Stk. 2. ¿..

§ 781. Indgreb i meddelelseshemmeligheden må kun foretages, såfremt
1) der er bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt,

2) indgrebet må antages at være af afgørende betydning for efterforskningen og

3) efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, en forsætlig overtrædelse af straffelovens kapitler 12 eller 13 eller en overtrædelse af straffelovens §§ 124, stk. 1, 125, 127, stk. 1, 193, stk. 1, 245, 252, stk. 1, 266, 281, 286, stk. 1 eller 289 eller en overtrædelse af udlændingelovens § 59, stk. 3.

Stk. 2. Er betingelserne i stk. 1, nr. 1 og 2, opfyldt, kan telefonaflytning og teleoplysning endvidere foretages, såfremt mistanken angår fredskrænkelser som omhandlet i straffelovens § 263, stk. 2, eller § 263, stk. 3, jf. stk. 2.

Stk. 3. Er betingelserne i stk. 1, nr. 1 og 2, opfyldt, kan teleoplysning endvidere foretages, såfremt mistanken angår gentagne fredskrænkelser som omhandlet i straffelovens § 265. Det samme gælder, såfremt mistanken angår en overtrædelse af straffelovens § 279 a eller § 293, stk. 1, begået ved anvendelse af en telekommunikationstjeneste.

Stk. 4. Brevåbning og brevstandsning kan desuden foretages, hvis der foreligger en særlig bestyrket mistanke om, at der i forsendelsen findes genstande, som bør konfiskeres, eller som ved en forbrydelse er fravendt nogen, som kan kræve dem tilbage.

Stk. 5. Aflytning efter § 780, stk. 1, nr. 2, kan kun foretages, når mistanken vedrører en forbrydelse, som har medført eller som kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier.

§ 782. Et indgreb i meddelelseshemmeligheden må ikke foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer, ville være et uforholdsmæssigt indgreb.

Stk. 2. Telefonaflytning, anden aflytning, brevåbning og brevstandsning må ikke foretages med hensyn til den mistænktes forbindelse med personer, som efter reglerne i § 170 er udelukket fra at afgive forklaring som vidne.
(§ 783: Regler om kendelser m.v.)
(§ 784: Advokatbeskikkelse før afgørelse)
(§ 785: Advokatens rettigheder)

§ 786. Det påhviler post og telegrafvæsenet, telefonselskaberne og andre tilsvarende offentlige og private virksomheder at bistå politiet ved gennemførelsen af indgreb i meddelelseshemmeligheden, herunder ved at etablere aflytning af telefonsamtaler m.v., ved at give de i § 780, stk. 1, nr. 3, nævnte oplysninger samt ved at tilbageholde og udlevere forsendelser m.v.

Stk. 2. Uden for de i § 780, stk. 1, nr. 3, nævnte tilfælde kan retten efter begæring fra politiet med samtykke fra indehaveren af en telefon eller andet kommunikationsapparat give de i stk. 1 nævnte selskaber m.v. pålæg om at oplyse, hvilke andre apparater der sættes i forbindelse med det pågældende apparat.

Stk. 3. Bestemmelsen i § 178 finder tilsvarende anvendelse på den, som uden lovlig grund undlader at yde den bistand, som er nævnt i stk. 1, eller at efterkomme et pålæg, som er givet efter stk. 2.

(§ 787: Advokatens rettigheder)

§ 788. Efter afslutningen af et indgreb i meddelelseshemmeligheden skal der gives underretning om indgrebet, jf. dog stk. 4. Har den person, til hvem underretning efter stk. 2 skal gives, været mistænkt i sagen, skal der tillige gives underretning herom og om, hvilken overtrædelse mistanken har angået.

Stk. 2. Underretning gives
1) ved telefonaflytning og teleoplysning til indehaveren af den pågældende telefon,
2) ved anden aflytning til den, der har rådighed over det sted eller det lokale, hvor samtalen er afholdt eller udtalelsen fremsat, og
3) ved brevåbning og brevstandsning til afsenderen eller modtageren af forsendelsen.

Stk. 3. Underretningen gives af den byret, som har truffet afgørelse efter § 783. Underretningen gives snarest muligt, såfremt politiet ikke senest 14 dage efter udløbet af det tidsrum, for hvilket indgrebet har været tilladt, har fremsat begæring om undladelse af eller udsættelse med underretning, jf. stk. 4. Er der i medfør af § 784, stk. 1, beskikket en advokat, skal genpart af underretningen sendes til denne.

Stk. 4. Vil underretning som nævnt i stk. 13 være til skade for efterforskningen, eller taler omstændighederne i øvrigt imod underretning, kan retten efter begæring fra politiet beslutte, at underretning skal undlades eller udsættes i et nærmere fastsat tidsrum, der kan forlænges ved senere beslutning. ¿¿

§ 789. Får politiet ved et indgreb i meddelelseshemmeligheden oplysning om en lovovertrædelse, der ikke har dannet og efter § 781, stk. 1, nr. 3, eller § 781, stk. 5, heller ikke kunne danne grundlag for indgrebet, kan politiet anvende denne oplysning som led i efterforskningen af den pågældende lovovertrædelse.

Stk. 2. Oplysninger, der er tilvejebragt ved et indgreb i meddelelseshemmeligheden, må ikke anvendes som bevis i retten vedrørende en lovovertrædelse, der ikke har dannet og efter § 781, stk. 1, nr. 3, eller § 781, stk. 5, heller ikke kunne danne grundlag for indgrebet.

Stk. 3. Retten kan bestemme, at stk. 2 ikke finder anvendelse, såfremt 1) andre efterforskningsskridt ikke vil være egnede til at sikre bevis i sagen, 2) sagen angår en lovovertrædelse, der efter loven kan medføre fængsel i 1 år og 6 måneder eller derover, og

3) retten i øvrigt finder det ubetænkeligt.

(§ 790: Viderebefordring ved brevåbning)

(§ 791: Destruktionsregler vedrørende det tilvejebragte materiale)

[136.] Bestemmelsen omfatter ting, der antages at være af betydning som bevismidler eller at burde konfiskeres, eller som ved forbrydelsen er fravendt nogen, af hvem de kan kræves tilbage.
[137.] Ved lov nr. 229 af 21/4 1999 om ændring af retsplejeloven (Beslaglæggelse, edition m.v.), der trådte i kraft 1/7 1999, er editionsbestemmelsen formuleret således: "§ 804. Som led i efterforskningen af en lovovertrædelse, der er undergivet offentlig påtale, kan der meddeles en person, der ikke er mistænkt, pålæg om at forevise eller udlevere genstande (edition), hvis der er grund til at antage, at en genstand, som den pågældende har rådighed over, kan tjene som bevis, bør konfiskeres eller ved lovovertrædelsen er fravendt nogen, som kan kræve den tilbage." Bestemmelsens stk. 4 indeholder samme begrænsning som den nugældende vedrørende vidnestatus.

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 kriminalitetsmønstre 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, herunder 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, hvidvasklovgivningen og den finansielle lovgivning skal behandles i denne sammenhæng. Endvidere skal de internationale tiltag på området, herunder i EUregi, indgå i arbejdet.
- Udvalget skal tillige overveje længere forældelsesfrister på en række områder.
- 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 retsplejeloven med henblik på at sikre tidssvarende bestemmelser om datakriminalitet.
- Gennemgangen skal således bl.a. omfatte straffelovens bestemmelser om urigtige erklæringer og dokumentfalsk og om industrispionage.
- Endvidere skal udvalget vurdere de kriminalitetsformer, som informationssamfundet, 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 muligt 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

Direktør Jørgen Christiansen
Arbejderbevægelsens Erhvervsråd

Statsadvokat Michael Clan
Statsadvokaten for særlig økonomisk kriminalitet

Professor, lic. jur. Vagn Greve
Københavns Universitet

Fuldmægtig Alexander Houen
Skatteministeriet
(fra december 1998)

Fuldmægtig Annemette Vestergaard Jacobsen
Skatteministeriet
(til oktober 1998)

Fuldmægtig Helle Jahn
Erhvervsministeriet
(fra august 1998)

Kommitteret Poul Dahl Jensen
Justitsministeriet

Statsautoriseret revisor Jesper Koefoed
Foreningen af Statsautoriserede Revisorer

Kontorchef, advokat Lau Kramer
Foreningen Registrerede Revisorer FRR

Fuldmægtig Lisbeth Krener
Erhvervsministeriet
(til august 1998)

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

Lektor Lars Bo Langsted
Handelshøjskolen i Århus

Kontorchef Kirsten Mandrup
Økonomiministeriet

Politimester Annemette Møller
Politimesterforeningen

Konsulent Lene Nielsen
Dansk Industri

Advokat Erik Overgaard

Advokatrådet

Generalsekretær Henrik Rothe
Advokatrådet
(fra marts 1999)

Sekretariat

Vicestatsadvokat Ulla Høg
Statsadvokaten for særlig økonomisk kriminalitet

Kst. 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 6 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)

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

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 arbejdsgrupper, og at en betænkning vedrørende samtlige af de i kommissoriet nævnte problemstillinger derfor først ville kunne foreligge på et meget senere tidspunkt end færdiggørelsen af en del af de indeholdte problemstillinger.

Udvalget har tidligere afgivet delbetænkning I vedrørende udviklingen i lovgivningen og kriminaliteten samt vedrørende hæleri og anden efterfølgende medvirken.

Denne delbetænkning indeholder to selvstændige emner fra udvalgets kommissorium og bygger på en delrapport fra arbejdsgruppe 6, der behandler spørgsmål vedrørende datakriminalitet. Denne delrapport er derefter tillige behandlet i arbejdsgruppe 2, der behandler spørgsmål vedrørende straffeloven, og i arbejdsgruppe 5, der behandler

spørgsmål vedrørende domsforhandling m.v. Betænkningen vedrører dels spørgsmålet om den strafferetlige behandling af personer, der udbreder børnepornografisk materiale, og af de personer, der modtager materialet. Dels vedrører den spørgsmålet om de straffeprocessuelle regler set i forhold til de særlige efterforskningsbehov ved IT-relateret kriminalitet, ikke blot i relation til børnepornografi, men i relation til kriminalitet generelt.

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

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

Kriminalassistent Kim Aarenstrup
Københavns politi, Afdeling B, CCU

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

Professor, lic. jur. Vagn Greve
Københavns Universitet

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

Fuldmægtig Henrik Oftebro-Svendsen
Fødevareministeriet

Sikkerhedschef Kjell Olsen (til november 1998)
UNI-C

Vicekriminalkommissær Ronald Pedersen
Rigspolitichefens afd. A, Rejseafdelingen

Systemrevisionschef Ole Stampe Rasmussen
PBS A/S

Kst. statsadvokatassessor Jens Madsen (sekretær)
Statsadvokaten for særlig økonomisk kriminalitet

Som nævnt er rapporten fra arbejdsgruppen vedrørende datakriminalitet for så vidt angår straffelovsspørgsmål 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

Landsdommer Bent Carlsen
Dommerforeningen

Vicestatsadvokat Ulla Høg
Statsadvokaten for særlig økonomisk kriminalitet

Kommitteret Poul Dahl Jensen
Justitsministeriet

Kst. statsadvokatassessor Jens Madsen
Statsadvokaten for særlig økonomisk kriminalitet

Politimester Annemette Møller
Politimesterforeningen

Generalsekretær Henrik Rothe
Advokatrådet

Fuldmægtig Lennart Houmann (sekretær)
Justitsministeriet

Rapporten er for så vidt angår straffeprocessuelle spørgsmål derefter behandlet i *arbejdsgruppe 5*, der har haft følgende sammensætning ved behandlingen:

Landsdommer Bent Carlsen (formand)
Dommerforeningen

Vicestatsadvokat Ulla Høg
Statsadvokaten for særlig økonomisk kriminalitet

Kontorchef Jens Kruse Mikkelsen
Justitsministeriet

Generalsekretær Henrik Rothe
Advokatrådet

Kst. statsadvokatassessor Jens Madsen (sekretær)
Statsadvokaten for særlig økonomisk kriminalitet

Under hensyntagen til, at arbejdsgruppen vedrørende datakriminalitet helt overvejende har været sammensat med eksperter på området, der ikke er medlemmer af udvalget, har udvalget i denne delbetænkning valgt tillige at anføre, hvordan medlemmerne af denne arbejdsgruppe har forholdt sig til de enkelte forslag.

1.4. Resumé

Betænkningen omhandler - med udgangspunkt i de nye problemstillinger, der følger med IT-udviklingen - dels

straffelovens § 235 om børnepornografi og dels mere generelt, om der er behov for at justere de straffeprocessuelle regler - især reglerne i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden - for at sikre, at der kan foretages den fornødne efterforskning i IT-sammenhænge.

I *kapitel 2* omtales nogle generelle problemstillinger i forbindelse med IT-anvendelse, især i relation til netsystemer. I den forbindelse gennemgås bl.a. spørgsmålet om dansk straffemyndighed ved kriminalitet via Internettet, særligt for så vidt angår salg og udbredelse af børnepornografi via Internettet. Det er udvalgets umiddelbare opfattelse, at den retstilstand, som de gældende jurisdiktionsbestemmelser må antages at indebære i forhold til salg og udbredelse af børnepornografi, er tilfredsstillende. Udvalget finder derfor ikke på det foreliggende grundlag behov for lovændringer på området. Da retspraksis af betydning for dette område er sparsom, og da udviklingen hele tiden åbner nye tekniske muligheder, finder udvalget, at udviklingen løbende bør følges nøje for at sikre, at straffelovens regler om straffemyndighed til stadighed er tidssvarende i forhold til den teknologiske udvikling.

I *kapitel 3* behandles spørgsmålet om ansvar for indholdet af informationssystemer. Udvalget finder, at udbredelse i en videre kreds på nogle områder bør sidestilles med erhvervsmæssig spredning, men har herudover ikke foreslået lovændringer på dette område.

I *kapitel 4* behandles straffelovens § 235 om børnepornografi. Udvalget foreslår, at bestemmelsens stk. 1 om udbredelse af børnepornografi ændres således, at ikke kun den erhvervsmæssige udbredelse, men også udbredelse i en videre kreds - f.eks. via Internettet - er omfattet. Udvalget foreslår endvidere, at strafmaksimum i stk. 1 forhøjes fra fængsel i 6 måneder til fængsel i 2 år.

For så vidt angår straffelovens § 235, stk. 2, om besiddelse af børnepornografi foreslår udvalget, at bestemmelsen udvides til også at omfatte den, der, uden at besiddelseskravet er opfyldt, mod vederlag retsstridigt gør sig bekendt med de af bestemmelsen omfattede børnepornografiske fremstillinger. Med hensyn til bestemmelsen i stk. 2 finder udvalget, at den nuværende begrænsning af straffen til bøde bør bevares som normalstrafferammen. Udvalget finder imidlertid, at der bør være mulighed for under skærpende omstændigheder at idømme hæfte eller fængsel indtil 6 måneder.

I *kapitel 5* omtales efterforskningsmuligheder hos Internetudbydere og teleselskaber samt kryptering. Udvalget foreslår, at teletrafikken logges i et omfang, der tilgodeser behovet for at kunne efterforske kriminalitet, og at de loggede oplysninger opbevares i 6 måneder. Et flertal i udvalget foreslår, at disse pligter reguleres i lovform, mens et mindretal finder, at spørgsmålet så vidt muligt skal løses ved en selvregulering i branchen.

I *kapitel 6* behandles retsplejelovens efterforskningsregler set i relation til aktuelle IT-problemstillinger.

Med hensyn til adgang til indholdet af digitale meddelelser finder udvalget, at den gældende retstilstand, hvorefter bestemmelserne om edition eller ransagning og beslaglæggelse finder anvendelse på meddelelser, der befinder sig hos enten afsenderen eller modtageren, bør opretholdes. Med hensyn til adgang til f.eks. email hos Internetudbyderen finder udvalgets flertal, at denne situation skal sidestilles med traditionelle (fysiske) breve og behandles efter de regler om indgreb i meddelelseshemmeligheden, der gælder for sådanne breve. Et mindretal finder, at adgang til email hos Internetudbydere bør behandles efter reglerne om edition.

Med hensyn til teleoplysninger finder udvalgets flertal, at oplysninger herom fortsat bør reguleres i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden. Et mindretal finder, at teleoplysninger bør behandles efter reglerne om edition.

Udvalget finder, at adgang til teleoplysninger vedrørende sendemasttrafik bør reguleres i retsplejelovens § 780 om indgreb i meddelelseshemmeligheden, og at dette indgreb kun skal være muligt i særligt kvalificerede sager.

Et flertal i udvalget finder, at teleselskaber ikke skal kunne meddele samtykke til indhentelse af teleoplysninger vedrørende offentlige telefoner, men at de almindelige betingelser for indgreb i meddelelseshemmeligheden skal være opfyldt. Et mindretal finder, at teleselskaberne bør kunne give samtykke.

Med hensyn til spørgsmålet om, hvorvidt området for, ved hvilke kriminalitetsformer der kan foretages indgreb i meddelelseshemmeligheden, skal udvides, finder udvalgets flertal, at der bør være hjemmel til sådanne indgreb i sager om overtrædelse af straffelovens § 235 om børnepornografi. Et af flertallets medlemmer finder, at det herudover bør overvejes at have hjemmel til at foretage disse indgreb i sager om misbrug af intern viden og

kursmanipulation efter lov om værdipapirhandel m.v. Et mindretal finder, at der bør indsættes en generel hjemmel til indgreb i meddelelseshemmeligheden i alle sager, der kan straffes med fængsel i 1 år og 6 måneder eller derover, såfremt der i den konkrete sag reelt ikke er andre efterforskningsmuligheder.

Kapitel 7 indeholder udvalgets forslag med bemærkninger.

[Forside] [Indholdsfortegnelse] [Top] [Næste dokument]

Justitsministeriet Version 1.0 den 8. september 1999
Denne publikation findes på adressen: http://jm.schultzboghandel.dk

---

KAPITEL 2 - GENERELLE PROBLEMSTILLINGER

2.1. Netsystemer

Gennem de seneste år er IT-udviklingen forstærket eksponentielt gennem udviklingen af det verdensomspændende Internet. Navnlig udviklingen af den Internetteknologi, der almindeligvis går under betegnelsen the World Wide Web (også kaldet WWW), har understøttet en række nye former for informationsudveksling med heraf følgende retlige (herunder strafferetlige) implikationer.

Gennem the World Wide Web forbindes et antal databaser, hvis informationsindhold hver for sig fremtræder med en ensartet grafisk brugergrænseflade - de såkaldte "hjemmesider". Når en bruger ved hjælp af en computer, der er programmeret med en såkaldt webbrowser, retter henvendelse 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 struktur. Disse Internetoperatører kan opdeles således[(1)]:

1) Netværksoperatører, der alene stiller den overordnede teknologi til rådighed.

2) Internetudbydere, der etablerer adgangen til Internettet. Disse kan opdeles i:

a) Content Providers, der tilvejebringer den information, der er tilgængelig.

b) Hosts, der udlejer plads på serveren til kunder eller stiller nyhedsgrupper til rådighed på sin newsserver.

c) Access Providers, der sælger adgang til Internettet (hvilket almindeligvis omfatter email funktioner og adgang til the World Wide Web).

Udviklingen indebærer som en naturlig konsekvens også en øget risiko for retsstridig brug af disse teknologier.

En opgørelse over antallet af værtscomputere (hosts)[(2)] 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.

Udviklingen har da også allerede medført, at de processuelle muligheder for at efterforske IT-relateret kriminalitet er blevet ændret for at imødekomme de nye behov. I 1996[(3)] blev retsplejelovens § 781 ændret således, 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 anvendelse af en telekommunikationstjeneste.

---

[1].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.
[2]. Hobbes' Internet Timeline.
(http://info.isoc.org./guest/zakon/Internet/History/HIT.html.)
[3]. Lov nr. 388 af 22/5 1996.

2.2. Forskellige internationale anbefalinger

IT-udviklingen indebærer mange internationalt relaterede problemstillinger, og udviklingen i det internationale arbejde på IT-området har derfor stor betydning for, hvilke reelle muligheder der er for at bekæmpe IT-relateret kriminalitet.(4) Det gælder både spørgsmålet om, hvorvidt der er tilsvarende straffebestemmelser - og dermed mulighed for at bistå med strafprocessuelle tvangsindgreb - og spørgsmålet om, hvilke efterforskningstiltag der kan anvendes.

Blandt de centrale internationale anbefalinger kan nævnes følgende (hvoraf nogle af punkterne nævnes senere i betænkningen ved de enkelte problemstillinger):

OECD påbegyndte i 1984 en analyse af medlemsstaternes lovgivning vedrørende IT- relateret kriminalitet. Resultatet blev publiceret i 1986(5). Det blev anbefalet i rapporten, at medlemsstaterne overvejede en straffelovgivning vedrørende computerrelateret berigelse, falsk, hærværk, piratkopiering og hacking, jfr. bilag 1.

Europarådet inkluderede fra 198586 computerrelateret kriminalitet i CDPCs(6) arbejdsprogram. Arbejdet tog bl.a. udgangspunkt i OECDs ovennævnte rapport, og der udfærdigedes i 1989 guidelines - delt i en "minimum list" og en "optional list" - bl.a. med henblik på at opnå en vis harmonisering af lovgivningen, da der ofte var tale om grænseoverskridende kriminalitet. I 1989 vedtoges rekommandation nr. R(89)9, der anbefalede, at medlemsstaterne bl.a. tog hensyn til disse guidelines i deres lovgivning(7). På "the minimum list" er OECDs rekommandationer i lidt udbygget form, og der er tilføjet to nye emner, idet også henholdsvis aflytning og halvlederbeskyttelse er medtaget. "The optional list" har herudover ændring af data eller programmer, computer spionage og uberettiget brug af computer eller programmer, jfr. bilag 1.

Europarådet nedsatte i 1991 "Committee of Experts on Procedural Law Problems connected with Computerrelated Crime" (PCPC). I 1995 vedtoges rekommandation R(95)13 vedrørende efterforskning, internationalt samarbejde m.v., der anbefalede, at ransagning og beslaglæggelse skulle kunne ske i edbmiljøer som i andre miljøer, at der i visse tilfælde skulle kunne foretages indgreb i meddelelseshemmeligheden, m.v., jfr. bilag 1.

Rådet for EU udfærdigede 17/1 1995 en resolution om lovlig aflytning af telekommunikation(8), der anbefalede, at der i en række henseender blev taget hensyn til de efterforskningsmæssige behov, jfr. bilag 1.

OECD udfærdigede 27/3 1997 rekommandationer vedrørende "Guidelines for cryptography policy", der både fremhævede betydningen af kryptering i relation til datasikkerhed og beskyttelse af privatlivet og betydningen af, at kryptering ikke udgør en risiko for den offentlige sikkerhed og retsforfølgning. Rekommandationerne indeholder dog ingen mere præcise anvisninger til, hvordan disse modstridende interesser tilgodeses samtidig.

Europarådet arbejder fortsat med IT-relateret kriminalitet, og CDPC har i 1997 nedsat en Committee of Experts on Crime in Cyberspace (PCCY)(9), der arbejder med en konvention vedrørende såvel de strafferetlige som de processuelle aspekter, herunder det internationale samarbejde og adgangen til i et vist omfang via en PC at efterforske over grænserne.

Interpol har - især ved arbejdsgruppen The Interpol European Working Party on Information Technology Crime - bl.a. med Europarådets rekommandation nr. R(89)9 som udgangspunkt arbejdet med den strafferetlige dækning på området. Derudover er nedsat igangværende underarbejdsgrupper, der bl.a. ser på kriminelt misbrug af Internettet, elektroniske betalingsmidler og manipulation med kommunikationsnet.

Særligt vedrørende Internettet gælder det i dag for alle internationale organisationer, at de forsøger at få afklaret, hvad de nuværende og fremtidige muligheder for anvendelse af Internettet betyder for de områder, de beskæftiger sig med.

Af mere specielle fora, der har udfærdiget handlingsplaner bl.a. vedrørende kriminelles anvendelse af IT-mulighederne og efterforskningsbehov, kan nævnes Gruppen på Højt Plan, der blev nedsat af det Europæiske Råd og i april 1997 udfærdigede en handlingsplan til bekæmpelse af organiseret kriminalitet(10), og G8landenes erklæring af 10/12 1997 om hightech crime(11).

I EU foreligger der et af Rådet foreløbigt godkendt udkast til fælles aktion vedrørende bekæmpelse af børnepornografi på Internettet(12). Udkastet påpeger bl.a., at medlemsstaterne skal sikre et hurtigt og effektivt samarbejde i disse sager, og peger bl.a. på en mulighed for at regulere Internetudbydere således, at trafikrelaterede data, hvor det er muligt, opbevares i det tidsrum, der kan være nødvendigt for at kunne sende disse data til de retsforfølgende myndigheder. Der er ikke angivet noget anbefalet tidsrum for denne opbevaring.

Endvidere foreligger EuropaParlamentets og Rådets beslutning af 25/1 1999 om vedtagelse af en flerårig EUhandleplan til fremme af en mere sikker anvendelse af Internettet ved bekæmpelse af ulovligt og skadeligt indhold på globale net(13). Handleplanen vedrører bl.a. fremme af selvregulering i branchen og af ordninger til overvågning af indhold (f.eks. børnepornografisk indhold og indhold, der opfordrer til had på grund af race, køn, religion, nationalitet eller etnisk herkomst).

---

4. Problemstillingerne vedrørende den internationale dimension er meget udførligt gennemgået af professor Ulrich Sieber i en artikelserie - Internet Law - i Computer Law & Security Report 1997 nr. 36 og 1998 nr. 1. Det konkluderes bl.a., at rent nationale kontroltiltag er ineffektive ved internationale net, og at det derfor er absolut nødvendigt at finde supranationale og internationale løsninger.

5. OECD-rapport ICCP nr. 10, Computerrelated crime : Analysis of legal policy

6.Comité Directeure pour les Problèmes Criminelles. På engelsk kaldet the European Committee on Crime Problems.

7. Rekommandationen, rapporten og guidelines er trykt af Europarådet i 1990 (Computerrelated Crime).

8. EFT 1996 C 329/1.

9. Problèmes Criminelles - Comité d'Èxperts sur la Criminalité dans CyberÉspace.

10. 6726/4/97 REV 4.

11. Nogle punkter fra disse dokumenter er omtalt i afsnit 5 og 6. G8landenes erklæring er gengivet i bilag 1.

12. Rådets pressemeddelelse fra mødet 34 december 1998 (13673/98 (Presse 427)), gengivet i bilag 1.

13. Nr. 276/1999/EF, EFT 1999 L 33/1.

2.3. Straffemyndighed

2.3.1. Generelt vedrørende straffemyndighed

Generelle regler om dansk straffemyndighed (jurisdiktionskompetence) er fastsat i straffelovens §§ 612.

Hovedreglen om dansk straffemyndighed findes i straffelovens § 6, nr. 1. Efter denne bestemmelse hører handlinger, der foretages i den danske stat, under dansk straffemyndighed (*territorialprincippet*). Forbrydelser, der er begået her i landet, kan således strafforfølges ved danske domstole uanset gerningsmandens nationalitet.

Udtrykket "handlinger, der foretages i den danske stat" betegner sprogligt de forbrydelser, som begås ved en eller flere handlinger på territoriet. I almindelighed vil gerningsmanden (eller en medvirkende) være fysisk til stede på det sted, hvor handlingen foretages. Der er imidlertid ikke noget til hinder for, at en enkeltpersons handling også kan lokaliseres til et sted, hvor gerningsmanden ikke på handlingstidspunktet befinder sig.

Begår en person, der befinder sig i Sverige, ved hjælp af sin computer indbrud i en computer her i landet, må handlingen lokaliseres ikke blot til Sverige, hvor gerningsmanden fysisk befinder sig, men også til Danmark, hvor indbruddet sker. Der vil således foreligge dansk straffemyndighed efter straffelovens § 6, nr. 1. I sådanne tilfælde vil det således ikke være nødvendigt at anvende straffelovens § 9 om virkningsstedet for at statuere dansk straffemyndighed, selv om gerningsmanden ikke på handlingstidspunktet befandt sig på dansk område, jfr. nedenfor.

Ordet "handlinger" i § 6, nr. 1, antages i almindelighed også at omfatte forsøgs og medvirkenshandlinger. Det indebærer, at forsøgs og medvirkenshandlinger, der begås på dansk område, skaber dansk jurisdiktion over for den pågældende, selv om den forbrydelse, som forsøgs eller medvirkenshandlinger knytter sig til, fuldbyrdes eller tænkes fuldbyrdet i udlandet[(14)]. Det må anses for uafklaret, om en på dansk område foretagen forsøgs eller medvirkenshandling skaber jurisdiktion efter § 6, nr. 1, hvis den forbrydelse efter dansk ret, som handlingen knytter sig til, skal fuldbyrdes i et land, hvor forholdet er straffrit. Som eksempel kan nævnes medvirken på dansk grund til samleje med børn mellem 1215 år, der skal finde sted i et land, hvor den seksuelle lavalder er 12 år.

Udvalget er ikke bekendt med retsafgørelser om dette spørgsmål. Det er derfor ikke muligt at sige noget sikkert om, hvorvidt det i det nævnte eksempel vil have betydning, om de pågældende mindreårige er bragt med fra Danmark, eller om der er tale om "lokale" børn. Meget taler efter udvalgets opfattelse for dansk straffemyndighed i hvert fald i de tilfælde, hvor der er tale om medbragte børn.

[14.] Hurwitz anfører i Den danske Kriminalret, Alm. Del, s. 102, at det for en anvendelse af § 6 ikke kan kræves, at hele den forbryderiske virksomhed er foregået inden for landets område, når blot væsentlige dele deraf er foregået her i landet. Det fremgår ikke, hvad denne indskrænkende fortolkning af § 6 bygger på.

Som et andet eksempel kan nævnes, at en person i Danmark bistår et søskendepar, der ønsker at have seksuelt forhold til hinanden, med formaliteterne omkring emigration til et land, hvor blodskam ikke er strafbart. I denne situation vil der efter udvalgets opfattelse ikke kunne straffes i Danmark for medvirken.

Der er efter udvalgets opfattelse ikke noget umiddelbart behov for en yderligere lovregulering på dette område. Der foreligger endvidere ikke tilstrækkelig analyse af aktuelle situationer til at vurdere, om der inden for det strafferetlige område i almindelighed findes problemstillinger, der kan give anledning til at overveje en lovregulering.

Spørgsmålet om, hvorvidt forsøgs og medvirkenshandlinger er selvstændigt omfattet af § 6, har den praktiske betydning, at der ved dansk straffemyndighed baseret på § 6 ikke gælder de begrænsninger, der f.eks. følger af § 7 om, at forholdet også skal være strafbart i gerningslandet (det vil her sig det land, hvor forbrydelsen fuldbyrdes eller tænkes fuldbyrdet) og af § 10, stk. 2, hvorefter straffen skal holde sig inden for strafmaksimum i det pågældende andet lands lovgivning.

Fra retspraksis kan nævnes:

I en Østre landsrets dom af 5. oktober 1989 (Domme i kriminelle sager 198789, s. 4) erkendte den tiltalte forsøg på anstiftelse af narkotikakriminalitet vedrørende modtagelse af et parti heroin i Tyskland med henblik på videreoverdragelse i Tyskland og Holland. På grund af pasproblemer havde han formidlet alt fra Danmark (telefonisk formidlet kontakter, mødetider og mødesteder for de implicerede). Byretten anvendte straffelovens § 7, stk. 1, nr. 2, som grundlag for dansk straffemyndighed. Landsretten fandt, at tiltaltes handlinger var undergivet dansk straffemyndighed efter § 6, nr. 1.

I sagen UfR 1998.877 H havde de tiltalte her i landet fremstillet tre brevbomber og adresseret dem til personer i England. Forehavendet mislykkedes dog, dels fordi svensk politi udtog brevbomberne af den postkasse i Sverige, hvori de var blevet anbragt, dels fordi det anvendte sprængstof viste sig ikke at være virksomt. Under sagen var der spørgsmål om, hvorvidt der var straffemyndighed her i landet, når brevbomberne var blevet postet i Sverige, hvor forsøg med utjenligt objekt ikke er strafbart. Højesteret udtalte herom: "Fremstillingen af en brevbombe her i landet hører under dansk straffemyndighed, jfr. straffelovens § 6, nr. 1, uanset hvor modtageren befinder sig, og uanset hvor afgivelse til postbesørgelse sker." Landsrettens domfældelse for forsøg på bombesprængning efter straffelovens § 183, stk. 2, jfr. § 21, samt medvirken hertil blev stadfæstet.

I Nordisk Strafferetskomités betænkning Straffrättslig jurisdiktion i Norden (Nord 1992:17) er spørgsmålet om lokalisering af forsøgs og medvirkenshandlinger kort behandlet side 29 f. og 108 f. Se også Jørn Vestergaard i Kriminalistisk Instituts Årbog 1991 s. 109 ff og (samme artikel) i Juristen 1992 s. 162 ff.

