NOU Norges offentlige utredninger **2003: 27**

Lovtiltak mot datakriminalitet

Delutredning I om Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi

Utredning fra Datakrimutvalget oppnevnt ved kgl. res. 11. januar 2002.
Avgitt til Justis- og politidepartementet 4. november 2003.

Statens forvaltningstjeneste
Informasjonsforvaltning

Oslo 2003

ISSN 0333-2306
ISBN 82-583-0736-3

Sats/Trykk: AIT Trondheim AS/AIT Otta AS

Til Justis- og politidepartementet

Datakrimutvalget ble opprettet ved kongelig resolusjon 11. januar 2002. Etter mandatet skal utvalget utrede lovtiltak mot datakriminalitet. I delutredning I kommer utvalget med forslag til gjennomføring i norsk rett av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi, undertegnet av Norge i Budapest 23. november 2001.

Datakrimutvalget legger med dette frem en utredning med lovutkast. Utvalgets innstilling er enstemmig med unntak av forslaget til bestemmelse om sikringspålegg, som ett medlem ikke slutter seg til.

Oslo, 4. november 2003

Stein Schjølberg
leder

Christina Christensen	Beate S. Dagslet	Marius Stub
Inger Marie Sunde	Berit Svendsen	Bjørn Erik Thon
Benedict de Vibe		

Ole Jacob Garder
Helene Wegner

Innhold

Kapittel 1
Sammendrag, bakgrunn, begrepsbruk mv.

1.1 Sammendrag

Delutredning I inneholder forslag til nødvendige lovtiltak for gjennomføring av Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi 8. november 2001 (heretter konvensjonen) i norsk rett. Lovforslagene omfatter utkast til enkelte endringer i straffeloven og straffeprosessloven. Før øvrig oppfyller norsk rett i alt vesentlig forpliktelsene i konvensjonen.

Konvensjonen er delt inn i fire kapitler. Kapittel 1 gjelder begrepsbruken. Videre regulerer kapittel 2 tiltak som skal iverksettes på nasjonalt nivå, mens kapittel 3 omhandler internasjonalt samarbeid. Konvensjonens avsluttende bestemmelser er samlet i kapittel fire.

I utredningen kapittel 1 gjøres det rede for utvalgets sammensetning og mandat. Videre beskriver utvalget kort den historiske utviklingen av det internasjonale samarbeidet innenfor området datakriminalitet. Deretter gjør utvalget rede for begrepene som er benyttet i konvensjonen og definert i artikkel 1.

I utredningen kapittel 2 behandler utvalget de straffebestemmelsene som er beskrevet i konvensjonen artikkel 2 til 13. Punkt 2.10 om vern av opphavsrett er etter anmodning fra utvalget utarbeidet av professor Jon Bing, Universitetet i Oslo.

Artikkel 2 gjelder datainnbrudd. Utvalget har vurdert straffeloven § 145 annet ledd og kommet frem til at denne bestemmelsen er i samsvar med forpliktelsene i artikkel 2. Det forutsettes imidlertid at Norge avgir en erklæring i henhold til artikkel 40. Videre anbefaler utvalget at strafferammen endres.

Utvalget har kommet frem til at det ikke er nødvendig med lovendringer for å gjennomføre konvensjonens bestemmelser om kriminalisering av dataavlytting i artikkel 3, dataskadeverk i artikkel 4, systemskadeverk i artikkel 5, elektronisk dokumentfalsk i artikkel 7, databedrageri i artikkel 8, vern av opphavsrett og nærstående rettigheter i artikkel 10, medvirkning og forsøk i artikkel 11, foretaksstraff i artikkel 12 og sanksjoner i artikkel 13.

Artikkel 6 gjelder ulike former for ulovlig befatning med tilgangsdata. Etter utvalgets syn rammes ikke handlingen som beskrevet i artikkel 6, av gjeldende straffelovgivning. Utvalget foreslår derfor en ny straffebestemmelse som kriminaliserer spredning av tilgangsdata som ny § 145 b i straffeloven.

Artikkel 9 omhandler barnepornografi. Utvalget har kommet frem til at straffeloven § 204 første ledd bokstav d dekker de handlingene som er beskrevet i artikkel 9. Det forutsettes imidlertid at Norge benytter reservasjonsadgangen i artikkel 9 nr. 4 for så vidt gjelder artikkel 9 nr. 1 bokstav d. Likefullt mener utvalget at enhver befatning med barnepornografi som utgangspunkt bør rammes av straffeloven. Utvalget kommer tilbake til denne problemstilling i delutredning II.

Konvensjonen artikkel 14 til 22 fastsetter straffeprosessuelle forpliktelser. Disse er behandlet i utredningen kapittel 3.

Utvalget antar at det ikke er nødvendig med lovendringer for å gjennomføre de generelle bestemmelsene i artikkel 14 og 15.

I henhold til artikkel 16 er statene forpliktet til å gi kompetent myndighet adgang til å sikre lagrede data som deretter kan benyttes som bevis i en straffesak. *Utvalgets flertall,* alle medlemmene unntatt Sunde, foreslår en ny bestemmelse i straffeprosessloven for å gjennomføre artikkel 16. Forslaget til ny § 215 a gir påtalemyndigheten adgang til å pålegge en person å sikre elektronisk lagrede data som antas å ha betydning som bevis. Videre regulerer bestemmelsen utlevering av trafikkdata som er sikret gjennom et sikringspålegg. En utvidet utleveringsplikt er etter flertallets oppfatning nødvendig for å gjennomføre artikkel 17. *Mindretallet*, Sunde, foreslår en noe annerledes utformet bestemmelse om sikringspålegg.

Artikkel 18 pålegger statene å gi kompetent myndighet adgang til å utstede pålegg om utlevering av lagrede data og abonnementsinformasjon. Etter utvalgets oppfatning oppfyller straffeloven § 210 forpliktelsene i artikkel 18. Det er derfor ikke nødvendig med endringer i norsk rett.

Utvalget anser det nødvendig med en lovendring for å gjennomføre artikkel 19 nr. 4. Statene

er etter denne bestemmelsen forpliktet til å sikre kompetent myndighet adgang til å pålegge systemadministrator eller andre personer med kjennskap til hvordan et datasystem fungerer plikt til å gi opplysninger som kan lette gjennomføringen av ransaking. Utvalget foreslår derfor en ny § 199 a i straffeprosessloven om opplysningsplikt ved ransaking av et datasystem.

Artikkel 20 gjelder innhenting av trafikkdata i sanntid. Norge oppfyller ikke kravet i bestemmelsen til å åpne for innhenting av trafikkdata i sanntid ved etterforskning av forbrytelsene som er nevnt i artikkel 2 til 11, jf. artikkel 14 nr. 2 bokstav a. Etter utvalgets oppfatning bør Norge benytte reservasjonsadgangen på dette punktet. Det samme gjelder artikkel 21 som regulerer avlytting av innholdsdata.

Artikkel 22 oppstiller krav til det stedlige virkeområdet til straffebud som er fastsatt i samsvar med artikkel 2 til 11 i konvensjonen. Utvalget er av den oppfatning at Norge bør endre straffeloven § 12 for å sikre at den som handler i strid med bestemmelsene i konvensjonen, skal kunne straffes i Norge, uavhengig av om forbrytelsen er begått i Norge eller i utlandet.

Artikkel 23 til 35 fastsetter hvilke regler som skal gjelde for det internasjonale samarbeidet. Disse bestemmelsene er behandlet i utredningen kapittel 4. Etter utvalgets oppfatning nødvendiggjør ikke bestemmelsene lovendringer, men Norge bør benytte seg av reservasjonsadgangen i artikkel 29 nr. 4. Konvensjonen åpner for at statene kan forbeholde seg retten til ikke å etterkomme en anmodning om sikring av lagrede data dersom forfølgningen gjelder andre forhold enn dem som er nevnt i artikkel 2 til 11, og det samtidig er grunn til å tro at vilkåret om dobbel straffbarhet ikke er oppfylt.

1.2 Oppnevning og mandat

Datakrimutvalget ble nedsatt av Regjeringen ved kgl. res. 11. januar 2002. Utvalget ble gitt slik sammensetning:

- Sorenskriver Stein Schjølberg, leder
- Seniorrådgiver Christina Christensen
- Rådgiver Beate S. Dagslet
- Rådgiver, nå kst. tingrettsdommer Marius Stub
- Førstestatsadvokat Inger Marie Sunde
- Teknologidirektør Berit Svendsen
- Forbrukerombud Bjørn Erik Thon
- Advokat Benedict de Vibe

Varamedlemmer, ikke oppnevnt i statsråd:

- Ass. sikkerhetsdirektør Anders Venemyr
- Kst. statsadvokat Erik Moestue
- Seksjonssjef Bente Øverli

Anders Venemyr har møtt som stedfortreder for Berit Svendsen siden oktober 2002, Bente Øverli har møtt som stedfortreder for Bjørn Erik Thon siden desember 2002 og Erik Moestue møtte som stedfortreder for Inger Marie Sunde våren 2003.

Frem til august 2003 var politifullmektig Ole Jacob Garder sekretær for utvalget. Fra august 2003 overtok førstekonsulent Helene Wegner.

Utvalget avholdt sitt første møtet 28. februar 2002. Til sammen har utvalget avholdt 25 møter.

Nedenfor følger utdrag av utvalgets mandat:

> «Straffelovrådet utredet i 1985 ulike rettslige spørsmål knyttet til datakriminalitet. Siden den gang har det skjedd mye på dette området, ikke minst gjennom fremveksten av Internett. Etter Justisdepartementets syn er det derfor grunn til på ny å foreta en samlet gjennomgåelse av de strafferettslige og straffeprosessuelle spørsmål som IKT-kriminalitet reiser, og foreslår at det oppnevnes et utvalg som skal utrede dette nærmere. Skal samfunnet kunne møte de utfordringer dagens og morgendagens kriminalitetsbilde stiller oss overfor, må lovverket være tilpasset den nye tids krav, innenfor de rammer hensynet til den enkeltes personvern og rettssikkerhet setter.
>
> *2. Europarådskonvensjonen om IKT-kriminalitet.*
>
> Europarådet vedtok 8. november 2001 en konvensjon om IKT-kriminalitet (Convention on Cybercrime). Konvensjonen ble undertegnet av Norge 23. november 2001, og til sammen har 31 stater undertegnet. Konvensjonen er foreløpig ikke ratifisert av noen av konvensjonsstatene, og har derfor ennå ikke trådt i kraft.
>
> Gjennom å slutte seg til konvensjonen, forplikter konvenssjonstatene seg til å kriminalisere nærmere bestemte handlinger. Dette gjelder bl.a. datainnbrudd, databedrageri og ulike former for befatning med barnepornografi. Videre forplikter partene seg til å innføre visse tvangsmidler til bruk under politiets etterforsking både av saker om IKT-kriminalitet og av andre straffesaker. Det følger bl.a. av konvensjonen at politiet på nærmere grunnlag skal kunne pålegge enhver å sikre data som er lagret. Politiet skal i tillegg kunne beslaglegge og ransake datamaskiner. For det tredje gir konvensjonen bestemmelser om det gjensidige samarbeidet mellom konvensjonsstatene. Konvensjonen bygger på det utgangspunkt at

statene er forpliktet til raskt å yte hverandre bistand under etterforskingen av saker om IKT-kriminalitet. For å muliggjøre dette, er statene forpliktet til å opprette et kontaktpunkt som skal være bemannet 24 timer i døgnet syv dager i uken (24/7-network).

For at Norge skal kunne ratifisere konvensjonen, er det nødvendig med visse lovendringer. Blant annet er det nødvendig å gi regler om midlertidig sikring av data. Utvalget skal utrede hvilke endringer som må til for å gjennomføre konvensjonen i norsk rett, og foreslå bestemmelser som tilfredsstiller konvensjonens krav.

På de punktene hvor konvensjonen åpner for at statene kan reservere seg, jf. artikkel 42, skal utvalget i tillegg vurdere om denne adgangen bør benyttes. På de punktene hvor statene er gitt en viss valgfrihet med hensyn til gjennomføringen av konvensjonsforpliktelsene, jf. artikkel 40, skal utvalget på samme måte vurdere hvordan denne valgfriheten bør benyttes.

3. Andre lovgivningsspørsmål

I tillegg til de spørsmål som er nevnt under pkt. 2, skal utvalget vurdere om det er behov for andre endringer i straffeloven eller i straffeprosessloven. Utvalget kan foreslå endringer i eksisterende bestemmelser, eller helt nye regler, i den utstrekning det er behov for det. Utvalget bør undersøke om det foreligger internasjonale instrumenter eller initiativ som kan ha betydning for spørsmålene som utvalgsarbeidet reiser.

Utvalget bør iallfall vurdere:

– om straffelovens stedlige virkeområde er hensiktsmessig avgrenset når det gjelder ulovlig materiale på nettet, jf. RG 2001 s. 219,
– straffelovens regler om datainnbrudd og skadeverk,
– om det er behov for lovendringer for å styrke det strafferettslige vernet mot terrorangrep mot datainstallasjoner eller for å kunne bruke IKT for mer effektivt i etterforskingen av saker om terrorisme, enten terrormålet er et dataanlegg eller andre interesser,
– om politiet har tilstrekkelig adgang til å kreve at ulovlig materiale fjernes fra nettet, og
– om det bør innføres en loggføringsplikt når det gjelder trafikkdata.

4. Forholdet til personvern- og rettssikkerhetshensyn mv.

Utvalget må i tillegg til hensynet til samfunnsbeskyttelse vurdere rettssikkerhetsmessige aspekter og hensynet til personvern og ytringsfrihet. Ved drøftelsen av enkeltspørsmål skal utvalget gjøre rede for hvordan disse hensynene berøres og for hvordan disse hensynene bør veies mot hverandre.

Utvalget skal vurdere de økonomiske og administrative konsekvensene av sine forslag, og minst ett forslag skal baseres på uendret ressursbruk, jf. utredningsinstruksen pkt. 3.1.

Utvalget skal utarbeide forslag til lovtekst. Lovforslaget skal være i samsvar med Norges internasjonale forpliktelser, og utarbeides i tråd med Justisdepartementets veiledning Lovteknikk og lovforberedelse (2000).

5. Sammensetning og frister

[…]

Utvalget skal avslutte sitt arbeid innen 31. desember 2003. Hvis ikke annet senere avtales med Justisdepartementet, bes utvalget om å fremme en delinnstilling innen 31. desember 2002 med forslag til gjennomføring av Europarådskonvensjonen i norsk rett, slik at regjeringen hurtigst mulig kan fremme forslag om lovendringer og ratifisere konvensjonen.»

1.3 Internasjonal utvikling

Den første internasjonale organisasjonen som tok initiativ til retningslinjer for harmonisering av straffebestemmelser om datakriminalitet, var OECD. I 1986 vedtok OECD å anbefale medlemslandene å vurdere behovet for straffebestemmelser etter en liste av handlinger som skulle fungere som en fellesnevner. Anbefalingene var basert på en rapport fra en ekspertkomité, se Computer-related Criminality: Analysis of Legal Policy in the OECD-Area.

Europarådet vedtok i 1989 rekommandasjon R(89)9 om datarelatert kriminalitet som anbefaler harmonisering av straffebestemmelser. Europarådets anbefalinger bygger hovedsakelig på arbeidet i OECD.

Videre vedtok Europarådet i 1995 anbefalinger om straffeprosessuelle problemer i tilknytning til informasjonsteknologi i rekommandasjon R(95) 13. Anbefalingene omhandlet blant annet ransaking og beslag, teknisk overvåkning, elektroniske bevis, bruk av kryptering og internasjonalt samarbeid.

FN organiserte sin første internasjonale konferanse som også omfattet datakriminalitet, i Havana, Cuba, i 1990. En resolusjon ble deretter vedtatt i desember 1990 av FNs generalforsamling. På en konferanse i Wien i april 2000 ble særlig straffeprosessuelle spørsmål drøftet.

G-8 landene etablerte i 1997 «Subgroup of High-Tech Crime» og vedtok samme år ti prinsipper i kampen mot datakriminalitet. Det ble blant annet organisert et 24/7-nettverk som nå inkluderer minst 30 land. Etter 11. september 2001 har tiltakene vært fokusert på å forebygge terrorhandlinger.

Den Europeiske Union (EU) har deltatt i konvensjonsarbeidet i Europarådet og har også selv gjennomført harmoniseringstiltak. Kommisjonen fremla 19. april 2002 forslag om harmonisering av straffebestemmelser i et forslag til rådsrammebeslutning om angrep på informasjonssystemer.[1)]

Et internasjonalt konvensjonsforslag er også utarbeidet ved Stanford University, USA.[2)]

Europarådets konvensjon om IKT-kriminalitet 8. november 2001 vedlegges denne utredning. Konvensjonen, med den forklarende rapporten, er også publisert på Internett[3)].

En tilleggsprotokoll til konvensjonen ble åpnet for undertegnelse 28. januar 2003. Protokollen gjelder kriminalisering av rasistiske og fremmedfiendtlige handlinger begått i et datasystem. Utvalget legger til grunn at en vurdering av tilleggsprotokollen om rasisme og fremmedhat ligger utenfor utvalgets mandat.