Er handlingen ikke foretaget i Danmark, men har den virkning her i landet, kan den efter omstændighederne være undergivet dansk straffemyndighed. I de tilfælde, hvor en handlings strafbarhed afhænger af eller påvirkes af en indtrådt eller tilsigtet følge, betragtes handlingen således tillige som foretaget dér, hvor virkningen er indtrådt eller tilsigtet at skulle indtræde, jfr. straffelovens § 9 (*virkningsprincippet*).

Bestemmelsen giver bl.a. dansk straffemyndighed i tilfælde, hvor en person fra udlandet afsender et ærekrænkende brev til en person her i landet, eller hvor en person fra udlandet ved et skud over den danske landegrænse dræber en person her i landet. For så vidt angår forsøg og medvirken, indebærer bestemmelsen i § 9 sammenholdt med § 6, at der er dansk straffemyndighed i forhold til personer, der i udlandet begår forsøgs eller medvirkenshandlinger, såfremt den forbrydelse, som forsøgs eller medvirkenshandlingen angår, faktisk fuldbyrdes eller tilsigtes fuldbyrdet her i landet.

Det kan undertiden give anledning til tvivl, om dansk straffemyndighed følger umiddelbart af § 6, eller om den følger af § 6 sammenholdt med § 9. Spørgsmålet om den indbyrdes afgrænsning mellem handlingssted og virkningssted er imidlertid i denne situation uden selvstændig praktisk betydning.

I UfR 1999.513 Ø havde tiltalte fra udlandet begået insiderhandel ved køb af aktier, der blev effektueret gennem en bank i København. Selv om gerningsmanden befandt sig i udlandet, og købet var formidlet gennem en schweizisk investeringsrådgiver og bankforbindelse, blev forholdet anset for omfattet af straffelovens § 6, nr. 1, under hensyn til, at aktierne blev købt i den danske stat.

Har den kriminelle virksomhed - hverken for så vidt angår handling eller virkning - ingen tilknytning til dansk område, kan der i visse tilfælde være dansk straffemyndighed efter straffelovens § 7 (*personalprincippet*).

Efter straffelovens § 7 hører strafbare handlinger, der er begået i udlandet, under dansk straffemyndighed, såfremt gerningsmanden er dansk statsborger eller bosat her i landet. For så vidt angår handlinger, der er foretaget uden for folkeretligt anerkendt statsområde, kræves det efter § 7, stk. 1, nr. 1, at handlingen kan medføre højere straf end hæfte, mens det for så vidt angår handlinger, der er foretaget inden for sådant område, kræves, at handlingen er strafbar både efter gerningsstedets lov og efter dansk lov, jfr. § 7, stk. 1, nr. 2 (dobbelt strafbarhed).

Personalprincippet udstrækkes ved § 7, stk. 2, til personer, der alene opholder sig her i landet, når de samtidig har indfødsret eller bopæl i Finland, Island, Norge eller Sverige.

De ovennævnte bestemmelser suppleres af straffelovens § 8. Efter denne bestemmelse er der i en række nærmere opregnede tilfælde dansk straffemyndighed i forhold til udlandshandlinger uden hensyn til, hvor gerningsmanden hører hjemme. Det gælder bl.a. med hensyn til handlinger der krænker den danske stats selvstændighed, sikkerhed, forfatning m.v., jfr. § 8, nr. 1. Det gælder også i tilfælde, hvor "handlingen er omfattet af en mellemfolkelig overenskomst, ifølge hvilken Danmark er forpligtet til at foretage retsforfølgning", jfr. § 8, nr. 5.

Når der sker påtale her i landet af udlandshandlinger, skal pådømmelsen finde sted efter dansk lovgivning, jfr. straffelovens § 10. Det er derfor en forudsætning for, at der i anledning af udlandshandlinger kan gøres strafansvar gældende ved de danske domstole, at den pågældende danske straffebestemmelse ikke efter sit gerningsindhold er territorialt begrænset til dansk område. Må man konstatere, at den danske straffebestemmelse, der i givet fald skulle straffes efter, slet ikke er blevet overtrådt, når der er handlet i udlandet, er det selvsagt ikke relevant at overveje spørgsmålet om dansk straffemyndighed, jfr. f.eks. UfR 1998.1027 H.

I de tilfælde, hvor en udlandshandling er undergivet dansk straffemyndighed i medfør af straffelovens § 7, kan der ikke idømmes strengere straf end efter gerningsstedets lovgivning, jfr. straffelovens § 10, stk. 2. Denne begrænsning må formentlig også gælde i tilfælde, hvor grundlaget for dansk straffemyndighed er straffelovens § 8, nr. 6.

2.3.2. Særligt vedrørende salg og udbredelse af børnepornografi via Internettet

Som det fremgår af det ovenfor anførte, bygger udformningen af de gældende regler om dansk straffemyndighed i vidt omfang på, at verden er opdelt i stater med hver deres territorium, hvortil forbrydelser stedligt kan henføres.

Denne opfattelse kan komme under pres i relation til strafbare handlinger, der indbefatter et informationsrelateret gerningsindhold, når denne information spredes ved hjælp af det verdensomspændende Internet. Det kendetegner således al Internetkommunikation, at den involverer et stort antal netforbindelser, der ikke har noget centralt knudepunkt. Uanset om der er tale om afsendelse af en postmeddelelse eller spredning af information fra hjemmesider via "the World Wide Web", ved gerningsmanden derfor ikke - nødvendigvis - hvor den pågældende information modtages: En elektronisk postmeddelelse adresseres altid til en eller flere elektroniske postadresser, men selv om mange af disse postadresser er organiseret under nationale domænenavne (f.eks. ".dk domænet"), siger dette i sig selv intet om, hvor de vil blive læst. En dansk statsborger kan f.eks. uden vanskelighed have elektronisk postadresse under det svenske topdomænenavn, men desuagtet altid læse sin post i Danmark. Ligeledes kan en hjemmeside, som har WWW adresse under det danske topdomænenavn, læses fra hele verden, medmindre der er foretaget særlige tekniske blokeringsforanstaltninger.

Dette forhold, at kommunikation på nettet spredes til en ubekendt flerhed af modtagere, beskrives undertiden således, at Internet har skabt et "elektronisk cyberspace", der bryder med den klassiske geografiske virkelighedsopfattelse. I strafferetlig henseende indebærer dette, at der er skabt nye muligheder for at begå forbrydelser, der uden bistand fra andre personer indtræder på et andet sted end der, hvor gerningsmanden befinder sig. I relation til disse forbrydelser er det dernæst blevet vanskeligt at fastlægge virkningsstedet.

Også fastlæggelsen af selve handlingsstedet kan give anledning til vanskeligheder. At gerningsmanden "lægger information ud på Internet" kan således indebære begivenheder, der udspiller sig inden for flere forskellige jurisdiktioner: Informationen kan f.eks. være placeret under et dansk topdomænenavn, men ligge på en web server, der fysisk er placeret i Sverige, men som drives af en tysk Internetleverandør. Dernæst kan hjemmesiden i kraft af såkaldte links være stillet til rådighed for modtageren via andre hjemmesider og "portaler", til hvilke der tilsvarende kan høre forskellige medaktører med hver deres nationalitet. Ved vurderingen af, om et givet informationsdelikt er undergivet dansk straffemyndighed, kan det derfor - med udgangspunkt i den relevante gerningsbeskrivelse - blive nødvendigt at sondre mellem disse forskelligartede funktioner.

Der sker derudover i et vist omfang det, at information fra udlandet "spejles" på danske Internetudbyderes udstyr, dvs. at særligt populære homepages indlægges på Internetudbyderens server. Formålet med denne spejling er at optimere transmissionstiderne på Internettet, således at kunderne til disse homepages ikke belaster datatrafikken til udlandet.

I det følgende behandles disse jurisdiktionsspørgsmål med henblik på tilfælde, hvor handlingen består i salg eller udbredelse af børnepornografisk materiale via Internettet.

Et *salg* kan stedfæstes til flere forskellige lokaliteter. Som muligheder kan peges på det sted, hvor sælger opholder sig på salgstidspunktet, det sted, hvor køber opholder sig, det sted, hvor købsaftalen indgås, det sted, hvor betalingen sker, det sted, hvor varen befinder sig o.s.v.

Der kan således foreligge mange kombinationer, hvor salget kan have større eller mindre tilknytning til flere forskellige steder. Det er ikke i alle enkeltheder afklaret, hvilke former for tilknytning der kræves, for at et salg i jurisdiktionsmæssig henseende kan lokaliseres til et givet sted.

Som det fremgår af det ovenfor anførte, kan der ikke i straffelovens § 6, nr. 1, indlægges et krav om, at hele den kriminelle virksomhed skal være foretaget i den danske stat. Når blot en del af virksomheden er foretaget her i landet, kan forholdet være undergivet dansk straffemyndighed efter denne bestemmelse.

På den baggrund må et salg efter udvalgets opfattelse anses for foretaget i Danmark, hvis en eller flere af de væsentlige faktorer, der indgår i en salgssituation, har tilknytning til dansk område. Det typiske vil være, at sælgeren eller køberen, eventuelt begge, opholder sig i Danmark. Men et salg vil efter omstændighederne også kunne henføres til dansk område, selv om f.eks. køberen og sælgeren befinder sig i udlandet, jfr. UfR 1999.513 Ø om insiderhandel, der er omtalt ovenfor i afsnit 2.3.1.

Udbredelse af børnepornografisk materiale via Internettet må utvivlsomt lokaliseres til det sted, hvor gerningsmanden opholder sig på det tidspunkt, hvor den pågældende lægger materialet ind på en webserver, der er

forbundet med Internettet. En person, der i Danmark lægger børnepornografi ind på en webserver, vil således være undergivet dansk straffemyndighed efter straffelovens § 6, nr. 1, uanset om serveren befinder sig i udlandet, og uanset hvor i verden det pågældende materiale er tilgængeligt.

En sådan handling må imidlertid antages også at kunne lokaliseres til den server, som materialet lægges ind på, og hvorfra den videre udbredelse herefter sker. Lægger en person, der befinder sig i Tyskland, børnepornografi ind på sin hjemmeside, der betjenes via en server i Danmark, er stedet, hvor handlingen (d.v.s. udbredelsen) må anses for foretaget ikke blot Tyskland, men også Danmark. Forholdet er dermed undergivet dansk straffemyndighed i medfør af straffelovens § 6, nr. 1.

Er der ikke lagt særlige begrænsninger ind, er materialet i kraft af Internettets globale karakter tilgængeligt fra hele verden, og "virkningen" af handlingen kan således tænkes at indtræde i alle lande. Spørgsmålet er derfor, om handlingen i kraft af virkningsprincippet i § 9 tillige kan anses for foretaget i alle de lande, hvor materialet er tilgængeligt.

Rækkevidden af virkningsprincippet i § 9 i relation til overtrædelser via Internettet er bl.a. behandlet af Peter Blume, Helen Holdt, Ruth Nielsen og Thomas Riis i "IT-retlige emner" (Jurist og Økonomforbundets forlag 1998), s. 276:

- "Denne regel har stor betydning ved anvendelse af Internet. Mange handlinger foretaget på Internet kan have virkning i mange af de tilkoblede lande, idet Internet jo netop fungerer uafhængigt af territoriale grænser. Det kan sagtens tænkes, at det ikke var tilsigtet, at de pågældende handlinger skulle have virkning i Danmark, hvorved straffelovens § 9 kan få en uheldig konsekvens for Internetbrugere i andre lande."

Forfatterne synes herved - med en vis beklagelse - at nå frem til, at § 9 medfører, at virkningerne af aktiviteter på Internet ofte vil indtræde her i landet på en sådan måde, at danske domstole vil være kompetente til at behandle sager der udspringer heraf.

De eksempler fra praksis, der refereres i samme fremstilling, er i overvejende grad fra amerikansk ret og vedrører i det væsentlige civilretlige sager. På s. 280 f. resumeres en dom (Telco Communications Inc. v. An Apple A Day Inc.), der vedrører injurierende og ærekrænkende udtalelser. En virksomhed, der drives i én amerikansk delstat, distribuerer via Internet nogle krænkede pressemeddelelser vedrørende en konkurrent, der driver virksomhed i en anden delstat. Dommen fastslår, at distribution via Internet giver en domstol i denne anden delstat jurisdiktion, fordi pressemeddelelserne er tilgængelige i domstolsstaten, og de injurierende virkninger af pressemeddelelserne konkret fandtes at have gjort størst skade dér. Sagsøgte bestred, at domstolen havde jurisdiktion i den pågældende sag, idet sagsøgte ikke (i øvrigt) udførte forretninger i domstolsstaten.

For så vidt angår markedsføring anføres det i "Forbrugernes retsbeskyttelse i grænseoverskridende digitale net" (Erhvervsministeriet 1997), s. 68:

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

Se også Jan Trzaskowski, Forbrugerstyrelsen, i UfR 1998 B, s. 285. Det anføres her, at der ved vurderingen af, hvortil reklame på Internettet retter sig, bl.a. må lægges vægt på, om der er foretaget tekniske begrænsninger i materialets geografiske tilgængelighed, om en vare, der udbydes til salg via Internettet, kun sælges i visse nærmere angivne lande, hvilket sprog oplysningerne er affattet på og valg af Top Level Domain (TLD), f.eks. ".dk".

Den fastlæggelse af markedsføringslovens anvendelsesområde, der er behandlet i de to sidstnævnte fremstillinger, indebærer samtidig en fastlæggelse af dansk straffemyndighed efter straffelovens § 6, nr. 1, i forhold til denne type overtrædelser.

Efter udvalgets opfattelse kan det ikke antages, at straffelovens § 9 uden videre omfatter det forhold, at en person i udlandet placerer materiale på en Internethjemmeside, der er tilgængelig for Internetbrugere her i Danmark. At

dette materiale er tilgængeligt her i landet kan således kun siges at være en følge af udbredelsen, hvis tilgængeliggørelsen på den udenlandske hjemmeside specifikt tager sigte på at nå brugere i Danmark (f.eks. gennem særlige foranstaltninger, der specielt retter sig imod de danske Internetbrugere). I sidstnævnte situation vil straffelovens § 6, nr. 1, som udgangspunkt være anvendelig.

En generel anvendelse af § 9 i disse tilfælde ville i øvrigt føre til en uacceptabel vidtgående jurisdiktion. Danmark ville i så fald have jurisdiktion i forhold til alle informationer på Internettet, som er tilgængelige i Danmark, og som er strafbare efter dansk ret. Tænker man sig tilsvarende regler i andre lande, ville det betyde, at en person, der her i landet f.eks. indlægger voksenpornografisk materiale på Internettet, ville kunne straffes i lande, hvor sådant materiale er strafbart, selv om den pågældende i øvrigt er uden indflydelse på, om nogen i det pågældende land skaffer sig adgang til materialet. Tilsvarende ville gælde for oplysninger, der efter dansk ret er lovlige, men som efter lovgivningen i visse lande er strafbare, f.eks. som blasfemi.

En så vidtgående jurisdiktion ville betyde, at personer, der lægger materiale ind på Internettet, forinden måtte foretage nærmere retlige undersøgelser for at sikre sig, at materialet er lovligt efter lovgivningen i alle de lande, hvor det er tilgængeligt for andre brugere af Internettet. Hvis man ønsker et globalt Internet, giver det ikke mening at stille et sådant uopfyldeligt krav til brugerne.

Det kan også give anledning til tvivl, om en straffemyndighed i forhold til handlinger, der har så begrænset tilknytning til landet, i alle tilfælde vil være forenelig med folkeretten.

Sammenfattende må det således antages, at der er dansk straffemyndighed efter straffelovens § 6, nr. 1, i forhold til handlinger, der består i salg eller udbredelse af børnepornografi via Internettet, hvis salget eller udbredelsen har tilknytning til dansk område. Tilknytningen kan bestå i, at gerningsmanden har ophold i Danmark på handlingstidspunktet, eller i anvendelse af salgs eller udbredelsesmidler, der befinder sig eller målrettet tager sigte på dansk område. Det er derimod ikke tilstrækkeligt til at anse udbredelse af materiale for foretaget indenlands, at brugere her i landet kan hente materialet ned fra servere, der er placeret i udlandet.

Straffelovens § 235 er efter sit gerningsindhold ikke begrænset til salg, udbredelse m.v., der kan lokaliseres til Danmark. Kan salg og udbredelse af børnepornografi efter det ovenfor anførte ikke anses for foretaget her i landet, kan der således være dansk straffemyndighed efter § 7, hvis betingelserne i denne bestemmelse er opfyldt. En dansk statsborger, der under ophold i Tyskland via Internettet udbreder børnepornografi via en server i Frankrig, vil således kunne straffes herfor i Danmark, hvis forholdet tillige er strafbart efter tysk eller fransk ret, d.v.s. efter lovgivningen i de lande, hvor handlingen (udbredelsen) må anses for foretaget.

Det er udvalgets umiddelbare opfattelse, at den retstilstand, som de gældende jurisdiktionsbestemmelser må antages at indebære i forhold til salg og udbredelse af børnepornografi, er tilfredsstillende. Udvalget finder derfor ikke på det foreliggende grundlag behov for lovændringer på området./P

Da retspraksis af betydning for de her behandlede spørgsmål imidlertid indtil nu har været sparsom, og da udviklingen hele tiden åbner nye tekniske muligheder, som stiller lovgivningen og retsanvendelsen over for nye udfordringer, kan det ikke udelukkes, at der i fremtiden kan forekomme tilfælde, der vil afsløre mangler ved de gældende jurisdiktionsregler. Der kan derfor være grund til løbende at følge udviklingen nøje for at sikre, at straffelovens regler om straffemyndighed til stadighed er tidssvarende i forhold til den teknologiske udvikling.

2.4. Informationsspredning

2.4.1. Generelt om kriminalisering af spredning

Lovgivningen regulerer i forskellige henseender (f.eks. i forbindelse med piratkopiering og dekodningsudstyr) spredning af information, som gerningsmanden ikke har rettigheder over, eller hvis indhold i sig selv er strafbart. Der stilles normalt krav om, at denne spredning er erhvervsmæssig, hvis den skal være omfattet af straffebestemmelser med højere strafferamme. For så vidt angår lov om radio og fjernsynsvirksomhed er kun erhvervsmæssig spredning af dekodningsudstyr strafbart.

På baggrund af Internetudviklingen har udvalget drøftet hensigtsmæssigheden 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 teleinformationsteknologi 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 forholdsvis intens regulering af såvel frekvenstildelingen som det informationsmæssige indhold i offentlig radio og tvtransmission, har disse teknologier ikke givet anledning til strafferetlige problemstillinger i samme omfang, som det er tilfældet i forbindelse med brugen af Internettet. Ved fremkomsten af de såkaldte bulletinboards (dvs. informationssystemer, typisk baseret på en PC, der ved hjælp af telenettet gav mulighed for opkald 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 telefonopkald, der har været til rådighed i den enkelte telefonforbindelse.

Den udbredte anvendelse af WWW har imidlertid givet denne problemstilling en langt større dimension, eftersom WWWteknologien (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 problem om spredningens omfang indebærer WWWteknologien vanskeligheder med hensyn til at identificere den gerningsmand, der spreder den pågældende information, og herunder også det land, som den efterforskende myndighed i givet fald skal samarbejde med med henblik på at opnå de fornødne tilladelser til straffeprocessuelle tvangsindgreb.

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 spredning 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 edbprogrammer, børnepornografi m.v.

Udvalget finder på denne baggrund, at den traditionelle begrænsning til erhvervsmæssig spredning i dag kan være en utilstrækkelig strafferetlig beskyttelse, 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(15). 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 udtalelser m.v.

---

15. Dette er i overensstemmelse med, hvad arbejdsgruppen vedrørende datakriminalitet har foreslået.

2.4.2. Særlige eksempler på spredning

Spørgsmålet om spredning af børnepornografisk materiale behandles særskilt i afsnit 4.

De eksempler, der nævnes i det følgende, giver ikke anledning til forslag om ændring af de strafferetlige regler(16). De giver derimod anledning til overvejelser omkring, hvorvidt der kan være anledning til at forbedre mulighederne for at efterforske kriminalitet, der begås under anvendelse af store netsystemer. Der henvises til afsnit 5 og 6 vedrørende disse overvejelser.

---

16. Som eksempel på spredning kan også nævnes antisemitisk materiale. Ifølge en rapport af 4/3 1998 fra The InterParliamentary Council Against Antisemitism er der mere end 600 websites med denne type materiale, og tallet

er voksende. Rådet opfordrer både til en effektiv strafferetlig beskyttelse, og til at Internetudbydere for så vidt angår krænkende, men ikke strafbart materiale, i videst mulig omfang ikke giver adgang til det.

2.4.2.1. Kursmanipulation og insiderviden

Ved børsreform I i 1986, insiderloven i 1991 og børsreform II i 1995 blev der henholdsvis indført meget omfattende generelle insiderregler og et generelt forbud mod kursmanipulation. Reglerne har en almindelig maksimumstraf på fængsel i 1 år og 6 måneder, men straffen kan stige til fængsel i 4 år ved forsætlig og særlig grov overtrædelse eller ved et større antal forsætlige overtrædelser. Der er tale om et område, der er blevet markant ny og opkriminaliseret i de senere år.

Sideløbende hermed er Internettet blevet et forum for udveksling af investeringsoplysninger. Brugerne kan på forskellige websites indlægge oplysninger om selskaber, investeringserfaringer m.v. - og de kan gøre det anonymt. Vil de være helt sikre på, at de ikke kan lokaliseres via registreringer af brugen i deres egen eller Internetudbyderes log over brugen, kan de enten bruge en PC, der er almindelig adgang til, eller de kan gå via dækadresser, hvor det oftest reelt vil være umuligt at finde frem til brugeren.

Kan man finde frem til den, der har videregivet insideroplysninger ved at lægge dem på Internettet, vil han kunne straffes efter værdipapirhandelloven. Tilsvarende gælder for brugere, der handler på baggrund af sådanne oplysninger - hvis man er i stand til at bevise, at de ikke betragtede oplysningerne som almindelig kendte. Det vil være nærliggende at betragte oplysningerne som offentliggjorte, når de er spredt ud på Internettet, selv om den korrekte fremgangsmåde via Fondsbørsen ikke er fulgt, ligesom en del brugere formentlig vil gå ud fra, at oplysningerne allerede er offentliggjort på korrekt vis.

De samme problemer opstår ved kursmanipulation, hvor især overtrædelse af værdipapirhandellovens § 34, stk. 3, nr. 1, jfr. § 39, om offentliggørelse eller udspredelse af urigtige oplysninger om en værdipapirudsteder, der er egnet til at påvirke kursen, kan tænkes at foregå via Internettets kommunikationsmuligheder. Tilsvarende gælder for straffelovens § 296, stk. 1, nr. 1, om udspredelse af løgnagtige meddelelser, hvorved prisen på varer, værdipapirer eller lignende genstande kan påvirkes.

I en sag fra foråret 1997 var der på en investeringswebside i Danmark indlagt en urigtig oplysning om, at en aktieanalyse var på vej, der ville anbefale aktiekøb i et selskab op til kurs 90, hvor kursen aktuelt lå på 75. Bl.a. på grund af manglende opbevaring af al relevant logning har det indtil nu ikke været muligt at identificere gerningsmanden.

I en sag fra USA gav gerningsmanden urigtige oplysninger om en mulig takeover på en tilsvarende website og rådede til aktiekøb, mens han selv solgte sine aktier i stedet.

Det må formodes, at straffebestemmelsen i værdipapirhandellovens § 94, der både dækker insiderhandel og kursmanipulation, giver mulighed for at henføre en spredning via Internettet til den kvalificerede bestemmelse om forsætlig, grov overtrædelse, der har et strafmaksimum på 4 år. Der er således en tilstrækkelig strafferetlig dækning også i relation til formidling af sådan information via Internettet.

Set i relation til netsystemerne er det efterforskningsmæssige et væsentligt problem i disse sagstyper, herunder især spørgsmålet om, hvorvidt den relevante logning fortsat eksisterer på efterforskningstidspunktet. For så vidt angår Internetudbyderes logning behandles dette spørgsmål i afsnit 5.1. Endvidere vil der i nogle sager kunne være behov for indgreb i meddelelseshemmeligheden, jfr. afsnit 6.5.

2.4.2.2. Markedsføring på eller via Internettet

Den almindelige markedsføring på Internettet - med de tilknyttede problemstillinger omkring muligheden for at kontrollere, at reglerne om moms og skat overholdes - behandles ikke i denne sammenhæng. Ved siden af den lovlige markedsføring af produkter og ydelser åbner Internettet imidlertid for nye muligheder i forbindelse med kriminalitet, der for at kunne begås kræver markedsføring.

Ud over de muligheder, der ligger i markedsføring direkte på nettet, er der også åbnet for en omfattende markedsføring via Internettet. I modsætning til traditionel direkte markedsføring, der er forbundet med betydelige portoudgifter, er det minimale omkostninger, der er forbundet med at emaile. Såkaldt junk mail eller spamming (uopfordrede email tilbud) er derfor blevet et tiltagende problem.

Ifølge EuropaParlamentet og Rådets direktiv af 20/5 1997 om forbrugerbeskyttelse i forbindelse med aftaler vedrørende fjernsalg[(17)] skal medlemslandene fastsætte regler om begrænsninger i anvendelsen af visse fjernkommunikationsteknikker. Der kræves forudgående forbrugersamtykke ved anvendelse af et automatisk opkaldssystem uden menneskelig medvirken (opkaldsautomat) og af telefax. For andre fjernkommunikationsteknikker, som tillader en individuel kommunikation, skal medlemsstaterne sørge for, at de kun kan anvendes, hvis forbrugeren ikke klart modsætter sig det. Efter direktivets artikel 3 og bilag II finder direktivet ikke anvendelse på visse finansielle tjenesteydelser, herunder investeringsservice og tjenester vedrørende termins og optionsforretninger.

Med hensyn til de ydelser, der er omfattet af investeringsservicedirektivet (ISD)[(18)], har Kommissionen afgivet en erklæring om, at den anerkender forbrugerbeskyttelsens betydning i forbindelse med aftaler om finansielle tjenesteydelser og vil undersøge, hvorledes forbrugerbeskyttelse kan integreres i politikken vedrørende finansielle tjenesteydelser. ISD artikel 13 indeholder følgende bestemmelse:

- "Bestemmelserne i dette direktiv er ikke til hinder for, at investeringsselskaber, der har fået meddelt tilladelse i en anden medlemsstat, kan gøre reklame for deres tjenesteydelser med alle de kommunikationsmidler, som står til rådighed i værtslandet, dersom de overholder de regler for den pågældende reklames form og indhold, der er begrundet i hensynet til samfundsmæssige interesser."

---

17. 97/7/EF - fjernsalgsdirektivet.
18. Direktiv 93/22/EØF

De eksempler af strafferetlig relevans, der ses anvendt, har både form af markedsføring på Internettet og af junk mail.

Pyramidestrukturer (der bl.a. kendes fra de traditionelle indsamlingssager, hvor hver ny deltager skal få flere nye til at betale, mod at alle på et tidspunkt selv er modtagere) er et eksempel. Gerningsmand og gerningsland kan være svære at identificere, for Internetadressen kan være en dækadresse (eller sendt via en anonym remailer) og navnet forkert, selv om der kunne lokaliseres en adresse eller konto. Med hensyn til omfanget af udbydere bemærkes, at Forbrugerombudsmanden i oktober 1997 holdt "International Internet Sweep Day" (en søgning på Internettet efter aktuelle tilbud) sammen med 29 lande efter pyramidearrangementer, Multilevelmarketing og Networkmarketingkoncepter[(19)]. Det resulterede for Danmarks vedkommende i, at Forbrugerombudsmanden skrev til 74 udbydere af betænkelige markedsføringskoncepter. Nogle af de mest graverende af disse sager er efterfølgende sendt til Rigsadvokaten[(20)]. I september 1998 holdt over 30 lande en ny "International Internet Sweep Day". Danmark koncentrerede sig især om de såkaldte "getrichquick"sider. Der blev fundet tegn på pyramidespil eller vildledende markedsføring på 32 Internetsider, heraf 12 danske. Forbrugerombudsmanden har som tidligere i første omgang skrevet til de pågældende.

Advanced fee fraud er et andet eksempel. Forholdet består her i, at der tilbydes varer eller lån eller credit cards uden bankkontakt og sikkerhedsstillelse (eventuelt i kombination med en pyramidestruktur) mod forudbetaling af et relativt beskedent beløb, hvorefter der typisk lukkes ned, når der er modtaget tilstrækkeligt med penge, og helst før politiet underrettes og iværksætter efterforskning.

---

19. Sweep Day er omtalt på s. 17 i Forbrugerstyrelsens årsberetning for 1997. Det nævnes også, at sagerne blev indberettet til Erhvervsministeriet og Justitsministeriet, og at Forbrugerombudsmanden påpegede, at han fandt lovgivningen på området utilstrækkelig, både med hensyn til politiets efterforskningsmuligheder og med hensyn til at forbyde pyramidespil og pyramidearrangementer.
20. Rigsadvokaten har i fortsættelse heraf bedt Statsadvokaten for særlig økonomisk kriminalitet om at være ansvarlig for at koordinere efterforskningen i sager om pyramidespil m.v.

Også ved *investeringsbedragerier* - et område der i forvejen har tiltagende international karakter - anvendes Internettet. Det kan nævnes i den forbindelse, at de såkaldte "sidegadevekselerer", hvis virksomhed nu er omfattet af regler om tilladelse og tilsyn i EUlandene, uhindret kan fortsætte deres virksomhed fra et land, der ikke har tilsvarende reguleringer, og markedsføre via Internettet. Der kendes allerede eksempler herpå.

Spørgsmålet er, om den meget omfattende udbredelsesform via Internettet kvalificerer de handlinger, der allerede er strafbelagt.

Ofte vil der være tale om forhold, der er omfattet af straffelovens § 279 om bedrageri. Denne bestemmelse har en kvalificeret straffebestemmelse i straffelovens § 286, hvorefter den sædvanlige maksimumstraf på fængsel i 1 år og 6 måneder kan stige til 8 år, når forbrydelsen er af særlig grov beskaffenhed, eller når et større antal forbrydelser er begået. Udvalget er ikke bekendt med domme, hvor markedsføring via Internettet er indgået i tiltalen, men forsøg på via Internettet at nå en stor kreds af potentielle ofre enten ved generelt udbud eller ved at maile til potentielle kunder kan indgå i domstolenes vurdering af forholdenes grovhed.

Det bemærkes, at den til bedrageri krævede vildfarelse kan stamme fra indholdet af annoncering (bedrageri mod almenheden).

Desuden vil der kunne straffes for overtrædelse af markedsføringsloven, hvis markedsføringen sker til eller fra Danmark[(21)]. Muligheden for at læse indholdet i Danmark er næppe nok til, at loven kan anvendes, hvis indholdet ikke er målrettet mod Danmark.

Hvis man vil udtrykke, at markedsføring via Internettet bør være et særligt kvalificerende moment, kan man overveje at ændre straffelovens § 286, stk. 2, således, at der efter "når et større antal forbrydelser er begået" indsættes "eller er forsøgt begået" med tilhørende bemærkninger om, at der især er tænkt på markedsføring via Internettet eller tilsvarende brede forsøg.

Udvalget har overvejet dette spørgsmål, men ud fra den betragtning, at det må antages allerede at være gældende ret, og at en præcisering måske vil kunne medføre uheldige modsætningsslutninger på andre områder, har udvalget valgt ikke at foreslå ændringer.

Set i relation til netsystemerne kan der også i disse sagstyper være særlige efterforskningsmæssige problemer, herunder især spørgsmålet om, hvorvidt den relevante logning fortsat eksisterer på efterforskningstidspunktet. For så vidt angår Internetudbyderes logning behandles dette spørgsmål i afsnit 5.1. Endvidere vil der i nogle sager kunne være behov for indgreb i meddelelseshemmeligheden, jfr. afsnit 6.5.

---

21. Jfr. afsnit 2.3 om straffemyndighed.

Justitsministeriet Version 1.0 den 8. september 1999
Denne publikation findes på adressen: http://jm.schultzboghandel.dk

---

KAPITEL 3 - ANSVAR FOR INDHOLDET AF INFORMATIONSSYSTEMER

Et spørgsmål, der har været aktuelt siden de tidlige BBS'er(22) startede med opskrifter på bomber og narkotika, oplysninger om passwords og calling cards m.v., er, om den, der administrerer BBS'et(23) - eller den aktuelle homepage på Internettet - kan gøres ansvarlig for indholdet. Det må i den forbindelse bemærkes, at som ved de ovennævnte investeringshomepages er situationen ofte den, at andre også uploader, og at indehaveren derfor ikke nødvendigvis ved, hvad han har liggende.