1.4 Begrepsbruk

I konvensjonen artikkel 1 er enkelte sentrale begreper definert. Disse definisjonene skal legges til grunn ved fastsettelsen av forpliktelsene i de øvrige bestemmelsene i konvensjonen.

Datasystem

I artikkel 1 bokstav a er «computer system» definert som:

> «any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data».

Konvensjonen bruker «computer system» for å betegne en innretning som består av maskinvare og/eller programvare, beregnet på eller brukt til automatisk behandling av digitale data.

Konvensjonens bruk av begrepet «any device» tyder på at konvensjonen tar høyde for de siste årenes tekniske utvikling som har resultert i en konvergens mellom det vi tradisjonelt kjenner som områdene for tele, IT og media. I henhold til konvensjonen antas det ikke å være avgjørende hvilken type innretning som behandler dataene. Utvalget legger derfor til grunn at begrepet «computer system» er ment å være teknologinøytralt. Dette medfører at det ikke er avgjørende for resultatet om innretningen er (en del av) et tradisjonelt datasystem eller en annen innretning som har tilsvarende funksjoner. Innretningen kan være frittstående eller knyttet sammen i nettverk. Det elektroniske kommunikasjonsnettet som binder innretningene sammen kan være jordbasert eller radiobasert. Teknologivalget vil ikke være avgjørende for hvorvidt innretningen er å betrakte som et «computer system».

En slik forståelse er i tilfelle i tråd med forståelsen nasjonalt innenfor området for elektronisk kommunikasjon slik den fremstilles i Ot.prp. nr. 58 (2002-2003) Om lov om elektronisk kommunikasjon. Utvalget finner det hensiktsmessig å legge til grunn en teknologinøytral forståelse av begrepet «computer system» og bruker i det følgende det norske begrepet «datasystem».

Data

«Computer data» er definert i artikkel 1 bokstav b som:

> «any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function».

Konvensjonens definisjon av «computer data» bygger på ISO-definisjonen av data. Konvensjonen bruker begrepet «computer data» for å klargjøre at alle data som behandles elektronisk eller i annen direkte prosesserbar form er omfattet.

ISO-definisjonen av data ligger også til grunn for den norske forståelsen av begrepet «data». Data i denne sammenhengen forstås vanligvis som en elektronisk representasjon av informasjon.

Utvalget legger i det følgende en vid forståelse av begrepet data til grunn, der det avgjørende er om informasjonen er egnet til elektronisk behandling. Teknologivalget innenfor området elektronisk kommunikasjon vil dermed ikke være avgjørende for om noe faller inn under betegnelsen «data».

Tjenestetilbyder

Begrepet «service provider» er definert i artikkel 11 bokstav c som:

---

1) Se http://europa.eu.int/information_society/topics/telecoms/internet/crime/index_en.htm.
2) Se http://cisac.stanford.edu.
3) Se http://conventions.coe.int.

«i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
ii. any other entity that processes or stores computer data on behalf of such communication service or user of such service».

Konvensjonen legger til grunn at begrepet «service provider» omfatter både private og offentlige tjenestetilbydere, uavhengig av om tilbudet retter seg mot allmennheten eller mot en lukket brukergruppe. I henhold til konvensjonens bruk av begrepet «tjenestetilbyder» er det heller ikke avgjørende om tilbyderens tjeneste er gratis eller ytes mot vederlag. Begrepet «tjenestetilbyder» inkluderer tilknyttede enheter og andre som lagrer eller på annen måte behandler data på vegne av tjenestetilbyder. Rene innholdsleverandører omfattes ikke av begrepet, forutsatt at leverandøren ikke også tilbyr elektroniske kommunikasjonstjenester eller andre relevante tjenester.

Begrepsbruken i konvensjonen skiller seg dermed fra bruken av begrepet «tilbyder» i lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven). Tilbyder defineres i ekomloven § 1-5 nr. 14 som «enhver fysisk eller juridisk person som tilbyr andre tilgang til elektronisk kommunikasjonsnett eller -tjeneste». Felles for tilbyderne etter denne loven er at de alle i en eller annen form tilbyr slik tilgang til eksterne fysiske eller juridiske personer. Dersom en virksomhet utelukkende leverer slik tilgang innad i egen virksomhet, er som hovedregel ikke virksomheten å anse som en tilbyder i lovens forstand.

Konvensjonen skiller seg også fra en lignende definisjon i Ot.prp. nr. 31 (2002-2003) om lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester (ehandelsloven). Her defineres begrepet «tjenesteyter» som en fysisk eller juridisk person som tilbyr informasjonssamfunnstjenester. En informasjonssamfunnstjeneste er i henhold til Ot.prp. nr. 31 (2002-2003) enhver tjeneste som vanligvis ytes mot vederlag og som formidles elektronisk, over avstand og etter individuell anmodning fra en tjenestemottaker, samt enhver tjeneste som består i å gi tilgang til, eller overføre informasjon over, et elektronisk kommunikasjonsnett, eller i å være nettvert for data som leveres av tjenestemottakeren. Taletelefoni og telefaks- og telekstjenester faller utenfor loven. Forståelsen av begrepet «tjenesteyter» kommenteres ikke nærmere i merknadene til lovforslaget. Vederlagskravet står imidlertid tilsynelatende nokså sterkt i denne definisjonen.

Utvalget finner at begrepet tjenestetilbyder i konvensjonen ikke fullt ut er identisk med begrepet «tilbyder» i Ot.prp. nr. 58 (2002-2003). Det er i tillegg usikkert om begrepet tjenesteyter dekker begrepet tjenestetilbyder i konvensjonen.

Utvalget legger i det følgende en forståelse av begrepet tjenestetilbyder til grunn som omfatter alle private og offentlige tjenestetilbydere, uavhengig av om tilbudet er rettet mot allmennheten eller mot lukkede brukergrupper, og uavhengig av om det ytes vederlag for tjenesten.

Trafikkdata

I artikkel 1 bokstav d er begrepet «traffic data» definert som:

> «any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service».

Trafikkdata er en kategori av data hvor det er spesielle lovreguleringsbehov. I konvensjonens forstand er trafikkdata en kategori av data som oppstår i kommunikasjonskjeden for å kunne rute kommunikasjonen fra kommunikasjonens start til slutt. Trafikkdata er definert i merknadene til Ot.prp. nr. 58 (2002-2003) om lov om elektronisk kommunikasjon. I henhold til denne definisjonen er trafikkdata data som er nødvendig for overføring av kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik overføring. Med trafikkdata menes for eksempel data som angir kommunikasjonens opphavssted, bestemmelsessted, rute, klokkeslett, dato, omfang, varighet og underliggende tjenester. Med behandling menes enhver bruk av trafikkdata, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter.

Utvalget legger til grunn at konvensjonens definisjon av trafikkdata i hovedsak er i samsvar med den norske definisjonen i merknadene til ekomloven, jf. Ot.prp. nr. 58 (2002-2003). Det er derfor neppe behov for eller hensiktsmessig å fravike definisjonen av trafikkdata slik den brukes i konvensjonen.

Generelt

Den øvrig begrepsbruken i innstillingen er i overensstemmelse med språkbruken ellers i lovgivningen. I denne begrepsbruken er det ikke tatt

høyde for den tekniske utviklingen som har ført til sammensmelting av tele, IT og media (konvergens). Utvalget vil komme tilbake med eventuelle forslag til oppdatering av begrepsbruken i straffelovgivningen, blant annet på bakgrunn av den tekniske utviklingen, i delutredning II.

Kapittel 2
Straffebestemmelser

2.1 Innledende bemerkninger

I den forklarende rapporten til konvensjonen fremheves det at harmonisering av straffebud vil lette bekjempelsen av datakriminalitet, både på nasjonalt og internasjonalt nivå. Videre reduseres risikoen for jurisdiksjoner med lavere standard, såkalte «data havens». Det internasjonale samarbeidet vil også bli styrket ved utveksling av erfaringer med andre stater. Dernest vil harmonisering av nasjonale straffebestemmelser muliggjøre utlevering av lovbrytere statene imellom.

Straffebestemmelsene i kapittel 2 fastsetter minstekrav til gjennomføringen av konvensjonen i nasjonal rett. Statene kan for øvrig opprettholde eller vedta straffebestemmelser som er mer vidtgående enn konvensjonens bestemmelser. Konvensjonsbestemmelsene er i stor utstrekning basert på retningslinjene i Europarådets rekommandasjoner R(89) og R(95) om datakriminalitet og det arbeidet som tidligere har vært utført av blant annet OECD og FN.

Konvensjonen benytter teknologinøytral tekst slik at bestemmelsene kan få anvendelse både på nåværende og fremtidig teknologi.

Statene kan avgrense mot mindre eller ubetydelige handlinger («petty or insignificant misconduct») ved implementering av bestemmelsene i artikkel 2 til 10, se den forklarende rapporten punkt 37.

Straffebestemmelsene rammer bare forsettlige handlinger. Forsettskravet fastlegges i samsvar med nasjonal rett. I enkelte tilfeller åpner konvensjonen for subjektive tilleggskrav. For eksempel kan konvensjonsstatene oppstille vinnings hensikt som et vilkår for å straffe for databedrageri, jf. artikkel 8.

Konvensjonen åpner for at statene kan reservere seg mot å gjennomføre enkelte av bestemmelsene, jf. artikkel 42, og for deklarasjoner om tilleggsvilkår, jf. artikkel 40.

I enkelte artikler er det et vilkår at handlingen er uberettiget eller rettsstridig («without right»). Det innebærer at en handling ikke alltid vil være straffbar selv om de øvrige vilkårene i straffebudet er oppfylt. I tillegg til de vanlige straffrihetsgrunnene som samtykke, nødrett og nødverge, kan også andre omstendigheter føre til at straffansvar ikke inntrer. Det fremgår av den forklarende rapporten punkt 38 at konvensjonen ikke setter grenser for hvilke omstendigheter som skal kunne føre til at handlingen ikke er straffbar. Statene kan for eksempel bestemme at en handling er straffri hvis den er lovlig foretatt av offentlig myndighet, for eksempel for å trygge den offentlige ro og orden, beskytte nasjonale interesser eller under etterforsking av straffbare handlinger.

2.2 Datainnbrudd – artikkel 2

2.2.1 Folkerettslige forpliktelser

Konvensjonen artikkel 2 omhandler datainnbrudd («illegal access») og lyder:

> «Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.»

Artikkel 2 beskytter datasystemers integritet og tilgjengelighet, og rammer selve den rettsstridige tilgang til eller inntrengning i et datasystem. Bestemmelsen er ment å rekke vidt og omfatter i følge den forklarende rapporten punkt 44 både «hacking», «cracking» og «computer trespass».

Bestemmelsen rammer rettsstridig tilgang til datasystemer – både enkeltstående maskiner og elektroniske nettverk, jf. definisjonen av «datasystem» i artikkel 1 bokstav a, se punkt 1.4.

Der er ikke et vilkår at gjerningsmannen har gjort seg kjent med innholdet av dataene som han har skaffet seg tilgang til. Det avgjørende er om innholdet eller deler av det er gjort tilgjengelig for vedkommende.

Videre kan det være et vilkår for straffansvar at tilgangen er urettmessig («without right»), se punkt 2.1. Autorisert testing for å avsløre svakheter i sikkerhetssystemet faller dermed utenfor bestemmelsens anvendelsesområde. Det å skaffe seg tilgang til de delene av et system som etter sin art er ment å være åpne for allmennheten, rammes heller ikke av bestemmelsen. Eksempler kan være besøk på en nettside, eller bruk av informasjonskapsler («cookies»).

Statene er i artikkel 2 annet punktum gitt anledning til å innskrenke området for den straffbare handlingen ved å fastsette nærmere angitte tilleggsvilkår for at straffansvar skal inntre, jf. artikkel 40. Et mulig tilleggsvilkår for straffansvar er at tilgangen til datasystemet ble oppnådd ved beskyttelsesbrudd («infringing security measures»).

2.2.2 Gjeldende rett

Datainnbrudd rammes av straffeloven § 145 annet ledd. Formålet med bestemmelsen er å beskytte både samfunnets og privates interesse i konfidensialitet og behovet for å kunne stole på datasystemers pålitelighet (integritetshensynet). Videre beskytter bestemmelsen den kommersielle verdien av dataene (vederlagsinteressen). Det siste følger av Ot.prp. nr. 35 (1986-87) s. 21 og Rt. 1994 s. 1610.

Bestemmelsen rammer det å skaffe seg tilgang til data ved å bryte en beskyttelse. Ikke enhver form for sikkerhetsforanstaltninger regnes som beskyttelse i § 145 sin forstand. I NOU 1985: 31 Datakriminalitet heter det på side 31:

> «Tanken bak bestemmelsen er at det primært hviler på innehaveren av anlegget å sørge for beskyttelse mot innsyn fra uberettigede. Først når det er tatt rimelige foranstaltninger i så måte, kan han kreve hjelp fra strafferettsapparatet».

En tilsvarende avgrensning ble lagt til grunn av departementet i Ot.prp. nr. 35 (1986-87) s. 20. Departementet tilføyde imidlertid alternativet «eller på lignende måte» i bestemmelsen. Hensikten var å markere at formuleringen i annet ledd rammer tilfeller hvor tilgangen til data er å anse som «kvalifisert uberettiget», jf. Ot.prp. nr. 35 (1986-87) s. 20. Høyesterett stiller i tråd med ordlyden krav til en viss beskyttelse for at dataene skal være vernet av straffeloven § 145 annet ledd, jf. Rt. 1998 side 1971, men det er ikke avklart hvor mye som skal til. I tvilstilfeller vil henvisningen til brevbruddsbestemmelsen i første ledd kunne gi veiledning, jf. NOU 1985: 31 Datakriminalitet side 31. Fordi et brev enkelt kan åpnes av uvedkommende ved at forseglingen brytes, er ikke formålet med forseglingen å gjøre innholdet fysisk utilgjengelig for andre. Hensikten med forseglingen er å markere at innholdet ikke er offentlig tilgjengelig. Det samme hensynet bør også være relevant for tolkningen av kravet til beskyttelsesbrudd i annet ledd. Det tilsier at hvis den som påberoper beskyttelse har iverksatt skritt som gjør at utenforstående må forstå at innholdet ikke er allment tilgjengelig, så bør vilkåret anses oppfylt.

«Data eller programutrustning» skal tolkes vidt. «Data» omfatter all elektronisk lagret informasjon. Med «programutrustning» menes instruksjonene til datamaskinen, det vil si dataprogrammer, jf. Ot.prp. nr. 35 (1986-87) s. 20. Begrepene må av hensyn til første ledd avgrenses mot data som ikke er maskinlesbare.

I begrepet «skaffe seg adgang til» ligger det ikke et krav om at inntrengeren har tilegnet seg kunnskap om innholdet av informasjonen. Det er nok at dataene er gjort tilgjengelig for inntrengeren gjennom beskyttelsesbruddet.

Henvisningen til at dataene må være lagret, henspeiler på alle former for elektroniske lagringsmedier, herunder harddisk, disketter, CD-ROM, DAT-taper mv. Et krav må imidlertid være at de lagrede dataene kan avleses maskinelt eller avspilles.

Paragraf 145 inneholder et krav om at tilgangen til dataene må være «uberettiget». Beskyttelsesbrudd kan være rettmessig for eksempel hvis den berettigede gir en person fullmakt til å forsøke å forsere en passordbeskyttelse for å teste systemsikkerheten.

Strafferammen er bøter eller fengsel inntil 6 måneder, jf. § 145 første ledd. Forsøk er straffbart, jf. straffeloven § 49. Skyldkravet er forsett, jf. § 40. Medvirkning straffes på samme måte, jf. § 145 fjerde ledd.

2.2.3 Utvalgets vurderinger

Det første spørsmålet som oppstår er om det er det samme objektet som er beskyttet i artikkel 2 og i straffeloven § 145 annet ledd, det vil si om «data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler» har et like vidt anvendelsesområde som «the whole or any part of a computer system». På bakgrunn av redegjørelsen for artikkel 2 og § 145 annet ledd i punkt 2.2.1 og 2.2.2 har utvalget kommet frem til at anvendelsesområde til § 145 annet ledd er tilstrekkelig vidt.

Videre må utvalget ta stilling til om strafferam-

men i § 145 annet ledd er tilfredsstillende. Strafferammen er bøter eller fengsel inntil 6 måneder. Dermed vil ikke de tvangsmidlene som krever strafferamme høyere enn 6 måneder kunne benyttes i en sak om datainnbrudd. Det gjelder blant annet utvalgets forslag til bestemmelse om sikringspålegg. I henhold til artikkel 14 nr. 2 skal de prosessuelle bestemmelsene som er omfattet av konvensjonen, kunne anvendes ved overtredelser av straffebud som gjennomfører forpliktelsene i artikkel 2 til 11. Spørsmålet blir dermed om det skal gis særskilt adgang til å benytte de aktuelle tvangsmidlene i forbindelse med datainnbrudd selv om kravet til strafferamme ikke er innfridd, eller om strafferammen i § 145 annet ledd bør økes.

Etter utvalgets oppfatning er datainnbrudd en mer straffverdig handling enn dagens strafferamme skulle tilsi. Både hensynet til forholdsmessighet mellom lovbrudd og straff (proporsjonalitet) og hensynet til forholdsmessighet mellom straffen for ulike lovbruddstyper (ekvivalens) taler for at strafferammen bør økes. Utvalget går i delutredning I inn for å øke strafferammen i straffeloven § 145 første og annet ledd til «bøter eller fengsel inntil 6 måneder *eller begge deler*». I delutredning II vil utvalget komme tilbake til spørsmålet om strafferammen bør økes ytterligere.

Utvalget har kommet frem til at § 145 annet ledd ellers er i samsvar med de kravene konvensjonen stiller. En forutsetning er imidlertid at Norge erklærer at man ønsker å benytte det valgfrie tilleggsvilkåret i artikkel 2 annet punktum om beskyttelsesbrudd, «infringing security measures», jf. artikkel 40.

2.3 Dataavlytting - artikkel 3

2.3.1 Folkerettslige forpliktelser

Konvensjonen artikkel 3 gjelder dataavlytting («illegal interception») og lyder:

> «Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.»

Artikkel 3 rammer det å fange opp data på en rettsstridig måte. Handlingen representerer den samme typen krenkelse som tradisjonell avlytting og opptak av muntlige samtaler mellom personer. Bestemmelsen får anvendelse på alle former for elektronisk dataoverføring, enten det er ved hjelp av telefon, faks, e-post eller filoverføring.

Bestemmelsen rammer det å avlytte, fange opp eller overvåke innholdet av informasjon ved bruk av tekniske hjelpemidler. Avlyttingen kan skje direkte ved tilgang til og bruk av datasystemet, eller indirekte ved bruk av elektronisk avlyttingsutstyr. Videre kan avlyttingen omfatte opptak. Henvisningen til at avlyttingen må skje ved hjelp av tekniske hjelpemidler innebærer en begrensing av bestemmelsens rekkevidde.

Begrepet «non-public» retter seg mot selve overføringen av informasjon, og ikke innholdet av denne. Dette betyr at selv offentlig tilgjengelig informasjon kan være «non-public» i konvensjonens forstand. Det avgjørende er om de kommuniserende parter har hatt til hensikt å kommunisere fortrolig. Begrepet fanger også opp tilfeller hvor informasjonen er ment å være utilgjengelig inntil mottaker har betalt for den. Et typisk eksempel er betal-tv.

Bestemmelsen verner også mot oppfanging av data via elektromagnetisk stråling. Slik stråling vil typisk kunne genereres fra kabler. Selv om dette ikke er «data» i vanlig forstand, vil slik stråling kunne omdannes til maskinlesbare data.

Videre rammer bestemmelsen bare rettsstridig dataavlytting, jf. begrepet «without right», se punkt 2.1.

2.3.2 Gjeldende rett

Den generelle bestemmelsen om dataavlytting i norsk rett er straffeloven § 145 annet ledd. Foruten å verne lagrede data, beskytter bestemmelsen også mot uberettiget tilgang til data eller programutrustning under overføring.

Kravet til beskyttelsesbrudd i § 145 annet ledd gir ikke like god mening i forhold til data under overføring som det gjør for lagrede data. Dette har lovgiver tatt hensyn til ved å tilføye formuleringen «på lignende måte». I Ot.prp. nr. 35 (1986-87) s. 20 heter det:

> «Ved at 'på lignende måte' er føyd til, blir tolkningen av vilkåret om å bryte en beskyttelse ikke så avgjørende. Poenget er at § 145 bare kan

> ramme tilfeller hvor det å skaffe seg adgang til data må karakteriseres som *kvalifisert uberettiget* [utvalgets utheving]. Å bryte en beskyttelse er et slikt kvalifiserende moment, men det vil også kunne tenkes lignende situasjoner hvor det å ta seg inn til data vil være så graverende at § 145 bør få anvendelse. § 145 får også anvendelse på informasjon som overføres ved telex, telefax og lignende, og i disse tilfeller gir ikke alltid kravet om å bryte en beskyttelse den riktige avgrensningen. Ved vurderingen kan sammenhengen med første ledd gi en viss veiledning. For øvrig vil avgjørelsen måtte bero på et skjønn hvor også andre momenter ved handlingen og handlingssituasjonen trekkes inn.»

Uttalelsen viser at oppfanging av data under overføring rammes av bestemmelsen. Dette til tross for at det man normalt betegner som beskyttelsestiltak, ikke er iverksatt.

Overføringen må skje ved «elektroniske eller andre tekniske midler». Dersom dataene for eksempel overføres på et lagringsmedium via posten, vil en uberettiget oppfanging rammes av bestemmelsens første ledd.

Oppfangingen av dataene må være uberettiget. På samme måte som ved lagrede data, innebærer vilkåret en ordinær rettsstridsreservasjon.

Avlytting av telefonsamtaler rammes av straffeloven § 145 a, mens avlytting av vernede tjenester rammes av straffeloven § 262. Utvalget går imidlertid ikke nærmere inn på disse særbestemmelsene.

2.3.3 Utvalgets vurderinger

Det første spørsmålet som må avklares, er om det å «skaffe seg adgang» i straffeloven § 145 annet ledd er et like vidt begrep som «interception» i artikkel 3. Utvalget legger til grunn at det er selve tilgangen til data under overføring som er avgjørende, ikke om inntrengeren har skaffet seg kunnskap om innholdet. Utvalget har på denne bakgrunnen kommet frem til at anvendelsesområdet til § 145 annet ledd er tilstrekkelig vidt.

Artikkel 3 åpner for at straffebud mot dataavlytting begrenses til å omfatte de tilfellene der tekniske hjelpmidler («technical means») er benyttet. Videre gjelder artikkel 3 bare ikke-offentlige («non-public») overføringer av data. Disse vilkårene skaper ingen problemer for gjennomføringen av konvensjonen ettersom straffeloven § 145 har et videre anvendelsesområde.

Artikkel 3 åpner i motsetning til artikkel 2 ikke for å sette brudd på en beskyttelse som vilkår for straffansvar. Til tross for at straffeloven § 145 annet ledd inneholder et vilkår om at gjerningsmannen må ha brutt «en beskyttelse eller på lignende måte» skaffet seg tilgang til dataene, har utvalget kommet frem til at anvendelsesområdet til § 145 ikke er snevrere enn hva konvensjonen krever på dette punktet.

I henhold til forarbeidene til § 145 verner bestemmelsen om data som overføres via telefaks, telex og lignende, se Ot.prp. nr. 35 (1986-87) s. 20. Det samme må etter utvalgets oppfatning gjelde for annen overføring av data fra et datasystem. Kryptering eller annen form for utilgjengeliggjøring er ikke påkrevd. Etter utvalgets oppfatning vil det være avgjørende dersom overføringen ikke er offentlig. Er overføringen av en slik karakter, vil en rettsstridig oppfanging anses for å være «kvalifisert uberettiget», jf. Ot.prp. nr. 35 (1986-87) s. 20.

Et eksempel kan illustrere standpunktet. Dersom det blir rettet en mottaker mot et datasystem som fanger opp elektromagnetiske stråler, og disse strålene kan gjenskapes til logisk informasjon, vil handlingen rammes av artikkel 3. For at handlingen skal rammes av straffeloven § 145 annet ledd, kreves det at de elektromagnetiske strålene fanges opp ved brudd på en beskyttelse eller at gjerningsmannen på lignende måte uberettiget skaffer seg tilgang til dataene. Det første straffalternativet er neppe anvendelig. Oppfanging av ubeskyttet informasjon kan etter utvalgts syn vanskelig anses som brudd på en beskyttelse. Spørsmålet blir derfor om uttrykket «på liknende måte» er anvendelig. Etter utvalgets syn må spørsmålet besvares bekreftende. Oppfanging av informasjon på den måten som her er beskrevet, forutsetter at gjerningspersonen har iverksatt visse tiltak. Slike tiltak vil etter utvalgets oppfatning gjøre avlyttingen «kvalifisert uberettiget», jf. Ot.prp. nr. 35 (1986-87) s. 20.

På denne bakgrunnen har utvalget kommet frem til at § 145 annet ledd dekker forpliktelsene i konvensjonen selv om bestemmelsen oppstiller beskyttelsesbrudd som vilkår. Utvalget legger til grunn at oppfanging av en ikke-offentlig overføring av data ved bruk av tekniske hjelpemidler vil være «kvalifisert uberettiget», og dermed rammes av § 145 annet ledd.

Etter utvalgets oppfatning oppfyller straffeloven § 145 annet ledd forpliktelsene i artikkel 3. Det er derfor ikke behov for lovendringer.

2.4 Dataskadeverk – artikkel 4

2.4.1 Folkerettslige forpliktelser

Konvensjonen artikkel 4 omhandler dataskadeverk («data interference») og lyder:

«1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.»

Formålet med bestemmelsen er å sikre at data har samme beskyttelse mot forsettlig skadeverk som fysiske ting. Bestemmelsen beskytter integriteten til og den lovlige bruken av lagrede data. Artikkel 4 gjelder ikke skade på data under kommunikasjon, jf. den forklarende rapporten punkt 60.

Bestemmelsen rammer skade, forringelse, sletting, endring og utilgjengeliggjøring av lagrede data. Alternativene er ment å fange opp ulike tilfeller hvor data på en eller annen måte blir endret.

Skadeverk begått ved hjelp av virus og «trojanske hester» er omfattet av denne bestemmelsen. Selv virus som ikke forårsaker noen skade, og for eksempel bare viser et reklameinnslag e.l., vil omfattes av alternativet «alteration». Implanteringen fører til at eksisterende data blir endret. Dersom viruset som er implantert ikke skader dataene, men derimot selve datasystemet, rammes handlingen av artikkel 5.

Bestemmelsen gjelder også skadeverk som utføres uten bruk av tekniske hjelpemidler. I den forklarende rapporten punkt 61 benyttes uttrykket «any action». Det er heller ikke et krav at handlingen skjer fra et datasystem til et annet. Følgelig rammer bestemmelsen det å skade data på en lokal, frittstående harddisk.

Artikkel 4 rammer bare rettsstridig skadeverk, jf. begrepet «without right», se punkt 1.4. Hvis handlingen er iverksatt eller godkjent av den berettigede til dataene, vil den ikke være rettsstridig. Et eksempel er testing av sikkerheten til et datasystem. Dataskadeverk som følge av slik autorisert testing rammes ikke av bestemmelsen.

Statene kan etter artikkel 4 nr. 2 sette betydelig skade som vilkår for straffansvar.

2.4.2 Gjeldende rett

Straffeloven § 291 rammer det å ødelegge eller skade en gjenstand. Data i seg selv er neppe beskyttet av bestemmelsen, jf. blant annet NOU 1985: 31 s. 9 og 10 og Ot.prp. nr. 35 (1986-87) s. 7 og 8. Derimot er det ikke tvilsomt at et lagringsmedium er en «gjenstand» i § 291 sin forstand. Endring av data innebærer skadeverk overfor lagringsmediet, jf. Ot.prp. nr. 35 (1986-87) s. 14. Ved å endre eller slette data blir lagringsmediet påvirket slik at det ikke kan benyttes som forutsatt.

Det er tvilsomt om data under kommunikasjon rammes av § 291, jf. NOU 1985: 31 s. 10. Utvalget kjenner ikke til rettspraksis som avklarer spørsmålet.

Skyldkravet er forsett, jf. straffeloven § 40. Forsøk og medvirkning er straffbart.

2.4.3 Utvalgets vurderinger

Etter utvalgets oppfatning oppfyller straffeloven § 291 forpliktelsene i artikkel 4. Selv om data som sådan ikke er beskyttet av bestemmelsen, vil lagrede data være tilknyttet et lagringsmedium. Etter utvalgets mening vil endring av data føre til at lagringsmediet anses for å være skadet, og at § 291 følgelig er anvendelig. Videre omfatter ikke forpliktelsene i artikkel 4 data under overføring. Det er derfor ikke behov for å endre norsk rett på dette punktet.

2.5 Systemskadeverk – artikkel 5

2.5.1 Folkerettslige forpliktelser

Konvensjonen artikkel 5 omhandler forstyrrelser av datasystemer («system interference») og lyder:

> «Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.»

Bestemmelsen forplikter statene til å kriminalisere handlinger som forhindrer rettmessig bruk av datasystemer og systemer for elektronisk kommunikasjon, jf. den forklarende rapporten punkt 65. Mens artikkel 4 beskytter selve dataene, er det datasystemet som er beskyttet i artikkel 5, det vil

si funksjonaliteten til maskinvare og programvare sett i sammenheng.

Uttrykket «functioning of a computer system» er vidtrekkende, og innebærer at enhver type funksjonalitet er beskyttet. Bestemmelsen åpner for at statene kan sette som vilkår at funksjonaliteten er vesentlig svekket («serious hindering»).

Artikkel 5 rammer bare rettstridige handlinger, jf. «without right».

2.5.2 Gjeldende rett

Systemskadeverk kan etter omstendighetene rammes av flere bestemmelser. Det vises til redegjørelsen for straffeloven § 291 under punkt 2.4.2. Ettersom utvalget har kommet frem til at § 291 dekker gjerningsbeskrivelsen i artikkel 5, gjør det ikke rede for andre bestemmelser som kan tenkes å være anvendelige.

2.5.3 Utvalgets vurderinger

Utvalget har kommet frem til at forpliktelsene i artikkel 5 dekkes av straffeloven § 291 hva gjelder simpelt systemskadeverk, og § 291, jf. § 292, hva gjelder grovt skadeverk. Etter utvalgets oppfatning er det derfor ikke nødvendig med endringer i norsk rett.

2.6 Ulovlig tilgjengeliggjøring av tilgangsdata – artikkel 6

2.6.1 Folkerettslige forpliktelser

Konvensjonen artikkel 6 omhandler ulovlige tilgjengeliggjøring av tilgangsdata m.m. («misuse of devices») og lyder:

«1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
   a) the production, sale, procurement for use, import, distribution or otherwise making available of:
      i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
      ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,
      with intent that it be used for the purpose of committing any of the offences established in articles 2 through 5; and
   b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.»

Artikkel 6 har som mål å forebygge straffbare handlinger som beskrevet i artikkel 2 til 5. I følge den forklarende rapporten punkt 71 krever slike straffbare handlinger ofte spesielle hjelpemidler. Ved å kriminalisere visse former for befatning med denne typen hjelpemidler, styrkes arbeidet med å avverge datakriminalitet.

Artikkel 6 nr. 1 bokstav a underpunkt i forplikter konvensjonsstatene til å kriminalisere produksjon, salg, kjøp, import, distribusjon og andre former for tilgjengeliggjøring av elektroniske innretninger, utstyr og dataprogrammer som primært er designet for eller tilpasset til å begå straffbare handlinger som beskrevet i artikkel 2 til 5. Videre er statene i henhold til underpunkt ii forpliktet til å kriminalisere tilsvarende befatning med passord, tilgangskoder og lignende informasjon som er egnet til å gi tilgang til hele eller deler av et datasystem.

Artikkel 6 nr. 1 bokstav b gjelder besittelse av tilgangsmidler som nevnt i bokstav a, med den hensikt at de skal brukes til å begå en straffbar handling som beskrevet i artikkel 2 til 5. Bestemmelsen

åpner for at det settes som vilkår for straffansvar at gjerningsmannen besitter et bestemt antall tilgangsmidler.

Artikkel 6 nr. 3 åpner for at statene kan reservere seg mot å gjennomføre enkelte av forpliktelsene i artikkel 6 nr. 1, jf. artikkel 42. Reservasjonsadgangen omfatter imidlertid ikke bokstav a underpunkt ii når det gjelder salg, distribusjon og annen form for tilgjengeliggjøring av tilgangsdata.

2.6.2 Gjeldende rett

I norsk straffelovgivning finnes det ingen straffebestemmelse som fullt ut dekker de handlingene som er beskrevet i artikkel 6. Derimot dekker straffeloven §§ 317 og 262 deler av gjerningsinnholdet. I tillegg vil flere av handlingene som er beskrevet i artikkel 6, kunne rammes som forsøk på eller medvirkning til andre forbrytelser, for eksempel datainnbrudd etter straffeloven § 145 annet ledd.

Den som besitter eller sprer et passord eller lignende tilgangsdata som er ervervet ved en straffbar handling, vil kunne straffes etter straffeloven § 317 om heleri. Bestemmelsen rammer den som «mottar eller skaffer seg eller andre del i utbytte av en straffbar handling, eller som yter bistand til å sikre slikt utbytte for en annen». Med «utbytte» menes «noe som har vært fremskaffet ved en straffbar handling eller som på annen måte står i nær sammenheng med en straffbar handling. I Rt. 1995 s. 1872 har Høyesterett lagt til grunn at også en PIN-kode vil kunne være utbytte i lovens forstand dersom de «har økonomisk betydning og er egnet til å bli disponert over». Tilsvarende må etter utvalgets oppfatning gjelde passord og andre tilgangskoder, selv om det er uklart hvor langt avgjørelsen rekker. For utvalget er det imidlertid ikke nødvendig å gå nærmere inn på dette.