Har den pågældende selv indlagt strafbar information, kan der dømmes derfor, uanset om handlingen er knyttet til et netsystem eller ej. F.eks. dømtes en mand ved Københavns byrets dom af 15/6 1998 og Østre landsrets ankedom af 22/3 1999 for overtrædelse af straffelovens § 266 b for spredning af racistiske ytringer, idet han havde indlagt adskillige racistiske udtalelser på en website for en nyhedsgruppe.

Den svenske højesteret har i en dom af 22/2 1996(24) antaget (efter domfældelse i byretten og frifindelse i landsretten), at sysop'en ikke kunne gøres ansvarlig, når hans eneste aktivitet bestod i, at ophavsretligt beskyttede programmer kunne downloades fra hans BBS. Tiltalen lød på, at sysop'en havde gjort programmerne tilgængelige for almenheden. Højesteret anførte, at der var en åbenbar mangel i den ophavsretlige beskyttelse af programmer(25).

Igen ligger problemstillingen i udbredelsen. Man kan også gå på biblioteket og finde opskrifter på mange ting, så forskelligheden beror for noget af indholdets vedkommende mere på, at man typisk her udbreder til en større kreds, der har let adgang til materialet fra deres PC, og som måske føler sig fristet til at afprøve opskrifterne(26)

Formidling af opskriften på eller oplysningen om noget, der kan benyttes til at begå noget strafbart, er ikke efter den almindelige fortolkning af forsøgs og medvirkensbestemmelserne i straffelovens § 21 og § 23 generelt omfattet af disse bestemmelser. Hvis selve indholdet er strafbart (f.eks. børnepornografi eller salg af tyvekoster), vil sysop'en eller indehaveren af homepagen antagelig kunne dømmes for medvirken ved passivitet, hvis hans kendskab (evt. burde viden) til indholdet kan bevises. Hans ejerskab vil formentlig betyde, at han har en handlepligt, dvs. at han skal slette indhold, der realiserer gerningsindholdet i en straffebestemmelse.(27)

---

22. Bulletin Board Systems eller elektroniske opslagstavler.

23. Kaldet sysop'en (systemoperatøren).

24. "BBSmålet", NJA 1996 s. 79.

25. Ifølge Thomas CarlénWendels, Nätjuridik - Lag och rätt på Internet, Juristförlaget 1997, s. 52, er dommens resultat omdiskuteret i Sverige.

26. Ikke mindst tilvirkning af bomber er meget udførligt beskrevet i "The Terrorist's Handbook", der i hvert fald siden 1993 har cirkuleret på BBS'er m.v. I forbindelse med en hærværkssag om sprængning af hjemmelavede bomber oplyste én af de afhørte, at han havde fremstillet og sprængt bomber, og at han havde opskriften fra den nævnte håndbog, der lå på en PC på en dansk erhvervsskole.

27. Der kan i den forbindelse henvises til UfR 1996.209 H, hvor udgiveren af et annoncehæfte (der ikke var omfattet af medieansvarsloven) blev idømt en bøde for overtrædelse af markedsføringsloven ved medvirken til en annoncørs reklamering med ulovlig tilgift. Det siges ved Højesterets vurdering af, om den pågældende havde

udvist uagtsomhed: "Højesteret finder det herved afgørende, om tiltalte ved et umiddelbart gennemsyn af annoncerne - et gennemsyn, som det naturligt må påhvile en udgiver af et annoncehæfte at foretage som en rutine - burde have indset, at der i de pågældende annoncer utvivlsomt reklameredes med ulovlig tilgift."

Formidling af opskrifter og hjælpemidler kan under særlige omstændigheder være strafbar, jfr. Roskilde rets dom af 19/12 1996, hvor der dømtes for forsøg på medvirken til hacking i et tilfælde, hvor der var en udtrykkelig opfordring til en mindre, kendt kreds til at prøve (og til ikke at ændre) passwords, der var lagt på BBS'et.

Derudover kan man overveje, om de stort set aldrig brugte bestemmelser i straffelovens § 136 og § 266 a kan udstrækkes til at omfatte dele af indholdet.

Efter straffelovens § 136, stk. 1, straffes den, som uden derved at have forskyldt højere straf offentlig tilskynder til forbrydelse, med op til 4 års fængsel. Det antages, at § 136, stk. 1, er uanvendelig ved mindre alvorlige lovovertrædelser. Efter straffelovens § 266 a straffes den, der, uden at forholdet omfattes af §§ 136 og 266, offentligt fremsætter udtalelser, der tilstræber at fremkalde voldshandlinger eller hærværk, med op til 1 års fængsel. Straffelovens § 136 er brugt i UfR 1938.407 Ø, hvor en redaktør blev dømt for i en artikel om et bombeattentat mod forsvarsministerens villa delvis indirekte at have opfordret til at anvende kraftigere bomber over for ministre. Straffelovens § 266 a er brugt i Odense rets dom af 1/7 1986, hvor en politiker blev dømt for i en valgudsendelse i tv at have fremsat udtalelser, der tilstræbte ødelæggelse af karlitlofter i skoler og institutioner.

Udvalget er ikke bekendt med andre domme om overtrædelse af disse bestemmelser. Bestemmelserne er klart forudsat at kunne anvendes, hvor betingelserne for at dømme for forsøg på medvirken ikke er opfyldt, men de indeholder begge et tilskyndelses/tilstræbningsmoment, der nok skal være mere målrettet end det typiske indhold på et BBS eller en homepage. Derimod vil offentlighedskravet formentlig være opfyldt i langt de fleste tilfælde, hvor der distribueres via BBS eller Internettet.

Selv om der i nogle tilfælde således vil kunne dømmes for medvirken til et strafbart indhold ved passivitet og i særlige tilfælde for forsøg på medvirken til den forbrydelse, indholdet (password, calling card o.l.) kan bruges til, og selv om det kunne være af interesse ved et særligt opfordrende indhold at afprøve en eventuel anvendelse af straffelovens § 136 og § 266 a, er der for en del af indholdet af opskrifter eller passwords o.l. næppe nogen anvendelig straffebestemmelse.

Det skal dog anføres, at indehaveren - såfremt han har (eventuelt burde have) kendskab til indholdet - vil blive dækket af de af udvalgets forslag, der regulerer spredning til en større kreds, i det omfang der er tale om et kriminaliseret indhold.

Man kunne overveje at opstille et krav om, at informationssystemer såsom BBS'er og homepages skal underkastes et anmeldelseskrav. I tilknytning til en sådan ordning kunne man f.eks. stille betingelse om kontrolforanstaltninger mod informationer af retsstridigt eller anstødeligt indhold. Regler af et sådant indhold kan dog tænkes at komme i strid med de principper, der er udtrykt ved reglerne om den formelle ytringsfrihed i grundlovens § 77 og i Den Europæiske Menneskerettighedskonventions artikel 10. Hertil kommer, at en regulering, der i realiteten kun er anvendelig ved nationale BBS'er - selv om den tillige krævede, at sysop'en havde pligt til at være bekendt med indholdet - næppe vil få den fornødne gennemslagskraft, når Internettets internationale struktur tages i betragtning. Endvidere er det praktisk umuligt for en sysop løbende at gøre sig bekendt med alt det materiale, som der kan skaffes adgang til over sådanne. Endelig er det vanskeligt at afgrænse BBS'er og homepages og gennemføre kontrolforanstaltninger, når et stort antal private og juridiske personer etablerer sådanne.

Sverige har i 1998 vedtaget en lov [(28)] om ansvar for elektroniske opslagstavler. Lovens § 1 definerer en elektronisk opslagstavle som en tjeneste til elektronisk formidling af meddelelser, hvor der ved meddelelser forstås tekst, billede, lyd eller information i øvrigt. Efter lovens § 2 gælder loven ikke for almindelig kommunikation, interne formidlinger, tjenester, der er beskyttet af trykkefrihedsforordningen eller ytringsfrihedsgrundloven, eller email. Efter lovens § 3 skal indehaveren af en elektronisk opslagstavle underrette den, der tilslutter sig, om sin identitet og om, i hvilken udstrækning indkomne meddelelser bliver tilgængelige for andre brugere. Efter lovens § 4 skal den, der administrerer (tillhandahåller) en elektronisk opslagstavle, for at kunne opfylde sin pligt efter § 5, have et sådant overblik over tjenesten, som med rimelighed kan kræves under hensyntagen til virksomhedens omfang og indretning.

Lovens § 5 indeholder den centrale pligt: Den, der administrerer den elektroniske opslagstavle, skal fjerne eller forhindre videre spredning af en indlagt meddelelse, hvis indholdet åbenbart er af en art som anført i angivne §'er i den svenske straffelov: Agitation, ophidselse mod folkegrupper, børnepornografi og ulovlig voldsskildring, eller hvis det er åbenbart, at der er tale om en ophavsretskrænkelse.

Efter lovens § 6 straffes overtrædelse af § 3 med bøde. Efter lovens § 7 straffes overtrædelse af § 5 - medmindre forholdet er omfattet af straffeloven eller ophavsretsloven - med bøde eller fængsel i højst 6 måneder, der i grove tilfælde kan stige til fængsel i højst 2 år, mens straffen i mindre sager kan bortfalde. Efter lovens § 8 kan udstyr, der er anvendt ved overtrædelser af § 7, konfiskeres for at forebygge yderligere kriminalitet, eller hvis der i øvrigt foreligger særlige grunde.

Den danske medieansvarslov indeholder en mulighed for, at massemedier i form af tekster, billeder og lydprogrammer, der periodisk udbredes til offentligheden, efter anmeldelse til Pressenævnet kan blive omfattet af loven, hvis de har karakter af nyhedsformidling[(29)]). Det nævnes i lovforslagets bemærkninger[(30)], at det kun er ved envejskommunikation, hvor modtageren ikke kan påvirke produktet, at der er mulighed for at begrænse ansvarsplaceringen til bestemte personer.

---

28. Lag (1998:112) om ansvar för elektroniska anslagstavlor. Loven bygger på forslaget i betænkning SOU 1996:40 om elektronisk dokumenthantering fra IT-utredningen, der i let ændret form blev fremsat som regeringens proposition 1997/98:15 af 2/10 1997.
29. Jfr. § 1, nr. 3, og § 8 i medieansvarsloven, lov nr. 348 af 6/6 1991 med senere ændringer.
30. FT 1990/91 A 3047

Det fremgår i øvrigt af lovforslaget, at medieansvarudvalgets flertal havde foreslået, at der indførtes en bestemmelse om objektivt bødeansvar for selve medieforetagendet ved visse grove freds og ærekrænkelser. Mindretallet fandt derimod bl.a., at der var grund til at frygte, at en ændret ansvarsordning ville påvirke den redaktionelle frihed. Justitsministeriet tilsluttede sig mindretallet bl.a. under henvisning til, at det ville indebære en latent risiko for en langt videregående afsmittende virkning for informationsfriheden her i landet.

Medieudvalget har senere behandlet Internetspørgsmålet i en betænkning fra 1996[(31)]. Det siges[(32)] om indholdet af Internet indledningsvis, at "der er tale om et område, hvor hovedparten af udviklingen hverken kan styres eller reguleres". Det anføres, at man kan diskutere, om der er behov for ansvarsregler for indholdet af Internet i lighed med medieansvarslovens regler, og at en sådan ansvarsregulering i givet fald burde fokusere på den personkreds, der i relation til massemedierne betragtes som "den ansvarshavende redaktør".

Medieudvalget anbefaler[(33)], at Internetudgivelser, som kan sammenlignes med traditionelle massemedier, gennem anmeldelse til Pressenævnet lader sig omfatte af medieansvarsloven. Udvalget finder derimod ikke, at der er grund til at ændre på den gældende retstilstand med hensyn til indholdsmæssig regulering af Internet. Udvalget henviser dels til, at dette ville have censurlignende karakter, og dels til de administrationsmæssige vanskeligheder.

---

31. Betænkning nr. 1320/1996 om medierne i demokratiet.
32. Betænkningen s. 432 ff.
33. Betænkningen s. 438 f.

Udvalget har drøftet behovet og mulighederne for regulering af ansvaret for indholdet af informationssystemer. I det omfang udbredelsen i en videre kreds (f.eks. via Internettet) sidestilles med erhvervsmæssig udbredelse i straffebestemmelser herom - jfr. afsnit 2.4.1 - vil dette dække en del af reguleringsbehovet. Disse lovændringer får imidlertid ikke betydning for udbredelse af oplysninger, hvor udbredelsen ikke i dag er strafbar. Det gælder f.eks. opskrifter på bomber og syntetisk narkotika. Og lovændringerne indebærer ikke i sig selv nogen pligt for administrator til at undersøge, hvad der er lagret af information.

Udvalget finder imidlertid, at den i afsnit 2.4.1 beskrevne regulering (jfr. herved som eksempel afsnit 4.4.2 om

børnepornografi) dækker den væsentligste del af det område, hvor en regulering kan komme på tale. Uanset at det i særlige sammenhænge kan være ønskeligt, finder udvalget ikke anledning til at foreslå lovændringer vedrørende udbredelse af oplysninger om kemiske processer eller andre oplysninger, som det i dag ikke er ulovligt at udbrede, selv om de vil kunne have skadelig virkning i kraft af modtagerens anvendelse af oplysningerne. Det vil bl.a. være vanskeligt at afgrænse, under hvilke omstændigheder udbredelse af oplysningerne burde være lovlig, f.eks. i forskningsmæssige sammenhænge.

Med hensyn til at etablere en registreringsordning og en særlig undersøgelsespligt med hensyn til, hvad der uploades, finder udvalget, at man med den nuværende IT-struktur næppe kan opnå det ønskede formål i et bare rimeligt omfang med en sådan regulering. Det ville formentlig kun betyde, at man distribuerede uden for dansk jurisdiktion ved at up og downloade fra en fremmed homepage. En sådan regulering ville endvidere være i klar strid med de principper, der traditionelt har ligget til grund for reglerne om, at post og telefonvæsen ikke er ansvarlige for indholdet af de meddelelser, der formidles via disse systemer, og at indholdet af det formidlede ikke overvåges.

Sammenfattende finder udvalget, at reguleringen bør begrænses til det i afsnit 2.4.1 skitserede, der - hvis den nødvendige tilregnelse i form af forsæt eller uagtsomhed kan bevises - regulerer den væsentligste del af området[(34)] [(35)].

---

34. Spørgsmålet om ansvar for Internetudbydere behandles i et direktivforslag af 23/12 1998 (KOM(1998) 586 endelig udg. (EFT 1999 C 30/4)) om visse retlige aspekter af elektronisk handel i det indre marked. Efter artiklerne 1214 i dette forslag skal alle typer af Internetudbydere, jfr. afsnit 2.1, som hovedregel være anvarsfri i relation til transmissioner, de ikke har indflydelse på. For så vidt angår hosts er det dog en forudsætning, at hosten ikke har viden om ulovlig aktivitet uden at reagere derpå. Det foreslås i artikel 15, at medlemsstaterne ikke generelt må forpligte Internetudbyderne til at overvåge den information, de formidler

35. Arbejdsgruppen vedrørede datakriminalitet fandt ligeledes, at der ikke var behov for en mere vidtgående regulering.

Justitsministeriet Version 1.0 den 8. september 1999
Denne publikation findes på adressen: http://jm.schultzboghandel.dk

---

KAPITEL 4 - STRAFFELOVENS 235 OM BØRNEPORNOGRAFI

4.1. Bestemmelsens forhistorie

Frem til 1969, hvor straffen for billedpornografi blev ophævet[(36)], var børnepornografi strafbar på lige fod med anden billedpornografi. Ved ophævelsen af pornografibestemmelsen i straffelovens § 234, der bl.a. vedrørte offentliggørelse eller udbredelse af utugtige billeder, forsvandt ligeledes hjemlen til at straffe offentliggørelse og udbredelse af børnepornografiske billeder.

Derimod har produktionen af børnepornografiske billeder m.m. til stadighed været kriminaliseret. Der vil i disse tilfælde altid ske overtrædelse af en eller flere bestemmelser i straffelovens kapitel 24, i det mindste af straffelovens § 232 om blufærdighedskrænkelse, herunder for medvirken. Såfremt eksisterende optagelser, der ikke selvstændigt opfylder kravene, sammenkædes på en måde, så helhedsresultatet bliver pornografisk, vil straffelovens § 264 d kunne anvendes.

I 1980[(37)] indsattes en bestemmelse, der indholdsmæssigt svarede til den nugældende § 235, stk. 1, men kun gav mulighed for bødestraf. Begrundelsen for bestemmelsen[(38)] var, at det i praksis var vanskeligt at gennemføre en straffesag for optagelsen, hvis billederne var optaget i udlandet. En del af de hørte myndigheder m.m. vendte sig direkte mod en kriminalisering af denne art. Der pegedes blandt andet på de fra de tidligere bestemmelser velkendte afgrænsningsproblemer. Der var også uenighed om strafferammen[(39)]. Flere statsadvokater udtalte sig til fordel for en bødebestemmelse; rigsadvokaten, statsadvokaten i København og politidirektøren gik ind for et strafmaksimum på 6 måneders fængsel. Straffelovrådet pegede på, at en viden om pornografiske billeders kriminalitetshæmmende virkning må medinddrages i overvejelserne om en nykriminalisering kunne begrundes.

---

36. Ved lov nr. 224 af 4/6 1969.

37. Ved lov nr. 252 af 16/6 1980.

38. Jfr. lovforslaget, FT 1979/80, 2. samling, A 1761.

39. Det lovudkast, der var udsendt til høring, lød således: "§ 235. Den, som offentliggør, sælger eller på anden måde udbreder eller i sådan hensigt fremstiller eller skaffer sig utugtige billeder af børn, straffes med bøde (hæfte eller fængsel indtil 6 måneder)."

Straffelovrådet indhentede en redegørelse fra Berl Kutchinsky. Hans konklusion på en indgående analyse var:

- "Det må siges ganske utvetydigt, at vi ikke med sikkerhed kan fastslå, at der er en præcis og direkte årsagssammenhæng mellem pornografi og seksuelle overgreb mod børn. ¿ Men der findes et stort antal indicier på, at en sådan sammenhæng [mellem udbudet af børnepornografi og et fald i antallet af sædelighedsforbrydelser mod børn] eksisterer."

Han skønnede, at man måske forhindrede ca. 50 kriminelle overgreb på børn i Danmark om året gennem den tilgængelige børnepornografi.

Straffelovrådets hovedsynspunkt var:

- "Det synspunkt, der kunne begrunde en straffebestemmelse om fremstilling og udbredelse af børnepornografi, må være et ønske og en forventning om, at man på denne måde kan bidrage til at forebygge, at børn benyttes til optagelser, der i sig selv udgør strafbare forhold. Et forbud mod udbredelse skal have det formål at formindske efterspørgslen efter sådanne optagelser og dermed bidrage til at modvirke forekomsten af strafbare krænkelser af børn."
- Det udtaler videre, at "nykriminalisering i almindelighed [må] forudsætte et nogenlunde solidt grundlag for at antage, at anvendelsen af strafferetlige midler vil have overvejende gavnlige virkninger. Det kan diskuteres, om en kriminalisering af børnepornografi på indeværende tidspunkt er tilstrækkeligt begrundet, ¿".

Straffelovrådet fandt, at bestemmelsen kun skulle dække det erhvervsmæssige salg og den erhvervsmæssige udbredelse, og at der kun skulle være bødestraf. Den gennemførte bestemmelse svarede til Straffelovrådets forslag:

- "*§ 235*. Den, som erhvervsmæssigt sælger eller på anden måde udbreder eller med forsæt hertil fremstiller eller skaffer sig utugtige fotografier, film eller lignende af børn, straffes med bøde."

Straffelovrådet afgav i 1987 en betænkning[(40)], der indeholdt en generel gennemgang af straffelovens strafferammer. § 235 bruges heri udtrykkeligt[(41)] som eksempel på en af de bestemmelser, hvorom det "uden videre [kan] fastslås, at de er af en så lidet alvorlig karakter, at de ikke bør kunne straffes med mere end en bøde eller allerhøjest med en kort frihedsstraf". Det nævnes videre[(42)], at den eneste grund til at anbringe § 235 i straffeloven er, "at der ikke findes nogen særlov, i hvilken straffebestemmelsen naturligt kan anbringes."

I 1989[(43)] ændredes strafferammen til bøde, hæfte eller fængsel indtil 6 måneder. Justitsministeriet skrev i bemærkningerne til lovforslaget[(44)]:

- "Siden forbudet mod handel med børnepornografi blev optaget i straffelovens § 235 i 1980, har der kun været et begrænset antal sager om overtrædelse af forbudet. Uanset om der aktuelt kan påvises noget praktisk behov for en strafferammeskærpelse, kan man generelt rejse det spørgsmål, om en strafferamme med bøde for denne type kriminalitet fortsat kan anses for passende og tidssvarende, også med hensyn til de groveste former, som denne forbrydelse kan fremtræde i.
- Efter regeringens opfattelse er handel med børnepornografi en forbrydelse, der må ses på med større alvor, end den nugældende strafferamme med bøde er udtryk for."

---

40. Betænkning nr. 1099/1987 om strafferammer og prøveløsladelse.
41. Betænkningen s. 92.
42. Betænkningen s. 100.
43. Ved lov nr. 272 af 3/5 1989.
44. FT 1988/89 A 2858.

Lovændringen harmonerede med de internationale drøftelser om beskyttelse af børn, der samme år resulterede i artikel 34 i FNs konvention af 20/11 1989 om barnets rettigheder, hvorefter deltagerstaterne skal beskytte børn mod alle former for seksuel udnyttelse og seksuelt misbrug og med henblik herpå især tage alle passende nationale, bilaterale og multilaterale forholdsregler for at forhindre:

a) at et barn overtales eller tvinges til at deltage i nogen form for ulovlig seksuel aktivitet;

b) at børn udnyttes til prostitution eller andre former for ulovlig seksuel aktivitet;

c) at børn udnyttes i pornografiske forestillinger og materialer.

Europarådet anbefalede i rekommandation nr. R (91) 11 medlemslandene at overveje det tilrådelige i at kriminalisere besiddelse af børnepornografi, og i FNs Menneskerettighedskommissions resolution 1992/74 opfordredes medlemslandene til at kriminalisere besiddelsen af børnepornografi. Endvidere anbefalede Nordisk Råd

i rekommandation 9/1994 en kriminalisering i Norden af besiddelse af børnepornografi.

I 1994[(45)] indsattes bestemmelsens stk. 2, der kriminaliserer besiddelsen af grovere former for børnepornografi:

- "Stk. 2. Den, som besidder fotografier, film eller lignende af børn, der har samleje eller anden kønslig omgængelse end samleje, straffes med bøde. På samme måde straffes den, som besidder fotografier, film eller lignende af børn, der har kønslig omgang med dyr, eller som anvender genstande på groft utugtig måde."

Begrundelsen for lovforslaget[(46)] var især:

- "På baggrund af, at produktion af børnepornografi i mange tilfælde sker ved grove alvorlige strafbare handlinger mod børn, kan det virke stødende, at besiddelsen af materialet ikke er strafbar. Et forbud mod besiddelse af børnepornografisk materiale markerer en klar afstandtagen fra seksuelt misbrug af børn, samtidig med at det bidrager til at værne børns rettigheder. Dertil kommer, at et forbud mod besiddelse muligvis vil kunne medføre en vis begrænsning af efterspørgslen efter børnepornografisk materiale og dermed også produktionen og de dertil knyttede seksuelle overgreb mod børn."

Med hensyn til afgrænsningen af det omfattede pornografiske materiale nævnes, at

- "Derved tilsigtes en afbalanceret løsning, der på den ene side rammer billeder optaget i forbindelse med, at der er begået alvorlige strafbare handlinger over for børn, mens besiddelsen af mindre grove billeder fortsat vil være tilladt og muligvis kan have en kriminalitetsdæmpende effekt."
- "Justitsministeriet foreslår endvidere, at strafferammen bliver bøde. Det indebærer, at politiet afskæres fra at foretage ransagning af en ikkesigtets bolig, rum eller gemmer med henblik på for eksempel beslaglæggelse af børnepornografisk materiale .¿. Formålet med denne del af forslaget er i videst muligt omfang at værne den enkelte mod indgreb i privatlivets sfære. Forslaget udelukker imidlertid ikke, at der efter omstændighederne kan foretages ransagning hos en person, der er sigtet for besiddelse af børnepornografisk materiale¿"

---

45. Ved lov nr. 1100 af 21/12 1994.
46. FT 1994/95 A 467

Det nævnes i lovforslaget, at spørgsmålet om, hvornår der foreligger besiddelse, undertiden kan give anledning til tvivl, navnlig hvor materialet udbredes via elektroniske midler. Det siges herom:

- "Ved betragtning af tvudsendelser (eksempelvis sendt via satellit) eller billeder, der overføres fra en database til egen edbskærm, vil billedet ikke kunne siges at være i betragterens besiddelse. Er der derimod tale om, at billedet lagres, det være sig på videobånd, harddisk, diskette eller lign., således at den pågældende selv kan kalde billedet frem igen, må materialet anses for at være i vedkommendes besiddelse."

Bestemmelsen har herefter i dag følgende ordlyd:

- "§ 235. Den, som erhvervsmæssigt sælger eller på anden måde udbreder eller med forsæt hertil fremstiller eller skaffer sig utugtige fotografier, film eller lignende af børn, straffes med bøde, hæfte eller fængsel indtil 6 måneder.
- *Stk. 2*. Den, som besidder fotografier, film eller lignende af børn, der har samleje eller anden kønslig omgængelse end samleje, straffes med bøde. På samme måde straffes den, som besidder fotografier, film eller lignende af børn, der har kønslig omgang med dyr, eller som anvender genstande på groft utugtig måde."

Folketinget har den 19/11 1998 behandlet 3 forslag om ændring af straffelovens § 235:

- 1. Beslutningsforslag af 27/10 1998[(47)] opfordrer Justitsministeren til snarest at fremsætte lovforslag bl.a. om ændring af straffelovens § 235 således at:
- 1) Strafmaksimum for erhvervsmæssig udbredelse forhøjes til fængsel i 3 år.
- 2) Bytning sidestilles med erhvervsmæssig udbredelse,

- 3) Enhver besiddelse er strafbar uanset materialets grovhed.
- 1. Beslutningsforslag af 27/10 1998[(48)] opfordrer Justitsministeren til, at strafmaksimum i straffelovens § 235 forhøjes til fængsel i 3 år inden udgangen af folketingsåret.
- 2. Lovforslag af 12/11 1998[(49)] forslår, at straffelovens § 235 ændres således at:
- 1) Strafmaksimum i stk. 1 forhøjes til fængsel i 6 år.
- 2) Strafmaksimum i stk. 2 forhøjes til fængsel i 6 måneder.

- [47.] B 22 (KRF), FT 1998/99 A 1618.
  [48.] B 24 (KF), FT 1998/99 A 1625.
  [49.] Nr. L 83 (DF), FT 1998/99 A 2095.

4.2. Omfanget af bestemmelsens brug

Antallet af anmeldelser vedrørende overtrædelser af straffelovens § har siden 1995 været stigende. De registrerede anmeldelsestal for perioden 19921998 har været følgende[(50)]:

1992: 7 anmeldelser; 1993: 7 anmeldelser; 1994: 5 anmeldelser; 1995: 6 anmeldelser; 1996: 23 anmeldelser; 1997: 28 anmeldelser og 1998: 36 anmeldelser. De reelle anmeldelsestal for 1997 og 1998 er dog væsentlig større, jfr. det nedenfor oplyste om anmeldelser til Rigspolitichefen.

For nogle af anmeldelserne og de senere domme er der tale om sager i et større samlet sagskompleks, hvorfor anmeldelsestallene ikke i alle tilfælde giver et fuldstændigt korrekt billede af mængden af sager. Tendensen vedrørende antallet af sager er dog yderst klar. Anmeldelsestallene for 1997 og 1998 skal ses i sammenhæng med en række henvendelser til Rigspolitichefens hjemmeside, jfr. nedenfor, der i denne periode ikke er blevet opdateret som anmeldelser og derfor ikke indgår i den almindelige statistik over anmeldelser. Det er nærliggende at antage, at denne stigning, i hvert fald delvist, kan forklares med en stigende brug af Internettet i samme periode.

I perioden 1992-1997 fordeler antallet af domfældelser[(51)] sig som følger:

1992: 3 domfældelser; 1993: 2 domfældelser; 1994: 1 domfældelse; 1995: 3 domfældelser; 1996: 10 domfældelser og 1997: 13 domfældelser.

[50.] Tallene stammer fra politiets kriminalregister.
[51.] Med under domfældelser regnes også bødeforlæg og afgørelser efter straffelovens §§ 6870.

Blandt de afgjorte sager kan som eksempler nævnes følgende:

- *Aalborg rets dom af 16/3 1993*
  Der var rejst tiltale for 4 forhold af straffelovens § 235, heraf 1 som forsøg og 2 som medvirkende. Der blev dømt for et forhold, hvor tiltalte i digitaliseret form havde lagret utugtige billeder af børn på en database, hvortil andre mod betaling kunne få adgang. Ved bevisførelsen fandtes det ikke nærmere fastlagt, i hvilket omfang der var sket salg eller anden udbredelse, udover at der var konstateret foretaget et betydelig antal træk på fotografierne og udbredelsen må antages at være sket til en større personkreds i mange lande. Tiltalte havde endvidere solgt fotografier på diskette. I de 3 andre forhold blev tiltalte frifundet. Tiltalte blev idømt en straf på 40 dages hæfte.
- *Lemvig rets dom af 14/2 1997*
  Der var rejst tiltale for overtrædelse af både § 235, stk. 1 og stk. 2. Vedrørende stk. 1 udtalte retten, at det kan lægges til grund, at tiltalte oprettede en database med det formål, at brugere via telefonnettet kunne skaffe sig adgang til databasen og se eller hente billeder mod senere vederlag. Brugere kunne kun downloade de billeder, der var angivet i fillisten. Retten lagde til grund, at filen ikke var tilgængelig for brugere, hvorfor det ikke fandtes bevist, at tiltalte havde forsøgt erhvervsmæssigt at udbrede utugtige billeder af børn. For

overtrædelse af stk. 2 idømtes tiltalte 10 dagbøder à 200 kr., idet han havde været i besiddelse af et billede af børn, som var omfattet af stk. 2.

- *Københavns byrets dom af 23/9 1997*
  Der var rejst tiltale for overtrædelse af straffelovens § 235, stk. 2, (og straffelovens § 284, jfr. §§ 276 og 279 a samt § 286, jfr. § 279 a). Overtrædelsen af § 235, stk. 2, vedrørte besiddelse af 2 billeder af børn omfattet af bestemmelsen. Tiltalte blev straffet for besiddelse af det ene billede. Tiltalte blev endvidere dømt for overtrædelse af de andre anførte bestemmelser. Straffen blev fastsat til 1 års betinget fængsel.
- *Vordingborg rets dom af 24/9 1997*
  Den tiltalte var bl.a. tiltalt for gennem ca. 4 måneder med forsæt til erhvervsmæssigt salg eller anden udbredelse bl.a. via Internettet at have sat sig i besiddelse af ikke under 533 børnepornografiske fotografier og gennem 5 dage at have udbredt ca. 40 fotografier bl.a. via Internettet. Den tiltalte blev frifundet for tiltalen vedrørende straffelovens § 235, stk. 1, fordi der ikke var grundlag for at antage, at han havde noget erhvervsmæssigt sigte med udbredelsen, men blev dømt for overtrædelse af bestemmelsens stk. 2. (Den tiltalte blev idømt 14 dagbøder à 150 kr.).
- *Østre landsrets dom af 10/12 1998*
  Der var rejst tiltale for overtrædelse af straffelovens § 235, stk. 2, (og straffelovens § 210, § 216, § 222, § 224 og § 232). For så vidt angik overtrædelse af § 235, stk. 2, var der rejst tiltale for at have besiddet mange billeder/fotografier samt flere videofilm, indeholdende børnepornografi omfattet af bestemmelsen. Tiltalte erkendte forholdet. Der blev endvidere dømt for hovedparten af anklageskriftets øvrige forhold. Straffen blev fastsat til fængsel i 5 år.

Siden medio 1997 har der været mulighed for brugere af Internettet for at henvende sig til såkaldte "hotlines", hvis de får mistanke om børnepornografi over Internettet. Den første hotline blev etableret medio 1997 af Red Barnet, der efter aftale med Rigspolitichefens IT-støtteenhed videresender alle henvendelser til enheden. Der blev modtaget ca. 700 henvendelser i 1997 og 1025 i 1998. I august 1998 etablerede Rigspolitichefen på sin hjemmeside en service, hvortil borgerne kan anmelde IT-relateret kriminalitet, herunder børnepornografi på Internettet. Der er siden da modtaget 350 henvendelser om børnepornografi (pr. 12/1 1999). Nogle få Internetudbydere har tillige iværksat hotlines, hvortil deres kunder kan henvende sig vedrørende ulovligheder. En af disse udbydere har videregivet 86 henvendelser (pr. 12/1 1999), som udbyderen har modtaget siden ordningens start i juli 1998. Efter det af Rigspolitichefens IT-støtteenhed oplyste vedrører alle henvendelserne børnepornografi, og det hører til den absolutte undtagelse, at et site med børnepornografi anmeldes flere gange.