Også straffeloven § 262 om dekodingsinnretninger kan få anvendelse på handlinger som beskrevet i artikkel 6. Etter første ledd rammer bestemmelsen det å besitte eller spre en dekodingsinnretning i den hensikt å skaffe noen uautorisert tilgang til en vernet tjeneste, for eksempel kodede radio- og fjernsynssignaler. Uttrykket «dekodingsinnretning» er definert i tredje ledd. Etter forarbeidene vil både PIN-koder og andre koder som gir tilgang til vernede tjenester, kunne være dekodingsinnretninger i lovens forstand, jf. Ot.prp. nr. 51 (2000-2001) s. 14.

Disse straffebestemmelsene må suppleres med de alminnelige reglene om forsøk og medvirkning. Den som overlater et datavirus til en annen for at vedkommende skal begå skadeverk, jf. straffeloven § 291, vil kunne straffes for medvirkning dersom han regner det for sikkert eller overveiende sannsynlig at hovedmannen kommer til å begå skadeverk, og at hans eget bidrag vil stå i et medvirkende årsaksforhold til dette, jf. Husabø, *Straffansvarets periferi,* s. 239-240. Det samme gjelder hvor et dataprogram eller et passord legges ut på Internett, selv om vedkommende på gjerningstidspunktet ikke vet om programmet eller passordet vil blir brukt til å begå straffbare handlinger, og i tilfelle av hvem. Kommer hovedmannen bare til forsøksstadiet, for eksempel fordi datainnbruddet ikke lykkes, vil medvirkeren kunne straffes for medvirkning til forsøk. Og dersom hovedmannen ennå ikke har passert forsøkspunktet, eller derom medvirkerens bidrag ikke sto i noen medvirkende årsaksforhold til det etterfølgende skadeverket, vil medvirkeren etter omstendighetene kunne straffes for forsøk på medvirkning.

2.6.3 Utvalgets vurderinger

2.6.3.1 Behov for lovendringer?

Straffeloven § 317 om heleri gjelder som nevnt bare utbytte av straffbare handlinger, og omfatter dermed blant annet ikke de tilfellene hvor gjerningspersonen har gjettet passordet, eller forsøkt seg frem ved hjelp av en datamaskin. Straffeloven § 262 om dekodingsinnretninger gjelder som nevnt bare passord som gir tilgang til vernede tjenester. Bestemmelsen rammer ikke passord som gir tilgang til andre former for data, for eksempel bedriftshemmeligheter eller sensitive personopplysninger. Etter utvalgets syn kan det derfor ikke være tvilsomt at artikkel 6 gjør det nødvendig med lovendringer, jf. også NOU 2002: 4 Ny straffelov s. 319. Dette gjelder selv om reservasjonsadgangen i artikkel 6 nr. 3 benyttes, og selv om man tar hensyn til at flere av de handlingene konvensjonen omfatter, vil kunne rammes som forsøk på eller medvirkning til andre straffbare handlinger.

2.6.3.2 Bør Norge bruke reservasjonsadgangen?

Artikkel 6 åpner som nevnt for at statene kan reservere seg mot deler av bestemmelsen. Etter artikkel 6 nr. 3 er statene bare forpliktet til å gjennomføre artikkel 6 nr. 1 bokstav a underpunkt ii om salg, distribusjon og annen spredning av passord, tilgangskoder mv. som gir adgang eller tilgang til et datasystem. Statene kan dermed velge ikke å kriminalisere besittelse eller spredning av hackerverktøy, virus og andre dataprogrammer som hovedsakelig er utformet for å begå forbrytelser som nevnt i artiklene 2 til 5, jf. artik-

kel 6 nr.1 bokstav a underpunkt i og bokstav b.

Ved vurderingen av om Norge bør reservere seg, er det etter utvalgets oppfatning naturlig å ta utgangspunkt i at artikkel 6 retter seg mot ulike forberedelseshandlinger. Etter norsk rett er slike handlinger normalt straffrie. Et grunnleggende synspunkt i norsk lovgivningstradisjon er at straffelovgivningen ikke bør ramme flere handlinger enn det reelt sett er grunn til å kriminalisere, jf. Straffelovkommisjonens prinsipielle drøftelse i NOU 2002: 4 Ny straffelov s. 79-86. Straff er samfunnets skarpeste reaksjon mot uønsket atferd, og bør brukes med varsomhet. Særlig varsom bør man være med å kriminalisere forberedelseshandlinger. Slike handlinger krenker normalt ikke beskyttelsesverdige interesser, og det kan være usikkert om den straffbare handlingen som forberedes, vil bli gjennomført. I straffeloven finnes det derfor bare få bestemmelser som retter seg mot forberedelseshandlinger. De fleste av disse gjelder alvorlige straffbare handlinger, for eksempel anslag mot rikets sikkerhet (straffeloven § 94) og andre terrorhandlinger (straffeloven § 147 a fjerde ledd). En nærmere oversikt er gitt i Husabø, *Straffansvarets periferi*, s. 316-336.

Utvalget ser først på spørsmålet om det bør være straffbart å *besitte* datavirus og andre skadevoldende dataprogrammer i den hensikt å begå visse straffbare handlinger. Det er uten videre klart at besittelsen isolert sett ikke krenker beskyttelsesverdige interesser. Samtidig er det en latent risiko for at den som besitter slike programmer, vil spre dem til andre. Slik spredning kan skje uforvarende, for eksempel ved at viruset sprer seg selv uten at vedkommende har kjennskap til det, men også i den hensikt å forvolde skade. Man kan også tenke seg at viruset sendes til noen som selv skal bruke det til straffbare formål.

Etter utvalgets oppfatning er imidlertid denne latente risikoen neppe i seg selv tilstrekkelig grunn til å kriminalisere selve besittelsen, heller ikke når hensikten er å begå eller medvirke til å begå straffbare handlinger. Selv om besittelsen normalt er klart uønsket sett fra samfunnets side, er den neppe i seg selv straffverdig. Ser man bort fra de straffebud som rammer besittelse av særlig farlige gjenstander, for eksempel plutonium og uran (straffeloven § 152 a) eller sprengstoff (straffeloven § 161), er det normalt ikke straffbart å besitte gjenstander som vil kunne benyttes til straffbare formål, heller ikke om det var hensikten med anskaffelsen. Det er for eksempel ikke straffbart å erverve eller inneha et skytevåpen, selv ikke om hensikten bevislig er å ta noen av dage, dersom vedkommende har tillatelse etter lov 9. juni 1961 nr. 1 om skytevåpen og ammunisjon mv. (våpenloven) §§ 7 og 8. Selve besittelsen krenker heller ikke andres interesser på samme måte som besittelse av for eksempel barnepornografi, jf. straffeloven § 204 første ledd bokstav d, eller offentlige interesser på samme måte som besittelse av narkotika, jf. straffeloven § 162 første ledd.

I forlengelsen av dette vil utvalget fremheve at det kritikkverdige ved handlingen ikke først og fremst ligger på dens objektive side, men på den subjektive. Særlig klart er dette når det gjelder dataprogrammer som kan brukes til både lovlige og ulovlige formål. Det man i tilfelle vil reagere mot, er langt på vei gjerningspersonens subjektive forestillinger om hva han skal bruke programmet til. En slik subjektivisering av straffansvaret kan i seg selv være uheldig, jf. Husabø, *Straffansvarets periferi,* s. 376-377. I tillegg kan betydningen av rent subjektive elementer innebære en viss risiko for uriktige domfellelser, jf. NOU 2002: 4 Ny straffelov s. 96-97. Dette har sammenheng med at vurderingen av om den mistenkte har til formål å begå straffbare handlinger, som oftest vil måtte skje ut fra slutninger basert på de ytre omstendigheter i saken. Selv om dommeren skal la all rimelig tvil komme den tiltalte til gode, vil usikkerheten ved bevisbedømmelsen under skyldspørsmålet kunne bli større enn ellers.

Utvalget vil også peke på at en straffebestemmelse som rammer besittelse av dataprogrammer indirekte vil øke kontrollnivået i den private sfære. Siden Norge er folkerettslig forpliktet til å la konvensjonens straffeprosessuelle bestemmelser få anvendelse på alle de handlinger konvensjonen gjelder, jf. artikkel 14 nr. 2 bokstav a, vil man måtte åpne for bruk av tvangsmidler mot den som med skjellig grunn mistenkes for besittelse av slike programmer. Som Husabø peker på, har ikke det bare positive sider, jf. Straffansvarets periferi s. 377-378. Bruk av tvangsmidler vil uvegerlig utgjøre et større eller mindre integritetsinngrep overfor den som rammes. I tillegg vil ransakingen eller beslaget kunne gi politiet forskjellige former for overskuddsinformasjon det ellers ikke ville fått tilgang til. Selv om kravet til mistanke vil bidra til at tvangsmidler iallfall ikke kan anvendes overfor dem som er helt utenfor mistanke, vil også den som med skjellig grunn mistenkes for en straffbar handling kunne være uskyldig. På et tidlig stadium av etterforskningen er det ikke alltid lett å vite hvem som er hvem. Man må derfor ta i betraktning at tvangsmidler vil kunne bli benyttet overfor dem som ikke har noe med saken å gjøre. Denne risikoen vil øke dersom straffebudet langt på vei

henviser til rent subjektive forhold hos gjerningsmannen.

På denne bakgrunn mener utvalget at Norge bør reservere seg mot å oppstille straffansvar for besittelse av visse dataprogrammer, jf. artikkel 6 nr. 1 bokstav a punkt i og bokstav b.

Etter utvalgets syn er det heller ikke tilstrekkelig grunn til å gjøre *spredning* av slike dataprogrammer til en selvstendig forbrytelse. Riktignok kan det være større grunn til å reagere mot spredning enn mot ren besittelse, siden den som sender et program fra seg, mister kontrollen over hva det brukes til. Slike handlinger vil imidlertid ofte allerede være straffbare etter de alminnelige reglene om forsøk og medvirkning. Et eget straffebud som rammer videreformidling vil dermed få begrenset selvstendig betydning.

Under enhver omstendighet er det vanskelig å se at risikoen for at et dataprogram kan bli brukt av andre til straffbare formål, gir tilstrekkelig grunn til å straffesanksjonere selve spredningen. De straffebud som av preventive hensyn retter seg mot en abstrakt fare av denne type (såkalte abstrakte faredelikter), retter seg gjerne mot situasjoner hvor liv og helse står på spill, for eksempel knivforbudet i straffeloven § 352 a og farts- og promillebestemmelsene i lov 18. juni 1965 nr. 4 (vegtrafikkloven) §§ 6 og 22. Spredning av dataprogrammer berører ikke slike hensyn. Behovet for preventiv lovgivning reduseres dessuten av at det i vår sammenheng vil finnes en hovedmann som vil kunne gjøres strafferettslig ansvarlig, hvis det først er begått en straffbar handling. Det gjør det mindre naturlig enn ellers å kriminalisere selve farefremkallelsen.

Utvalget har etter dette kommet til at man inntil videre bør bruke den reservasjonsadgang bestemmelsen gir, og fremmer derfor i denne omgang ikke forslag om å kriminalisere verken besittelse eller spredning av hackerverktøy, virus og andre dataprogrammer som hovedsakelig er utformet for å begå forbrytelser som nevnt i artiklene 2 til 5, jf. artikkel 6 nr.1 bokstav a punkt i og bokstav b.

2.6.3.3 Nærmere om utformingen av bestemmelsen

Etter artikkel 6 nr. 3 er statene forpliktet til å kriminalisere salg, distribusjon og annen spredning av passord, tilgangskoder mv. som gir adgang eller tilgang til et datasystem. Det første spørsmålet som da oppstår, er om konvensjonens forpliktelse bør gjennomføres gjennom en endring av én eller flere eksisterende straffebestemmelser, eller gjennom en ny bestemmelse.

Så vidt utvalget kan se, er det ingen straffebestemmelse i straffeloven som fra før rammer lignende forhold som det artikkel 6 retter seg mot. Å endre straffeloven §§ 317 eller 262 er av flere grunner uaktuelt. Den nye straffebestemmelsen bør derfor plasseres i et nytt straffebud, for eksempel som ny § 145 b.

Når det gjelder bestemmelsens *objektive gjerningsinnhold*, må man først ta stilling til *hvilke data* som skal rammes. Konvensjonen retter seg mot «computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed», jf. punkt 1.1 ovenfor. Bestemmelsen kan derfor ikke begrenses til å gjelde passord, men må gjelde alle former for data som kan gi tilgang til hele eller deler av et datasystem. Det er dermed uten betydning om dataene er bærere av tall, symboler eller bokstaver, om disse i kombinasjon er meningsbærende, og om dataene er kryptert. Dernest oppstår spørsmålet om hvilke former for *befatning* med tilgangsdata som bør omfattes av straffebudet. Etter konvensjonen må straffebudet iallfall ramme det å selge, distribuere eller på annen måte gjøre slike data tilgjengelige for andre. Statene kan derimot velge om også produksjon, import, anskaffelse til bruk (jf. artikkel 6 nr. 1 bokstav a) og besittelse (jf. artikkel 6 nr. 1 bokstav b) skal rammes. Etter utvalgets syn er det imidlertid neppe tilstrekkelig grunn til å kriminalisere dette, og viser i den forbindelse til de prinsipielle synspunkter det ble gjort rede for i punkt 1.3.1 ovenfor. – Medvirkning straffes på samme måte, jf. konvensjonen artikkel 11 nr. 1.

Når det gjelder *skyldkravet*, blir spørsmålet om det bør kreves at gjerningspersonen har til hensikt å begå straffbare handlinger, slik konvensjonen legger opp til, eller om det bør være tilstrekkelig med alminnelig forsett. I NOU 2002: 4 Ny straffelov s. 168 og s. 175-176 drøfter Straffelovkommisjonen om det er grunn til å videreføre hensiktskravet i straffebud som rammer forberedelseshandlinger, slik denne bestemmelsen vil gjøre. Etter kommisjonens oppfatning bør hensiktskravet bare beholdes når den straffbare handlingen kun er straffverdig når den foretas i den hensikt straffebudet nevner. Det å spre passord mv. kan etter utvalgets oppfatning være straffverdig selv om gjerningspersonen ikke har til hensikt å begå en forbrytelse, siden forsettskravet vil innebære at han må ha holdt det for sikkert eller overveiende sannsynlig at noen vil bruke det til å begå en straffbar handling. Til dette kommer at et hensiktskrav vil skape bevisproblemer for påtalemyndigheten, som i sin tur vil kunne bidra til å redusere straffebudets praktiske betydning. Alminnelig forsett bør derfor være tilstrekkelig.

Konvensjonen angir ingen bestemt *strafferamme* utover å kreve at straffen skal være «effective, proportionate and dissuasive», jf. artikkel 13 nr. 1. Statene står dermed langt på vei fritt ved fastsettelsen av straffenivået. Etter utvalgets syn er det naturlig å ta utgangspunkt i at straffebudet systematisk sett rammer rene forberedelseshandlinger. Strafferammen bør derfor ikke være for høy, og iallfall ikke høyere enn strafferammen i de straffebudene som typisk vil kunne overtres ved hjelp av passordet mv. Mest praktisk er kanskje datainnbrudd og skadeverk, jf. straffeloven §§ 145 annet ledd og 291 annet ledd. Strafferammen for datainnbrudd er fengsel inntil 6 måneder, mens straffen for skadeverk er bøter eller fengsel inntil 1 år. Både hensynet til forholdsmessighet mellom lovbrudd og straff (proporsjonalitet) og hensynet til forholdsmessighet mellom straffen for ulike lovbruddstyper (ekvivalens) taler for at strafferammen i utgangspunktet settes til bøter eller fengsel i 6 måneder eller begge deler. Strafferammen vil dermed normalt ikke overstige strafferammen for noen av de lovbrudd den aktuelle forberedelseshandlingen knytter seg til, men den kan etter omstendighetene være lavere. Bakgrunnen for det er at en forberedelseshandling normalt er mindre straffverdig enn det å fullbyrde en (annen) forbrytelse. Samtidig er strafferammen høy nok til å åpne for bruk av tvangsmidler etter straffeprosessloven, slik konvensjonen forplikter oss til, jf. artikkel 14 nr. 2 bokstav a.

I enkelte særlig alvorlige tilfeller kan imidlertid en slik strafferamme bli for lav, for eksempel ved omfattende spredning av passord som gir tilgang til sensitive opplysninger. Utvalget foreslår derfor en forhøyet strafferamme på fengsel inntil 2 år i grove tilfeller. I lovutkastet er det angitt hvilke momenter det særlig skal legges vekt på ved avgjørelsen av om spredningen er grov.

Datakriminalitet har ofte et *internasjonalt* preg. Mens tradisjonell kriminalitet ofte forutsetter at gjerningspersonen og den fornærmede er i nærheten av hverandre, vil datakriminalitet rettet mot norske interesser kunne begås fra en hvilken som helst datamaskin hvor som helst i verden, på tvers av landegrensene. Er en straffbar handling begått i samvirke mellom flere, kan gjerningspersonene befinne seg i hvert sitt land på gjerningstidspunktet. Undertiden kan det også være vanskelig å fastslå i hvilket land den straffbare handlingen er begått.

Disse forholdene taler etter utvalgets oppfatning for at bestemmelsen føyes til i straffeloven § 12 første ledd nr. 3. Endringen medfører at overtredelse av bestemmelsen kan straffes i Norge uavhengig av om forbrytelsen er begått i Norge eller i utlandet. Derimot vil ikke en handling begått i utlandet av en utlending kunne straffes i Norge. Fordi norske statsborgere ikke kan utleveres til land utenfor Norden, jf. utleveringsloven § 2, er det viktig å sikre at nordmenn som begår slike forbrytelser i utlandet, kan pådømmes i Norge og sone her.

2.7 Elektronisk dokumentfalsk – artikkel 7

2.7.1 Folkerettslige forpliktelser

Artikkel 7 i konvensjonen gjelder elektronisk dokumentfalsk («computer related forgery») og lyder:

> «Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.»

Formålet med artikkel 7 er å sikre at elektroniske dokumenter har det samme vern mot forfalskning som fysiske dokumenter. Det grunnleggende hensynet bak bestemmelsen er behovet for å verne om dataenes integritet.

Bestemmelsen rammer det å tilføye, endre, slette eller skjule data som er ment å skulle legges til grunn i en rettslig sammenheng. Skyldkravet er forsett. Bestemmelsen åpner for at det settes som vilkår for straffansvar at forfalskningen av dataene må være utført i en bestemt hensikt («with the intent that it be considered or acted upon for legal purposes as if it were authentic»).

Data er «inauthentic» i konvensjonens forstand når de stammer fra en annen enn den angivelige utsteder, jf. den forklarende rapporten punkt 82. Statene står imidlertid fritt til å velge hvorvidt de ønsker å la autentisiteten også omfatte innholdet av dataene.

I medhold av artikkel 7 annet punktum, jf. artikkel 40, kan statene gjøre straffansvaret betinget av at gjerningspersonen har til hensikt å begå bedrageri eller en annen lignende forbrytelse.

2.7.2 Gjeldende rett

Dokumentfalsk rammes av straffeloven § 182 første ledd. Det er lagt til grunn i rettspraksis at bestemmelsen også rammer forfalskning av elektroniske dokumenter, jf. Rt. 1991 s. 532 (BBS-dommen).

Straffeloven § 182 gjelder data som er «eftergjort eller forfalsket». Data anses for å være eftergjort når de i sin helhet stammer fra andre enn den angivelige utsteder, og forfalsket når innholdet er endret, jf. Bratholm/Matningsdal, *Straffeloven*, s. 405-406.

Det er et krav at dataene blir benyttet som om de er ekte eller uforfalsket. Dersom utsteder av data åpent tilkjennegir at dataene er falske, rammes ikke handlingen av bestemmelsen.

De forfalskede dataene må være «benyttet» for å rammes av straffeloven § 182 første ledd. Spørsmålet om hvorvidt endring eller sletting av data innebærer at dataene blir «benyttet» i lovens forstand ble, under noe tvil, besvart bekreftende av Straffelovrådet i NOU 1985: 31 *Datakriminalitet* s. 12. Begrunnelsen var at databehandling er automatisert, slik at forfalskningen og benyttelsen av dataene smelter sammen i én handling.

Spørsmålet ble berørt av Høyesterett i Rt. 1991 s. 532 (BBS-dommen). Saken gjaldt manipulasjon av data. Siktede byttet ut trygdemottakeres kontonummer med sine egne:

> «Det er i og for seg klart at uberettigede endringer av data etter omstendighetene kan rammes som benyttelse av falsk dokument, jf drøftelsen i NOU 1985: 31 side 11-12. For byretten var det omtvistet om de forfalskede data kunne sies å være benyttet. Byretten kom til at så var tilfellet, og det er jeg enig i.»

Handlingen må være utført i «rettsstridig hensikt».

Straffeloven § 185 annet ledd rammer selve forfalskningen når den skjer i den hensikt å benytte dokumentet eller la det benytte på en straffbar måte.

2.7.3 Utvalgets vurderinger

Som påpekt i kapittel 2.7.2, rammer hovedregelen om dokumentfalsk i straffeloven § 182 bruken av et falsk eller ettergjort dokument. Konvensjonen artikkel 7 retter seg derimot mot selve forfalskningen. Utvalget er, under tvil, kommet frem til at det støtter Straffelovrådets konklusjon i NOU 1985: 31, se punkt 2.7.3, for så vidt gjelder automatiserte tilfeller, jf. Rt. 1991 s. 532. I de tilfellene der data forfalskes uten at de er del av en automatisert prosess, for eksempel ved elektronisk scanning av dokumenter, legger utvalget til grunn at handlingen rammes av straffeloven § 185 annet ledd. Etter utvalgets oppfatning er det derfor ikke nødvendig med endringer i norsk rett.

2.8 Databedrageri – artikkel 8

2.8.1 Folkerettslige forpliktelser

Konvensjonen artikkel 8 omhandler databedrageri («computer related fraud») og lyder:

> «Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
> a) any input, alteration, deletion or suppression of computer data;
> b) any interference with the functioning of a computer system,
> with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.»

Artikkel 8 har som formål å sikre adgang til å strafforfølge nye former for bedrageri som den senere tids teknologiske utvikling har muliggjort. Manipulering med kredittkort er et praktisk eksempel.

Bestemmelsen forplikter konvensjonsstatene til å kriminalisere det å påføre en annen tap ved å manipulere data eller forstyrre et datasystem i den hensikt å skaffe seg eller andre økonomisk gevinst.

For det første rammes altså det å tilføye, endre, slette eller skjule data, jf. artikkel 8 bokstav a. Enhver form for manipulering av data er dermed omfattet. For det andre rammes tilfeller hvor data ikke direkte er benyttet eller påvirket av handlingen, jf. artikkel 8 bokstav b. For eksempel vil all form for manipulering av maskinvare eller programutrustning være omfattet, dersom virkningen er at datasystemet ikke fungerer som forutsatt.

Handlingen må påføre en annen fysisk eller juridisk person tap («loss of property»). Tapet må være av økonomisk karakter, og kan omfatte både penger og andre ytelser av økonomisk verdi. Det er også et krav at tapet må være en direkte følge av handlingen, jf. den forklarende rapporten punkt 88.

Videre åpner bestemmelsen for at statene stiller som vilkår for å straffe at gjerningsmannen utførte handlingen i den hensikt å skaffe seg eller andre urettmessig økonomisk gevinst.

2.8.2 Gjeldende rett

Databedrageri rammes av straffeloven § 270 første ledd nr. 2 som ble tilføyd ved lov 12. juni 1987 nr. 53. Bakgrunnen for lovendringen var et behov for å kunne straffesanksjonere bedragerilignende handlinger der ingen er forledet, for eksempel fordi prosessen er helautomatisk.

Straffeloven § 270 første ledd nr. 2 rammer den som i den hensikt å skaffe seg eller andre uberettiget vinning, rettsstridig påvirker resultatet av en automatisk databehandling og derved volder tap eller fare for tap for noen. Påvirkningen kan enten skje ved bruk av uriktige eller ufullstendige opplysninger, ved endring i data eller programutrustning eller på annen måte. Det første alternativet rammer for eksempel innmating av uriktige lønnsopplysninger i et datasystem og manipulering med bankkort. Det andre alternativet kan anvendes ved endringer i eksisterende data eller programvare.

Tapet eller faren for tap trenger ikke nødvendigvis å gjelde en bestemt person. Det er heller ikke et krav at en person er forledet, cf. § 270 første ledd nr. 1.

2.8.3 Utvalgets vurderinger

Etter utvalgets oppfatning oppfyller straffeloven § 270 første ledd nr. 2 forpliktelsene i artikkel 8. Det er derfor ikke behov for endringer i norsk rett.

2.9 Datarelatert barnepornografi – artikkel 9

2.9.1 Folkerettslige forpliktelser

Artikkel 9 i konvensjonen omhandler barnepornografi, og lyder:

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
   a) producing child pornography for the purpose of its distribution through a computer system;
   b) offering or making available child pornography through a computer system;
   c) distributing or transmitting child pornography through a computer system;
   d) procuring child pornography through a computer system for oneself or for another person;
   e) possessing child pornography in a computer system or on a computer-data storage medium.
2. For the purpose of paragraph 1 above, the term «child pornography» shall include pornographic material that visually depicts:
   a) a minor engaged in sexually explicit conduct;
   b) a person appearing to be a minor engaged in sexually explicit conduct;
   c) realistic images representing a minor engaged in sexually explicit conduct.
3. For the purpose of paragraph 2 above, the term «minor» shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Formålet med artikkel 9 er å ramme ulike former for elektronisk produksjon, distribusjon og besittelse av barnepornografi. Bestemmelsen gjelder bare barnepornografi som er elektronisk basert. Bakgrunnen for bestemmelsen er en erkjennelse av at enhver form for tilgjengeliggjøring av barnepornografi via elektroniske nett, herunder Internett, øker faren for seksuelt misbruk av barn. Derfor er det viktig å kriminalisere alle ledd i kjeden, fra produksjon via distribusjon, til besittelse, jf. den forklarende rapporten punkt 98.

Artikkel 9 nr. 1 bokstav a rammer produksjon av barnepornografi, men bare når formålet er å distribuere pornografien via et datasystem.

Bokstav b retter seg både mot det å tilby barnepornografi og å gjøre slikt materiale tilgjengelig via et datasystem. Det første alternativet krever en oppfordring fra gjerningspersonen om å ta imot det pornografiske materialet og forutsetter at gjerningspersonen selv kan skaffe materialet, jf. den forklarende rapporten punkt 95. Det andre alternativet rammer for eksempel det å lage nettsider med barnepornografisk materiale, samt å lage, samle eller tilgjengeliggjøre hyperlenker til slike nettsider.

Bokstav c rammer distribusjon og overføring av barnepornografi via et datasystem. Distribusjon innebærer aktiv spredning til flere, mens overføring retter seg mot videresending fra en person til en annen.

I henhold til bokstav d skal konvensjonsstatene kriminalisere aktiv anskaffelse av barnepornografi for seg selv eller andre via et datasystem, for eksempel ved å laste det ned fra Internett.

Bokstav e gjelder det å besitte barneporno-

grafisk materiale i et datasystem eller på et separat elektronisk lagringsmedium, for eksempel CD-ROM.

Begrepet «barnepornografi» er definert i artikkel 9 nr. 2. Bare data som kan gjenskapes til materiale med en visuell karakter er omfattet. Eksempler kan være stillbilder, filmer og videosnutter. Lydfiler er derimot ikke omfattet.

I henhold til artikkel 9 nr. 3 skal alle personer under 18 år anses for å være mindreårige. Aldersgrensen er i tråd med FNs barnekonvensjon artikkel 1. Mange stater opererer med lavere aldersgrenser i relasjon til barnepornografi. Statene er derfor gitt anledning til å erklære at de vil benytte en lavere aldersgrense enn 18 år, men ikke lavere enn 16 år.

Artikkel 9 nr. 4 åpner for at statene kan reservere seg mot å gjennomføre forpliktelsene i artikkel 9 nr. 1 bokstav d og e og nr. 2 bokstav b og c, jf artikkel 42.

2.9.2 Gjeldende rett

En rekke former for befatning med barnepornografi er kriminalisert i straffeloven § 204. Bestemmelsen ble endret ved lov 1. august 2003 nr. 86 som trådte i kraft 1. oktober 2003. Paragraf 204 første ledd bokstav d rammer den som produserer, innfører, besitter, overlater til en annen eller mot vederlag gjør seg kjent med barnepornografi.

Begrepet «besittelse» omfatter blant annet oppbevaring av barnepornografi på elektroniske lagringsmedier, for eksempel server, harddisk, disketter og CD-ROM. Gjerningspersonen må ha rådighet over materialet, men besittelseskravet oppstiller ikke et krav om at han må ha materialet fysisk hos seg. Plassering på et web-hotell i utlandet vil følgelig være omfattet. I henhold til forarbeidene til bestemmelsen foreligger det ikke straffbar besittelse dersom man bare leser eller ser på det barnepornografiske materialet på egen skjerm, uten at materialet er lastet ned, det vil si lagret på maskinens harddisk, jf. Ot. prp. nr. 28 (1999-2000) s. 99. I henhold til rettspraksis er det for eksempel ikke tilstrekkelig at materiale er lagret på såkalte 'Temporary Internet Files', se dom fra Eidsivating lagmannsrett 26. september 2002.

I forarbeidene til endringslov 1. august 2003 nr. 86 legger departementet til grunn at begrepet «skildringer» også omfatter fiktive eller animerte bilder, jf. Ot.prp. nr. 45 (2002-2003) s. 55.

Barnepornografi er definert som kjønnslige skildringer i rørlige og urørlige bilder hvor det gjøres bruk av barn. Etter lovendringen 1. august 2003 er barn definert som personer som er eller fremstår som under 18 år. Ved vurderingen av om en person fremstår som under 18 år, må man ta utgangspunkt i bildematerialet for å forsøke å fastslå den avbildede personens alder. Personer over 18 år som blir fremstilt som om de er barn, for eksempel ved utkledning og sminke, omfattes ikke av definisjonen i bokstav d, jf. Ot.prp. nr. 45 (2002-2003) s. 55.

I annet ledd tredje punktum gjøres det unntak for kjønnslige skildringer som er forsvarlige ut fra et kunstnerisk, vitenskapelig, informativt eller lignende formål.

I forbindelse med lovendringen 1. august 2003 nr. 86 ble det innført en straffritaksregel i § 204 femte ledd. Straff etter første ledd bokstav d kan falle bort for den som tar og besitter et bilde av en person mellom 16 og 18 år, dersom denne har gitt sitt samtykke og de to er omtrent jevnbyrdige i alder og utvikling.

Videre rammes den som forleder noen under 18 år til å la seg avbilde som ledd i kommersiell fremstilling av rørlige og urørlige bilder med seksuelt innhold eller produserer slike fremstillinger hvor noen under 18 år er avbildet, av straffeloven § 204 første ledd bokstav f. Begrepet «med seksuelt innhold» har et videre nedslagsfelt enn begrepet «kjønnslige skildringer» og omfatter for eksempel mykpornografisk nakenfotografering, jf. Ot.prp. nr. 28 (1999-2000) s. 99.

2.9.3 Utvalgets vurderinger

Straffeloven § 204 oppfyller langt på vei forpliktelsene i artikkel 9. Imidlertid krever artikkel 9 nr. 1 bokstav d at statene straffesanksjonerer anskaffelse av barnepornografi. Selve anskaffelseshandlingen er ikke straffbar etter norsk rett. Etter utvalgets oppfatning er behovet for et eget straffalternativ som rammer anskaffelsen, overflødig ved siden av alternativene «besitter» og «innfører». Handlingen vil kunne straffes som besittelse idet materialet er lastet ned. Utvalget har derfor kommet frem til at Norge bør benytte reservasjonsadgangen i artikkel 9 nr. 4 for så vidt gjelder artikkel 9 nr. 1 bokstav d.

Artikkel 9 nr. 2 forplikter statene til å kriminalisere befatning med pornografisk materiale der en person fremstår («appearing») som barn. Etter endringen ved lov 1. august 2003 regnes en person som *fremstår* som under 18 år, som barn i relasjon barnepornografibestemmelsen. Utvalget mener derfor at norsk rett er i samsvar konvensjonsforpliktelsene på dette punktet.

Etter utvalgets oppfatning er det ikke nødvendig med endringer i norsk rett for å gjennom-

føre artikkel 9, forutsatt at reservasjonsadgangen i artikkel 9 nr. 4 benyttes.

For øvrig bemerker utvalget at det som utgangspunkt mener at enhver befatning med datarelatert barnepornografi bør kriminaliseres. Utvalget vil komme tilbake til spørsmålet i delutredning II.

2.10 Vern av opphavsrett og nærstående rettigheter - artikkel 10

Dette kapitlet ble på forespørsel fra utvalget utarbeidet av professor dr. juris Jon Bing. Utredningen ble overlevert utvalget 8. juli 2002, og er tatt inn i sin helhet:

2.10.1 Folkerettslige forpliktelser

Konvensjonens art. 10 omhandler vern av opphavsrett og nærstående rettigheter og lyder:

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Konvensjonen om «cybercrime»[1] art 10 er organisert i tre punkter. I art 10(1) angis konvensjoner som er relevante for vern av opphavsrett («infringement of copyright»), mens det i art 10(2) angis konvensjoner som er relevante for nærstående rettigheter («infringement of related rights»). Det vil si at ikke alle immaterielle rettigheter fanges opp av konvensjonen, Explanatory Report[2] pkt 109 nevner eksplisitt patentrettigheter og rettigheter knyttet til varemerker. Andre rettigheter som faller utenfor vil være rett til integrerte kretser, rett til mønster (loven vil i nær fremtid erstattes av en lov om rett til design), firmarett (som antagelig må anses som relatert til varemerker i konvensjonens forstand), goodwill mv.