Ifølge Rigspolitichefens IT-støtteenhed afhænger omfanget af den enkelte sag af, hvilken type persongruppe der er involveret. Hos enheden opdeler man persongrupperne i tre hovedgrupper:

- Nysgerrige der grundet omtale af problemet søger efter materiale på Internettet og opbygger en begrænset samling, som kan indgå i forbindelse med udveksling af pornografisk materiale i øvrigt på Internettet. I disse sager indgår der fra nogle ganske få billeder til nogle hundrede.
- Samlere med pædofile tilbøjeligheder, hvis hovedinteresse er rettet mod utugtigt billedmateriale, og som søger at komme ind i de lukkede egentlige pædofile globale sammenslutninger. Der er danske eksempler på, at sådanne samlere har billedsamlinger indeholdende 10.000-40.000 billeder.
- Pædofile med tilknytning til en eller flere lukkede globale sammenslutninger, hvor forudsætningen for deltagelse er at frembyde nyt billedmateriale i form af digitale fotos eller videoklip samt "liveoptagelser" vist for en større eller mindre del af sammenslutningens medlemmer.

Med hensyn til den sidstnævnte type gruppe blev der den 3/9 1998 gennemført en samlet aktion mod nogle hundrede mistænkte, hvoraf 78 blev anholdt. Myndighederne i 19 lande gennemførte i forening aktionen. Der blev ikke foretaget anholdelser i Danmark. I den gruppe, som aktionen var rettet mod, var det en forudsætning for at opretholde medlemsskabet, at man løbende skulle tilføre den samlede gruppe nye utugtige billeder, som man ikke tidligere havde set. Denne omstændighed indebar, at der til stadighed skulle produceres nyt materiale.

4.3. Andre landes regulering

4.3.1. Norsk ret

Den norske straffelov indeholder følgende bestemmelse:

- "§ 211. Med bøter eller med fengsel inntil 2 år eller med begge deler straffes:
- a) den som holder offentlig foredrag eller istandbringer offentlig forestilling eller utstilling av utuktig eller pornografisk innhold,
- b) den som utgir, frambyr til salg eller leie eller på annen måte søker å utbre, eller som med hensikt å foreta slik utbredelse innfører utuktige eller pornografiske skrifter, bilder, filmer, videogram eller lignende,
- c) den som overlater utuktige eller pornografiske skrifter, bilder, film, videogram og liknende til personer under 18 år,
- d) den som besitter eller innfører bilder, film, videogram eller lignende, hvor noen som er, må regnes å være eller fremstilles som å være under 16 år, er vist på en utuktig eller pornografisk måte.
- Med utuktige eller pornografiske skildringer menes i denne paragraf kjønnslige skildringer som virker støtende eller på annen måte er egnet til å virke menneskelig nedverdigende eller forrående, herunder kjønnslige skildringer med bruk av barn, dyr, vold, tvang og sadisme.
- Medvirkning straffes på samme måte.
- Med bøter eller fengsel inntil 6 måneder eller begge deler straffes den som av uaktsomhet foretar noen sådan handling som er nevnt i denne paragraf.
- På samme måte straffes den innehaver eller overordnede som forsettlig eller av uaktsomhet unnlater å hindre at det i en virksomhet blir foretatt handling som nevnt i denne paragraf.
- Ved straffeutmålingen legges det i skjerpende retning vekt på om de utuktige eller pornografiske skildringer omfatter bruk av barn, dyr, vold, tvang og sadisme.
- Paragrafen gjelder ikke for film eller videogram som Statens filmkontrol ved forhåndskontroll har godkjent til ervervsmessig framvisning eller omsetning."

4.3.2. Svensk ret

Den svenske brottsbalk indeholder i kapitel 16 følgende bestemmelser:

- "10 a § Den som skildrar barn i pornografisk bild med uppsåt att bilden sprids eller som sprider sådan bild av barn döms, om inte gärningen med hänsyn till omständigheterna är försvarlig, för barnpornografibrott till böter eller fängelse i högst två år."

Den svenske regering har den 8/12 1997 fremsat proposition 1997/98:43, hvor bestemmelsen foreslås ændret, jfr. neden for, ligesom der foreslås en lov om forbud mod ind og udførsel af børnepornografi. Det behandledes af Riksdagen den 13/5 1998 og henlagdes, da gennemførelsen kræver grundlovsændring.

Den foreslåede nye § 10 a lyder således:

"Den som

- 1. skildrar barn i pornografisk bild,
- 2. sprider, överlåter, upplåter, förevisar eller på annat sätt gör en sådan bild av barn tillgänglig för någon annan,
- 3. förvarvar eller bjuder ut en sådan bild av barn,
- 4. förmedlar kontakter mellan köpare och säljare av sådana bilder av barn eller vidtar någon annan liknande åtgärd som syftar till att främja handel med sådana bilder, eller
- 5. innehar en sådan bild av barn
- döms för barnpornografibrott till fängelse i högst två år eller, om brottet är ringa, till böter eller fängelse i högst sex månader.
- Med barn avses en person vars pubertetsutveckling inte är fullbordad eller som, när det framgår av bilden och omständigheterna kring den, är under 18 år.
- Den som i yrkesmässig verksamhet eller annars i förvärvssyfte av oaktsamhet sprider en sådan bild som avses i första stycket, döms som sägs där.
- Är ett brott som avses i första stycket at anse som grovt skall dömas för grovt barnpornografibrott till fängelse lägst sex månadar och högst fyra år. Vid bedömande av om brottet är grovt skall särskilt beaktas om det har begåtts yrkesmässigt eller i vinstsyfte, utgjort ett led i brottslig verksamhet som utövats systematisk eller i störra omfattning, avsett en särskilt stor mängd bilder eller avsett bilder där barn utsätts för särskilt hensynslös behandling.

- Förbuden mot skildring och innehav gäller inte den som tecknar, målar eller på något annat liknande hantverksmässigt sätt framställar en sådan bild som avses i första stycket, om bilden inte är avsedd att spridas, överlåtas, upplåtas, förevisas eller på annat sätt göras tillgänglig för andra. Även i andra fall skall en gärning inte utgöra brott, om särskilda omständigheter gör att gärningen måste anses uppenbart befogad."

4.3.3. Tysk ret

Den tyske Strafgesetzbuch indeholder i § 184 om "Verbreitung pornographischer Schriften" følgende bestemmelser om børnepornografi:

- "(3) Wer pornographische Schriften (§ 11 Abs. 3)(52), die Gewalttätigkeiten, den sexuellen Missbrauch von Kindern oder sexuelle Handlungen von Menschen mit Tieren zum Gegenstand haben,
- 1. verbreitet,
- 2. öffentlich ausstellt, anschlägt, vorführt oder sonst zugänglich macht oder
- 3. herstellt, bezieht, liefert, vorrätig hält, anbietet, ankündigt, anpreist, einzuführen oder auszuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Sinne der Nummern 1 oder 2 zu verwenden oder einem anderen eine solche Verwendung zu ermöglichen,
- wird, wenn die pornographischen Schriften den sexuellen Missbrauch von Kindern zum Gegenstand haben, mit Freiheitssstrafe von drei Monaten bis zu fünf Jahren, sonst mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
- (4) Haben die pornographischen Schriften (§ 11 Abs. 3) in den Fällen des Absatzes 3 den sexuellen Missbrauch von Kindern zum Gegenstand und geben sie ein tatsächliches Geschehen wieder, so ist die Strafe Freiheitsstrafe von sechs Monaten bis zu fünf Jahren, wenn der Täter gewerbsmässig oder als Mitglied einer Bande handelt, die sich zur fortgesetzen Begehung solcher Taten verbundet hat.
- (5) Wer es unternimmt, sich oder einem Dritten den Besitz von pornographischen Schriften (§ 11 Abs. 3) zu verschaffen, die den sexuellen Missbrauch von Kindern zum Gegenstand haben, wird, wenn die Schriften ein tatsächliches Geschehen wiedergeben, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer die in Satz 1 bezeichneten Schriften besitz.
- (6) ¿Absatz 5 gilt nicht für Handlungen, die ausschliesslich der Erfüllung rechtmässiger dienstlicher oder beruflicher Pflichten dienen."

---

52. Den nævnte bestemmelse lyder således: "Den Schriften stehen Ton und Bildträger, Abbildungen und andere Darstellungen in denjenigen Vorschriften gleich, die auf diesen Absatz verweisen."

4.3.4. Fransk ret

Den franske Code Pénal indeholder følgende bestemmelse:

- "Art. 22723 Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image d'un mineur lorsque cette image présente un caractère pornographique est puni d'un an d'emprisonnement et de 300.000 F d'amende.
  Le fait de diffuser une telle image, par quelque moyen que ce soit, est puni des mêmes peines.
  Les peines sont portées à trois ans d'emprisonnement et à 500.000 F d'amende lorsqu'il s'agit d'un mineur de quinze ans."

4.4. Udvalgets overvejelser

4.4.1. Generelle overvejelser

Udvalget har generelt drøftet de hensyn, der skal afvejes mod hinanden i en regulering af området vedrørende børnepornografi. Der er enighed om, at der skal være tungtvejende grunde til, at der gribes ind over for

informationsfriheden, og at ethvert indgreb skal begrænses til det nødvendige.

Hensynet bag reguleringen er beskyttelsen af børn. Ud fra dette synspunkt blev det i forbindelse med det oprindelige lovforslag i 1979 klart tilkendegivet, at tegninger ikke var omfattet af reguleringen. I forbindelse med den seneste ændring i 1994 fremhæves det i bemærkningerne, at ikke alene tegninger, men også billeder frembragt ved hjælp af edb, som ikke afbilder et virkeligt samleje eller anden kønslig omgængelse, falder uden for bestemmelsen. Især den sidste begrænsning giver anledning til bevisproblemer, idet f.eks. computergenererede billeder fremtræder som identiske med egentlige billeder.

Udvalget har drøftet, om også computergenererede fremstillinger eller andre fremstillinger, der har fuldstændig lighed med fotografier o.l., bør være omfattet af den strafferetlige regulering. Udvalget finder, at hensynet til beskyttelse af børn mod misbrug ikke nødvendiggør, at sådanne fremstillinger omfattes af reguleringen. Med hensyn til de bevisspørgsmål, der kan opstå, har Justitsministeriet i forbindelse med den sidste lovændring vedrørende computerskabte billeder givet udtryk for(53), at det vil påhvile tiltalte at sandsynliggøre, at billederne er frembragt ved hjælp af edb. Anfører tiltalte omstændigheder, der i et vist omfang bestyrker påstanden, må anklagemyndigheden føre modbevis f.eks. ved at godtgøre, at man på alle tænkelige måder har forsøgt at bevise tiltaltes påstand, men uden resultat. Udvalget finder på denne baggrund, at der ikke er behov for en strafferetlig regulering af sådanne fremstillinger.

Det er selvsagt også vanskeligt at håndhæve en dansk lovgivning, idet materialet kan være placeret på en server i en jurisdiktion, der ikke strafbelægger børnepornografi, og hvorfra transmissionen til Danmark sker i krypteret form. Udvalget finder imidlertid, at problemer af denne type - der ikke er specielle for børnepornografi - ikke bør afholde Danmark fra at have den ønskede strafferetlige regulering.

Under udvalgets diskussion af, om der er behov for ændringer i eller suppleringer af de nuværende regler om børnepornografi i straffelovens § 235, er der især peget på tre spørgsmål.

For det første må det overvejes, om det nuværende gerningsindhold i stk. 1 fortsat skal være begrænset til den erhvervsmæssige udbredelse(54). For det andet må det undersøges, om besiddelseskriteriet i stk. 2 er egnet til at dække de relevante situationer i forbindelse med IT-udbredelse. For det tredje må der tages stilling til, om strafferammerne fortsat må anses for de rigtige.

---

53. Justitsministeriets besvarelse af 30/11 1994 af spørgsmål nr. 13 fra Folketingets Retsudvalg vedrørende forslag til lov om ændring af straffeloven (besiddelse af børnepornografi) (L 38 - bilag 14).
54. Som nævnt i afsnit 4.1 blev bestemmelsen begrænset til det erhvervsmæssige salg eller den erhvervsmæssige udbredelse i overensstemmelse med Straffelovrådets forslag. I 1979 var afgrænsningsproblemstillingen i relation til private overdragelser, og udbredelsesformer som Internettet var endnu ikke aktuelle.

4.4.2. Straffelovens § 235, stk. 1

Der henvises til afsnit 2.4.1 vedrørende udvalgets generelle overvejelser. Som anført i det afsnit finder udvalget, at udviklingen på IT-området har medført, at en begrænsning til kriminalisering af - eller til en højere strafferamme for - erhvervsmæssig spredning i dag er en utilstrækkelig strafferetlig beskyttelse, og at man bør kriminalisere udbredelse i en videre kreds i samme omfang. Dette gælder også for spredning af børnepornografi.

Som straffelovens § 235 er formuleret i dag, kan spredning af utugtige fotografier, film o.l. af børn kun straffes efter den kvalificerede bestemmelse i stk. 1, hvis det kan bevises, at gerningsmanden har haft forsæt til erhvervsmæssig spredning. Er det ikke situationen, kan der alene straffes efter stk. 2 med bødestraf for gerningsmandens besiddelse af de utugtige billeder, der er omfattet af denne bestemmelse. Til belysning af problemstillingen kan nævnes Vordingborg rets dom af 24/9 1997, som er omtalt nærmere ovenfor i afsnit 4.2.

Justitsministeren har den 18/11 1997 besvaret et spørgsmål fra Folketingets Retsudvalg om, hvorvidt ministeren ville overveje at ændre straffelovens § 235 således, at udbredelse på Internettet kan straffes på samme måde som den erhvervsmæssige udbredelse. Baggrunden for spørgsmålet var ovennævnte dom fra Vordingborg ret. Ministeren henviste bl.a. til, at der var nedsat et udvalg om økonomisk kriminalitet og datakriminalitet, og at der vil være anledning til at overveje, om der er behov for ændring af § 235.

Udvalget finder, at det også i relation til børnepornografi er rimeligt, at der ikke stilles krav om "erhvervsmæssig" udbredelse, hvis udbredelsen sker i en videre kreds. Udvalget har især lagt vægt på, at adgang til børnepornografi via Internettet muliggør en meget omfattende udbredelse.

Det er utvivlsomt, at en del af denne udbredelse ikke er erhvervsmæssig, men udvalget finder, at også ikkeerhvervsmæssig udbredelse af billeder i en videre kreds kan være egnet til at understøtte produktion af børnepornografi, og at kriminalisering af sådan udbredelse dermed kan tjene til at forebygge de samme misbrug, som forbud mod den erhvervsmæssige udbredelse.

Som eksempel på en situation, hvor der tale om samme risici for udnyttelse af børn ved ikkeerhvervsmæssig udbredelse som ved den erhvervsmæssige udbredelse, kan nævnes distribution i "klubber" på Internettet vedrørende børnepornografi, hvor der er regler i klubben om, at man for at være medlem skal sende et bestemt antal billeder til alle medlemmer af klubben, hvorefter man modtager samme antal billeder, som man sender. Også sådanne ikkeerhvervsmæssige situationer bør være omfattet af reguleringen, hvis klubben har et større antal medlemmer.

En ændring af straffelovens § 235, stk. 1, vil bringe dansk ret på linie med norsk, svensk, tysk og fransk ret, der ikke stiller krav om, at udbredelsen skal være erhvervsmæssig, jfr. afsnit 4.3.

Der henvises til afsnit 7.2 vedrørende udvalget forslag.

4.4.3. Straffelovens § 235, stk. 2

Også kravet i straffelovens § 235, stk. 2, om "besiddelse" har givet udvalget anledning til overvejelser - både om, hvad der ligger i begrebet, og om, hvorvidt Internettet giver anledning til nye overvejelser omkring, hvad der bør være kriminaliseret.

Som nævnt i afsnit 4.1 er det forudsat i lovforslaget til den nugældende bestemmelse, at selve det at se på børnepornografiske billeder, der overføres fra en database til egen computerskærm, ikke etablerer en besiddelsessituation i modsætning til en lagring, hvor den pågældende selv kan kalde billedet frem igen.

Denne afgrænsningsbeskrivelse kan give anledning til overvejelser omkring, hvorvidt Internetadgang til børnepornografiske billeder altid etablerer en besiddelsessituation.

Når oplysninger hentes fra hjemmesider, placeres alle sidens komponenter på harddisken i cachen, og skærmvisningen sker fra denne lagring. Cachen er et område til midlertidige Internetfiler, der typisk kan indeholde 25 % af pladsen på harddisken, men af brugeren kan indstilles til at indeholde en defineret procentdel (fra 1 % og op). Cachen vil således kunne indeholde alle hjemmesider, der har været besøgt, for en længere periode, og brugeren vil kunne hente alle de gemte komponenter frem fra cachen, der bl.a. registrerer komponentnavn, Internetadresse og dato for bl.a. seneste åbning. Det afhænger af system og valgte indstillinger, om det kan aflæses, at en komponent har været hentet igen i cachen.

Der er enighed i udvalget om, at besiddelseskravet i straffelovens § 235, stk. 2, skal forstås således, at der tillige indgår et subjektivt moment. Der skal være tale om en lagring, den pågældende har besluttet at foretage eller at udnytte. De lagringer, der er en del af den almindelige tekniske proces ved adgang til netsystemer, giver derfor nogle særlige problemstillinger. I det omfang det kan bevises, at den pågældende bruger cachen som lagringsplads med henblik på at genfremkalde derfra, er denne form for lagring omfattet af besiddelsesbegrebet. Dette gælder også, når beslutning herom først træffes på et senere tidspunkt end lagringen (f.eks. i forbindelse med, at den pågældende opdager, at der kan genfremkaldes fra cachen).

Hvis den pågældende har givet besked til systemet om at lagre, vil der altid være tale om besiddelse, men også i de situationer, hvor lagringen er en del af den almindelige tekniske proces, vil der således være tale om besiddelse, hvis den pågældende har udnyttet eller vil udnytte denne lagringsform til at genfremkalde cachens (eller et tilsvarende teknisk mellemlagers) indhold af børnepornografisk materiale(55),(56).

Efter det for udvalget oplyste har der i de p.t. kendte sager altovervejende været tale om, at billederne var blevet downloadet, og at bestemmelsen derfor var anvendelig uden at komme ind på cachens indhold.

I en række tilfælde vil der imidlertid ikke blive downloadet, idet den pågældende blot vil gå ind på særlige Internetområder med børnepornografi, eventuelt til et frit område, hvor brugen eventuelt kan bevises via logning.

---

55. Sidstnævnte problemstilling, hvor gerningsindholdet realiseres, når der træffes en beslutning vedrørende en allerede etableret besiddelse, svarer til, hvad der gælder for ulovlig omgang med hittegods, jfr. straffelovens § 277, og for underslæb, jfr. straffelovens § 278. Efter § 277 er det tillige strafbart, når beslutningen om tilegnelse træffes på et tidspunkt, hvor varetægtsforholdet på tilfældig måde er etableret.
56. Dette svarer til den afgrænsning af besiddelse i IT-mæssig sammenhæng, som arbejdsgruppen vedrørende datakriminalitet fandt skulle lægges til grund

---

Kriminaliseringen af besiddelse er som nævnt i afsnit 4.1 sket på baggrund af opfordringer fra bl.a. Europarådet, FN og Nordisk Råd, og udgangspunktet for disse opfordringer har været at begrænse efterspørgslen efter børnepornografi. På den baggrund kan det virke utilstrækkeligt at holde en benyttelsesform, der i dag i vidt omfang har afløst fysisk besiddelse, udenfor. Det må også indgå i overvejelserne, at man ved brug af Internettet ofte vil kunne få adgang til at se et billede, der ligger på en server i udlandet under omstændigheder, som ikke gør det muligt at retsforfølge besidderen af serveren.

Det er på den anden side klart, at hvis Internetbrugere kommer ind på de særlige områder, hvor der er fri adgang til børnepornografi, uden at de har noget ønske om at se børnepornografi eller som et enkelt nysgerrigt besøg, er der ikke tale om handlinger, hvor der er behov for at kriminalisere. Det er ikke sådanne situationer, der er egnede til at understøtte produktionen af børnepornografi.

Bevismæssigt vil det være meget vanskeligt at gennemføre sager, hvor selve det at se børnepornografi kriminaliseres, ligesom der vil være en vanskelig afgrænsning til de mere tilfældighedsprægede situationer, der efter udvalgets opfattelse i hvert fald ikke bør omfattes af en regulering.

Det må imidlertid antages, at der i et vist omfang er en erhvervsmæssigt præget produktion - hvor sælgeren eller udbrederen er omfattet af bestemmelsen i straffelovens § 235, stk. 1 - og at brugerkredsen ved den erhvervsmæssige udnyttelse af børn i højere grad vil kunne identificeres, fordi også betalingsstrømme vil kunne indgå i bevisførelsen. Det er formentlig også den form for udnyttelse, hvor det strafferetlige system kan have den største præventive virkning.

Ved spørgsmålet om, hvorvidt man skal kriminalisere det, at en person mod vederlag retsstridigt gør sig bekendt med børnepornografi, har udvalget haft med i sine overvejelser, at det samlede omfang af børnepornografien synes at være voksende, jfr. ovenfor under afsnit 4.2. Dette betyder, at den samlede mængde af bagvedliggende krænkelser formentligt også er voksende. En del børnepornografiske ydelser leveres på en sådan vis, at der ikke hos modtageren er tale om besiddelse i straffelovens § 235, stk. 2's forstand, hvorfor det vil være relevant at kriminalisere selve det forhold mod vederlag at gøre sig bekendt med børnepornografi.

Dertil kommer, at når der betales vederlag for en børnepornografisk ydelse, vil det ud fra et synspunkt af samme art som det, der ligger bag kriminalisering af hæleri, være naturligt at kriminalisere aftageren af ydelsen. Uanset at den person, der betaler for at gøre sig bekendt med børnepornografien, ikke i straffelovens forstand kommer i besiddelse af børnepornografien, har han modtaget en egentlig ydelse, nemlig muligheden for at se den pågældende børnepornografi. Dette minder om hæleri, hvor hæleren modtager et gode fra den, der har begået førforbrydelsen. Herudover vil en kriminalisering kunne være medvirkende til at formindske efterspørgslen efter børnepornografiske ydelser og derved forhåbentligt være med til at formindske mængden af de bagvedliggende krænkelser. Dette synspunkt er endnu et moment, der ligner hælerisynspunktet, idet hovedformålet med kriminalisering af hæleri er et ønske om at forhindre førforbrydelserne.

På denne baggrund finder udvalget, at det forhold, at en person mod vederlag retsstridigt gør sig bekendt med børnepornografiske fremstillinger, bør kriminaliseres. Forslaget omfatter enhver form for modydelse, der har karakter af et vederlag, herunder at der byttes med andre ydelser. Ved en sådan regulering styrker man indsatsen mod erhvervsmæssig udnyttelse af børn, idet kundernes forhold tillige omfattes af den strafferetlige regulering. Forsæt skal foreligge på det tidspunkt, hvor betalingen sker, og det skal vedrøre adgang til børnepornografiske fremstillinger.

Udvalget har drøftet, om en kriminalisering bør vedrøre samme fremstillinger som straffelovens § 235, stk. 1, eller begrænses til de fremstillinger, der er nævnt i straffelovens § 235, stk. 2. Kriminaliseringen kan både ses som et hælerilignende supplement til stk. 1, hvad der kan gøre det naturligt, at reguleringen vedrører samme fremstillinger som stk. 1, og som et supplement til besiddelsesreglen i stk. 2, hvad der kan gøre det naturligt at reguleringen vedrører samme fremstillinger som stk. 2.

Udvalget vil ikke udelukke, at det i et vist omfang kan dæmme op for mere grov kriminalitet, at der er mulighed for at se på noget mindre groft end det, der er omfattet af stk. 2. Dertil kommer, at i alle de tilfælde, som ses omtalt fra praksis, har fremstillingerne eller en stor del af disse været af en art, der var omfattet af stk. 2. Endvidere kan det give en mindre velbegrundet regulering, hvis eksempelvis en person ikke må købe et blad, men godt måtte besidde det, hvis en anden person forærer ham det.

Udvalget har på denne baggrund fundet, at reguleringen bør svare til den, der er i straffelovens § 235, stk. 2. Reguleringen kan derfor eventuelt ske som en udvidelse af den nugældende bestemmelse.

Der henvises til afsnit 7.2 vedrørende udvalgets forslag.

4.4.4. Strafferammen

Bestemmelsen i straffelovens *§ 235, stk. 1*, blev indsat i straffeloven i 1980. Dengang var der alene bøde i strafferammen. Dette var i overensstemmelse med flertallets opfattelse i Straffelovrådet[(57)]; rådet gav dog ingen explicit begrundelse herfor. I 1989 ændredes strafferammen, således at dens maksimum nu er fængsel i 6 måneder. Dette blev begrundet under henvisning til de grovest tænkelige former for handel med børnepornografiske billeder[(58)].

Denne strafferamme har i praksis vist sig tilstrækkelig ved de hidtil behandlede sager. Det er imidlertid udvalgets opfattelse, at det nugældende maksimum kan være for lavt, når det tages i betragtning, hvad beskyttelsesinteressen i § 235 er.

§ 235 skal for det første forhindre den krænkelse af privatlivets fred, der følger af udbredelser af billeder af denne art. Forholdet svarer for så vidt til straffelovens § 264 d om videregivelse af billeder af den pågældende under omstændigheder, der åbenbart kan forlanges unddraget offentligheden, og § 264 c om at skaffe sig eller uberettiget udnytte billeder, som er optaget under de i § 264 a nævnte omstændigheder. Både § 264 d og § 264 c har strafmaksima på 6 måneders fængsel ligesom § 235.

Derimod skal § 235 ikke anvendes på den direkte krænkelse af barnet under optagelsen af de pornografiske film eller billeder. I disse tilfælde anvendes de almindelige bestemmelser om voldtægt, samleje med mindreårig, anden kønslig omgængelse end samleje, kønslig omgængelse med en person af samme køn, blufærdighedskrænkelse osv., jfr. straffelovens kapitel 24. En forhandler, der bestiller billeder af denne art optaget hos en producent, kan straffes for medvirken til den pågældende sædelighedsforbrydelse.

Mellem producenten og den sluttelige køber eller besidder af det pornografiske materiale er der typisk en mellemhandler, der står for distributionen. I mange tilfælde foretages denne distribution for vindings skyld. Hvis den pornografiske film er bestilt af mellemhandleren, kan der som nævnt straffes for medvirken til sædelighedsforbrydelsen. Selv om dette ikke er tilfældet, er det naturligt at antage, at en betydelig del af de producerede film m.m. er optaget med henblik på et senere salg. I sådanne tilfælde kan man ikke straffe køberen (mellemhandleren) for den oprindelige sædelighedsforbrydelse, men alene efter § 235. § 235 skal således hindre mellemhandlerens køb af filmen m.m. og på den måde bidrage til, at den oprindelige optagelse og den oprindelige sædelighedsforbrydelse ikke gennemføres.

Ved vurderingen af strafværdigheden må det lægges til grund, at dette gør det rimeligt at anvende en noget højere strafferamme end ved de nævnte fredskrænkelser. Udvalget foreslår derfor, at strafmaksimum forhøjes fra de nuværende 6 måneder til 2 år. Dette er den nuværende højestestraf i Finland, Norge og Sverige, mens Island som Danmark har 6 måneder.

Med hensyn til *§ 235, stk. 2*, med den i afsnit 4.4.3 nævnte udvidelse er der tale om væsentligt mindre grove forhold end mellemhandlerens og distributørens. Den nuværende strafferamme - bøde - vil i den overvejende del af

tilfældene være passende. Bestemmelsen i det nugældende stk. 2 blev indsat så sent som i 1994[59], og udvalget finder, at den nuværende begrænsning af straffen til bøde bør bevares som normalstrafferammen.

Udviklingen i anvendelsen af Internettet og distribution af børnepornografi via Internettet har imidlertid udviklet sig således, at udvalget finder, at der bør være mulighed for under skærpende omstændigheder at idømme hæfte eller fængsel indtil 6 måneder. Som eksempel på, hvad der skal betragtes som skærpende omstændighed, kan nævnes, at den pågældende betaler betydelige beløb for at modtage børnepornografisk materiale. Der vil ligeledes foreligge skærpende omstændigheder, hvis den pågældende besidder et meget stort antal børnepornografiske fremstillinger, eller et større antal fremstillinger af særlig grove forhold, f.eks. voldtægt af børn.

---

57. FT 1979/80 2. samling A sp. 1765.
58. FT 1988/89 A sp. 2858.
59. FT 1994/95 A sp. 467.

KAPITEL 5 - EFTERFORSKNING - MULIGHEDER I PRAKSIS

5.1. Krav til Internetudbydere og teleselskaber om registrering af logoplysninger og opbevaring heraf

Manglende eller mangelfulde oplysninger hos Internetudbydere udgør et efterforskningsmæssigt problem. Problemet bliver ikke mindre, når der efterforskes forhold, hvor der er anvendt en række Internetadresser til dispositionen, så alt - incl. det land, der reelt opereres fra - er skjult.

Modhensynet - der taler for få registreringer og kortvarig opbevaring af oplysningerne hos formidlerne - er især hensynet til privatlivets fred. Under drøftelserne blev dog også nævnt, at der er tale om en meget stor teknisk usikkerhed med hensyn til loggens indhold og fuldstændighed, og at krav på dette område er omkostningskrævende.

Det kan også fremhæves, at det på nogle potentielle gerningsmænd formentlig vil kunne have en vis forebyggende effekt, hvis de ved, at transaktionerne logges, og at loggen opbevares i en længere periode.

Det er klart ikke muligt at tilgodese disse modsatrettede hensyn fuldt ud. Der er heller ikke tale om et problem, der kan totalløses via dansk lovgivning, men i et vist omfang vil en dansk regulering være en god hjælp.

EU udfærdigede den 17/1 1995 en resolution om lovlig aflytning af telekommunikation[(60)]. Bl.a. skal de retshåndhævende myndigheder have adgang til den opkaldte parts nummer ved udgående forbindelser, den opkaldende parts nummer ved indgående forbindelser, alle signaler målet har udsendt, forbindelsens begyndelses og afslutningstidspunkter samt varighed, faktiske bestemmelsesnummer og mellemliggende kaldenumre, hvis kommunikationen er blevet omstyret. Resolutionen nævner ikke spørgsmålet om opbevaringstid for oplysninger.

I G8-landenes erklæring af 10/12 1997 om hightech crime[(61)] nævnes i principerklæringens punkt V, at retssystemerne skal tillade bevaring og hurtig adgang til elektroniske data, og i punkt IX, at informations og telekommunikationssystemer i mulige omfang skal udformes, så det hjælper til at forhindre og opdage netværksmisbrug og letter sporing af kriminelle og indsamling af beviser.

Professor Ulrich Sieber nævner i sin rapport af 1/1 1998 til EU Kommissionen[(62)] Trace Back Procedures som et meget væsentligt punkt. Det siges i rapporten:

- "The study showed that one of the main problems for prosecuting computer crime is the anonymity provided by international computer networks. This anonymity must not be completely removed since privacy protection for users and anonymity (e.g. for social minority groups) is an important social value which should not be given up in international computer networks. However, on the other side, it should be possible, under welldefined legal circumstances (such as court orders) to lift anonymity in order to trace back the authors of illegal actions (such as hackers) or of illegal or harmful contents (such as paedophiles). Today such trace back procedures are often hindered or made impossible due to the features of the TCP/IP protocol of the Internet and in addition especially by the activities of anonymous remailers and the use of free access software."