I både konvensjonen art 10(1) og (2) henvises det til at det er de forpliktelser som vedkommende land har etter de nevnte konvensjonene som er aktuelle, dvs at reservasjoner mv i forhold til konvensjonene, tilsvarende begrenser forpliktelsene etter konvensjonen om «cybercrime» art 10 (jfr Explanatory Report pkt 110 *in fine*).

Det er for både konvensjonen om «cybercrime» art 10(1) og 10(2) gjort unntak for ideelle rettigheter («moral rights»), eksemplifisert i Explanatory Report pkt 112 med henvising til Bernkonvensjonen art 6bis (respekt for verket, jfr åndsverkloven § 3). På samme sted henvises det til WCT[3] art 5, dette er imidlertid *ikke* – slik jeg forstår det – en bestemmelse om ideelle rettigheter, men en bestemmelse om databaser:

> *Compilations of Data (Databases)*
>
> Compilations of data or other material, in any form, which by reason of the selection or arrangement of their contents constitute intellectual creations, are protected as such …

Bestemmelsen angir at kompilasjoner som er «intellectual creations» er vernet som sådanne, etter norsk rett vil de være vernet som samleverk, jfr åndsverkloven § 5.[4] Det er derfor litt vanske-

[1] Convention on Cybercrime, European Treaty Series no 185.
[2] Council of Europe, Convention of Cybercrime – Explanatory Report adopted 8 November 2001.
[3] Jfr straks nedenfor for full referanse.
[4] Dette er et vern *qua* åndsverk, databaser vernes også etter en nærstående rettighet som "kataloger" der hvor kravene til verkshøyde ikke er oppfylt, jfr åndsverkloven § 43. Dette faller utenfor konvensjonens område fordi det er en nærstå-

lig å forstå Explanatory Report på dette punktet,[5] men det spiller ingen stor rolle, ettersom konvensjonen jo tillater et mer vidtrekkende vern enn det minimum konvensjonen krever.

Konvensjonen art 10(1) henviser til tre andre konvensjoner for så vidt gjelder vern av *opphavsrett*:

Bern-konvensjonen om vern av litterære og kunstneriske verk, paristeksten av 24.7.1971. I henhold til Kgl res av 8.6.1995 ble det fattet vedtak om ratifikasjon av paristeksten, og Norge avga erklæring til WIPO[6] 11.7.1995 med virkning fra 11.7.1995. Det antas at åndsverkloven oppfyller Norges forpliktelser etter Bern-konvensjonen.

Avtale om handelsrelaterte sider ved immaterielle rettigheter,[7] i henhold til Kgl res av 8.4.1994 ble denne avtalen undertegnet i Marrakesh 15.4. 1994. Samtykke til ratifikasjon ble gitt ved Kgl res av 2. 2.1994 og ratifikasjonsdokumentet ble deponert i Genève 7.12.1994.[8] Etter art 9 henvises det til Bern-konvensjonens parisertekst, som medlemmene må overholde, jfr ovenfor. I tillegg spesifiseres at datamaskinprogrammer skal vernes som litterære verk (art 10(1), at databaser som møter originalitetskravet, skal vernes som åndsverk (art 10(2), for så vidt likelydende med WTC art 5 sitert ovenfor), og at rettighetshavere til datamaskinprogrammer og film (som et minimum) skal beholde rett til utleie av eksemplar til allmennheten. For så vidt gjelder datamaskinprogrammer, fremgår de samme forpliktelsene av rådets direktiv av 14.5. 1991 om rettslig vern av datamaskinprogrammer,[9] og for utleie av rådets direktiv 19.11.1992 om utleie- og utlånsrettigheter samt visse nærstående rettigheter.[10] Åndsverkloven er endret på grunnlag av disse direktivene, og man må anta at forpliktelsene etter avtalen er implementert i norsk rett.

WIPO Copyright Treaty. World Intellectual Property Organization Copyright Treaty (WCT) ble vedtatt i Geneve 20.12.1996, men er – som det fremgår av Explanatory Report pkt 111 – ennå ikke trådt i kraft. Directive 200½9/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society[11] tar bl a sikte på å implementere denne traktaten. Kulturdepartementet arbeider med å fremme forslag til endring av åndsverkloven innen implementeringsfristen 22.12.2002. Som det fremgår av Explanatory Memorandum pkt 111, anses man ikke forpliktet av konvensjonen om «cybercrime» til å kriminalisere det vern som gis etter WCT forut for at WCT trer i kraft. Imidlertid er traktaten om «cybercrime» art 10 her ikke helt klar, ettersom artikkelen angår «infringement of copyright», mens WCT også omhandler forpliktelser mht rettslig beskyttelse av tekniske innretninger som verner åndsverk (art 11) og rettighetsadministrative opplysninger (art 12). Disse forpliktelsene i WCT angår ikke vern av åndsverk, og etter ordlyden skulle man vel tro at disse bestemmelsene faller utenfor traktaten om «cybercrime» art 10(1). Denne uklarheten spiller mindre rolle for Norge, ettersom man vil implementere «adequate legal protection» for krenkelse av disse bestemmelsene i henhold til InfoSoc-direktivet art 6 og 7.[12]

Etter konvensjonen om «cybercrime» art 10(2) skal man også knytte strafferettslige sanksjoner til krenkelse av «related rights» eller «neighbouring rights»,[13] dvs *nærstående rettigheter* eller *naborettigheter*. Dette uttrykket brukes i Norge om rettigheter som er regulert i åndsverkloven, men som ikke er opphavsrettigheter. Også her henvises det til tre andre traktater:

Roma-konvensjonen – Internasjonal konvensjon om rettsvern for de rettigheter som tilkommer utøvende kunstnere, fremstillere av fonogrammer samt kringkastingsinstitusjoner. Norge tiltrådte konvensjonen med virkning fra 10.7.1978, jfr St prp nr 141 (1976-1977) og Kgl res 28.7.1978. Da Norge tiltrådte konvensjonen, jfr St prp nr 141 (1976-1977), ble det tatt forbehold for fire forhold:

Det ble tatt forbehold om at Norge bare ville anvende art 12 for så vidt angår offentlig fremføring i ervervsøyemed (etter art 16 § 1 *litra* a(ii)).

Det ble tatt forbehold om at bare fonogramprodusenter som var hjemmehørende i et annet konvensjonsland, skal kunne kreve vederlag for sekundærbruk av fonogrammer her i landet (etter art 16 § 1 *litra* a(iii)).

Det ble tatt forbehold om å gjøre gjeldende materiell gjensidighet for så vidt angår betaling for sekundærbruk av fonogrammer. Det betyr at pro-

ende rettighet det ikke er henvist til i oversikten i art 10(2), jfr nedenfor.

5) Jeg finner ikke noen bestemmelse i WCT som synes å verne ideelle rettigheter direkte.

6) World Intellectual Property Organisation, som administrerer Bern-konvensjonen.

7) Trade-Related Aspects of Intellectual Property Rights, ofte omtalt som TRIPS, en av de grunnleggende avtalene for Verdens handelsorganisasjon (WTO).

8) Det vises til St prp nr 65 (1993-1994), Innst S nr 43 (1994-1995) samt Stortingsvedtak av 30.11.1994.

9) 91/250/EØF.

10) 92/100/EØF.

11) OJ L 167/10, i Norge gjerne omtalt som InfoSoc-direktivet.

12) Det antas at dette i nasjonal rett vil få en utforming som ikke er svært forskjellig fra åndsverkloven § 54a, som gir et strafferettslig vern mot krenkelse av tekniske innretninger for beskyttelse av datamaskinprogrammer.

13) Jfr Explanatory Memorandum pkt 108.

dusent i land A ikke får bedre vern i land B enn produsent i land B får i land A (etter art 16 § 1 *litra* a(iv)).

Det ble tatt forbehold om å kumulere nasjonalitets- og territorialkriteriet når det gjelder vern for kringkastingssendinger, dvs bare å verne slik sending dersom sendeselskapet har sitt hovedsete i et annet konvensjonsland og sendingen blir kringkastet fra sender i det samme landet (etter art 6 § 2).

Ved innføringen av en vederlagsrett i 1989 for utøvende kunstnere og fonogramprodusenter for sekundærfremføring i kringkasting, endret Norge sin reservasjon i henhold til art 16 § 1 *litra* a(ii) til å ta forbehold mot anvendelse av reglene i art 12 for alle andre sekundærfremføringer enn de som skjer i kringkasting. I tråd med det prinsipp som er nevnt ovenfor, er derfor Norges forpliktelser etter traktaten om «cybercrime» art 10(2) begrenset på samme måte.

Avtale om handelsrelaterte sider ved immaterielle rettigheter, jfr foran om detaljer. Art 14 inneholder bestemmelser om vern for utøvende kunstnere, fonogramprodusenter og kringkastere. Etter TRIPS art 14(6) kan imidlertid et medlemsland «fastsette vilkår, begrensninger, unntak og forbehold i den grad det tillates etter Roma-konvensjonen». Det antas at forpliktelsene etter TRIPS oppfylles dersom forpliktelsene etter Roma-konvensjonen er implementert i nasjonal rett.

World Intellectual Property Organisation Performances and Phonograms Treaty (WPPT) av 20.12. 1996 er – i likhet med WCT – ikke trådt i kraft, og er derfor ikke forpliktende før dette tidspunkt, jfr Explanatory Memorandum pkt 111. Jeg har ikke full oversikt over bestemmelsene i denne traktaten, men vil tro at de er implementert i norsk rett som følge av Roma-konvensjonen.

Felles for de to bestemmelsene er at det gjøres gjeldende visse betingelser for at man er forpliktet til å innføre et strafferettslig vern av krenkelser:

«Wilfully». Det er bare krenkelser som er begått «wilfully» som omfattes. Dette er kommentert i Explanatory Report pkt 113, hvor det fremheves at dette brukes i stedet for «intentionally». Explanatory Report forklarer dette ved henvisning til kravet i TRIPS art 61 (sitert nedenfor).

«On a commercial scale». Det er bare krenkelser «i kommersiell målestokk» som omfattes, dette er igjen begrunnet med en henvisning til TRIPS art 61 (sitert nedenfor), jfr Explanatory Report pkt 114. I norsk opphavsrett har man vel ikke noe kriterium som svarer direkte til dette, selv om man flere steder bruker kriteriet «ervervsøyemed», som i alle fall er beslektet med «i kommersiell målestokk».

«By means of a computer system». Det er bare krenkelser foretatt ved hjelp av «a computer system» som omfattes. Dette følger vel av formålet med konvensjonen om «cybercrime», og gjør i og for seg bestemmelsene mediespesifikke. I alminnelighet vil bestemmelsene i norsk åndsverklov være medienøytrale, selv om det finnes spesialbestemmelser særlig for datamaskinprogrammer. Uttrykket «computer system» er definert i konvensjonen art 1(a) som «any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data», jfr kommentarene i Explanatory Report pkt 23-24. Dette generelle punktet er det ingen grunn til å kommentere særskilt her, og skulle heller ikke by på spesielle problemer.

Traktaten om «cybercrime» art 10(3) gir en mulighet for at det i nasjonal lovgivning ikke innføres straffereaksjoner i forhold til de krenkelser som er nevnt i art 10(1) og (2). Dette kan skje på grunnlag av to forutsetninger:

Det skjer i «limited circumstances», som eksempler nevnes i Explanatory Report pkt 116 parallellimport og utleie.

Det finnes «other effective remedies», som eksempel nevnes i Explanatory Report pkt 116 «civil and/or administrative measures».

Forutsetningen er også at man møter minstekravet i TRIPS art 61:

> Medlemmene skal fastsette straffeprosessuelle og strafferettslige tiltak som skal anvendes i alle fall i tilfeller av … piratkopiering av opphavsrettslige varer i kommersiell målestokk. Straffetiltakene skal omfatte fengsling og/eller pengebøter som er tilstrekkelige til å virke forebyggende og som er i samsvar med det straffenivå som anvendes ved forbrytelser av tilsvarende alvorlighetsgrad. Etter omstendighetene skal tiltakene også omfatte beslag, konfiskasjon og tilintetgjørelse av de ulovlige varene og av alle materialer og alt utstyr som hovedsakelig ble benyttet da forbrytelsen ble begått. Medlemmene kan fastsette straffeprosessuelle og strafferettslige tiltak som skal komme til anvendelse i andre tilfeller av krenkelse av immaterielle rettigheter, særlig når krenkelsen er forsettlig og i kommersiell målestokk.

Det er lite tvilsomt at norsk rett møter dette kravet.

2.10.2 Gjeldende rett

Som kort redegjort ovenfor, er systemet i konvensjon for «cybercrime» at den forplikter medlemslandene å ha strafferettslige sanksjoner for brudd på det vern som etableres av de konvensjonene det

henvises til, med forbehold om WTC og WPPT, hvor forpliktelsen ikke anses å inntreffe før disse konvensjonene trer i kraft.

Som nevnt antas Bern-konvensjonens paristekst å være implementert i norsk åndsverklov, det samme gjelder Roma-konvensjonen. Dermed antas også forpliktelsene etter TRIPS i forhold til opphavsrettigheter og nærstående rettigheter å være oppfylt.

Hovedbestemmelsen om straff er åndsverkloven § 54:

> Med bøter eller fengsel inntil tre måneder straffes den som forsettlig eller uaktsomt bryter denne lov ved:
> a) å overtre bestemmelser gitt til vern for opphavsretten i eller i medhold av 1. og 2. kapittel, bestemmelsene i § 39j eller § 41a, eller forbud nedlagt etter § 35 eller § 48, eller bestemmelser utferdiget av opphavsmannen etter § 39k andre ledd,
> b) å overtre bestemmelser gitt i eller i medhold av 5. kapittel, § 45c, § 46, § 47 eller § 48 siste ledd,
> c) å innføre eksemplar av åndsverk eller av arbeider og opptak som nevnt i § 42, § 43, § 43a, § 45 og § 45a hensikt å gjøre dem tilgjengelige for allmennheten, når eksemplarene er fremstilt utenfor riket under slike forhold at en tilsvarende fremstilling her i riket ville vært i strid med loven, eller
> d) å fremby eller på annen måte gjøre tilgjengelig for allmennheten arbeider eller opptak som er nevnt i § 42, § 43, § 43a, § 45 eller § 45a, når eksemplarene er fremstilt i strid med disse bestemmelser eller innført i strid med bokstav c i paragrafen her,
> e) å innføre eksemplar av opptak som nevnt i § 45 i den hensikt å gjøre dem tilgjengelig for allmennheten i ervervsøyemed, når tilvirkeren ikke har samtykket til innførselen og eksemplar av samme opptak med samtykke av tilvirkeren frembys her i riket. Departementet kan i forskrifter gjøre unntak fra denne bestemmelsen for innførsel av eksemplar fra nærmere bestemte land.
>
> Den som forsettlig eller uaktsomt medvirker til overtredelse som nevnt i første ledd straffes på samme måte.
>
> Er overtredelse som nevnt i første og annet ledd forsettlig, og foreligger det særlig skjerpende forhold, er straffen bøter eller fengsel inntil tre år. Ved vurderingen av om særlig skjerpende forhold foreligger, skal det først og fremst legges vekt på den skade som er påført rettshavere og andre, den vinning som lovovertrederen har hatt og omfanget av overtredelsen for øvrig.
>
> Forsøk på forsettlig overtredelse som nevnt i første til tredje ledd kan straffes likt med den fullbyrdete overtredelse.
>
> Den som forsettlig eller uaktsomt unnlater å påføre de i § 52 nevnte opplysninger på et verk som han forestår trykkingen av, straffes med bøter.
>
> Overtredelse av tredje ledd jf fjerde ledd påtales av det offentlige. Overtredelse av de øvrige bestemmelser i paragrafen her påtales ikke av det offentlige med mindre det begjæres av fornærmede eller en organisasjon jf sjuende ledd, eller finnes påkrevd av allmenne hensyn.
>
> Er denne lov overtrådt ved at et verk er brukt på en måte som er nevnt i § 13, § 14, § 17 fjerde ledd og § 34, kan påtale begjæres også av den organisasjon som kan inngå avtale etter § 36, så lenge fornærmede ikke motsetter seg det.

Etter åndsverkloven § 54, 1.ledd *litra* a henvises det til åndsverkloven kap 1, hvor man finner hovedreglene om opphavsmannens enerett, og som implementerer Bern-konvensjonen. Det henvises også til kap 2, som inneholder avgrensninger av enerettighetene til fordel for allmennheten. Det er ikke i detalj gjennomgått hvorvidt dette tilfredsstiller konvensjonen om «cybercrime», her stilles det opp et krav om strafferettslige sanksjoner for alle bestemmelsene i Bern-konvensjonens materielle del. Men det må være tillatt å anta at dette er tilstrekkelig. Det subjektive skyldkravet er forsett eller uaktsomhet, som må anses som mer enn tilstrekkelig. Kravet til at loven må ramme ervervsmessige krenkelser er oppfylt, ettersom det ikke er gjort unntak for slik utnyttelse, og det er ikke noe unntak for krenkelser i datamaskinbaserte systemer. Selv om det ikke er gjort en detaljert gjennomgang, representerer det ikke noen risiko å gå ut fra at norsk rett her allerede oppfyller kravene i konvensjonen om «cybercrime».

Etter åndsverkloven § 54, 1.ledd *litra* b henvises det til åndsverkloven kap 5, som inneholder hovedreglene om vern av utøvende kunstneres prestasjoner, fonogramprodusenter og kringkastere, og som implementerer Roma-konvensjonen. Bestemmelsen suppleres av åndsverkloven § 54, 1.ledd *litra* c og d, som rammer innføring eller markedsføring av eksemplar av åndsverk, arbeider eller opptak som er nevnt i bl a åndsverkloven § 42 (vern av utøvende kunstneres prestasjoner), åndsverkloven § 45 (fonogramprodusenters rettigheter) eller § 45a (kringkasteres rettigheter).[14] Åndsverklo-

[14] Bestemmelsen nevner også åndsverkloven § 43, som angir *sui generis* vernet for databaser (katalogregelen) og § 43a som gir vern til et fotografisk bilde (til forskjell fra et fotografisk verk). Det er ikke krav i konvensjonen om "cybercrime" at dette skal vernes.

ven § 54, 1.ledd *litra* e kriminaliserer parallellimport av opptak.[15] Explanatory Report pkt 116 angir at man kan unnta dette etter konvensjonen om «cybercrime» art 10(3), men det er altså kriminalisert etter norsk rett.

For skyldkrav, kravet til at det man rammer ervervsmessige krenkelser og krenkelser ved datamaskinbaserte systemer, gjelder det samme som nevnt i forhold til åndsverkloven § 54, 1.ledd *litra* a. Igjen må det være lov å anta, uten en detaljert gjenomgang, at norsk rett her allerede tilfredsstiller kravene i konvensjonen om «cybercrime».

Når det gjelder WCT og WPPT er disse ikke trådt i kraft. WCT inneholder flere bestemmelser som ikke er implementert i norsk rett, og – som nevnt – er et revisjonsarbeid i gang, høringsnotat ventes I nær fremtid. Slik jeg leser WPPT, inneholder den materielle bestemmelser som allerede synes implementert gjennom Roma-traktaten (som WPPT ikke berører, jfr art 1(1)). Dette gjelder rett til å gjøre egne prestasjoner tilgjengelig for allmennheten, rett til å fiksere slike prestasjoner, rett til eksemplarfremstilling, rett til utleie, og rett til å gjøre opptak tilgjengelig for allmennheten. Det kan imidlertid ikke utelukkes at man ved en nærmere tolkning finner detaljer som krever justeringer i norsk rett.

2.10.3 Behov for endringer i norsk rett

Etter gjennomgangen ovenfor, foreligger det – slik jeg ser det – ikke behov for endringer i norsk rett for å implementere traktaten om «cybercrime». Unntaket er forpliktelsene i forhold til WCT, her forutsetter imidlertid traktatens Explanatory Report at forpliktelsen ikke inntrer før traktaten trer i kraft. Dessuten arbeider Kulturdepartementet for tiden med implementering av InfoDoc-direktivet, som igjen antas å tilfredsstille kravene etter WCT. I så måte må det være tilstrekkelig for utvalget å påpeke behovet for implementering av WCT i norsk rett, og understreke at man forutsetter at den pågående revisjonen vil ta hensyn til dette.

2.10.4 Utvalgets kommentar

Utvalget slutter seg til professor Jon Bings vurderinger.

[15] Det har vært tvil om hvorvidt dette også omfatter videogrammer, etter kjennelse i Borgarting lagmannsrett av 15. 12.1999, jfr *Lov&Data* 61/2000, må man anta at også slik parallellimport rammes.

2.11 Medvirkning og forsøk – artikkel 11

2.11.1 Folkerettslige forpliktelser

Artikkel 11 i konvensjonen omhandler forsøk og medvirkning og lyder:

> «1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.
> 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.
> 3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.»

Artikkel 11 nr. 1 forplikter statene til å kriminalisere medvirkning («aiding or abetting») til straffbare handlinger som nevnt i artikkel 2 til 10 i konvensjonen. I henhold til den forklarende rapporten punkt 119 kan det kreves at medvirkeren har forsett med hensyn til utførelsen av den straffbare handlingen. For eksempel rammes ikke en tjenestetilbyder av bestemmelsen dersom tjenestetilbyderen ikke handlet forsettlig, selv om vedkommendes tjenester muliggjorde en straffbar handling utført for eksempel på Internett.

Etter artikkel 11 nr. 2 forpliktes statene til å kriminalisere forsøk («attempt») på straffbare handlinger som nevnt i artiklene 3, 4, 5, 7, 8 og 9 nr. 1 bokstav a og bokstav c.

Det er opp til statene å fastlegge innholdet av medvirknings- og forsøksansvaret.

Det følger av artikkel 11 nr. 3 at statene er gitt adgang til å reservere seg mot å gjennomføre hele eller deler av artikkel 11 nr. 2, jf. artikkel 42.

2.11.2 Gjeldende rett

Straffebestemmelsene som er relevante for gjennomføringen av konvensjonen, står i straffelovens kapittel om forbrytelser. Dermed er forsøk på overtredelse straffbart, jf. straffeloven § 49 første ledd.

Videre følger det av alle de aktuelle straffebudene at medvirkning er straffbart.

2.11.3 Utvalgets vurderinger

Etter utvalgets oppfatning er det ikke behov for endringer i norsk rett for å kunne ratifisere konvensjonen.

2.12 Foretaksstraff – artikkel 12

2.12.1 Folkerettslige forpliktelser

Artikkel 12 i konvensjonen gjelder foretaksstraff og lyder:

«1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:
   a) a power of representation of the legal person;
   b) an authority to take decisions on behalf of the legal person;
   c) an authority to exercise control within the legal person.
2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.
3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.»

Bestemmelsen pålegger statene å gi regler som åpner for at juridiske personer kan holdes ansvarlige for kriminelle handlinger som er utført til fordel for foretaket.

Fire kumulative vilkår må være oppfylt for at forpliktelsen i artikkel 12 skal inntre: For det første gjelder forpliktelser i artikkel 12 nr. 1 bare juridiske personers overtredelser av straffebud som gjennomfører forpliktelsene i artikkel 2 til 11. Videre må handlingen være utført til fordel for foretaket. Handlingen må for det tredje være utført av en fysisk person i en ledende stilling som enten opptrer individuelt eller som del av et selskapsorgan. Medvirkning er også omfattet. For det fjerde må den fysiske personen enten ha rett til å representere foretaket, jf. bokstav a, eller rett til å treffe avgjørelser på vegne av foretaket, jf. bokstav b, eller rett til å utøve kontroll innen foretaket, jf. bokstav c.

Etter artikkel 12 nr. 2 skal foretaksstraff kunne anvendes når en handling er begått av en person som er underordnet lederen. Bestemmelsen fastsetter tre kumulative vilkår for at forpliktelsen skal inntre. For det første må overtredelsen være begått av en underordnet. Overtredelsen må for det andre være begått til fordel for foretaket. Og for det tredje må manglende kontroll eller oppfølging fra en fysisk person i en ledende stilling, jf. nr. 1, ha muliggjort overtredelsen. Med det tredje vilkåret siktes det til unnlatelse av å ta hensiktsmessige og rimelige forholdsregler for å forhindre at ansatte begår lovbrudd på vegne av foretaket, jf. den forklarende rapporten punkt 125.

Ansvar for foretak oppstår bare dersom den ledende personen eller den underordnede har «acted within the scope of their authority», jf. den forklarende rapporten punkt 125.

Statene kan velge om foretaksansvaret skal være strafferettslig eller sivilrettslig, jf. artikkel 12 nr. 3. Et vilkår er imidlertid at sanksjonen må tilfredsstille kravene i artikkel 13 nr. 2.

Det følger av artikkel 12 nr. 4 at bruk av foretaksansvar ikke kan ekskludere personlig straffansvar.

2.12.2 Gjeldende rett

I henhold til straffeloven § 48 a kan et foretak straffes dersom «et straffebud er overtrådt av noen som har handlet på vegne av et foretak». Med «foretak» menes selskap, forening eller annen sammenslutning, enkeltpersonforetak, stiftelse, bo eller offentlig virksomhet, jf. § 48 a annet ledd. Bestemmelsen krever ikke at en enkeltperson kan stilles til ansvar for overtredelsen. Både kumulative og anonyme feil omfattes.

Overtredelsen må være begått av noen som handlet på «vegne av foretaket». Vilkåret innebærer i utgangspunktet krav om et tilknytningsforhold som gir foretaket en reell instruksjons- og kontrollmulighet. Et ordinært ansettelsesforhold er normalt tilstrekkelig, mens oppdragstakere som

er selvstendige næringsdrivende i utgangspunktet ikke kan pådra foretak ansvar. Unntak kan imidlertid tenkes dersom foretakets instruksjons- og kontrollmulighet er reell, jf. Rt. 1982 s. 645.

Straffansvaret er fakultativt. Selv om vilkårene for foretaksstraff er til stede, er det opp til retten å vurdere hvorvidt et foretak skal ilegges straff i den enkelte sak. Straffeloven § 48 b bokstavene a til g oppstiller retningslinjer for når foretaksstraff bør ilegges. De samme momentene har også betydning for straffeutmålingen.

2.12.3 Utvalgets vurderinger

Utvalget legger til grunn at personkretsen som kan pådra et foretak straffansvar, er videre etter norsk rett enn det som følger av konvensjonen. For eksempel gjelder konvensjonen bare personer i en ledende stilling og ansatte underlagt deres kontroll. Konvensjonen synes også, i motsetning til norsk rett, å stille krav til at gjerningspersonen må kunne identifiseres. Videre gjelder forpliktelsen i artikkel 11 bare handlinger begått til fordel for foretaket. Norsk rett krever derimot bare at handlingen må være begått av noen som har handlet på vegne av foretaket.

Etter både konvensjonen og norsk rett er bruken av foretaksstraff fakultativ.

Etter utvalgets oppfatning er det derfor ikke nødvendig med endringer i norsk rett.

2.13 Tiltak og sanksjoner – artikkel 13

2.13.1 Folkerettslige forpliktelser

Artikkel 13 i konvensjonen omhandler tiltak og sanksjoner og lyder:

«1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.
2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.»

Artikkel 13 nr. 1 forplikter statene til å straffe overtredelser av straffebud som er fastsatt i samsvar med artikkel 2 til 11, med effektive, forholdsmessige og forebyggende sanksjoner, herunder straff som innebærer frihetsberøvelse. Sanksjonene skal gjenspeile den alvorlige karakteren av denne typen overtredelser, jf. den forklarende rapporten punkt 128.

Videre skal statene i henhold til artikkel 13 nr. 2 påse at juridiske personer som holdes ansvarlig i medhold av artikkel 12, omfattes av effektive, forholdsmessige og forebyggende strafferettslige eller ikke-strafferettslige sanksjoner, herunder økonomiske sanksjoner.

Det er opp til statene å vurdere hvilke sanksjoner som vil være effektive, forholdsmessige og forebyggende.

2.13.2 Gjeldende rett

Det er adgang til å idømme fengselsstraff ved overtredelser av alle de norske straffebudene som rammer handlinger som beskrevet i artikkel 2 til 11. Videre kan foretak ilegges bøter, jf. straffeloven § 48 a.

2.13.3 Utvalgets vurderinger

Siden samtlige relevante norske straffebestemmelser åpner for bruk av fengselsstraff, tilfredsstiller norsk rett etter utvalgets oppfatning konvensjonens krav. Etter utvalgets oppfatning er det derfor ikke behov for lovendringer.

Strafferammene vil for øvrig bli vurdert når utvalget tar fatt på arbeidet med delutredning II.

Kapittel 3
Prosessuelle bestemmelser

3.1 Prinsipper for gjennomføringen

Artikkel 14 og 15 i konvensjonen gir bestemmelser av generell karakter som gjelder gjennomføringen av de øvrige prosessuelle bestemmelsene i artikkel 16 til 21.

Artikkel 14 angir rekkevidden av de prosessuelle bestemmelsene og lyder:

«1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
   a) the criminal offences established in accordance with Articles 2 through 11 of this Convention;
   b) other criminal offences committed by means of a computer system; and
   c) the collection of evidence in electronic form of a criminal offence.
3. a) Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
   b) Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
      i. is being operated for the benefit of a closed group of users, and
      ii. does not employ public communications networks and is not connected with another computer system, whether public or private,

   that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.»

Artikkel 14 nr. 1 forplikter statene til å treffe nødvendige tiltak, rettslige eller andre, for å sikre at konvensjonens prosessuelle bestemmelser blir gjennomført ved etterforskning og forberedelse av straffesaker.

Etter artikkel 14 nr. 2 skal de straffeprosessuelle bestemmelsene få anvendelse i tre relasjoner. For det første skal bestemmelsene gis anvendelse på overtredelser av straffebud som gjennomfører forpliktelsene i artikkel 2 til 11, jf. artikkel 14 nr. 2 bokstav a. For det andre skal bestemmelsene gis anvendelse på straffbare handlinger som blir begått ved hjelp av et datasystem, jf. artikkel 14 nr. 2 bokstav b. For det tredje skal bestemmelsene gis anvendelse på sikring av elektroniske bevis i tilknytning til enhver straffbar handling, jf. artikkel 14 nr. 2 bokstav c.

Fra dette utgangspunktet er det gjort to unntak. Det første unntaket følger av artikkel 14 nr. 2, jf. artikkel 21, og gjelder avlytting av innholdsdata. Artikkel 21 fastslår at statene bare er forpliktet til å gi regler om avlytting av innholdsdata dersom det er tale om alvorlige straffbare handlinger («serious offences»). De straffbare handlingene som kan gi grunnlag for avlytting av innholdsdata skal være eksplisitt nevnt i loven. Statene står imidlertid fritt til å avgjøre hva som skal regnes som alvorlige straffbare handlinger. Begrunnelsen skyldes at mange stater, som følge av personvernhensyn, oppstiller begrensninger i adgangen til å utøve kommunikasjonskontroll.

Det andre unntaket følger av artikkel 14 nr. 3 bokstav a og berører innhenting av trafikkdata i sanntid, jf. artikkel 20. Statene er gitt adgang til å begrense muligheten for innhenting av trafikkdata i sanntid til bare å gjelde særskilt angitte overtredelser, jf. artikkel 42. Bestemmelsen åpner imid-

lertid bare for reservasjoner som er snevrere enn eventuelle begrensninger i adgangen til å avlytte innholdsdata. Statene oppfordres til å begrense eventuelle reservasjoner for å sikre et videst mulig anvendelsesområde for artikkel 20.

Videre kan de statene som på grunn av sin lovgivning på tiltredelsestidspunktet ikke har anledning til å benytte tvangsmidlene som er beskrevet i artikkel 20 og 21 på lukkede brukergrupper («closed group of users»), reservere seg, jf. artikkel 14 nr. 3 bokstav b. Statene er oppfordret til å begrense bruken av reservasjonsadgangen.

Artikkel 15 fastsetter prinsipper for gjennomføringen av de prosessuelle bestemmelsene og lyder:

«1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.»

Artikkel 15 nr. 1 forplikter statene til å sørge for at tiltakene som iverksettes for å gjennomføre artikkel 14 til 21, er underlagt nasjonale rettssikkerhetsprinsipper («conditions and safeguards»). Statene skal respektere internasjonale menneskerettsinstrumenter som de er bundet av, som for eksempel Den europeiske menneskerettskonvensjonen (EMK) med tilleggsprotokoller og FN-konvensjonen om sosiale og politiske rettigheter (SP). Statene er videre forpliktet til å gjennomføre forholdsmessighetsprinsippet, jf. artikkel 15 nr. 1.

I henhold til artikkel 15 nr. 2 skal rettssikkerhetsgarantiene blant annet inkludere rettslig eller annen form for uavhengig kontroll. Videre skal bruken av de prosessuelle virkemidlene være betinget av at nærmere bestemte vilkår er oppfylt. Dernest skal det fastsettes rammer for omfang og varighet. Det er opp til statene selv å avgjøre i hvilken utstrekning de ulike virkemidlene skal være underlagt restriksjoner som nevnt, under hensyn til internasjonale forpliktelser og nasjonale prinsipper. Inngripende prosessuelle virkemidler stiller generelt sett større krav til forholdsmessighet enn virkemidler av mindre inngripende karakter. Den forklarende rapporten punkt 147 fremhever reglene om avlytting av innholdsdata, jf. artikkel 21, som et inngripende virkemiddel. Sikringspålegg, jf. artikkel 16 og 17, er derimot et mindre inngripende virkemiddel.