IT-sikkerhedsrådet har i april 1998 udarbejdet en rapport om Privatliv på Internet[(63)]. Det nævnes i rapporten[(64)] vedrørende lagring af transaktionsoplysninger, at visse Internetleverandører gemmer sådanne oplysninger i 3 måneder - bl.a. for at gøre det muligt at efterkomme editionsbegæringer - mens andre ikke har nogen fast praksis. IT-sikkerhedsrådet bemærker, at en længerevarende opbevaring hos en Internetudbyder kan medføre betydelig risiko for indgreb i brugerens privatliv. Det nævnes, at Internetudbydere kun i få tilfælde benytter disse oplysninger i forbindelse med kundeafregninger. Det siges videre:

- "Det er væsentligt, at debatten herom tager udgangspunkt i en afvejning af på den ene side berettigede efterforskningshensyn og på den anden side vigtigheden af at undgå det totale overvågningssamfund, alene fordi den nye teknologi giver mulighed herfor.
- IT-sikkerhedsrådet finder det betænkeligt, at en praksis for opbevaring af transaktionsoplysninger alene baseres på efterforskningshensyn, der ikke er understøttet af særlig lovhjemmel, f.eks. i reglerne om indgreb i meddelelseshemmeligheden. Rådet finder, at Internetudbydere, bl.a. af sikkerhedsmæssige hensyn, bør opbevare så få oplysninger som muligt i så kort tid som muligt, idet udstrækningen af denne tid bl.a. må bestemmes ud fra hensynet til at gennemføre sædvanlige backupprocedurer m.v. Rådet skal bemærke, at et sådant minimumsprincip i øvrigt er i overensstemmelse med såvel den gældende registerlovgivning som med EUdirektivet om behandling af personoplysninger. Såvel hensynet til politiets efterforskning som hensynet til brugeren selv (f.eks. i forbindelse med senere bevisførelser om indgåede aftaler m.v.) taler for, at der etableres fastere principper for denne lagring.
  Rådet er dog også opmærksomt på, at særlige regler, f.eks. om bogføringspligt, kan indebære en pligt til at opbevare transaktionsoplysninger i længere tid."

---

60. Jfr. bilag 1.
61. Jfr. bilag 1.
62. Legal Aspects of ComputerRelated Crime in the Information Society, afsnit V.C.6.
63. Rapporten findes på http://www.fsk.dk./
64. Afsnittet: "Der bør være ensartede regler om lagring af transaktionsoplysninger".

Som nævnt i afsnit 2.2 foreligger der i EU et foreløbigt udkast til fælles aktion vedrørende børnepornografi på Internettet[(65)]. Udkastet peger bl.a. på en mulighed for at regulere Internetudbydere således, at trafikrelaterede data, hvor det er muligt, opbevares i det tidsrum, der kan være nødvendigt for at kunne sende disse data til de retsforfølgende myndigheder.

Det bemærkes, at minimumsprincippet vedrørende opbevaring af personidentificerbare oplysninger i EUdirektivet om behandling af personoplysninger[(66)] ikke er til hinder for, at der pålægges den registrerings og opbevaringspligt, der vurderes at være nødvendig for efterforskning af kriminalitet. Tilsvarende gælder med hensyn til de tiltag til beskyttelse af privatlivets fred, der er nævnt i EuropaParlamentet og Rådets direktiv 97/66/EF om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren[(67)].

Uanset hvilken opbevaringsperiode, der vurderes at være nødvendig, er det hensigtsmæssigt, at der etableres fastere principper, f.eks. i form af en lovregulering.

---

65. Gengivet i Rådets pressemeddelelse fra mødet 3.4. december 1998 (13673/98 (Presse 427)).
66. EuropaParlamentet og Rådets direktiv 95/46/EF af 24/10 1995 om beskyttelse af fysiske forbindelser i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, EFT 1995 L 281/31.
67. EFT 1998 L 24/1.

I afsnit 6 behandles spørgsmålet om retsplejelovens regler - herunder spørgsmålet om, hvornår reglerne om henholdsvis edition og indgreb i meddelelseshemmeligheden skal/bør kunne anvendes, og om der bør ske en udvidelse af området for, hvornår indgreb i meddelelseshemmeligheden kan benyttes.

I afsnit 2.4.2.1 er nævnt en sag om mulig kursmanipulation via Internettet, der illustrerer behovet for at kunne få logoplysninger. Tilsvarende gælder i en række andre sager. Som yderligere eksempel kan nævnes et anmeldelseskompleks fra december 1997, hvor en finsk virksomhed anmeldte, at der via en dansk Internetudbyder var hacket ind i deres anlæg, opnået fuld kontrol, viderehacket til andre maskiner rundt i verden og derefter rettet i logfiler og indlagt virus i processoren, så den måtte udskiftes. I Danmark anmeldte to virksomheder, at der via den finske virksomhed var hacket hos dem. Det er klart, at der er behov for logoplysninger fra den danske Internetudbyder[(68)] .

Med hensyn til de efterforskningsmæssige behov kan bl.a. følgende anføres:

Oplysninger om B-nummeret (det nummer, der ringes til) fastholdes i dag kun kortvarigt hos teleselskaberne, hvilket frembyder vanskeligheder for en efterfølgende efter forskning, idet der går tid til anmeldelse, visitering og opstart af efterforskning. Det vil også kunne være afgørende, at A-nummeret (det nummer, der ringes fra) og IPadressen videreføres og fastholdes i systemerne.

---

68. Arbejdsgruppen vedrørende datakriminalitet har drøftet de problemer, der kan være ved at anvende logudskrifter som bevis. Der var enighed om, at det kan være vanskeligt at føre (68)bevis for, at loggen er korrekt. Nogle af arbejdsgruppens medlemmer var af den opfattelse, at loggen generelt var et uegnet bevismiddel. Andre medlemmer anførte, at loggen i en række sager vil være egnet til at give oplysninger, så efterforskningen kan målrettes bedre, og at loggen i den endelige sag vil være understøttet af en række andre beviser. I nogle sager vil loggen være den eneste efterforskningsmulighed.

Ud fra et efterforskningsmæssigt synspunkt har det stor betydning, at Anummeret logges, uanset om den pågældende har benyttet muligheden for at blokere for visning af Anummeret hos den, der ringes til. Denne særlige mulighed må antages primært at skulle beskytte imod, at nummeret kan vises hos modtageren (indehaveren/brugeren af Bnummeret) og ikke at tage sigte på de registreringer, der kan være behov for i telekæden.

Det bemærkes, at i hvert fald én af de større Internetudbydere kun tilslutter til Internettet, hvis Anummeret samtidig registreres (hvilket sker, uanset om det er visningsbeskyttet eller ej).

Der er ud fra et efterforskningsmæssigt synspunkt ikke alene behov for at A og Bnummer samt IPadresse logges, men også for, at disse logoplysninger opbevares i et længere tidsrum, og endvidere for, at udbyderen logger, hvornår kunden har logget på og af.

I praksis har det under efterforskning vist sig, at teleselskabers og Internetudbyderes tidsangivelser i loggen har været upræcise. Det vil derfor set fra et efterforskningsmæssigt synspunkt være hensigtsmæssigt, hvis der stilles krav om, at der etableres et system med korrekt dansk realtid, f.eks. ved at serveren jævnligt synkroniseres med realtid. Hvis tidsregistreringer i logninger, der indgår i en efterforskning, ikke er korrekte, risikerer politiet at målrette efterforskningen mod forkerte personer.

Nogle sager har måttet opgives, fordi logningsinformationerne var mangelfulde, og der har været sager, der har været efterforsket mod forkerte sigtede (der i nogle tilfælde har været anholdt). Problemet har typisk været, at Anummeret manglede, og at tidsangivelsen var behæftet med for store usikkerhedsmarginer.

Spørgsmålet er, ikke mindst set i lyset af, at alle kan etablere sig som Internetudbydere, om der bør være mulighed for at straffe for manglende overholdelse af reglerne. Dette gælder f.eks. også i relation til hvidvasklovens krav til finanssektoren om ID-oplysninger og opbevaring af disse og af transaktionsoplysninger.

Det er endvidere efterforskningsmæssigt et problem, at almindeligt tilgængelige PCer (biblioteker, Internetcaféer m.v.) kan benyttes til at opnå anonymitet ved Internetanvendelsen. Det kunne derfor ud fra et efterforskningsmæssigt synspunkt være hensigtsmæssigt, hvis der ved benyttelse af almindeligt tilgængelige PCer blev stillet krav om identitetsregistrering og opbevaring heraf samt opbevaring af logoplysninger og om, hvem der har været på systemet hvornår.

Et tilsvarende efterforskningsmæssigt problem opstår, hvis en arbejdsgiver ikke logger oplysninger om

virksomhedens datatrafik, herunder brugeroplysninger, samt ved anvendelse af PCer på skoler, universiteter m.v.

Udvalget finder imidlertid, at det vil være urealistisk at tro, at det er muligt at gennemføre en effektiv regulering på disse områder[(69)]. Hvis efterforskningen viser, at en af disse PCer er blevet benyttet, og der ikke findes oplysninger om brugeren, må det i stedet forsøges via afhøringer at afgrænse den mulige brugerkreds. I disse situationer kan politiet i det mindste få indkredset, hvor en mere traditionel efterforskning skal sættes ind. Udvalget stiller derfor kun forslag om en regulering vedrørende udbydere, da oplysninger fra disse i mange tilfælde vil være den eneste mulighed for at udfinde det sted, der er handlet fra.

Udvalget finder, at der af efterforskningsmæssige grunde bør stilles krav om, at Internetudbydere og teleselskaber skal logge både A- og B-nummeret - for A-nummerets vedkommende uanset om den pågældende har benyttet muligheden for, at der ikke sker visning af A-nummeret. Endvidere bør udbyderen logge IPadresse for den, der ringer op, brugertid, tidspunkt for opkobling/nedkobling, opkoblingens længde og sessionstype (FTP/Telnet)[(70)]. Der bør tillige stilles krav om opbevaringsformat (læsbarhed). Derudover bør eventuelle kontooplysninger opbevares. Opbevaring af oplysninger skal ske i Danmark, hvis udbyderen er i Danmark, uanset om udbyderen er selvstændig eller filial af en udenlandsk virksomhed[(71)]

---

69. Arbejdsgruppen vedrørende datakriminalitet fandt ligeledes, at områderne ikke kunne reguleres effektivt.
70. Dette gælder, selv om udvalget er opmærksom på, at man remote kan anvende FTP/Telnet, dvs. fra en anden server end éns udbyders (så efterforskning vanskeliggøres eller umuliggøres på grund af indskydelse af en række udbydere), således at dette mest vil være en hjælp ved de mindre professionelle kriminelle.
71. Flere medlemmer af arbejdsgruppen vedrørende datakriminalitet har peget på, at der ved udvidede registrerings og opbevaringsregler samtidig bør stilles krav om foranstaltninger til beskyttelse mod uautoriseret adgang og manipulation.

Endvidere bør det tilstræbes, at det sikres, at korrekt dansk realtid registreres.

Opbevaringstiden for disse oplysninger bør set fra et efterforskningsmæssigt synspunkt ideelt være 5 år, svarende til bogføringsloven og hvidvaskloven, men da dette af praktiske grunde formentlig er for vidtgående så i hvert fald en periode, der muliggør efterforskning i de fleste sager, hvor der er behov for disse oplysninger.

Efter de for udvalget foreliggende oplysninger opbevares loggen vedrørende emails ofte i 6 måneder, mens der ikke i øvrigt er nogen fast praksis.

Udvalget har nærmere drøftet de forskellige hensyn, der kan tale for henholdsvis en længere og en kortere opbevaringstid. Efterforskningsmæssige hensyn taler for en frist på ikke under 1 år.

Ikke mindst i sager med ekstremt store datamæng der eller i sager, der efterforskningsmæssigt starter i et andet land, der derefter konstaterer, at der skal efterforskes også i Danmark, vil en kortere frist kunne betyde, at videre efterforskning umuliggøres. For langt de fleste sagers vedkommende vil en frist på 6 måneder imidlertid være tilstrækkelig.

Ved valg af en kortere frist tages et større hensyn til både privatlivets fred og de omkostninger,der påføres udbyderne. Særligt vedrørende hensynet til privatlivets fred tilsiger dette hensyn, at der logges mindst muligt, og at loggen opbevares i så kort tid som muligt, idet risikoen for, at oplysninger kommer på forkerte hænder, er større, jo længere opbevaringsperioden er.

Med hensyn til *retten* til at opbevare oplysninger kan det oplyses, at lovforslaget om behandling af personoplysninger (L 44 i folketingsåret 199899) indeholder regler herom. Lovforslaget har navnlig til formål at gennemføre direktivet om behandling af personoplysninger (95/46/EF). Lovforslaget blev ikke vedtaget i folketingssamlingen 199899, men agtes genfremsat i den kommende folketingssamling.

Det følger af lovforslagets § 5, stk. 5 (der har sin baggrund i direktivets artikel 6, stk. 1, litra e), at indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidspunkt end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles. Den dataansvarlige

skal efter lovforslagets anmeldelsesordning (lovforslagets kapitel 13) angive sletningsfristen i sin anmeldelse til Datatilsynet eller (hvis der ikke skal ske anmeldelse til Datatilsynet) opbevare dokumentation herfor.

Udvalget har på baggrund af drøftelserne valgt at anbefale en opbevaringsfrist på 6 måneder. Spørgsmålet om, hvorvidt udbyderen har ret til at opbevare logoplysninger ud over den pligtmæssige opbevaring i 6 måneder, må afgøres på grundlag af de ovenfor nævnte almindelige regler i registerlovgivningen[(72)].

Med hensyn til formen for reguleringen har udvalget indgående drøftet, om de ønskede registreringer og opbevaringen heraf ville kunne gennemføres ved en selvregulering.

Nogle medlemmer har henvist til, at der ikke er tale om en branche med etablerede traditioner med hensyn til selvregulering, eller med egne sanktionssystemer, ligesom der end ikke findes en registrering af Internetleverandører. Dette kan i sig selv tale mod en løsning med selvregulering, men dertil kommer, at der er tale om tiltag, der alene har efterforskningsmæssig interesse, og at efterforskningsmulighederne bør sikres gennem lovgivning herom. Dette svarer også til, at det f.eks. i § 3 h i lov om visse forhold på telekommunikationsområdet er fastsat, at udbydere af offentlige telenet og teletjenester uden udgift for staten skal sikre, at telecentralerne er indrettet således, at politiet kan få adgang til at foretage indgreb i meddelelseshemmeligheden.

---

72. Et flertal i arbejdsgruppen vedrørende datakriminalitet (Kim Aarenstrup, Mads Bryde Andersen, Jan Friis, Hans Jakob Paldam Folker, Michael Geskjær, Carsten Heilbuth, Ulla Høg, Helle Jahn, Jens Kruse Mikkelsen, Ronald Pedersen, Ole Stampe Rasmussen, Henrik OftebroSvendsen,) har på baggrund af arbejdsgruppens drøftelser fundet, at arbejdsgruppen skulle anbefale en opbevaringsfrist på 6 måneder. Et mindretal (Jan Carlsen) fandt, at der maksimalt skulle opbevares i 3 måneder med tvungen sletning efter udløbet af perioden.

Andre medlemmer har henvist til, at forpligtelsen bør kunne gennemføres ved selvregulering. Disse medlemmer mener ikke, at reglerne i lov om visse forhold på telekommunikationsområdet er egnede som retsgrundlag for den uoverskuelige mængde af Internetleverandører, for hvilke en forpligtelse af denne art får betydning.

Disse medlemmer har peget på, at der for tiden pågår intense bestræbelser på at gennemføre selvregulering indenfor Internetbranchen i en række henseender, og at man i tråd med den almindelige tendens i retning mod selvregulering bør give branchen mulighed for selv at tilvejebringe denne regulering, samtidig med at branchen alligevel skal tage stilling til spørgsmålet om, hvor længe man har *ret* til at opbevare sådanne logoplysninger. Når man vurderer udsigten til at gennemføre ønsket om opbevaring af logoplysninger i 6 måneder gennem selvregulering, må det i øvrigt tages i betragtning, at Internetleverandørerne kan have en økonomisk interesse i at følge en sådan praksis, eftersom udleveringen af de pågældende oplysninger sker mod betaling.

Et flertal i udvalget (Preben Bialas, Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Michael Clan, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Lau Kramer, Kirsten Mandrup, Annemette Møller, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder, at reguleringen skal ske ved lov[(73)].

Et mindretal i udvalget (Mads Bryde Andersen, Vagn Greve, Jesper Koefoed, Lars Bo Langsted) finder, at spørgsmålet så vidt muligt skal løses ved en selvregulering i branchen. Disse medlemmer er dog enige i en lovgivningsmæssig løsning, såfremt det viser sig, at reguleringsbestræbelserne ikke bærer frugt[(74)].

Der henvises til afsnit 7.3 vedrørende udvalgets forslag

---

73. I arbejdsgruppen vedrørende datakriminalitet fandt flertallet (Kim Aarenstrup, Jan Friis, Hans Jakob Paldam Folker, Michael Goeskjær, Ulla Høg, Helle Jahn, Jens Kruse Mikkelsen, Ronald Pedersen, Ole Stampe Rasmussen, Henrik OftebroSvendsen) ligeledes, at reguleringen burde ske ved lov.
74. I arbejdsgruppen vedrørende datakriminalitet fandt et mindretal (Mads Bryde Andersen, Jan Carlsen og Carsten Heilbuth) ligeledes, at selvregulering skulle anvendes. To af disse medlemmer (Mads Bryde Andersen og Carsten Heilbuth) var enige i en lovgivningsmæssig løsning, såfremt selvregulering viste sig ikke at være tilstrækkeligt.

5.2. Kryptering

Et særligt spørgsmål er, hvordan - og om - man kan sikre sig, at den teknologiske udvikling ikke sker på en måde, der reelt udelukker politiets efterforskning eller dog udelukker anvendelsen af visse særligt egnede metoder. Dette vanskelige spørgsmål er bl.a. behandlet af Mads Bryde Andersen og Peter Landrock i en artikel om "Kryptering og efterforskning"[(75)].

Den i afsnit 6.4 nævnte sendemastproblemstilling er for så vidt et eksempel herpå, men er dog primært et eksempel på, at lovgivningen ikke er tilpasset de faktiske situationer.

Et særligt vanskeligt og både nationalt og internationalt omdiskuteret område er anvendelsen af kryptering. Kryptering er på den ene side et uhyre velegnet middel til at beskytte informationer, og dermed også et meget velegnet middel til at forhindre kriminalitet. Samtidig kan en effektiv kryptering betyde, at politiet ikke reelt har mulighed for at efterforske. Forskellige lande har overvejet en række løsninger - fra forbud mod kryptering til kun at tillade bestemte krypteringsformer - men ingen har fundet på en velegnet løsning.

Spørgsmålet er også behandlet i flere rapporter fra regeringens ekspertudvalg om kryptering[(76)]. Dette udvalg behandler spørgsmålene om, hvorvidt det er muligt ved lovregulering eller på frivillig basis at nå frem til en anvendelse af kryptering, der sikrer en hensigtsmæssig balance mellem behovet for at anvende kryptering og behovet for at efterforske kriminalitet.

Udvalget vil pege på, at hvis det i en sag er sandsynligt, at væsentlige beviser kun forefindes i krypteret form, vil sagens øvrige bevisligheder - herunder indiciebeviser - formentlig blive tillagt relativt større vægt.

---

75. Juristen 1995, s. 306 ff.
76. Rapporterne er udgivet af Forskningsministeriet og findes på adressen http://fsk.dk.

Justitsministeriet Version 1.0 den 8. september 1999
Denne publikation findes på adressen: http://jm.schultzboghandel.dk

---

KAPITEL 6 - EFTERFORSKNING - RETSPLEJELOVENS REGLER

Spørgsmålene i dette afsnit vedrører især følgende problemstillinger:

a) Hvornår kan editionsreglerne anvendes?

b) Skal dele af det område, der i dag reguleres af reglerne om indgreb i meddelelseshemmeligheden, overflyttes til editionsområdet?

c) Hvem kan som indehaver af en telefon give samtykke til teleoplysninger?

d) Er der former for indgreb i meddelelseshemmeligheden, der ikke kan foretages efter de gældende regler, og skal der i givet fald skabes fornøden lovhjemmel?

e) Er der behov for at udvide området for, hvornår der kan gøres indgreb i meddelelseshemmeligheden?

Spørgsmål a) behandles i afsnit 6.1 om adgang til digitale meddelelser.

Spørgsmål b) behandles i afsnit 6.2 om lagrede teleoplysninger.

Spørgsmål c) behandles i afsnit 6.3 om teleoplysninger i henhold til samtykke.

Spørgsmål d) behandles i afsnit 6.4 om sendemaster.

Spørgsmål e) behandles i afsnit 6.5 om indgreb i meddelelseshemmeligheden i øvrigt.

De bestemmelser i retsplejeloven, der er relevante i denne forbindelse, er reglerne om edition og indgreb i meddelelseshemmeligheden. Disse regler er gengivet i uddrag i bilag 2.

Udvalget har drøftet, om der er - eller nødvendigvis er - forskel på reglerne om edition og reglerne om indgreb i meddelelseshemmeligheden med hensyn til, hvornår den sigtede bliver underrettet om et indgreb.

Som det fremgår, skal der ved indgreb i meddelelseshemmeligheden beskikkes en advokat, før retten træffer afgørelse. Efter retsplejelovens § 788 underrettes den, indgrebet er rettet mod, når indgrebet er afsluttet, men politiet har en frist på yderligere 14 dage til at anmode om, at underretning undlades eller udsættes. Underretning skal ikke gives til den sigtede, medmindre den sigtede er indehaver af telefonen eller lokaliteten eller direkte berørt af indgrebet.

Ved et retsmøde om en editionskendelse skal den sigtede ikke underrettes[(77)], men en eventuel forsvarer skal som hovedregel underrettes om retsmødet og er berettiget til at overvære det. Forsvareren må ikke uden rettens samtykke videregive oplysninger fra retsmødet.[(78)] Retsbogen, kendelsen og politirapporten om editionens gennemførelse indgår som almindelige bilag i straffesagen, og der kan kun i særlige situationer (hvis det undtagelsesvis er påkrævet på grund af hensynet til fremmede magter, til statens sikkerhed eller til sagens opklaring eller tredjemand) gives pålæg om, at oplysningerne ikke må videregives til den sigtede.[(79)]

Den, der skal pålægges edition, skal have lejlighed til at udtale sig før afgørelsen. Den pågældende kan underrette

den sigtede om indgrebet, medmindre der i særlige tilfælde gives pålæg efter retsplejelovens § 189 (hvorefter der kan pålægges et vidne tavshedspligt af hensyn til fremmede magter, til statens sikkerhed eller til opklaring af alvorlige forbrydelser). Bestemmelsen har i praksis også fundet anvendelse på selve editionshandlingen.

Ved den ændring af retsplejeloven, der er trådt i kraft 1/7 1999[(80)], er der ikke sket en ændring i retstilstanden omkring edition, men der er i § 804, stk. 2, jfr. § 803, stk. 1, indsat en klar henvisning til, at § 189 finder tilsvarende anvendelse.

---

77. Jfr. retsplejelovens § 748, stk. 1.
78. Jfr. retsplejelovens § 748, stk. 2.
79. Jfr. retsplejelovens § 745, stk. 4.
80. Lov nr. 229 af 21/4 1999 om ændring af retsplejeloven (Beslaglæggelse, edition m.v.).

6.1. Adgang til indholdet af digitale meddelelser

Digitale meddelelser kan teknisk sendes på forskellige måder, hvoraf den mest almindelige i dag er email. De nedenfor behandlede spørgsmål om email gælder tilsvarende for andre former for digitale meddelelser.

De behandlede spørgsmål vedrører alene, hvilket retsskridt der skal anvendes ved adgang til selve den digitale meddelelse. Oplysning om, hvem der er indehaver af en kendt email adresse, reguleres af reglerne om edition (på samme måde som adgangen til at få oplyst, hvem der er abonnent til et hemmeligt telefonnummer).

Spørgsmålet om adgang til email oplysninger opstår i flere situationer:

1) I relation til læst email, der forefindes på en PC ved ransagning.

2) I relation til ikke læst email, der kan indhentes via en PC i forbindelse med en ransagning, der omfatter denne.

3) I relation til adgang til læst email hos Internetudbyderen.

4) I relation til adgang til ikke læst email hos Internetudbyderen.

I *situation 1* er der ikke tvivl om, at de almindelige regler om ransagning og beslaglæggelse finder anvendelse.

I *situation 2* vil man i praksis sidestille situationen med den situation, hvor der ved ransagning findes et uåbnet brev. Her finder de almindelige regler om ransagning og beslaglæggelse ligeledes anvendelse, fordi brevet ikke er i et forsendelsesforløb, jfr. nedenfor og UfR 1992.373 V, der vedrørte et brev, der ikke var overgivet til forsendelse.

I Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter nævnes[(81)], at indgreb, der gennemføres inden kommunikationens påbegyndelse eller efter dens afslutning, bør bedømmes efter reglerne om ransagning og beslaglæggelse. Det siges videre:

- "Dette vil f.eks. gælde et brev eller anden forsendelse inden afsendelsen eller efter fremkomsten til adressaten, eller en båndoptagelse af en stedfunden samtale (eller et notat om samtalen), fundet hos en deltager. Det vil også gælde en kassette, som politiet ved en husundersøgelse finder i en automatisk telefonsvarer, og hvorpå personer, der har ringet til den pågældende telefon, har indtalt meddelelser, ligesom det vil gælde en telexstrimmel, som politiet finder siddende i en telexmaskine om morgenen, og hvorpå der til indehaveren af telexmaskinen i nattens løb er udskrevet meddelelser fra andre telexbrugere. Breve, der på posthuset er lagt i modtagerens postboks, men endnu ikke er afhentet af denne, er formentlig omfattet af reglerne om brevåbning, såfremt politiet ønsker med postvæsenets hjælp - og uden at modtageren gøres bekendt med indgrebet - at læse brevene. Hvis politiet derimod - f.eks. ved brug af en i bevaring taget boksnøgle - kan låse sig ind i postboksen, er man uden for reglerne om brevåbning, og politiet kan gå frem efter reglerne om beslaglæggelse. Virkningen af, at indgrebet bedømmes efter reglerne om ransagning og

beslaglæggelse, er dels, at betingelserne for indgrebets foretagelse er anderledes (og lempeligere), dels, at indgrebet ikke kan gennemføres hemmeligt."

En overførsel af disse regler på email vil betyde, at man er uden for området for indgreb i meddelelseshemmeligheden, når emailen er nået frem til adressatens adresse, hvilket må svare til, at der er adgang til emailen fra adressatens terminal.

I *situation 3 og 4* bliver spørgsmålet, om indgrebet får en anden karakter, hvis det gennemføres hos Internetudbyderen, således at oplysningerne ikke kan indhentes ved edition (der er det normale retsmiddel at bruge - i stedet for ransagning - hos helt uden for stående personer), men skal følge reglerne om indgreb i meddelelseshemmeligheden (telefonaflytning)[(82)].

Der er ved edition som ved indgreb i meddelelseshemmeligheden mulighed for, såfremt der er et særligt efterforskningsmæssigt behov, at den sigtede først på et senere tidspunkt underrettes om retsskridtet. Desuden kan der ved alvorlige forbrydelser pålægges den, mod hvem editionen er rettet, en strafbelagt tavshedspligt efter retsplejelovens § 189.

I den typiske situation vil den sigtede være bekendt med politiets efterforskning[(83)], idet formålet med editionen vil være at finde email, den sigtede har slettet, men som måske fortsat i et vist omfang kan fremfindes hos Internetudbyderen. Der vil således typisk være tale om læst email.

Der er enighed i udvalget om, at hvis der er tale om et fremadrettet indgreb, der har karakter af overvågning af korrespondancen, bør det være omfattet af regler om indgreb i meddelelseshemmeligheden. Dette er også lagt til grund i UfR 1999.178 VLK, hvor en kendelse om oplysninger om indgående email blev anset for omfattet af retsplejelovens § 780, stk. 1, nr. 1, om telefonaflytning.

Udvalget har delt sig i spørgsmålet om, hvorvidt dette også bør gælde for indgreb, der er bagudrettede.

Et flertal i udvalget (Mads Bryde Andersen, Preben Bialas, Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Vagn Greve, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Lars Bo Langsted, Kirsten Mandrup, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder ikke anledning til at foreslå ændringer i retsplejelovens regler om indgreb i meddelelseshemmeligheden.[(84)] Disse medlemmer finder således, at elektronisk post (e-post eller e-mail) ikke adskiller sig grundlæggende fra andre kommunikationsformer, der er omfattet af reglerne om indgreb i meddelelseshemmeligheden, og at der derfor ikke er grund til at give politiet en videre adgang til at foretage indgreb i kommunikation i form af elektronisk post.

---

81. S. 55.

82. Ifølge Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, s. 57, skal telekommunikation sidestilles med telefonsamtaler og ikke med postforsendelser

83. Medmindre de helt specielle regler om hemmelige ransagninger har fundet anvendelse, jfr. retsplejelovens § 799.

84. Et flertal i arbejdsgruppen vedrørende datakriminalitet (Mads Bryde Andersen, Jan Carlsen, Hans Jakob Paldam Folker, Carsten Heilbuth, Helle Jahn, Jens Kruse Mikkelsen, Ole Stampe Rasmussen) var af samme opfattelse som udvalgets flertal.

Efter disse medlemmers opfattelse må elektroniske breve sidestilles med traditionelle (fysiske) breve, jfr. retsplejelovens § 780, stk. 1, nr. 4 og 5. En sammenligning af kommunikationsforløbene ved henholdsvis traditionelle brevforsendelser og elektronisk post må efter disse medlemmers opfattelse føre til, at elektronisk post, der beror hos en Internetudbyder, må sidestilles med breve i en postboks, jfr. de ovenfor citerede forarbejder til de gældende bestemmelser.

Det er forudsat, at reglerne om indgreb i meddelelseshemmeligheden ikke omfatter indgreb, der gennemføres inden kommunikationens begyndelse eller efter dens afslutning. Reglerne finder således ikke anvendelse, hvis politiet kan skaffe sig meddelelsen ved et straffeprocessuelt tvangsindgreb mod afsender eller modtager af meddelelsen (jfr. reglerne om ransagning og beslaglæggelse). Hvis politiet derimod ønsker at skaffe sig meddelelsen med bistand fra

en kommunikationsformidler, må dette ske efter reglerne om indgreb i meddelelseshemmeligheden. Dette må gælde, uanset om kommunikationsformidleren er et telefonselskab, en postvirksomhed eller en udbyder af elektronisk kommunikation (herunder en Internetudbyder).

Kommunikationen kan efter de principper, der er lagt til grund ved udformningen af reglerne om indgreb i meddelelseshemmeligheden, kun siges at være afsluttet, når meddelelsen er kommet modtageren i hænde på en sådan måde, at politiet kan skaffe sig adgang til meddelelsen under en ransagning på modtagerens (fysiske) adresse eller ved anvendelse af midler beslaglagt under en sådan ransagning (en postboksnøgle eller en adgangskode til en elektronisk postkasse). Adgangskoden kan f.eks. være fast indkodet i Internetkommunikationsprogrammet (browseren) på den mistænktes computer, således at der ved opstart af programmet automatisk etableres forbindelse til den elektroniske postkasse hos Internetudbyderen. I denne situation vil det ikke være nødvendigt for politiet at gå frem efter reglerne om indgreb i meddelelseshemmeligheden.

Et mindretal i udvalget (Michael Clan, Annemette Møller) finder, at reglerne om edition bør anvendes, og at der ikke bør stilles de særlige krav, der gælder for indgreb i meddelelseshemmeligheden[(85)]

Der er tale om et indgreb, hvor oplysningerne - hvis de fortsat lå hos den sigtede - kunne tilvejebringes i medfør af de almindelige ransagningsregler. De henviser herudover til, at der ved den oprindelige stillingtagen i 1984 til datakommunikation er tænkt på en igang værende kommunikationsstrøm, hvor kommunikationen ikke er nået fysisk frem til den pågældende, og ikke på den særlige email struktur.

Disse medlemmer finder i øvrigt, at der altid bør beskikkes forsvarer i disse situationer, hvis det ikke allerede er sket.

Disse medlemmer lægger også vægt på, at den sigtede selv har valgt, at kommunikationen kan ske via kommunikationskanaler, hvor en tredjemand indgår i forløbet og besidder, hvad der kan sidestilles med en brevkopi. Situationen er meget atypisk i forhold til traditionelle postforsendelser, fordi Internetudbyderen straks har gjort forsendelsen tilgængelig for adressaten på dennes adresse. Der er således efter de principper, der gælder for f.eks. postforsendelser, telexkommunikation og meddelelser til telefonsvarere, ikke tale om et igangværende kommunikationsforløb. Når oplysningerne findes hos Internetudbyderen, er kommunikationen afsluttet. Ønsker man at føre særlig sikret korrespondance, må det ske ved sædvanlige lukkede forsendelser, der ikke er tilgængelige i andre systemer, eller der må anvendes særligt sikre krypteringsteknikker.

Det er også den fortolkning, der anlægges i retspraksis. F.eks. blev der i en sag om piratkopiering afsagt editionskendelse vedrørende email fra den sigtedes kendte email adresse og eventuelle andre adresser tilhørende ham, jfr. UfR 1998.1613 ØLK. Forsvareren gjorde både for byretten oglandsretten gældende, at der var tale om indgreb i meddelelseshemmeligheden, og at der derfor ikke kunne afsiges editionskendelse[(86)]. Byretten afsagde editionskendelse og anførte, at den hos Internetudbyderen beroende post ikke fandtes at være under forsendelse, men måtte ligestilles med post, der var kommet frem til den sigtedes bopæl. Østre landsret stadfæstede kendelsen af de af byretten anførte grunde.

Flertallets forslag er reelt ikke et forslag om ikke at ændre retstilstanden, men er et forslag om at begrænse de efterforskningsmuligheder, der, jfr. Østre landsrets kendelse, må antages at være i dag. Mindretallet finder mere principielt, at det ikke er acceptabelt at foreslå løsninger, der begrænser politiets nuværende muligheder for at efterforske og dermed begrænser mulighederne for at bekæmpe kriminalitet.

Der henvises til afsnit 7.4.

---

85. Et mindretal i arbejdsgruppen vedrørende datakriminalitet (Kim Aarenstrup, Jan Friis, Michael Goeskjær, Ulla Høg, Gunnar Kappel, Henrik OftebroSvendsen, Ronald Pedersen) var af samme opfattelse som udvalgets mindretal. De fandt dog, at forudsætningen for at anvende editionsreglerne må være, at der beskikkes en forsvarer i disse situationer, hvis det ikke allerede er sket.

86. Der ville på grund af sagstypen ikke have kunnet afsiges kendelse om indgreb i meddelelseshemmeligheden, idet piratkopiering ikke er en af de kriminalitetstyper, hvor der kan foretages sådanne indgreb, jfr. retsplejelovens § 781.

6.2. Teleoplysninger

Den første lovregulering af området skete ved lov nr. 202 af 11/6 1954, hvor der indsattes følgende bestemmelse som retsplejelovens § 750 a. Bestemmelsen blev ved lov nr. 243 af 8/6 1978 flyttet uændret til § 788:

- "*§ 788*. Det kan endvidere ved rettens kendelse bestemmes, at vedkommende telefonadministration skal meddele politiet oplysninger om, hvilke telefoner der i et bestemt tidsrum sættes eller har været sat i forbindelse med en bestemt telefon, når
- 1) der er påviselig grund til at antage, at de ønskede oplysninger vil være af betydning for opklaring af en af de i § 787, stk. 1, omhandlede forbrydelser[(87)], eller
- 2) det skønnes sandsynligt, at opklaring af en forbrydelse kun vil være mulig gennem de ønskede oplysninger, og foranstaltningen står i rimeligt forhold til forbrydelsens karakter, eller
- 3) det må antages, at det kun ved hjælp af de ønskede oplysninger er muligt at finde frem til den, der gør sig skyldig i gentagne fredskrænkelser som omhandlet i straffelovens § 265.
- *Stk. 2*. I påtrængende tilfælde kan politiet uden forudgående retskendelse træffe bestemmelse som i stk. 1 nævnt. § 787, stk. 3,[(88)] finder da tilsvarende anvendelse."

I Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter foreslog udvalget[(89)], at de dagældende regler blev ændret således, at der ved alle former for kriminalitet kunne gives teleoplysninger, hvis indehaveren samtykkede (den nugældende § 786, stk. 2, i retsplejeloven). Det nævntes endvidere[(90)], at teleoplysning hidtil kun havde været anvendt i beskedent omfang, og antagelig overvejende med indehaverens samtykke, men kunne tænkes at tiltrække sig større opmærksomhed i fremtiden også uden for samtykkesituationen.

Det fremgår af betænkningen[(91)], at udvalget foreslog et fælles kriminalitetskrav for alle indgreb i meddelelseshemmeligheden, hvilket for nogle af indgrebenes vedkommende betød strengere krav og for andre mildere krav, og at den særlige regel om fredskrænkelser ønskedes opretholdt i relation til teleoplysninger. For teleoplysningers vedkommende betød det fælles kriminalitetskrav, at den særlige mulighed for at få teleoplysninger, når det skønnedes sandsynligt, at opklaring af en forbrydelse kun ville være mulig gennem de ønskede oplysninger, og foranstaltningen stod i rimeligt forhold til forbrydelsens karakter, bortfaldt.

---

87. En række særligt opremsede forbrydelser samt forbrydelser med et strafmaksimum på 8 år eller derover.
88. Om underretning til retten med henblik på rettens godkendelse.
89. Betænkningen s. 61 f.
90. Betænkningen s. 63.
91. Betænkningen. s. 89 f.

Der opstod efterfølgende tvivl om, hvorvidt lagrede teleoplysninger skulle behandles efter reglerne om edition eller efter reglerne om indgreb i meddelelseshemmeligheden[(92)]. Østre landsret afsagde den 22/2 1991 kendelse om, at det var editionsreglerne, der skulle anvendes ved lagrede teleoplysninger. Vestre landsret anvendte i UfR 1992.638 VLK reglerne om teleoplysninger[(93)]. Dette er også lagt til grund i de i afsnit 6.4 omtalte sendemastkendelser.

Domstolene stiller i dag krav om, at både editionsreglerne og reglerne om indgreb i meddelelseshemmeligheden skal være opfyldt, før der kan afsiges kendelse vedrørende lagrede teleoplysninger[(94)].

Et flertal i udvalget (Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Vagn Greve, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Lars Bo Langsted, Kirsten

Mandrup, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder ikke anledning til at foreslå ændringer af retsplejelovens regler om indgreb i meddelelseshemmeligheden i form af teleoplysning[(95)].

Regler om indgreb i meddelelseshemmeligheden er udtryk for en afvejning af på den ene side hensynet til en effektiv kriminalitetsbekæmpelse og på den anden side hensynet til borgernes privatliv.

---

92. Strafferetsplejeudvalget havde dog anført, betænkningen s. 210, at der ikke ved udeladelsen af ordene "eller har været sat", der fandtes i den gældende § 788, var tilsigtet nogen realitetsændring.
93. I UfR 1989.870 VLK havde landsretten tidligere fundet, at der ikke var hjemmel i retsplejelovens § 780, stk. 1, nr. 3, til at give bagudrettede teleoplysninger.
94. Jfr. UfR 1993.1 HKK og UfR 1995.374 HKK. Det nævnes i lovforslag L 41 199899 om beslaglæggelse, edition m.v., FT 1997/98 A 828, i bemærkningerne til § 801, at der ikke med lovforslaget tilsigtes ændringer i denne retstilstand. Dette er også lagt til grund i lovforslag nr. L 202 199596 om datakriminalitet, FT 1995/96 A 4068, jfr. lovforslagets pkt. 5.3 og 5.4 og den nugældende bestemmelse i retsplejelovens § 781, stk. 3.
95. Et mindretal i arbejdsgruppen vedrørende datakriminalitet (Jan Carlsen, Hans Jakob Paldam Folker, Helle Jahn, Jens Kruse Mikkelsen, Ole Stampe Rasmussen) var af samme opfattelse som udvalgets flertal.

Efter flertallets opfattelse tilsiger hensynet til beskyttelse af borgernes fortrolige kommunikation med andre også en beskyttelse af oplysninger om, *hvem* der er kommunikeret med. Dette er også lagt til grund i Strafferetsplejeudvalgets betænkning nr. 1024/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter.

Uanset et indgreb i form af indhentning af teleoplysninger kan siges at indebære en vis mindre grad af integritetskrænkelse end de øvrige indgreb i meddelelseshemmeligheden, herunder telefonaflytning, bør der efter disse medlemmers opfattelse - henset til de ovenfor beskrevne modhensyn - ikke gives politiet adgang til teleoplysninger efter (de væsentlig lempeligere) regler om edition.

En anvendelse af reglerne om edition vil således bl.a. indebære, at indgrebet som udgangspunkt kan anvendes ved alle former for kriminalitet. En begrænsning vil alene følge af en proportionalitetsafvejning i den konkrete sag, dvs. om indgrebet står i misforhold til sagens betydning og den ulempe, som indgrebet kan antages at medføre. Efter reglerne om indgreb i meddelelseshemmeligheden kan indgrebet - bortset fra enkelte i loven særligt opregnede lovovertrædelser - kun anvendes ved efterforskning af lovovertrædelser, der efter loven kan straffes med fængsel i 6 år eller derover.

For så vidt angår spørgsmålet om en udvidelse af reglerne om indgreb i meddelelseshemmeligheden - en udvidelse der i givet fald også vil få betydning for teleoplysninger - henvises til afsnit 6.5 nedenfor.

Mindretallets forslag (omtalt nedenfor) indebærer, at også pålæg til teleselskabet om registrering af teleoplysninger i en periode frem i tiden skal behandles efter reglerne om edition. Disse regler indeholder - i modsætning til reglerne om indgreb i meddelelseshemmeligheden - ikke bestemmelser om frister for sådanne indgreb, idet editionsregler i alt væsentligt er tænkt anvendt på allerede eksisterende oplysninger. Editionsreglerne indeholder heller ikke regler om beskikkelse af advokat for indehaveren af pågældende telefon og foreslås af mindretallet kun ændret således, at der skal ske forsvarerbeskikkelse for den sigtede, der ikke behøver at være identisk med indehaveren af telefonen. Mindretallets forslag indebærer således på flere punkter en svækkelse af de retsgarantier, som de gældende regler er udtryk for.

Et mindretal i udvalget (Mads Bryde Andersen, Preben Bialas, Michael Clan, Annemette Møller) finder, at det ved teleoplysninger, der allerede lagres i anden sammenhæng, bør være en tilstrækkelig garanti, at der skal afsiges editionskendelse[(96)]. Oplysningerne er ikke mere følsomme end en række andre oplysninger, der kan udleveres efter editionsreglerne, og det kræver i dag ikke et særligt indgreb fra teleselskabernes side at fremskaffe oplysningerne.

---

96. Et flertal i arbejdsgruppen vedrørende datakriminalitet (Kim Aarenstrup, Mads Bryde Andersen, Jan Friis, Michael Goeskjær, Carsten Heilbuth, Ulla Høg, Gunnar Kappel, Henrik OftebroSvendsen, Ronald Pedersen) var af

samme opfattelse som mindretallet.

Disse medlemmer er enige om, at forudsætningen for at anvende editionsreglerne skal være, at der beskikkes en forsvarer i disse situationer, hvis det ikke allerede er sket.

Mindretallet vil pege på, at teleoplysninger er det mindst indgribende af de indgreb, der reguleres af reglerne om indgreb i meddelelseshemmeligheden. Ved indgrebet får politiet ikke kendskab til indholdet af kommunikationen, ligesom kommunikationen ikke unddrages modtageren.

Betydningen af at kunne få teleoplysninger er endvidere betydelig større ved den kriminalitet, der kendes i dag, end den var, da strafferetsplejerådet foreslog den ensartede regulering af området. Dette har også efterfølgende medført behov for, at der blev skabt en særlig hjemmel i retsplejelovens § 781, stk. 2 og stk. 3, til at indhente teleoplysninger i hackersager og telefonmisbrugssager. Også for så vidt angår sager om børnepornografi er der i dag behov derfor, ligesom der i øvrigt vil kunne være behov i sagstyper, hvor Internettet indgår, f.eks. i sager om piratkopiering eller kursmanipulation. Også på områder uden for den IT-relaterede kriminalitet - f.eks. i sager om EUsvig eller afgiftssvig i øvrigt - er der på grund af mange personers samvirke og indbyrdes kommunikation et større behov end tidligere for at få oplysninger af denne type.

Området for teleoplysninger, der tidligere blev registreret i forbindelse med teleselskabernes kontrol eller i forbindelse med efterforskning, har ændret sig væsentligt gennem de senere år. Der sker i dag automatisk en omfattende registrering, og kunder kan vælge at få alle samtaler specificeret (i hvilket tilfælde oplysningerne vil kunne findes ved en ransagning). Der er således i vidt omfang ikke tale om, at teleoplysninger indhentes i specielt øjemed, men alene om almindelig adgang til data, teleselskabet allerede besidder.

Det fremgår af Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, s. 62, jfr. s. 254 ff., at udgangspunktet var, at teleoplysninger forudsatte, at der blev etableret en fastholdeanordning. Teleoplysninger havde således en anden karakter, end tilfældet er i dag, idet oplysningerne som udgangspunkt ikke forelå, men kunne tilvejebringes ved særlige tekniske indgreb. I modsætning til i dag kunne alle derfor forvente, at teleoplysninger ikke fandtes, medmindre der blev foretaget et særligt indgreb, mens det i dag er almindelig viden, at oplysningerne altid registreres hos teleselskabet.

Teleoplysninger, der alene angiver, hvilke telefonnumre m.v. der har været forbindelse til, adskiller sig indgrebsmæssigt markant fra de mere indgribende tiltag som telefonaflytning m.v. Det kan derfor være nærliggende at overveje, om adgangen til sådanne oplysninger i de tilfælde, hvor de allerede

registreres i andet øjemed, skal flyttes fra reglerne om indgreb i meddelelseshemmeligheden, således at alene editionsreglerne finder anvendelse.

Konsekvensen af at benytte editionsreglerne er, at de særlige krav i retsplejelovens § 781 til kriminalitetens art og indgrebets afgørende betydning for efterforskningen ikke finder anvendelse.

Det bemærkes i den forbindelse, at domstolene også ved edition vurderer, om indgrebet konkret er nødvendigt, og at disse regler også finder anvendelse på andre følsomme oplysninger - f.eks. oplysninger, der skal indhentes fra den sigtedes pengeinstitut eller revisor[(97)].

Editionsreglerne anvendes normalt ved alle oplysninger, uanset hvor følsomme de er, når oplysningerne er tilgængelige hos den, editionen rettes mod, uden særlige tiltag. Domstolene er derfor også ved edition vant til, at der er forskel på følsomheden af de ønskede oplysninger, og at dette kan have betydning for, hvornår og i hvilket omfang en begæring om edition - f.eks. i et pengeinstitut, hos en revisor eller hos en advokat - skal imødekommes.

---

97. Ved lov nr. 229 af 21/4 1999 om ændring af retsplejeloven (Beslaglæggelse, edition m.v.) er den almindelige proportionalitetsgrundsætning blevet lovfæstet bl.a. ved, at den nye § 805, stk. 1, har fået følgende formulering: "Beslaglæggelse må ikke foretages, og pålæg om edition må ikke meddeles, såfremt indgrebet står i misforhold til sagens betydning og det tab eller den ulempe, som indgrebet kan antages at medføre."

De særlige regler om teleoplysninger afviger således i dag - hvor der ikke skal foretages særlige indgreb for at fremskaffe dem - fra de regler der i øvrigt gælder for selv meget følsomme oplysninger, som personer eller selskaber besidder som et almindeligt led i deres virksomhed.

Disse medlemmer vil i den forbindelse også pege på, at en vis overvågning af en mistænkts adfærd også helt uden retskendelse er tilladt i visse tilfælde. Det gælder for almindelig skygning og vil efter lovforslaget om beslaglæggelse, edition m.v. også efter lovreguleringen af observation[(98)] gælde for fotografering, iagttagelse med kikkert o.l. af personer, der befinder sig på et ikke frit tilgængeligt sted, hvis indgrebet må antages at være af væsentlig betydning for efterforskningen og den aktuelle lovovertrædelse kan medføre frihedsstraf. Mere indgribende observationsformer (fjernbetjente eller automatisk virkende overvågningsapparater) stilles der større krav til, herunder krav om kendelse, og sker denne observation i bolig eller andre husrum svarer kravene til de almindelige krav ved indgreb i meddelelseshemmeligheden.

---

98. Lovforslagets § 791 a.

Justitsministeriet har i lovforslaget taget stilling til, om pejling skulle lovreguleres. Det siges herom:

- "Ved *pejling* forstås, at politiet monterer pejleudstyr på en genstand, f.eks. en bil, som politiet formoder kan være lastet med narkotika, med henblik på at kunne følge genstandens bevægelser på afstand. For en umiddelbar betragtning har pejling visse lighedspunkter med observation og aflytning. Ved hjælp af teknisk udstyr opnår politiet en viden, som normalt forudsætter, at man fysisk er til stede.
- Pejling giver imidlertid ikke mulighed for at optage billeder eller aflytte samtaler. Pejling har nærmest karakter af en "skygning" under anvendelse af tekniske hjælpemidler. Indgrebet ses derfor ikke at være af så væsentlig og indgribende karakter, at det bør sidestilles med andre efterforskningsmidler, der er reguleret i retsplejeloven.
- På den baggrund finder Justitsministeriet ikke anledning til at foreslå en lovregulering af politiets anvendelse af pejling.
- Det bemærkes, at Vestre Landsret den 16. september 1996 har afsagt kendelse om pejling (gengivet i *Ugeskrift for Retsvæsen 1996, s. 1496*). Landsretten fandt, at monteringen og anvendelsen af elektronisk sporingsudstyr på en mistænkts bil (pejling) ikke var et straffeprocessuelt tvangsindgreb. Efter landsrettens opfattelse var der tale om skygning under anvendelse af tekniske hjælpemidler, og et sådant efterforskningsskridt krævede ikke lovhjemmel og dermed heller ikke forudgående indhentelse af rettens kendelse."

Mindretallet vil særligt fremhæve, at der bl.a. ved afgørelsen af, hvor indgribende et indgreb pejling er, lægges vægt på, at der ikke er mulighed for at optage billeder eller aflytte samtaler. Teleoplysninger - der også efter disse medlemmers forslag fortsat vil kræve retskendelse - er ligeledes karakteriseret ved, at man kan følge den mistænktes bevægelser (ikke som ved peling fysiske bevægelser, men bevægelser på telekommunikationsnet), men ikke får andre personlige oplysninger i forbindelse med indgrebet.

Der henvises til afsnit 7.5 vedrørende udvalgets forslag.

6.3. Teleoplysninger i henhold til samtykke m.v.

[Forside] [Indholdsfortegnelse] [Gå til bund] [Forrige dokument] [Næste dokument]

6.3. Teleoplysninger i henhold til samtykke m.v.

Efter retsplejelovens § 786, stk. 2, kan der i alle sagstyper gives teleoplysninger i henhold til retskendelse, hvis indehaveren af apparatet meddeler samtykke.

I UfR 1996.18 VLK fandt Vestre landsret det efter forarbejderne til bestemmelsen betænkeligt at antage, at bestemmelsen havde haft tilfælde for øje, hvor der var tale om en offentlig telefon. De to teleselskaber kunne

derfor ikke give samtykke til at udlevere udskrifter over de telefonnumre, der var blevet kontaktet ved hjælp af et telekort.

- Sagen vedrørte indbrudstyverier, og der var under ransagning hos den sigtede fundet et telekort. Et vidne havde oplyst, at han havde set den sigtede telefonere fra en korttelefonboks og set, at der umiddelbart efter var ankommet en varebil til den sigtedes bopæl, hvor bilen blev læsset med nogle papkasser. Anklageren henviste til, at der var bestemte grunde til at antage, at der med telekortet var blevet kontaktet personer, som kunne mistænkes for hæleri. (Betingelserne for indgreb i meddelelseshemmeligheden var ikke opfyldt, idet sagen vedrørte tyveri, der dengang ikke gav mulighed for teleoplysninger, og mistanke om hæleri, hvis omfang der ikke kunne siges noget om).

Såfremt teleoplysninger helt eller overvejende bliver omfattet af editionsreglerne, vil en editionskendelse i denne situation rette sig til teleselskaberne.

Et flertal i udvalget (Preben Bialas, Susan Bramsen, Bent Carlsen, Vagn Greve, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Kirsten Mandrup, Lene Nielsen, Henrik Rothe) finder ikke, at teleselskaberne skal kunne meddele samtykke ved offentlige telefoner[(99)].

---

99. Et mindretal i arbejdsgruppen vedrørende datakriminalitet (Hans Jakob Paldam Folker, Helle Jahn, Jens Kruse Mikkelsen, Ole Stampe Rasmussen) var af samme opfattelse.

Bestemmelsen i retsplejelovens § 786, stk. 2, bygger på det synspunkt, at en telefonabonnent ikke i forhold til telefonselskabernes tavshedspligt kan anses for "uvedkommende" med hensyn til oplysninger om, hvem der ringer til abonnenten, og at der ikke er en sådan beskyttelsesværdig interesse i hemmeligholdelse hos personer, der kalder et andet telefonnummer, at udlevering af disse oplysninger til politiet med samtykke fra indehaveren af denne telefon bør omfattes af reglerne om indgreb i meddelelseshemmeligheden, jfr. Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, s. 62. I retspraksis er det fastslået, at bestemmelsen også finder anvendelse på oplysninger om udgående opkald fra en bestemt telefon, jfr. UfR 1996.169 ØLK.

Efter disse medlemmers opfattelse kan et telefonselskab ikke siges at have rådighed over en offentlig telefon på samme måde som en privat telefonabonnent har rådighed over sin telefon. Der er derfor ikke samme anledning til at give telefonselskabet adgang til med sit samtykke at fravige reglerne om indgreb i meddelelseshemmeligheden. Hvis man låner en privat telefon (eller stjæler en mobiltelefon) må man være indstillet på, at den pågældende telefonabonnent modtager udførlige samtalespecifikationer i forbindelse med telefonregningen. Benyttelsen af en offentlig telefon kan nærmest betragtes som et "ad hocabonnement", hvor man mod vederlag får (en begrænset) adgang til at benytte telefonnettet. Et indgreb mod en bruger af en offentlig telefon bør derfor sidestilles med et indgreb imod en privat telefonabonnent. De særlige hensyn, der i sin tid begrundede bestemmelsen i § 786, stk. 2, kan efter disse medlemmers opfattelse ikke udstrækkes til også at begrunde en lignende regel for offentlige telefoner.

Udvalget finder i øvrigt, at formuleringen i retsplejelovens § 786, stk. 1, bør tilpasses den terminologi, der anvendes i dag vedrørende post og televirksomhed.

Et mindretal i udvalget (Mads Bryde Andersen, Hans Henrik Brydensholt, Jørgen Christiansen, Michael Clan, Alexander Houen, Lars Bo Langsted, Annemette Møller) finder, at teleselskaberne - uanset hvilket regelsæt der finder anvendelse - skal kunne meddele samtykket, når der er tale om offentlige telefoner. Der er enighed om, at der skal beskikkes en forsvarer i disse situationer, hvis det ikke allerede er sket[(100)].

Disse medlemmer har i den forbindelse lagt vægt på, at der ikke kan være nogen berettiget forventning om, at indehaveren af en telefon ikke kan give politiet (adgang til) oplysning om, hvilken brug der har været gjort af telefonen. Med den retstilstand, der er i dag vedrørende indgreb i meddelelseshemmeligheden, betyder det, at der ved en lang række kriminalitetsformer ikke er mulighed for at få adgang til disse allerede registrerede oplysninger, hvis en offentlig telefon er benyttet (i modsætning til f.eks. en telefon, der ejes af en restaurant).

Spørgsmålet om samtykke ved offentlige telefoner er opstået som en konsekvens af, at oplysningerne i dag

registreres. Det er af samme grund ikke behandlet i Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, der, jfr. betænkningens s. 61 ff., især tager udgangspunkt i, at hovedområdet for teleoplysninger er truende, injurierende eller på andre måder generende telefonopkald til en privat abonnent. Udvalgets forventninger til, at indgrebet i fremtiden vil tiltrække sig større opmærksomhed, er især knyttet til, at telefonaflytninger er ressourcekrævende, og at det i en del sager kunne være af betydning for politiet at få oplyst, om bestemte telefoner, til hvis indehavere man har mistanke i sagskomplekset, bliver sat i forbindelse med hinanden.

I den ovenfor nævnte kendelse (UfR 1996.169 ØLK) blev det lagt til grund, at indehaveren af en stjålen mobiltelefon kunne meddele samtykke efter retsplejelovens § 786, stk. 2. Denne kendelse understøtter efter disse medlemmers opfattelse det synspunkt, at det formelle ejerskab er tilstrækkeligt til, at man er samtykkeberettiget, også når samtalerne utvivlsomt er abonnenten helt uvedkommende.

Et af udvalgets medlemmer (Erik Overgaard) har ikke taget stilling til, hvilken løsning der skal vælges.

Der henvises til afsnit 7.6 vedrørende udvalgets forslag.

[100.] Et flertal i arbejdsgruppen vedrørende datakriminalitet (Kim Aarenstrup, Mads Bryde Andersen, Jan Carlsen, Jan Friis, Michael Goeskjær, Carsten Heilbuth, Ulla Høg, Gunnar Kappel, Henrik OftebroSvendsen, Ronald Pedersen) var af samme opfattelse.

6.4. Særligt om sendemaster

En særlig variant af teleoplysninger er de såkaldte "masteoplysninger". Hvor den typiske situation ved teleoplysninger er, at der ønskes oplysninger vedrørende bestemte telefonnumre, er situationen ved masteoplysninger den, at der ønskes oplysninger om alle telefoner, der i et givet tidsrum har benyttet en bestemt sendemast.

Indgrebet er primært relevant i store sager om grove kriminalitetsformer, f.eks. sager om rockerdrab, ildspåsættelser o.l. Som et eksempel, hvor der kan være behov for indgreb af denne type, kan også nævnes en ny sag, hvor falske politifolk bortførte en chauffør og en lastbil med 7 mio. cigaretter.

I udtalelser i anledning af nedenfor nævnte afgørelse i UfR 1997.1021 H om behovet for at kunne få sendemastoplysninger er også peget på, at der kan være behov for masteoplysninger i forbindelse med terrorattentater eller igangværende gidselsituationer.

Udgangspunktet i de sager, hvor der er behov for indgrebet, er således, at et antal ukendte personer, der har begået en alvorlig forbrydelse, vurderes nødvendigvis at måtte have kommunikeret med hinanden umiddelbart før og efter gerningen, muligvis via mobiltelefoner. En mulighed, måske den eneste, for at komme opklaringen nærmere er at få en logudskrift fra sendemasten nærmest gerningsstedet for et tidsrum eksempelvis fra 1 time før til ½ time efter forbrydelsen for at kunne se, hvilke telefoner der har kommunikeret via masten i det relevante tidsrum.

Masteoplysninger er ikke selvstændigt reguleret i retsplejelovens § 780, men de udgør en særlig form for teleoplysninger, idet det alene er et spørgsmål om at få oplysninger om teleforbindelser og ikke om indholdet af kommunikationen.

Som eksempler på sendemastkendelser kan nævnes følgende, hvoraf 3 har været behandlet af Højesteret:

- *Højesterets kendelse af 28/6 1994*[(101)]
  Sagen vedrørte efterforskning i forbindelse med mistanke om grov narkotikakriminalitet og omfattende hæleri. Der blev i den forbindelse anmodet om kendelse om aflytning af samtaler, der foregik via mobiltelefon fra en bestemt ejendom, samt teleoplysninger vedrørende kommunikation med de pågældende mobiltelefoner.
  Byretten afsagde kendelse herom under henvisning til retsplejelovens § 780, stk. 1, nr. 1, nr. 2 og nr. 3. Østre Landsret ophævede kendelsen under henvisning til, at der ikke var hjemmel til at foretage

telefonaflytning af ikke nærmere angivne mobiltelefoner eller til at foretage aflytning af telefoner inden for et angivet afgrænset område.
Højesteret stadfæstede byrettens afgørelse med følgende begrundelse: "Højesteret finder, at bestemmelserne i retsplejelovens § 780, stk. 1, nr. 1, nr. 2 og nr. 3, efter deres ordlyd omfatter de her omhandlede indgreb. Indgrebene kan ikke anses for mere vidtgående end de tilfælde af aflytning, der traditionelt henføres under bestemmelserne, og der findes ikke grundlag for gennem en indskrænkende fortolkning at afskære anvendelsen af disse efterforskningsskridt. Idet betingelserne efter retsplejelovens § 781, stk. 1, efter det oplyste er opfyldt, tager Højesteret derfor anklagemyndighedens påstand til følge."

[101.] Kendelsen er ikke trykt i UfR, men Højesterets afgørelse er gengivet i note 1 til UfR 1996.1339 HKK.

UfR 1996.1339 HKK

Der blev anmodet om kendelse bl.a. om oplysning om, hvilke kommunikationsapparater der fra en dag kl. 22.00 til næste dag kl. 06.00 havde været sat i forbindelse med hinanden under aktivering af sendemaster, der geografisk dækkede en bestemt adresse og en radius på 1 km. herfra.
Byretten afsagde kendelse herom.
Vestre landsret ophævede kendelsen herom med følgende begrundelse: "Således som begæringen er udformet, vil indgrebet omfatte ikke telefoner m.v., der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat, men telefoner m.v., der sættes i forbindelse med en helt ubestemt kreds af telefoner eller andre kommunikationsapparater i et større område. Da et sådant indgreb ikke har hjemmel i retsplejelovens § 780, stk. 1, nr. 3, kan begæringen ikke tages til følge, og den påkærede kendelse om udlevering af de anførte optegnelser ophæves derfor."
Højesteret stadfæstede byrettens afgørelse bl.a. under henvisning til Højesterets kendelse af 28/6 1994.

Byretskendelse af 29/11 1996

- Sagen vedrørte efterforskning af drabsforsøg i forbindelse med skud mod 2 rockere. Der blev i den forbindelse anmodet om kendelse om oplysning om, hvilke kommunikationsapparater der den aktuelle dag mellem kl. 00.01 og 06.00 havde været sat i forbindelse med hinanden under aktivering af sendemaster, der geografisk dækkede den gade, hvor der var skudt, og en radius på 2 km. herfra. Byretten afsagde kendelse om dette indgreb, men begrænsede radius til 1 km.

Vestre landsrets kendelse af 21/12 1996

- Sagen vedrørte efterforskning af brandstiftelse. Der blev i den forbindelse anmodet om kendelse om oplysning om, hvilke kommunikationsapparater der en dag fra kl. 23.00 til næste dag kl. 01.00 og en anden dag fra kl. 01.00 til kl. 03.00 havde været sat i forbindelse med hinanden under aktivering af sendemaster, der geografisk dækkede et område, der var afgrænset af 3 gader.
  Byretten afsagde kendelse om det ønskede indgreb, og Vestre landsret stadfæstede kendelsen.

UfR 1997.1021 H

- Sagen vedrørte efterforskning i forbindelse med en bombe, der var placeret i en gade. Der blev anmodet om kendelse om oplysning om, hvilke kommunikationsapparater der fra en dag kl. 18.00 til næste dag kl. 06.00 havde været sat i forbindelse med hinanden under aktivering af sendemaster, der geografisk dækkede en bestemt adresse og en radius på 1 km. herfra.
  Byretten afslog med følgende begrundelse: "Da det ønskede indgreb vedrører et meget vidt og ubestemt antal telefoner, findes der ikke bestemte grunde til at antage, at der fra de pågældende telefoner er givet meddelelse af betydning for efterforskningen til eller fra mistænkte for forsøg på manddrab. Som følge heraf findes betingelserne i retsplejelovens § 781, stk. 1, nr. 1 og nr. 2, ikke opfyldt."
  Østre landsret afsagde den ønskede kendelse under henvisning til Højesterets afgørelser fra 1994 og 1996.
  For Højesteret blev det oplyst, at indgrebet ifølge teleselskaberne ville omfatte 25.00030.000 samtaler.
  Højesteret stadfæstede byrettens kendelse under henvisning til de nu foreliggende oplysninger om den manglende mulighed for nærmere afgrænsning af samtaleregistreringer vedrørende mobiltelefoner.[(102)] [(103)],

Afgørelsen fra 1997, der var en ændring af Højesterets tidligere praksis, har betydning både i relation til telefoner og i relation til trådløs datatransmission.

---

102. I note 1 til kendelsen henvises til en artikel af Ole Unmack Larsen i Juristen 1997 s. 35 ff. "Mobiltelefoner og retsplejelovens § 780, stk. 1, nr. 1, nr. 2 og nr. 3". I artiklen er bl.a. en beskrivelse af antallet af radioceller, daglige samtaler pr. celle og masternes rækkevidde.

103. Rigsadvokaten henviste i sit kæreskrift bl.a. til, at aflytning af en offentlig telefon i en lufthavn eller på en banegård ligeledes vil kunne omfatte en større personkreds og tillige vil være mere indgribende, idet politiet får kendskab til samtalens indhold

---

Rigsadvokaten har på baggrund af denne kendelse anbefalet over for Justitsministeriet, at der skabes lovhjemmel til at indhente sådanne teleoplysninger. Rigsadvokaten har i forbindelse hermed fremhævet, at masteoplysninger er et vigtigt efterforskningsmiddel, og at den utilsigtede krænkelse af en større personkreds, der af tekniske årsager kan blive omfattet, er af relativ beskeden karakter, ligesom der er pligt til snarest at destruere oplysninger, der er uden efterforskningsmæssig betydning. Endvidere kan indgrebet kun foretages under retlig kontrol og under iagttagelse af de almindelige proportionalitetsregler.

Det fremgår af Justitsministeriets lovforslag om beslaglæggelse, edition m.v.[(104)], at Justitsministeriet har overvejet i forbindelse med dette lovforslag at medtage et forslag, der skaber hjemmel til indhente de teleoplysninger, der er omtalt i Højesterets 1997kendelse, men at Justitsministeriet finder, der er behov for nærmere overvejelser navnlig om, hvordan en sådan hjemmel skal udformes for at tage højde for den teknologiske udvikling. Justitsministeriet har derfor fundet det rigtigst, at spørgsmålet indgår i overvejelserne i udvalget om økonomisk kriminalitet og datakriminalitet.

Østre landsret har ved en kendelse af 13/11 1998, jfr. UfR 1999.320 Ø, stadfæstet en kendelse om, at der kunne indhentes masteoplysninger i en sag om forsøg på manddrab. Landsretten lagde vægt på, at situationen adskilte sig fra den situation, der var aktuel ved Højesterets kendelse i 1997, idet der forelå oplysninger om én kortvarig telemeddelelse modtaget på en bestemt lokalitet, således at denne meddelelse skulle afgrænses over for et forholdsvis begrænset antal meddelelser eller samtaler. (Det drejede sig om 998 opkald over en periode på 50 minutter).

Som nævnt i afsnit 2.2 udfærdigede EU den 17/1 1995 en resolution om lovlig aflytning af telekommunikation[(105)]. Bl.a. bør de retshåndhævende myndigheder have mulighed for at kunne få så nøjagtig oplysning som mulig om mobile abonnenters geografiske placering inden for nettet.

Udvalget er enig i Rigsadvokatens betragtninger. Udvalget finder derfor, at der bør tilvejebringes en klar hjemmel til indgreb af denne type. For at sikre, at der tages højde for den teknologiske udvikling, bør formuleringen ikke specifikt vedrøre masteoplysninger, men vedrøre teleoplysninger, der ikke kan specificeres på kendelsestidspunktet.

De medlemmer af udvalget, der i øvrigt finder, at editionsreglerne frembyder tilstrækkelig garanti ved lagrede teleoplysninger, er enige med de øvrige medlemmer i, at masteoplysninger og tilsvarende oplysninger skal behandles efterindgreb i meddelelseshemmeligheden, da der er tale om meget bredere indgreb.

Udvalget finder herudover, at reglerne skal opfylde kravene til særligt kvalificere indgreb i meddelelseshemmeligheden[(106)].

Der henvises til afsnit 7.5 vedrørende udvalgets forslag.

---

104. FT 1998/99 A 828.

105. Jfr. bilag 1.

106. Der var også enighed i arbejdsgruppen vedrørende datakriminalitet om en regulering som den af udvalget foreslåede.

6.5. Indgreb i meddelelseshemmeligheden i øvrigt

6.5. Indgreb i meddelelseshemmeligheden i øvrigt

Som nævnt i afsnit 2.1 ændredes retsplejelovens § 781 i 1996[(107)] således, at der blev adgang til telefonaflytning og teleoplysninger i hackersager[(108)] og adgang til teleoplysninger i sager om overtrædelse af straffelovens § 279 a eller § 293, stk. 1, begået ved anvendelse af en telekommunikationstjeneste.

- Det siges i lovforslaget[(109)] om baggrunden for denne ændring bl.a.:
- "For så vidt angår spørgsmålet om *indgreb i meddelelseshemmeligheden* kan Justitsministeriet tilslutte sig Strafferetsplejeudvalgets principielle synspunkt (jf. bet. 1023/1984, s. 5152), hvorefter der generelt bør sættes snævre grænser for politiets indgreb i meddelelseshemmeligheden.
- Som også fremhævet af Strafferetsplejeudvalget er der imidlertid nye kriminalitetsformer, hvor sædvanlige efterforskningsmetoder ikke rækker til.
- Der må derfor foretages en afvejning mellem på den ene side den ulempe eller skade, som indgrebet er forbundet med for samfundet og for den enkelte, som indgrebet rammer, og på den anden side den betydning, indgrebet har som middel til opklaring og bekæmpelse af kriminalitet, samt kriminalitetens art og grovhed.
- Efter Justitsministeriets opfattelse har udviklingen siden 1985 - hvor Folketinget senest drøftede spørgsmålet om indgreb i meddelelseshemmeligheden over for "hackerkriminalitet" - vist behov for at anvende dette efterforskningsmiddel over for kriminalitet, der begås ad elektronisk vej, og hvor mere traditionelle efterforskningsmetoder derfor ikke er anvendelige. "Hackerkriminalitet" begås således typisk ved, at gerningsmanden fra sin egen pc'er og gennem et modem kobler sig på det offentlige telefonnet eller eventuelt et datanet og derfra gennem forurettedes modem eller en tilsvarende "indgang" skaffer sig adgang til forurettedes dataanlæg.
- Ganske vist er det som nævnt ovenfor i pkt. 4.2.2. muligt at foretage teleoplysning med samtykke fra en forurettet, jf. retsplejelovens § 786, stk. 2. Den fremgangsmåde er imidlertid langt fra altid tilstrækkelig. Der kan således være forurettede, der modsætter sig politiets indblanding, jf. herved ovenfor pkt. 4.1. om påtalespørgsmålet. Langt vigtigere er det imidlertid, at politiet når det f.eks. med samtykke fra en forurettet er lykkedes at finde en mistænkt ofte vil have behov for at foretage teleoplysninger med udgangspunkt i den mistænktes telefon m.v. for at belyse omfanget af hans mulige kriminelle aktivitet over for andre ofre. Hertil kommer yderligere, at der kan være behov for telefonaflytning; ikke så meget med hensyn til samtaler som med hensyn til datakommunikation for derigennem at klarlægge den nærmere karakter af den strafbare handling, dvs. hvad den mistænkte foretager sig med hensyn til fremmede dataanlæg.
- Det er på den baggrund Justitsministeriets opfattelse, at der i sager om overtrædelse af straffelovens § 263, stk. 2, og § 263, stk. 3, jfr. stk. 2, bør være mulighed for at foretage telefonaflytning og teleoplysning, uanset kriminalitetskravet ikke er opfyldt. Derimod ses der ikke at være anledning til at give mulighed for at foretage anden aflytning, brevåbning eller brevstandsning.

¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿

¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿

¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿¿

---

107. Ved lov nr. 388 af 22/5 1996.
108. Straffelovens § 263, stk. 2 og 3.
109. FT 1995/96 A 4068.

- På lignende måde som ved "hackerkriminalitet" begås også "tyveri af telefontid" ved hjælp af telefon eller anden telekommunikationstjeneste. Derfor er de mere traditionelle efterforskningsmetoder ikke anvendelige. For at opklare disse lovovertrædelser er der således behov for at foretage teleoplysning, ikke blot med udgangspunkt i en forurettets telefon m.v., jf. retsplejelovens § 786, stk. 2, (omtalt ovenfor i pkt. 4.2.2. og

4.3.), men også med udgangspunkt i den mistænktes telefon m.v.
- Det er på den baggrund Justitsministeriets opfattelse, at der i de omhandlede sager bør være mulighed for at foretage teleoplysning, uanset at kriminalitetskravet ikke er opfyldt. De almindelige regler om mistankekrav, indikationskrav og proportionalitetskrav vil fortsat finde anvendelse. ¿."

Bestemmelsen blev yderligere udvidet i 1997[(110)], så også grov vold, fareforvoldelse efter straffelovens § 252, stk. 1, grove tyverier og menneskesmugling (udlændingelovens § 59, stk. 3) blev omfattet.

Det siges i lovforslaget[(111)] om baggrunden for denne ændring bl.a.:

- "Justitsministeriet kan tilslutte sig det principielle synspunkt, som både af Strafferetsplejeudvalget og Folketinget blev lagt til grund ved udformningen af de nugældende regler om indgreb i meddelelseshemmeligheden, og hvorefter der generelt bør sættes snævre grænser for politiets indgreb i meddelelseshemmeligheden.
- Reglerne om politiets efterforskningsmidler må imidlertid også ses i lyset af de samfundsmæssige forhold og den udvikling, som sker med hensyn til kriminalitetens karakter.
- Der må derfor - når nye kriminalitetsformer og omfanget af disse giver anledning til det - foretages en afvejning mellem på den ene side den ulempe eller skade, som indgrebet er forbundet med for den, der udsættes for indgrebet, og på den anden side den betydning, indgrebet har som middel til opklaring og bekæmpelse af kriminalitet, og kriminalitetens art og grovhed.
- Ved denne afvejning indgår det således bl.a., om kriminaliteten har en karakter, som er egnet til at blive afdækket af politiet ved hjælp af indgreb i meddelelseshemmeligheden.
- Det er Justitsministeriets opfattelse, at indgreb i meddelelseshemmeligheden i mange tilfælde vil være et relevant efterforskningsmiddel i forhold til kriminalitet, som er kendetegnet ved, at den begås af flere personer i forening.
- Justitsministeriet finder på den baggrund, at der bør være adgang til indgreb i meddelelseshemmeligheden for kriminalitetsformer, der ofte begås af en flerhed af personer, i det omfang, der er tale om kriminalitet af en så alvorlig karakter, at sådanne indgreb er velbegrundede."

---

110. Ved lov nr. 411 af 6/10 1997.
111. FT 1996/97 A 2475

Ved samme lovændring indsattes bestemmelsen i retsplejelovens § 789, stk. 3, der brød med det hidtidige princip i bestemmelsens stk. 2 om, at tilfældighedsfund i forbindelse med indgreb i meddelelseshemmeligheden ikke måtte anvendes som bevis i retten vedrørende kriminalitet, der ikke ville have kunnet danne grundlag for det pågældende indgreb. Efter den nye bestemmelse kan retten tillade, at beviset anvendes, hvis andre efterforskningsskridt ikke er egnede til at sikre bevis i sagen, og sagen angår en lovovertrædelse, der kan medføre fængsel i 1 år og 6 måneder eller derover.

Det kan mere generelt overvejes, om disse efterhånden mange undtagelser fra hovedreglen om, at der skal være mulighed for fængsel i 6 år, er udtryk for, at bestemmelsen ikke længere er tidssvarende.

Særlig for IT-relateret kriminalitet er der i dag et efterforskningsmæssigt behov for en yderligere udvidelse af området med henblik på bekæmpelse af kriminalitet via Internettet, BBS'er o.l.

Det kan bl.a. fremhæves, at ved groft bedrageri, der f.eks. begås via Internetkommunikation, er der hjemmel til indgreb i meddelelseshemmeligheden. Det er imidlertid ikke sikkert, at man i den indledende efterforskningsfase kan give et rimeligt kvalificeret skøn over omfanget, hvilket efter omstændighederne betyder, at sådanne indgreb ikke kan anvendes. Dette er også baggrunden for, at telefonmisbrug, der omfattes af databedrageribestemmelsen i straffelovens § 279 a, i 1996 fik selvstændig hjemmel til teleoplysninger[(112)], uanset groft databedrageri opfylder kriminalitetskravet i retsplejelovens § 781, stk. 1.

F.eks. kan sager vedrørende overtrædelse af straffelovens § 235 om børnepornografi ikke efterforskes effektivt med de nugældende regler. Tilsvarende gælder for en række andre sager, f.eks. sager om insiderhandel, kursmanipulation og piratkopiering. Det gælder også industrispionage i forbindelse med husfredskrænkelser, der ellers var omfattet af forslaget i Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets

indgreb i meddelelseshemmeligheden og anvendelse af agenter og var medtaget i lovforslaget[(113)].

Udvalget finder at der i det omfang, hvor der er særligt behov herfor, bør skabes adgang til indgreb i meddelelseshemmeligheden ved IT-relateret kriminalitet. En bestemmelse herom bør dog begrænses til de efterforskningssituationer, hvor der reelt -som ved hacking og telefonmisbrug (hvor andres abonnementer belastes med samtaleafgiften) - ikke er andre effektive efterforskningsmuligheder, herunder efterforskning af kriminalitet, der begås via netværk.

Et flertal i udvalget (Mads Bryde Andersen, Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Vagn Greve, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Lars Bo Langsted, Kirsten Mandrup, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder i overensstemmelse med Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, s. 5152, at der generelt bør sættes snævre grænser for politiets indgreb i meddelelseshemmeligheden, men at der dog - som anført af Strafferetsplejeudvalget og lagt til grund af Folketinget ved senere ændringer af bestemmelserne - kan være særlige kriminalitetsformer, hvor sædvanlige efterforskningsmetoder ikke rækker til. Disse medlemmer finder således, at der løbende på baggrund af udviklingen i kriminalitetsformerne må tages stilling til, om der er behov for at udvide adgangen til indgreb i meddelelseshemmeligheden til flere straffebestemmelser. Der må i den forbindelse foretages en overordnet afvejning mellem på den ene side hensynet til en effektiv kriminalitetsbekæmpelse og på den anden side hensynet til borgernes privatliv[(114)].

Ved den nedenfor af mindretallet foreslåede bestemmelse vil efterforskning af en betydelig videre kreds af lovovertrædelser end i dag kunne danne grundlag for indgreb i meddelelseshemmeligheden, forudsat at andre efterforskningsmetoder ikke er egnede til at sikre bevis i sagen.

Disse medlemmer kan ikke støtte en sådan generel, væsentlig lempelse af kriminalitetskravet ved indgreb i meddelelseshemmeligheden.

---

112. Jfr. retsplejelovens § 781, stk. 3.

113. Lovforslag nr. L 164 (198485).

114. Et mindretal i arbejdsgruppen vedrørende datakriminalitet (Mads Bryde Andersen, Hans Jakob Paldam Folker, Michael Goeskjær, Helle Jahn, Jens Kruse Mikkelsen) var enig i de betragtninger, udvalgets flertal har på dette område

---

Flertallet finder i denne sammenhæng på det foreliggende grundlag kun anledning til at overveje, om der bør være adgang til at foretage indgreb i meddelelseshemmeligheden ved efterforskning af sager om udbredelse og besiddelse af børnepornografi, jfr. straffelovens § 235. Da denne kriminalitet - på samme måde som "hackerkriminalitet" - i dag i høj grad begås ad elektronisk vej, hvor mere traditionelle efterforskningsmetoder ikke er anvendelige, foreslår disse medlemmer, at der i sager af denne karakter bliver mulighed for indgreb i meddelelseshemmeligheden, uanset det sædvanlige kriminalitetskrav (6 års fængsel i strafferammen) ikke er opfyldt.

Et af flertallets medlemmer (Kirsten Mandrup) finder endvidere, at det tillige bør overvejes at skabe mulighed for indgreb i meddelelseshemmeligheden for så vidt angår efterforskning af sager om misbrug af intern viden og kursmanipulation efter lov om værdipapirhandel m.v. Dette medlem peger på, at det på dette område, hvor kriminalitetskravet på 6 års fængsel ikke er opfyldt, i praksis har vist sig, at traditionelle efterforskningsmetoder ikke i fuldt tilstrækkeligt omfang er egnet til at imødegå denne form for kriminalitet.

Flertallet er enig i, at dette er et område, hvor der kan være anledning til at overveje yderligere udvidelser. Flertallet vil heller ikke udelukke, at en nærmere analyse af andre områder kan vise, at der er behov for en regulering ud over den foreslåede. Der er på den baggrund enighed om, at det indgår i udvalgets videre arbejde, om der kan påpeges behov for yderligere reguleringer.

Et mindretal i udvalget (Preben Bialas, Michael Clan, Annemette Møller) finder, at den regulering, der kan være behov for ved IT-relateret kriminalitet, ikke skal bestå i, at der indsættes en henvisning til endnu flere paragraffer,

hvor sådanne indgreb er mulige, uanset hvordan kriminaliteten konkret er gennemført, men derimod skal være en regulering, der begrænses til mere specielle tilfælde og samtidig har en mere fremtidssikret formulering, således at indgreb i meddelelseshemmeligheden muliggøres i de situationer, hvor der i den konkrete sag er et meget stort behov for det, for at kunne opklare kriminaliteten, men ikke udvides herudover[(115)].

Retsplejelovens § 754 a om agenter har som et af kriterierne, at "andre efterforskningsskridt ikke vil være egnede til at sikre bevis i sagen" og retsplejelovens § 781 om indgreb i meddelelseshemmeligheden har som et af kriterierne, at "indgrebet må antages at være af afgørende betydning for efterforskningen". Ved siden af disse krav opstilles de særlige krav til kriminalitetens art.

Særligt vedrørende teleoplysninger henvises til afsnit 6.2. Som det fremgår, var det fra 1954 til 1985[(116)] muligt at få teleoplysninger, dels når oplysningerne ville være af betydning for opklaring af forbrydelser, der påtaltes af statsadvokaterne, og endvidere i alle andre sager, såfremt det skønnedes "sandsynligt, at opklaring af en forbrydelse kun vil være mulig gennem de ønskede oplysninger, og foranstaltningen står i rimeligt forhold til forbrydelsens karakter"[(117)].

Der er ikke i betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter anført nogen særlig begrundelse for den foreslåede begrænsning af området. Justitsministeriets strafferetsplejeudvalg anfører dog mere generelt[(118)], at der er enighed om, at der generelt set bør sættes snævre grænser for politiets indgreb i meddelelseshemmeligheden. Det siges endvidere:

- "Opgaven ved reglernes udformning må derfor bestå i på den ene side ikke urimeligt at beskære politiets mulighed for at opklare og dermed bekæmpe alvorlig kriminalitet, herunder narkotikakriminalitet, men på den anden side at stille sådanne begrænsninger op for anvendelsen af indgrebene, at de hastigt voksende tekniske muligheder ikke fører til en overhåndtagende offentlig aflytning af borgerne."

---

115. Et flertal i arbejdsgruppen vedrørende datakriminalitet (Kim Aarenstrup, Jan Carlsen, Jan Friis, Carsten Heilbuth, Ulla Høg, Gunnar Kappel, Henrik OftebroSvendsen, Ronald Pedersen, Ole Stampe Rasmussen) er enig i mindretallets forslag.

116. De nye regler blev indført ved lov nr. 227 af 6/6 1985.

117. Det siges i lovforslaget, FT 1953/54 A 2145, vedrørende denne bestemmelse, at da indgrebet er af væsentlig mindre betydning end egentlig aflytning, har man ikke fundet det nødvendigt at drage så snævre grænser for dette som for aflytning.

118. Betænkningen s. 51 og 54

Disse medlemmer finder, at indgreb i meddelelseshemmeligheden fortsat skal have karakter af indgreb, der kun foretages i nødvendigt omfang. De er imidlertid betænkelige ved, at de moderne kommunikationsformer i nogle tilfælde betyder, at kriminalitet ikke kan efterforskes. Situationen er her ikke den, at borgeren skal beskyttes mod politiets muligheder i det moderne samfund, men derimod den, at borgeren skal beskyttes mod de kriminelles muligheder i det moderne samfund.

De ændringer, der i de senere år er foretaget i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden, viser, hvor hurtigt bestemmelserne bliver utidssvarende i forhold til efterforskningsbehovet. De viser også, hvor relativt lang tid der går, fra efterforskningsbehovet konstateres (f.eks. ved hacking og telefonmisbrug), til der skabes fornøden lovhjemmel.

Den form, der anvendes i dag i retsplejelovens § 781, hvor der indsættes stadig flere undtagelser fra kravet om, at der skal kunne straffes med fængsel i 6 år, er ikke hensigtsmæssig i et samfund, hvor IT-anvendelsen er i konstant udvikling. Behovet for at kunne få masteoplysninger og for at kunne bekæmpe kriminalitet, der begås via Internettet, er ting, der ikke var anledning til at tage nærmere stilling til, da Justitsministeriets strafferetsplejeudvalg afgav betænkning i 1984, men mindre end 10 år efter var det aktuelle problemstillinger.

Disse medlemmer finder, at der på baggrund af den konstaterede udvikling i dag bør åbnes mulighed for, at domstolene kan afsige kendelse om indgreb i meddelelseshemmeligheden i alle situationer, hvor der reelt ikke er andre efterforskningsmuligheder. De finder dog, at denne mere generelle adgang bør være forbeholdt for

kriminalitet, der kan straffes med fængsel i 1 år og 6 måneder eller derover. I det omfang sådanne indgreb ønskes foretaget over for kriminalitet med et lavere strafmaksimum - som f.eks. børnepornografibestemmelsen i sin nuværende affattelse - må den eller de aktuelle bestemmelser fortsat nævnes særskilt.

Derudover finder disse medlemmer, at den model, der anvendes i dag, hvor der baseret på et konstateret behov indsættes henvisninger til flere straffebestemmelser, kun er velegnet i tilfælde, hvor der ønskes skabt mulighed for, at der altid kan foretages indgreb i meddelelseshemmeligheden ved den type lovovertrædelser. Derimod kan det være betænkeligt at udvide efter denne model, hvis behovet for indgreb i meddelelseshemmeligheden reelt kun er meget stort i de af sagerne, hvor f.eks. Internettet er benyttet. F.eks. vil en udvidelse til indgreb i meddelelseshemmeligheden ved børnepornografi - en udvidelse der er behov for i dag netop på grund af distributionen via Internettet - med den gældende model betyde, at indgreb (f.eks. poststandsning og telefonaflytning) kan ske også i sager, der ikke er IT-relaterede. Mindretallet tager ikke afstand fra, at der kan være behov for en sådan regulering, men vil alene fremhæve, at denne reguleringsform er mere indgribende i relation til de kriminalitetsformer, der nævnes, end den af mindretallet foreslåede.

Eksempelvis kan også nævnes, at mindretallet ikke finder, at der generelt er stort behov for, at der kan foretages indgreb i meddelelseshemmeligheden i sager om ophavsretslovskrænkelser i form af piratkopiering. Der vil derimod kunne være det i sager, hvor programmer distribueres via Internettet, ikke mindst hvis det er den eneste indgang til sagen. Såfremt flertallets indstilling vedrørende digitale meddelelser følges, jfr. afsnit 6.1, vil det f.eks. heller ikke længere være muligt at få oplysninger fra Internetudbyderen i sådanne sager, således som det blev tilladt i UfR 1998.1613 ØLK.

Tilsvarende gælder for de i afsnit 2.4.2.1 nævnte sager om kursmanipulation og insiderviden. I nogle sager, især de, der foregår via Internettet, vil indgreb i meddelelseshemmeligheden være en forudsætning for, at gerningsmanden kan findes. I andre sager har der ikke i praksis været et så stort behov derfor, at der har været anledning til at foreslå, at sådanne indgreb kunne foretages.

Problemet kan også opstå i de i 2.4.2.2 nævnte sager om markedsføring på eller via Internettet. Det vil kunne være vanskeligt i nogle sager - uanset om de i visse grovere tilfælde opfylder kriminalitetskravet - at vide ved efterforskningens start, om de vil blive omfattet.

Der henvises til afsnit 7.7 udvalgets forslag.

Justitsministeriet Version 1.0 den 8. september 1999
Denne publikation findes på adressen: http://jm.schultzboghandel.dk

---

KAPITEL 7 - UDVALGETS FORSLAG MED BEMÆRKNINGER

7.1. Dansk straffemyndighed ved salg og udbredelse via Internettet

Der henvises til afsnit 2.3 vedrørende de danske regler om straffemyndighed og udvalgets overvejelser.

Udvalget har særligt vurderet de danske regler om straffemyndighed i relation til salg og udbredelse af børnepornografi via Internettet.

Det er udvalgets umiddelbare opfattelse, at den retstilstand, som de gældende jurisdiktionsbestemmelser må antages at indebære i forhold til salg og udbredelse af børnepornografi, er tilfredsstillende. Udvalget finder derfor ikke på det foreliggende grundlag behov for lovændringer på området.

Da retspraksis af betydning for de her behandlede spørgsmål imidlertid indtil nu har været sparsom, og da udviklingen hele tiden åbner nye tekniske muligheder, som stiller lovgivningen og retsanvendelsen over for nye udfordringer, kan det ikke udelukkes, at der i fremtiden kan forekomme tilfælde, der vil afsløre mangler ved de gældende jurisdiktionsregler. Der kan derfor være grund til løbende at følge udviklingen nøje for at sikre, at straffelovens regler om straffemyndighed til stadighed er tidssvarende i forhold til den teknologiske udvikling.

7.2. Straffelovens § 235

Der henvises til afsnit 4.4 vedrørende udvalgets overvejelser.

Udvalget foreslår, at bestemmelsen i straffelovens § 235, stk. 1, om udbredelse af børnepornografi ændres således, at ikke kun den erhvervsmæssige udbredelse, men også udbredelse i en videre kreds er omfattet. En sådan ændring vil bl.a. betyde, at udbredelse via netværker, herunder Internettet, bliver omfattet også i tilfælde, hvor udbredelsen ikke er erhvervsmæssig, ligesom den vil være anvendelig i tilfælde, hvor der ikke kan føres det fornødne bevis for, at udbredelsen er erhvervsmæssig.

Udvalget foreslår endvidere, at strafmaksimum hæves til fængsel i 2 år, jfr. udvalgets vurderinger i afsnit 4.4.4.

Udvalget foreslår endvidere, at § 235, stk. 2, om besiddelse udvides til også at omfatte den, der mod vederlag retsstridigt gør sig bekendt med børnepornografiske fremstillinger. Udvalget har herved lagt vægt på, at en del børnepornografiske ydelser leveres på en sådan vis, at der ikke er tale om besiddelse i straffelovens § 235, stk. 2's forstand. Sådanne tilfælde bør efter udvalgets vurdering kriminaliseres ud fra de samme beskyttelseshensyn, der i øvrigt ligger til grund for § 235.

Med hensyn til bestemmelsen i stk. 2 finder udvalget, at den nuværende strafferamme - bøde - i den overvejende del af tilfældene vil være passende, og at den nuværende begrænsning af straffen til bøde bør bevares som normalstrafferammen.

Udviklingen i anvendelsen af Internettet og distribution af børnepornografi via Internettet har imidlertid udviklet sig således, at udvalget finder, at der bør være mulighed for under skærpende omstændigheder at idømme hæfte eller

fængsel indtil 6 måneder. Som eksempel på, hvad der skal betragtes som skærpende omstændighed, kan nævnes, at den pågældende betaler betydelige beløb for at modtage børnepornografisk materiale. Der vil ligeledes foreligge skærpende omstændigheder, hvis den pågældende besidder et meget stort antal børnepornografiske fremstillinger, eller et større antal fremstillinger af særlig grove forhold, f.eks. voldtægt af børn.

Straffelovens § 235 foreslås herefter affattet således:

"*§ 235*. Den, som erhvervsmæssigt sælger eller på anden måde udbreder utugtige fotografier, film eller lignende af børn, straffes med bøde, hæfte eller fængsel indtil 2 år. På samme måde straffes den, som i en videre kreds udbreder sådanne fremstillinger.

Stk. 2. Den, som retsstridigt besidder eller mod vederlag gør sig bekendt med fotografier, film eller lignende af børn, der

1) har samleje eller anden kønslig omgængelse end samleje eller

2) har kønslig omgang med dyr eller

3) anvender genstande på groft utugtig måde,

straffes med bøde eller under skærpende omstændigheder med hæfte eller fængsel indtil 6 måneder."

Stk. 1, 1. pkt., svarer til det nugældende stk. 1 med den ændring, at det ikke længere nævnes, at det at fremstille eller skaffe sig det nævnte materiale med forsæt til at overtræde bestemmelsen er strafbart. At dette tidligere var nævnt var begrundet i, at der oprindelig var tale om en bødebestemmelse, og at det derfor ikke uden en særlig bestemmelse herom var muligt at straffe for forsøg, jfr. straffelovens § 21, stk. 3. Da de almindelige forsøgsregler finder anvendelse, er der ikke behov for at nævne særlige forsøgssituationer.

Endvidere foreslås strafmaksimum forhøjet til 2 år.

Stk. 1, 2. pkt., indeholder den af udvalget foreslåede udvidelse, således at ikke alene den erhvervsmæssige udbredelse, men også udbredelse i en videre kreds, er dækket af bestemmelsen.

Bestemmelsen i stk. 2 er i forhold til den nugældende bestemmelse udvidet med, at en person uden at etablere en besiddelsessituation mod vederlag gør sig bekendt med de særlige former for børnepornografisk materiale. Det nævnte "vederlag" omfatter enhver form for modydelse, herunder at der byttes med andre ydelser. Kravet om retsstridighed betyder, at f.eks. adgang, der er efterforskningsmæssigt begrundet, herunder en adgang, der har til formål at finde billeder af forsvundne børn, ikke omfattes af bestemmelsen. Retsstridighedskravet svarer til, hvad der formuleres direkte i det svenske lovforslag, jfr. afsnit. 4.3.2, hvorefter bestemmelsen ikke gælder tilfælde, hvor særlige omstændigheder gør, at handlingen må anses for åbenbart beføjet.

Endvidere foreslås strafmaksimum forhøjet til 6 måneder.

7.3. Krav til Internetudbydere, teleselskaber m.v.

Der henvises til afsnit 5.1 vedrørende udvalgets overvejelser.

Som nævnt finder udvalget, at der bør stilles krav om, at Internetudbydere og teleselskaber skal logge både A og B-nummeret - for A-nummerets vedkommende uanset om den pågældende har benyttet muligheden for, at der ikke sker visning af Anummeret. Endvidere bør udbyderen logge IPadresse for den, der ringer op, brugertid, tidspunkt for opkobling/nedkobling, opkoblingens længde og sessionstype (FTP/Telnet). Der bør tillige stilles krav om opbevaringsformat (læsbarhed) og foranstaltninger til beskyttelse mod uautoriseret adgang og manipulation. Derudover bør eventuelle kontooplysninger opbevares. Opbevaring af oplysninger skal ske i Danmark, hvis udbyderen er i Danmark, uanset om udbyderen er selvstændig eller filial af en udenlandsk virksomhed.

Endvidere bør det tilstræbes, at det sikres, at korrekt dansk realtid registreres.

Udvalget har nærmere drøftet de forskellige hensyn, der kan tale for henholdsvis en længere og en kortere opbevaringstid.

Udvalget har på baggrund af drøftelserne valgt at anbefale en opbevaringsfrist på 6 måneder. Spørgsmålet om, hvorvidt udbyderen har *ret* til at opbevare logoplysninger ud over den pligtmæssige opbevaring i 6 måneder, må afgøres på grundlag af de almindelige regler i registerlovgivningen.

Med hensyn til formen for reguleringen har udvalget indgående drøftet, om de ønskede registreringer og opbevaringen heraf ville kunne gennemføres ved en selvregulering.

Nogle medlemmer har henvist til, at der ikke er tale om en branche med etablerede traditioner med hensyn til selvregulering, eller med egne sanktionssystemer, ligesom der end ikke findes en registrering af Internetleverandører. Dette kan i sig selv tale mod en løsning med selvregulering, men dertil kommer, at der er tale om tiltag, der alene har efterforskningsmæssig interesse, og at efterforskningsmulighederne bør sikres gennem lovgivning herom. Dette svarer også til, at det f.eks. i § 3 h i lov om visse forhold på telekommunikationsområdet er fastsat, at udbydere af offentlige telenet og teletjenester uden udgift for staten skal sikre, at telecentralerne er indrettet således, at politiet kan få adgang til at foretage indgreb i meddelelseshemmeligheden.

Andre medlemmer har henvist til, at forpligtelsen bør kunne gennemføres ved selvregulering. Disse medlemmer mener ikke, at reglerne i lov om visse forhold på telekommunikationsområdet er egnede som retsgrundlag for den uoverskuelige mængde af Internetleverandører, for hvilke en forpligtelse af denne art får betydning.

Disse medlemmer har peget på, at der for tiden pågår intense bestræbelser på at gennemføre selvregulering indenfor Internetbranchen i en række henseender, og at man i tråd med den almindelige tendens i retning mod selvregulering bør give branchen mulighed for selv at tilvejebringe denne regulering, samtidig med at branchen alligevel skal tage stilling til spørgsmålet om, hvor længe man har *ret* til at opbevare sådanne logoplysninger. Når man vurderer udsigten til at gennemføre ønsket om opbevaring af logoplysninger i 6 måneder gennem selvregulering, må det i øvrigt tages i betragtning, at Internetleverandørerne kan have en økonomisk interesse i at følge en sådan praksis, eftersom udleveringen af de pågældende oplysninger sker mod betaling.

Et flertal i udvalget (Preben Bialas, Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Michael Clan, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Lau Kramer, Kirsten Mandrup, Annemette Møller, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder, at reguleringen skal ske ved lov.

Et mindretal i udvalget (Mads Bryde Andersen, Vagn Greve, Jesper Koefoed, Lars Bo Langsted) finder, at spørgsmålet så vidt muligt skal løses ved en selvregulering i branchen, Disse medlemmer er dog enige i en lovgivningsmæssig løsning, såfremt det viser sig, at reguleringsbestræbelserne ikke bærer frugt.

7.4. Adgang til indholdet af digitale meddelelser

Der henvises til afsnit 6.1 vedrørende udvalgets overvejelser.

Udvalget har nærmere drøftet, om adgang til email (eller andre digitale meddelelser) hos udbyderen skal behandles efter retsplejelovens regler om edition eller om dens regler om indgreb i meddelelseshemmeligheden.

Der er enighed i udvalget om, at hvis der er tale om et fremadrettet indgreb, der har karakter af overvågning af indholdet af korrespondancen, bør det være omfattet af regler om indgreb i meddelelseshemmeligheden.

Udvalgets medlemmer har delt sig i spørgsmålet om, hvorvidt dette også bør gælde for indgreb, der er bagudrettede.

Et flertal i udvalget (Mads Bryde Andersen, Preben Bialas, Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Vagn Greve, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Lars Bo Langsted, Kirsten Mandrup, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder ikke anledning til at foreslå ændringer i retsplejelovens regler om indgreb i meddelelseshemmeligheden. Disse medlemmer finder således, at elektronisk post (epost eller email) ikke adskiller sig grundlæggende fra andre kommunikationsformer, der er omfattet af reglerne om indgreb i meddelelseshemmeligheden, og at der derfor ikke er grund til at give

politiet en videre adgang til at foretage indgreb i kommunikation i form af elektronisk post.

Efter disse medlemmers opfattelse må elektroniske breve sidestilles med traditionelle (fysiske) breve, jfr. retsplejelovens § 780, stk. 1, nr. 4 og 5. En sammenligning af kommunikationsforløbene ved henholdsvis traditionelle brevforsendelser og elektronisk post må efter disse medlemmers opfattelse føre til, at elektronisk post, der beror hos en Internetudbyder, må sidestilles med breve i en postboks, jfr. de ovenfor citerede forarbejder til de gældende bestemmelser.

Det er forudsat, at reglerne om indgreb i meddelelseshemmeligheden ikke omfatter indgreb, der gennemføres inden kommunikationens begyndelse eller efter dens afslutning. Reglerne finder således ikke anvendelse, hvis politiet kan skaffe sig meddelelsen ved et straffeprocessuelt tvangsindgreb mod afsender eller modtager af meddelelsen (jfr. reglerne om ransagning og beslaglæggelse). Hvis politiet derimod ønsker at skaffe sig meddelelsen med bistand fra en kommunikationsformidler, må dette ske efter reglerne om indgreb i meddelelseshemmeligheden. Dette må gælde, uanset om kommunikationsformidleren er et telefonselskab, en postvirksomhed eller en udbyder af elektronisk kommunikation (herunder en Internetudbyder).

Kommunikationen kan efter de principper, der er lagt til grund ved udformningen af reglerne om indgreb i meddelelseshemmeligheden, kun siges at være afsluttet, når meddelelsen er kommet modtageren i hænde på en sådan måde, at politiet kan skaffe sig adgang til meddelelsen under en ransagning på modtagerens (fysiske) adresse eller ved anvendelse af midler beslaglagt under en sådan ransagning (en postboksnøgle eller en adgangskode til en elektronisk postkasse). Adgangskoden kan f.eks. være fast indkodet i Internetkommunikationsprogrammet (browseren) på den mistænktes computer, således at der ved opstart af programmet automatisk etableres forbindelse til den elektroniske postkasse hos Internetudbyderen. I denne situation vil det ikke være nødvendigt for politiet at gå frem efter reglerne om indgreb i meddelelseshemmeligheden.

Et mindretal i udvalget (Michael Clan, Annemette Møller) finder, at reglerne om edition bør anvendes, og at der ikke bør stilles de særlige krav, der gælder for indgreb i meddelelseshemmeligheden. Der er tale om et indgreb, hvor oplysningerne - hvis de fortsat lå hos den sigtede - kunne tilvejebringes i medfør af de almindelige ransagningsregler. De henviser herudover til, at der ved den oprindelige stillingtagen i 1984 til datakommunikation er tænkt på en igangværende kommunikationsstrøm, hvor kommunikationen ikke er nået fysisk frem til den pågældende, og ikke på den særlige email struktur.

Disse medlemmer finder i øvrigt, at der altid bør beskikkes forsvarer i disse situationer, hvis det ikke allerede er sket.

Disse medlemmer lægger også vægt på, at den sigtede selv har valgt, at kommunikationen kan ske via kommunikationskanaler, hvor en tredjemand indgår i forløbet og besidder, hvad der kan sidestilles med en brevkopi. Situationen er meget atypisk i forhold til traditionelle postforsendelser, fordi Internetudbyderen straks har gjort forsendelsen tilgængelig for adressaten på dennes adresse. Der er således efter de principper, der gælder for f.eks. postforsendelser, telexkommunikation og meddelelser til telefonsvarere, ikke tale om et igangværende kommunikationsforløb. Når oplysningerne findes hos Internetudbyderen, er kommunikationen afsluttet. Ønsker man at føre særlig sikret korrespondance, må det ske ved sædvanlige lukkede forsendelser, der ikke er tilgængelige i andre systemer, eller der må anvendes særligt sikre krypteringsteknikker.

Det er også den fortolkning, der anlægges i retspraksis. F.eks. blev der i en sag om piratkopiering afsagt editionskendelse vedrørende email fra den sigtedes kendte email adresse og eventuelle andre adresser tilhørende ham, jfr. UfR 1998.1613 ØLK. Forsvareren gjorde både for byretten og landsretten gældende, at der var tale om indgreb i meddelelseshemmeligheden, og at der derfor ikke kunne afsiges editionskendelse[(119)]. Byretten afsagde editionskendelse og anførte, at den hos Internetudbyderen beroende post ikke fandtes at være under forsendelse, men måtte ligestilles med post, der var kommet frem til den sigtedes bopæl. Østre landsret stadfæstede kendelsen af de af byretten anførte grunde.

Flertallets forslag er reelt ikke et forslag om ikke at ændre retstilstanden, men er et forslag om at begrænse de efterforskningsmuligheder, der, jfr. Østre landsrets kendelse, må antages at være i dag. Mindretallet finder mere principielt, at det ikke er acceptabelt at foreslå løsninger, der begrænser politiets nuværende muligheder for at efterforske og dermed begrænser mulighederne for at bekæmpe kriminalitet.

[119.] Der ville på grund af sagstypen ikke have kunnet afsiges kendelse om indgreb i meddelelseshemmeligheden, idet piratkopiering ikke er en af de kriminalitetstyper, hvor der kan foretages sådanne indgreb, jfr. retsplejelovens § 781.

7.5. Teleoplysninger (incl. sendemaster)

Der henvises til afsnit 6.2 og 6.4 vedrørende udvalgets overvejelser.

Et flertal i udvalget (Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Vagn Greve, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Lars Bo Langsted, Kirsten Mandrup, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder ikke anledning til at foreslå ændringer af retsplejelovens regler om indgreb i meddelelseshemmeligheden i form af teleoplysning.

Regler om indgreb i meddelelseshemmeligheden er udtryk for en afvejning af på den ene side hensynet til en effektiv kriminalitetsbekæmpelse og på den anden side hensynet til borgernes privatliv.

Efter flertallets opfattelse tilsiger hensynet til beskyttelse af borgernes fortrolige kommunikation med andre også en beskyttelse af oplysninger om, *hvem* der er kommunikeret med. Dette er også lagt til grund i Strafferetsplejeudvalgets betænkning nr. 1024/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter.

Uanset et indgreb i form af indhentning af teleoplysninger kan siges at indebære en vis mindre grad af integritetskrænkelse end de øvrige indgreb i meddelelseshemmeligheden, herunder telefonaflytning, bør der efter disse medlemmers opfattelse - henset til de ovenfor beskrevne modhensyn - ikke gives politiet adgang til teleoplysninger efter (de væsentlig lempeligere) regler om edition.

En anvendelse af reglerne om edition vil således bl.a. indebære, at indgrebet som udgangspunkt kan anvendes ved alle former for kriminalitet. En begrænsning vil alene følge af en proportionalitetsafvejning i den konkrete sag, dvs. om indgrebet står i misforhold til sagens betydning og den ulempe, som indgrebet kan antages at medføre. Efter reglerne om indgreb i meddelelseshemmeligheden kan indgrebet - bortset fra enkelte i loven særligt opregnede lovovertrædelser - kun anvendes ved efterforskning af lovovertrædelser, der efter loven kan straffes med fængsel i 6 år eller derover.

For så vidt angår spørgsmålet om en udvidelse af reglerne om indgreb i meddelelseshemmeligheden - en udvidelse der i givet fald også vil få betydning for teleoplysninger - henvises til afsnit 7.7 nedenfor.

Mindretallets forslag (jfr. nedenfor) indebærer, at også pålæg til teleselskabet om registrering af teleoplysninger i en periode frem i tiden skal behandles efter reglerne om edition. Disse regler indeholder - i modsætning til reglerne om indgreb i meddelelseshemmeligheden - ikke bestemmelser om frister for sådanne indgreb, idet editionsregler i alt væsentligt er tænkt anvendt på allerede eksisterende oplysninger. Editionsreglerne indeholder heller ikke regler om beskikkelse af advokat for indehaveren af pågældende telefon og foreslås af mindretallet kun ændret således, at der skal ske forsvarerbeskikkelse for den sigtede, der ikke behøver at være identisk med indehaveren af telefonen. Mindretallets forslag indebærer således på flere punkter en svækkelse af de retsgarantier, som de gældende regler er udtryk for.

Et mindretal i udvalget (Mads Bryde Andersen, Preben Bialas, Michael Clan, Annemette Møller) finder, at det ved teleoplysninger, der allerede lagres i anden sammenhæng, bør være en tilstrækkelig garanti, at der skal afsiges editionskendelse. Oplysningerne er ikke mere følsomme end en række andre oplysninger, der kan udleveres efter editionsreglerne, og det kræver i dag ikke et særligt indgreb fra teleselskabernes side at fremskaffe oplysningerne.

Mindretallet vil pege på, at teleoplysninger er det mindst indgribende af de indgreb, der reguleres af reglerne om indgreb i meddelelseshemmeligheden. Ved indgrebet får politiet ikke kendskab til indholdet af kommunikationen, ligesom kommunikationen ikke unddrages modtageren.

Betydningen af at kunne få teleoplysninger er endvidere betydelig større ved den kriminalitet, der kendes i dag, end den var, da strafferetsplejerådet foreslog den ensartede regulering af området. Dette har også efterfølgende

medført behov for, at der blev skabt en særlig hjemmel i retsplejelovens § 781, stk. 2 og stk. 3, til at indhente teleoplysninger i hackersager og telefonmisbrugssager. Også for så vidt angår sager om børnepornografi er der i dag behov derfor, ligesom der i øvrigt vil kunne være behov i sagstyper, hvor Internettet indgår, f.eks. i sager om piratkopiering eller kursmanipulation. Også på områder uden for den IT-relaterede kriminalitet - f.eks. i sager om EUsvig eller afgiftssvig i øvrigt - er der på grund af mange personers samvirke et større behov end tidligere for at få oplysninger af denne type.

Disse medlemmer er enige om, at forudsætningen for at anvende editionsreglerne skal være, at der beskikkes en forsvarer i disse situationer, hvis det ikke allerede er sket.

Editionsreglerne anvendes normalt ved alle oplysninger, uanset hvor følsomme de er, når oplysningerne er tilgængelige hos den, editionen rettes mod, uden særlige tiltag. Domstolene er derfor også ved edition vant til, at der er forskel på følsomheden af de ønskede oplysninger, og at dette kan have betydning for, hvornår og i hvilket omfang en begæring om edition - f.eks. i et pengeinstitut, hos en revisor eller hos en advokat - skal imødekommes.

De særlige regler om teleoplysninger afviger således i dag - hvor der ikke skal foretages særlige indgreb for at fremskaffe dem - fra de regler, der i øvrigt gælder for selv meget følsomme oplysninger, som personer eller selskaber besidder som et almindeligt led i deres virksomhed.

Disse medlemmer foreslår, at retsplejelovens § 780, stk. 1, nr. 3, ændres således, at bestemmelsen alene omfatter masteoplysninger og tilsvarende oplysninger (udvidet teleoplysning).

For så vidt angår lagrede teleoplysninger, vil de herefter blive indhentet efter reglerne om edition, jfr. retsplejelovens § 827. Ved afgørelse om edition skal retten tage stilling til, om indgrebet står i misforhold til sagens betydning (hvilket efter seneste lovændring[(120)] er formuleret udtrykkeligt i § 805, stk. 1). Dette bør være en tilstrækkelig garanti for, at der kun gives teleoplysninger i sager, hvor retten har afvejet indgrebet mod sagens betydning.

---

120. Lov nr. 229 af 21/4 1999 om ændring af retsplejeloven (Beslaglæggelse, edition m.v.).

Særligt om masteoplysninger

Udvalget finder, at der bør tilvejebringes en klar hjemmel til indgreb i form af masteoplysninger o.l. De medlemmer af udvalget, der i øvrigt finder, at editionsreglerne frembyder tilstrækkelig garanti ved lagrede teleoplysninger, er enige med de øvrige medlemmer i, at masteoplysninger og tilsvarende oplysninger skal behandles efter reglerne om indgreb i meddelelseshemmeligheden, da der er tale om meget bredere indgreb. Udvalget finder herudover, at reglerne skal opfylde kravene til særligt kvalificerede indgreb i meddelelseshemmeligheden.

Udvalget foreslår, at sendemaster reguleres i retsplejelovens § 780, stk. 1, nr. 3 (hvis den nugældende nr. 3 ophæves) eller nr. 4, med følgende ordlyd:

"4) indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater inden for et nærmere angivet område der sættes i forbindelse med andre telefoner eller kommunikationsapparater (udvidet teleoplysning),"

Udvalget foreslår endvidere, at der kun skal være adgang til udvidet teleoplysning under de betingelser (mistanke om en forbrydelse, som har medført eller som kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier), der gælder for anden aflytning end telefonaflytning.

Det foreslås derfor, at der i § 781, stk. 5, efter "Aflytning efter § 780, stk. 1, nr. 2, indsættes "og udvidet teleoplysning efter § 780, stk. 1, [nr. 3] [nr. 4]".

7.6. Teleoplysninger i henhold til samtykke m.v.

7.6. Teleoplysninger i henhold til samtykke m.v.

Der henvises til afsnit 6.3 vedrørende udvalgets overvejelser.

Med hensyn til retsplejelovens § 786, stk. 1, foreslår udvalget, at "post og telegrafvæsenet, telefonselskaberne og andre tilsvarende offentlige og private virksomheder" ændres til "postvirksomheder og udbydere af offentlige telenet eller teletjenester". Ændringen bringer terminologien i overensstemmelse med lov nr. 89 af 8/2 1995 om postvirksomhed og med den nyere telelovgivning, jfr. herved f.eks. § 1, stk. 5, i lov om konkurrenceforhold og samtrafik i telesektoren, jfr. lovbekendtgørelse nr. 860 af 4/12 1998.

Med hensyn til samtykkereglen i retsplejelovens § 786, stk. 2, har udvalget delt sig i spørgsmålet om, hvorvidt teleselskaberne skal kunne meddele dette samtykke ved offentlige telefoner.

Et flertal i udvalget (Preben Bialas, Susan Bramsen, Bent Carlsen, Vagn Greve, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Kirsten Mandrup, Lene Nielsen, Henrik Rothe) finder ikke, at teleselskaberne skal kunne meddele samtykke ved offentlige telefoner.

Bestemmelsen i retsplejelovens § 786, stk. 2, bygger på det synspunkt, at en telefonabonnent ikke i forhold til telefonselskabernes tavshedspligt kan anses for "uvedkommende" med hensyn til oplysninger om, hvem der ringer til abonnenten, og at der ikke er en sådan beskyttelsesværdig interesse i hemmeligholdelse hos personer, der kalder et andet telefonnummer, at udlevering af disse oplysninger til politiet med samtykke fra indehaveren af denne telefon bør omfattes af reglerne om indgreb i meddelelseshemmeligheden, jfr. Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, s. 62. I retspraksis er det fastslået, at bestemmelsen også finder anvendelse på oplysninger om udgående opkald fra en bestemt telefon, jfr. UfR 1996.169 ØLK.

Efter disse medlemmers opfattelse kan et telefonselskab ikke siges at have rådighed over en offentlig telefon på samme måde som en privat telefonabonnent har rådighed over sin telefon. Der er derfor ikke samme anledning til at give telefonselskabet adgang til med sit samtykke at fravige reglerne om indgreb i meddelelseshemmeligheden. Hvis man låner en privat telefon (eller stjæler en mobiltelefon) må man være indstillet på, at den pågældende telefonabonnent modtager udførlige samtalespecifikationer i forbindelse med telefonregningen. Benyttelsen af en offentlig telefon kan nærmest betragtes som et "ad hocabonnement", hvor man mod vederlag får (en begrænset) adgang til at benytte telefonnettet. Et indgreb mod en bruger af en offentlig telefon bør derfor sidestilles med et indgreb imod en privat telefonabonnent. De særlige hensyn, der i sin tid begrundede bestemmelsen i § 786, stk. 2, kan efter disse medlemmers opfattelse ikke udstrækkes til også at begrunde en lignende regel for offentlige telefoner.

Et mindretal i udvalget (Mads Bryde Andersen, Hans Henrik Brydensholt, Jørgen Christiansen, Michael Clan, Alexander Houen, Lars Bo Langsted, Annemette Møller) finder, at teleselskaberne - uanset hvilket regelsæt der finder anvendelse - skal kunne meddele samtykket, når der er tale om offentlige telefoner. Der er enighed om, at der skal beskikkes en forsvarer i disse situationer, hvis det ikke allerede er sket.

Disse medlemmer har i den forbindelse lagt vægt på, at der ikke kan være nogen berettiget forventning om, at indehaveren af en telefon ikke kan give politiet (adgang til) oplysning om, hvilken brug der har været gjort af telefonen. Med den retstilstand, der er i dag vedrørende indgreb i meddelelseshemmeligheden, betyder det, at der ved en lang række kriminalitetsformer ikke er mulighed for at få adgang til disse allerede registrerede oplysninger, hvis en offentlig telefon er benyttet (i modsætning til f.eks. en telefon, der ejes af en restaurant).

Spørgsmålet om samtykke ved offentlige telefoner er opstået som en konsekvens af, at oplysningerne i dag registreres. Det er af samme grund ikke behandlet i Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, der, jfr. betænkningens s. 61 ff, især tager udgangspunkt i, at hovedområdet for teleoplysninger er truende, injurierende eller på andre måder generende telefonopkald til en privat abonnent. Udvalgets forventninger til, at indgrebet i fremtiden vil tiltrække sig større opmærksomhed, er især knyttet til, at telefonaflytninger er ressourcekrævende, og at det i en del sager kunne

være af betydning for politiet at få oplyst, om bestemte telefoner, til hvis indehavere man har mistanke i sagskomplekset, bliver sat i forbindelse med hinanden.

I den ovenfor nævnte kendelse (UfR 1996.169 ØLK) blev det lagt til grund, at indehaveren af en stjålen mobiltelefon kunne meddele samtykke efter retsplejelovens § 786, stk. 2. Denne kendelse understøtter efter disse medlemmers opfattelse det synspunkt, at det formelle ejerskab er tilstrækkeligt til, at man er samtykkeberettiget, også når samtalerne utvivlsomt er abonnenten helt uvedkommende.

Et medlem af udvalget (Erik Overgaard) har ikke taget stilling til, hvilken løsning der skal vælges.

7.7. Indgreb i meddelelseshemmeligheden i øvrigt

Der henvises til afsnit 6.5 vedrørende udvalgets overvejelser.

Udvalget finder, at der i det omfang, hvor der er særligt behov herfor, bør skabes adgang til indgreb i meddelelseshemmeligheden ved IT-relateret kriminalitet. En bestemmelse herom bør dog begrænses til de efterforskningssituationer, hvor der reelt - som ved hacking og telefonmisbrug (hvor andres abonnementer belastes med samtaleafgiften) - ikke er andre effektive efterforskningsmuligheder, herunder efterforskning af kriminalitet, der begås via netværk.

Et flertal i udvalget (Mads Bryde Andersen, Susan Bramsen, Hans Henrik Brydensholt, Bent Carlsen, Jørgen Christiansen, Vagn Greve, Alexander Houen, Helle Jahn, Poul Dahl Jensen, Jesper Koefoed, Lau Kramer, Lars Bo Langsted, Kirsten Mandrup, Lene Nielsen, Erik Overgaard, Henrik Rothe) finder i overensstemmelse med Justitsministeriets strafferetsplejeudvalgs betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, s. 5152, at der generelt bør sættes snævre grænser for politiets indgreb i meddelelseshemmeligheden, men at der dog - som anført af Strafferetsplejeudvalget og lagt til grund af Folketinget ved senere ændringer af bestemmelserne - kan være særlige kriminalitetsformer, hvor sædvanlige efterforskningsmetoder ikke rækker til. Disse medlemmer finder således, at der løbende på baggrund af udviklingen i kriminalitetsformerne må tages stilling til, om der er behov for at udvide adgangen til indgreb i meddelelseshemmeligheden til flere straffebestemmelser. Der må i den forbindelse foretages en overordnet afvejning mellem på den ene side hensynet til en effektiv kriminalitetsbekæmpelse og på den anden side hensynet til borgernes privatliv.

Ved den nedenfor af mindretallet foreslåede bestemmelse vil efterforskning af en betydelig videre kreds af lovovertrædelser end i dag kunne danne grundlag for indgreb i meddelelseshemmeligheden, forudsat at andre efterforskningsmetoder ikke er egnede til at sikre bevis i sagen.

Disse medlemmer kan ikke støtte en sådan generel, væsentlig lempelse af kriminalitetskravet ved indgreb i meddelelseshemmeligheden.

Flertallet finder i denne sammenhæng på det foreliggende grundlag kun anledning til at overveje, om der bør være adgang til at foretage indgreb i meddelelseshemmeligheden ved efterforskning af sager om udbredelse og besiddelse af børnepornografi, jfr. straffelovens § 235. Da denne kriminalitet - på samme måde som "hackerkriminalitet" - i dag i høj grad begås ad elektronisk vej, hvor mere traditionelle efterforskningsmetoder ikke er anvendelige, foreslår disse medlemmer, at der i sager af denne karakter bliver mulighed for indgreb i meddelelseshemmeligheden, uanset det sædvanlige kriminalitetskrav (6 års fængsel i strafferammen) ikke er opfyldt.

Et af flertallets medlemmer (Kirsten Mandrup) finder endvidere, at det tillige bør overvejes at skabe mulighed for indgreb i meddelelseshemmeligheden for så vidt angår efterforskning af sager om misbrug af intern viden og kursmanipulation efter lov om værdipapirhandel m.v. Dette medlem peger på, at det på dette område, hvor kriminalitetskravet på 6 års fængsel ikke er opfyldt, i praksis har vist sig, at traditionelle efterforskningsmetoder ikke i fuldt tilstrækkeligt omfang er egnet til at imødegå denne form for kriminalitet.

Flertallet er enig i, at dette er et område, hvor der kan være anledning til at overveje yderligere udvidelser. Flertallet vil heller ikke udelukke, at en nærmere analyse af andre områder kan vise, at der er behov for en regulering ud over den foreslåede. Der er på den baggrund enighed om, at det indgår i udvalgets videre arbejde, om

der kan påpeges behov for yderligere reguleringer.

Et mindretal i udvalget (Preben Bialas, Michael Clan, Annemette Møller) finder, at den regulering, der kan være behov for ved IT-relateret kriminalitet, ikke skal bestå i, at der indsættes en henvisning til endnu flere paragraffer, hvor sådanne indgreb er mulige, uanset hvordan kriminaliteten konkret er gennemført, men derimod skal være en regulering, der begrænses til mere specielle tilfælde og samtidig har en mere fremtidssikret formulering, således at indgreb i meddelelseshemmeligheden muliggøres i de situationer, hvor der i den konkrete sag er et meget stort behov for det, for at kunne opklare kriminaliteten, men ikke udvides herudover.

Retsplejelovens § 754 a om agenter har som et af kriterierne, at "andre efterforskningsskridt ikke vil være egnede til at sikre bevis i sagen" og retsplejelovens § 781 om indgreb i meddelelseshemmeligheden har som et af kriterierne, at "indgrebet må antages at være af afgørende betydning for efterforskningen". Ved siden af disse krav opstilles de særlige krav til kriminalitetens art.

Særligt vedrørende teleoplysninger henvises til afsnit 6.2. Som det fremgår, var det fra 1954 til 1985[(121)] muligt at få teleoplysninger, dels når oplysningerne ville være af betydning for opklaring af forbrydelser, der påtaltes af statsadvokaterne, og endvidere i alle andre sager, såfremt det skønnedes "sandsynligt, at opklaring af en forbrydelse kun vil være mulig gennem de ønskede oplysninger, og foranstaltningen står i rimeligt forhold til forbrydelsens karakter"[(122)].

Der er ikke i betænkning nr. 1023/1984 om politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter anført nogen særlig begrundelse for den foreslåede begrænsning af området. Justitsministeriets strafferetsplejeudvalg anfører dog mere generelt[(123)], at der er enighed om, at der generelt set bør sættes snævre grænser for politiets indgreb i meddelelseshemmeligheden. Det siges endvidere:

- "Opgaven ved reglernes udformning må derfor bestå i på den ene side ikke urimeligt at beskære politiets mulighed for at opklare og dermed bekæmpe alvorlig kriminalitet, herunder narkotikakriminalitet, men på den anden side at stille sådanne begrænsninger op for anvendelsen af indgrebene, at de hastigt voksende tekniske muligheder ikke fører til en overhåndtagende offentlig aflytning af borgerne."

---

121. De nye regler blev indført ved lov nr. 227 af 6/6 1985.
122. Det siges i lovforslaget, FT 1953/54 A 2145, vedrørende denne bestemmelse, at da indgrebet er af væsentlig mindre betydning end egentlig aflytning, har man ikke fundet det nødvendigt at drage så snævre grænser for dette som for aflytning.
123. Betænkningen s. 51 og 54.

Disse medlemmer finder, at indgreb i meddelelseshemmeligheden fortsat skal have karakter af indgreb, der kun foretages i nødvendigt omfang. De er imidlertid betænkelige ved, at de moderne kommunikationsformer i nogle tilfælde betyder, at kriminalitet ikke kan efterforskes. Situationen er her ikke den, at borgeren skal beskyttes mod politiets muligheder i det moderne samfund, men derimod den, at borgeren skal beskyttes mod de kriminelles muligheder i det moderne samfund.

De ændringer, der i de senere år er foretaget i retsplejelovens kapitel 71 om indgreb i meddelelseshemmeligheden, viser, hvor hurtigt bestemmelserne bliver utidssvarende i forhold til efterforskningsbehovet. De viser også, hvor relativt lang tid der går, fra efterforskningsbehovet konstateres (f.eks. ved hacking og telefonmisbrug), til der skabes fornøden lovhjemmel.

Den form, der anvendes i dag i retsplejelovens § 781, hvor der indsættes stadig flere undtagelser fra kravet om, at der skal kunne straffes med fængsel i 6 år, er ikke hensigtsmæssig i et samfund, hvor IT-anvendelsen er i konstant udvikling. Behovet for at kunne få masteoplysninger og for at kunne bekæmpe kriminalitet, der begås via Internettet, er ting, der ikke var anledning til at tage nærmere stilling til, da Justitsministeriets strafferetsplejeudvalg afgav betænkning i 1984, men mindre end 10 år efter var det aktuelle problemstillinger.

Disse medlemmer finder, at der på baggrund af den konstaterede udvikling i dag bør åbnes mulighed for, at domstolene kan afsige kendelse om indgreb i meddelelseshemmeligheden i alle situationer, hvor der reelt ikke er

andre efterforskningsmuligheder. De finder dog, at denne mere generelle adgang bør være forbeholdt for kriminalitet, der kan straffes med fængsel i 1 år og 6 måneder eller derover. I det omfang sådanne indgreb ønskes foretaget over for kriminalitet med et lavere strafmaksimum - som f.eks. børnepornografibestemmelsen i sin nuværende affattelse - må den eller de aktuelle bestemmelser fortsat nævnes særskilt.

Derudover finder disse medlemmer, at den model, der anvendes i dag, hvor der baseret på et konstateret behov indsættes henvisninger til flere straffebestemmelser, kun er velegnet i tilfælde, hvor der ønskes skabt mulighed for, at der altid kan foretages indgreb i meddelelseshemmeligheden ved den type lovovertrædelser. Derimod kan det være betænkeligt at udvide efter denne model, hvis behovet for indgreb i meddelelseshemmeligheden reelt kun er meget stort i de af sagerne, hvor f.eks. Internettet er benyttet. F.eks. vil en udvidelse til indgreb i meddelelseshemmeligheden ved børnepornografi - en udvidelse der er behov for i dag netop på grund af distributionen via Internettet - med den gældende model betyde, at indgreb (f.eks. poststandsning og telefonaflytning) kan ske også i sager, der ikke er IT-relaterede. Mindretallet tager ikke afstand fra, at der kan være behov for en sådan regulering, men vil alene fremhæve, at denne reguleringsform er mere indgribende i relation til de kriminalitetsformer, der nævnes, end den af mindretallet foreslåede.

Eksempelvis kan også nævnes, at mindretallet ikke finder, at der generelt er stort behov for, at der kan foretages indgreb i meddelelseshemmeligheden i sager om ophavsretslovskrænkelser i form af piratkopiering. Der vil derimod kunne være det i sager, hvor programmer distribueres via Internettet, ikke mindst hvis det er den eneste indgang til sagen. Såfremt flertallets indstilling vedrørende digitale meddelelser følges, jfr. afsnit 6.1, vil det f.eks. heller ikke længere være muligt at få oplysninger fra Internetudbyderen i sådanne sager, således som det blev tilladt i UfR 1998.1613 ØLK.

Tilsvarende gælder for de i afsnit 2.4.2.1 nævnte sager om kursmanipulation og insiderviden. I nogle sager, især de, der foregår via Internettet, vil indgreb i meddelelseshemmeligheden være en forudsætning for, at gerningsmanden kan findes. I andre sager har der ikke i praksis været et så stort behov derfor, at der har været anledning til at foreslå, at sådanne indgreb kunne foretages.

Problemet kan også opstå i de i 2.4.2.2 nævnte sager om markedsføring på eller via Internettet. Det vil kunne være vanskeligt i nogle sager - uanset om de i visse grovere tilfælde opfylder kriminalitetskravet - at vide ved efterforskningens start, om de vil blive omfattet.

Justitsministeriet Version 1.0 den 8. september 1999
Denne publikation findes på adressen: http://jm.schultzboghandel.dk

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>The page cannot be found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">
<STYLE type="text/css">
  BODY { font: 8pt/12pt verdana }
  H1 { font: 13pt/15pt verdana }
  H2 { font: 8pt/12pt verdana }
  A:link { color: red }
  A:visited { color: maroon }
</STYLE>
</HEAD><BODY><TABLE width=500 border=0 cellspacing=10><TR><TD>

<h1>The page cannot be found</h1>
The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.
<hr>
Please try the following:

Make sure that the Web site address displayed in the address bar of your browser is spelled and formatted correctly.
If you reached this page by clicking a link, contact
 the Web site administrator to alert them that the link is incorrectly formatted.

Click the Back button to try another link.

<h2>HTTP Error 404 - File or directory not found.
Internet Information Services (IIS)</h2>
<hr>
Technical Information (for support personnel)

Go to Microsoft Product Support Services and perform a title search for the words HTTP and 404.
Open IIS Help, which is accessible in IIS Manager (inetmgr),
 and search for topics titled Web Site Setup, Common Administrative Tasks, and About Custom Error Messages.

</TD></TR></TABLE></BODY></HTML>

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>The page cannot be found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">
<STYLE type="text/css">
  BODY { font: 8pt/12pt verdana }
  H1 { font: 13pt/15pt verdana }
  H2 { font: 8pt/12pt verdana }
  A:link { color: red }
  A:visited { color: maroon }
</STYLE>
</HEAD><BODY><TABLE width=500 border=0 cellspacing=10><TR><TD>

<h1>The page cannot be found</h1>
The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.
<hr>
Please try the following:

Make sure that the Web site address displayed in the address bar of your browser is spelled and formatted correctly.
If you reached this page by clicking a link, contact
 the Web site administrator to alert them that the link is incorrectly formatted.

Click the Back button to try another link.

<h2>HTTP Error 404 - File or directory not found.
Internet Information Services (IIS)</h2>
<hr>
Technical Information (for support personnel)

Go to Microsoft Product Support Services and perform a title search for the words HTTP and 404.
Open IIS Help, which is accessible in IIS Manager (inetmgr),
 and search for topics titled Web Site Setup, Common Administrative Tasks, and About Custom Error Messages.

</TD></TR></TABLE></BODY></HTML>