Statene er forpliktet til å vurdere belastningen ved bruk av prosessuelle virkemidler for tredjemenn, inkludert tjenestetilbydere. Videre skal statene vurdere å iverksette mulige tiltak for å avhjelpe eventuelle negative virkninger ved bruk av de prosessuelle virkemidlene for tredjemenn.

3.2 Sikring av lagrede data – artikkel 16 og 17

3.2.1 Folkerettslige forpliktelser

3.2.1.1 Hurtig sikring av lagrede data – artikkel 16

Artikkel 16 omhandler hurtig sikring av lagrede data og lyder:

«1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the com-

petent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.»

Formålet med bestemmelsen er å forplikte statene til å gi kompetent myndighet adgang til å sikre lagrede data som deretter kan benyttes som bevis i en straffesak. Data som er lagret i et datasystem, må anses som ustabile og skjøre. Viktig bevismateriale vil derfor lett kunne gå tapt.

Et pålegg om sikring (sikringspålegg) er mindre inngripende for den berørte enn alminnelig ransaking og beslag. Politiet får ikke innsyn i dataene og den pålegget retter seg mot beholder rådigheten. Bruk av sikringspålegg vil være et raskere virkemiddel når den som besitter dataene, er en man kan ha tiltro til, for eksempel en tjenestetilbyder.

Statenes plikt til å gi regler om sikring av lagrede data, jf. artikkel 16 og 17, omfatter bare data som allerede er lagret hos besitteren, jf. den forklarende rapporten punkt 153. Statene er heller ikke forpliktet til å pålegge virksomheter å installere tekniske løsninger som muliggjør sikring av data.

Bestemmelsen retter seg utelukkende mot elektronisk lagrede data. Data som er under overføring, uavhengig av om det er tale om innholds- eller trafikkdata, faller utenfor. Regler om innhenting av slike data er gitt i artikkel 20 og 21.

Det følger av artikkel 16 nr. 1 at bestemmelsen også omfatter trafikkdata. Ytterligere regler for trafikkdata er imidlertid gitt i artikkel 17.

Sikring («preservation») innebærer en plikt til å sikre integriteten av dataene. Statene står imidlertid fritt til å velge hvordan dataene skal sikres. Dataene kan «fryses» slik at legitime brukere ikke får tilgang til dem eller det kan tas en sikringskopi av dataene. Legitime brukere kan gis tilgang til dataene eller kopier av dem. Utformingen av sikringspålegget er avgjørende for graden av tilgang.

Begrepet «order or similarly obtain», jf. artikkel 16 nr. 1, innebærer at statene, i stedet for å benytte et rettslig eller administrativt sikringspålegg, kan benytte andre prosessuelle virkemidler som gir samme resultat. Formuleringen retter seg i første rekke mot stater som av ulike grunner ikke har, eller ikke ønsker å ha, prosessuelle regler som muliggjør bruk av sikringspålegg. Disse statene gis derfor muligheten til å benytte eksisterende prinsipper for ransaking, beslag og utleveringspålegg. Likevel henstilles statene til å vurdere å gi regler om sikringspålegg fordi det normalt vil muliggjøre en raskere gjennomføring av de nødvendige sikringsforanstaltningene.

Et sikringspålegg kan gjelde alle typer lagrede data, herunder data som omhandler forretningsforhold eller sensitive personopplysninger, jf. den forklarende rapporten punkt 161.

Et sikringspålegg skal både kunne omfatte data som er i en persons besittelse og som er underlagt vedkommendes kontroll, jf. artikkel 16 nr. 2. Kontrollalternativet er praktisk hvis dataene ikke er i en persons besittelse, men lagret et annet sted hvor de like fullt er underlagt vedkommendes kontroll, jf. den forklarende rapporten punkt 162.

Sikringspålegget må være spesifisert. Det innebærer at kompetent myndighet ikke kan sikre lagrede data ved å utferdige et blanco-pålegg som gjelder alle data i innehaverens besittelse.

Statene står fritt til å vurdere hvilken myndighet som skal gis kompetanse til å utferdige sikringspålegg, jf. den forklarende rapporten punkt 138.

Et sikringspålegg gir ikke kompetent myndighet innsyn i de lagrede dataene. Spørsmålet om hvorvidt innsyn skal gis, reguleres av nasjonale regler om ransaking, beslag og utleveringspålegg, jf. den forklarende rapporten punkt 163.

Et sikringspålegg skal ikke gjelde for et lengre tidsrom enn nødvendig. Det avgjørende vil være hvor lang tid kompetent myndighet behøver for å skaffe tillatelse til eventuell ransaking, beslag og utleveringspålegg. Sikringspålegg kan ikke gjelde for mer enn 90 dager av gangen, jf. artikkel 16 nr. 2. Det skal oppgis i sikringspålegget hvilket tidsrom det gjelder. Statene er gitt adgang til å åpne for at sikringspålegg kan fornyes ved utløpet av maksimumsperioden. Fornyelse av sikringspålegget vil være underlagt begrensningene som følger av forholdsmessighetsprinsippet, jf. artikkel 15 nr. 1.

Besluttes sikringspålegg etter anmodning fra fremmed stat, følger det av artikkel 29 nr. 7 at varigheten av et slikt pålegg skal være minst 60 dager. Minimumstidsrommet er satt for å gi den andre staten tid og anledning til å iverksette nødvendige prosedyrer for å skaffe seg tilgang til materialet. Slike prosedyrer kan eksempelvis være begjæring om bistand til ransaking, beslag og utleveringspålegg, jf. den forklarende rapporten punkt 162.

Etter artikkel 16 nr. 3 er statene forpliktet til

å fastsette bestemmelser som sikrer at iverksettelsen av et sikringspålegg holdes konfidensielt. Taushetsplikten påhviler den som kontrollerer de lagrede dataene og den som iverksetter sikringen. Plikten til å bevare taushet om sikringspålegget skal være tidsbegrenset, og tidsbegrensningen må fremgå av loven. Taushetsplikten er for det første ment å ivareta hensynet til etterforskningen. Det kan være av avgjørende betydning at mistenkte ikke får kjennskap til at etterforskning pågår før de nødvendige bevisene er sikret. For det andre ivaretar taushetsplikten personvernhensyn. Data som blir sikret kan vise seg å inneholde sensitive opplysninger av ulik karakter som de berørte har krav på fortrolighet om.

3.2.1.2 Hurtig sikring og delvis avdekking av lagrede trafikkdata – artikkel 17

Artikkel 17 omhandler hurtig sikring og delvis avdekking av lagrede trafikkdata og lyder:

«1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:
   a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
   b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.
2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.»

Artikkel 17 fastsetter ytterligere regler om sikringspålegg som gjelder trafikkdata. Årsaken er de spesielle trekkene ved trafikkdata som skiller disse fra andre lagrede data. Begrepet «trafikkdata» er definert i artikkel 1 bokstav d, se punkt 1.4.

Tilgang til trafikkdata er et viktig, og i mange tilfeller helt avgjørende, redskap for å avdekke kilden til eller målet for datakriminalitet. I motsetning til innholdsdata er trafikkdata ofte lagret i et begrenset tidsrom. Årsaken kan være pålagte begrensninger i nasjonal personvernlovgivning eller alminnelig forretningspraksis. Fordi lagringstiden ofte er kort, er det viktig å ha effektive sikringsforanstaltninger som er egnet til å sikre disse dataenes integritet, jf. den forklarende rapporten punkt 166.

Artikkel 17 nr. 1 bokstav a forplikter statene til, i tilfeller hvor flere tjenestetilbydere har vært involvert i en kommunikasjonsoverføring, å ha bestemmelser som muliggjør sikring av alle relevante trafikkdata. Hver enkelt av de involverte tjenestetilbydere kan besitte trafikkdata relatert til den enkelte overføring. Det er heller ikke uvanlig at trafikkdata tilknyttet en bestemt overføring blir delt mellom ulike tjenestetilbydere på grunn av sikkerhets-, forretnings- eller tekniske hensyn. For å være i stand til å spore opprinnelsen eller destinasjonen til en bestemt overføring, er man derfor ofte avhengig av å få tilgang til trafikkdata hos samtlige involverte tjenestetilbydere.

Det er opp til statene å finne en hensiktsmessig fremgangsmåte for sikringspålegg når trafikkdata er lokalisert hos flere tjenestetilbydere. Den forklarende rapporten punkt 168 angir ulike måter dette kan løses på. En mulighet kan være å pålegge kompetent myndighet å utferdige separate sikringspålegg for hver enkelt tjenestetilbyder. En annen, og foretrukket metode, er å utferdige ett enkelt sikringspålegg som gjelder alle tjenestetilbydere som det viser seg at har hatt befatning med den aktuelle overføringen. Alternativt kan tjenestetilbydere som er gitt sikringspålegg, pålegges å underrette andre tjenestetilbydere som overføringen kan spores tilbake til.

Et sikringspålegg innebærer som nevnt ikke at utferdigende myndighet får tilgang til de lagrede dataene. Kompetent myndighet vil på tidspunktet for utferdigelsen av et sikringspålegg som gjelder trafikkdata, mangle oversikt over eventuelle andre tjenestetilbydere som har vært involvert i overføringen. Siden trafikkdata ofte blir lagret i korte tidsrom, kan det føre til at viktige data går tapt. Artikkel 17 bokstav b åpner derfor for at kompetent myndighet umiddelbart skal gis tilgang til trafikkdata i den grad det er nødvendig for å avklare hvorvidt andre tjenestetilbydere har vært involvert. Den kompetente myndighet bør spesifisere hvilke trafikkdata man ønsker tilgang til.

3.2.2 Gjeldende rett

I norsk rett finnes det ingen direkte parallell til artikkel 16 og 17 nr. 1 bokstav a. Riktignok kan påtalemyndigheten etter straffeprosessloven § 216 treffe visse tiltak for å sikre bevis, men denne bestemmelsen er ikke alene tilstrekkelig til å oppfylle konvensjonens forpliktelser. Siden det uansett bør gis en ny lovbestemmelse om sikringspålegg, jf. punkt 3.2.3.1, går utvalget ikke nær-

mere inn på rekkevidden av straffeprosessloven § 216.

Når det derimot gjelder artikkel 17 nr. 1 bokstav b om utlevering av trafikkdata, antar utvalget at konvensjonsforpliktelsen oppfylles av straffeprosessloven § 210 om utleveringspålegg. Etter denne bestemmelsen kan retten, og i hastetilfeller også påtalemyndigheten, kreve å få utlevert «[t]ing som antas å ha betydning som bevis». Det er sikker rett at utleveringsplikten også omfatter elektronisk lagrede opplysninger, herunder trafikkdata, jf. Rt. 1992 s. 904.

Utleveringspålegg kan bare gis personer som har vitneplikt, jf. straffeprosessloven § 210. I henhold til § 118 kan retten ikke ta imot forklaring som et vitne ikke kan gi uten å krenke lovbestemt taushetsplikt. Ekomloven § 2-9 første ledd fastsetter taushetsplikt for «innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon, herunder opplysninger om tekniske innretninger og fremgangsmåter», og omfatter dermed både trafikkdata og andre former for data. Taushetsplikten er likevel ikke til hinder for at det gis opplysninger til påtalemyndigheten eller politiet om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse, jf. § 2-9 tredje ledd.

Bevisforbudet etter straffeprosessloven § 118 gjelder imidlertid ikke ubetinget. Etter bestemmelsens første ledd første punktum kan departementet samtykke i at vitnet gis anledning til å forklare seg uten hinder av taushetsplikten. Samtykke kan bare nektes dersom forklaringen vil kunne utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold, jf. annet punktum. Samferdselsdepartementet har i vedtak 23. juni 1995 nr. 39 delegert samtykkekompetansen til Post- og teletilsynet. En tilbyder har dermed plikt til å utlevere elektronisk lagrede data etter § 210 i den utstrekning Post- og teletilsynet samtykker.

På visse vilkår kan retten bestemme at underretning om utleveringspålegg kan utsettes, jf. straffeprosessloven § 210a.

3.2.3 Utvalgets vurderinger

3.2.3.1 Behov for lovendringer?

Straffeprosessloven § 216 oppfyller som nevnt ikke fullt ut forpliktelsene i artikkel 16 og 17 nr. 1 bokstav a. Det er derfor uten videre klart at konvensjonens bestemmelser om midlertidig *sikring* av data gjør det nødvendig med lovendringer.

Derimot kan man spørre om det er nødvendig å endre straffeprosessloven § 210 for å oppfylle forpliktelsen i artikkel 17 nr. 1 bokstav b om *utlevering av trafikkdata*. Adgangen til å gi utleveringspålegg overfor tjenestetilbydere er betinget av at Post- og teletilsynet gir fritak fra taushetsplikten etter ekomloven § 2-9 første ledd, jf. punkt 3.2.2. Skal denne ordningen videreføres, vil tilsynet i tilfelle måtte gi fritak i alle de saker som faller innenfor artikkel 17 nr. 1 bokstav b. Etter utvalgets syn er det i utgangspunktet lite å vinne på en slik ordning. Utvalget foreslår derfor at det bør gis en egen bestemmelse om utlevering av trafikkdata som er sikret gjennom et sikringspålegg, jf. nedenfor. I spørsmålet om utformingen av en ny bestemmelse om sikringspålegg har utvalget delt seg i et flertall og et mindretall.

3.2.3.2 Nærmere om utformingen av bestemmelsen

Det første spørsmålet som oppstår ved utformingen av en bestemmelse om sikringspålegg, er hvilke former for *data* bestemmelsen skal omfatte. Etter konvensjonen artikkel 16 nr. 1 skal et sikringspålegg kunne omfatte «specified computer data, including traffic data, that has been stored by means of a computer system». Uttrykket «computer data» favner vidt, og omfatter som tidligere nevnt alle former for data, herunder e-post og andre former for innholdsdata, jf. artikkel 1 bokstav b og punkt 1.4 ovenfor. Utvalget legger til grunn at den norske gjennomføringsbestemmelsen må gis en tilsvarende vid utforming.

Spørsmålet om hvilke *vilkår* et sikringspålegg bør gjøres betinget av, er overlatt til konvensjonsstatene å avgjøre, jf. artikkel 16 nr. 4. Det vil derfor neppe være i strid med konvensjonen å kreve at det må foreligge «skjellig grunn» til mistanke om nærmere angitte straffbare handlinger, slik straffeprosessloven krever for bruk av tvangsmidler. Et slikt krav vil i tilfelle innbære at «det må være mer sannsynlig at siktede har begått den straffbare handling saken gjelder enn at han ikke har det», jf. Rt. 1993 s. 1302. Utvalget har imidlertid kommet til at terskelen for bruk av sikringspålegg bør ligge noe lavere. Hensynet til en effektiv kriminalitetsbekjempelse taler for at politiet på et relativt tidlig stadium av etterforskningen bør kunne utferdige et sikringspålegg for å sikre bevis til bruk i straffesaken. Hensynet til den mistenktes personvern trekker isolert sett i motsatt retning, jf. neste avsnitt. Etter utvalgets oppfatning vil et sikringspålegg gjennomgående utgjøre et mindre inngrep overfor den mistenkte enn både beslag etter straffeprosessloven § 203 og utleveringspålegg etter

staffeprosessloven § 210, siden politiet ikke vil få tilgang til de dataene pålegget gjelder. Etter utvalgets syn bør det derfor i utgangspunktet være tilstrekkelig at det foreligger en begrunnet mistanke om at det er begått en straffbar handling. Dette kravet vil være oppfylt dersom det foreligger visse objektive holdepunkter for at den mistenkte har begått den handlingen saken gjelder. En helt løs mistanke vil derimot ikke være tilstrekkelig.

Et særlig spørsmål er om adgangen til å utferdige sikringspålegg bør variere etter hvilke data pålegget retter seg mot. For den mistenkte vil nok sikring av privat e-post eller andre opplysninger av utpreget personlig karakter, lett fremstå som mer inngripende enn for eksempel sikring av visse former for trafikkdata. Selv om de dataene som lagres ikke skal tilflyte politiet, vil også selve lagringen utgjøre et visst inngrep i personvernet til den som rammes. Et sikringspålegg innebærer at det innhentes og lagres opplysninger om den sikringen retter seg mot, uten at vedkommende har gitt sitt samtykke til lagringen og uten at han er varslet om eller gjort kjent med pålegget. Når opplysningene først er sikret, vil de senere kunne beslaglegges i medhold av straffeprosessloven § 203 eller for øvrig brukes og misbrukes til forskjellige formål, uten at den opplysningene knytter seg til, vil kunne forhindre det. Faren for misbruk er formodentlig nokså beskjeden når sikringspålegget retter seg mot en av store, profesjonelle aktørene i markedet, men vil nok kunne være større når pålegget retter seg mot mindre seriøse tjenestetilbydere eller mot privatpersoner. Hvor stort personverninngrep det her er tale om, vil imidlertid variere etter hvilke opplysninger sikringen gjelder, hvem som har eller gis tilgang til opplysningene og hvor lenge opplysningene skal lagres. Ved vurderingen av om pålegg om sikring skal utferdiges, mener *utvalgets flertall,* alle medlemmene unntatt Sunde, at politiet blant annet skal ta i betraktning om tjenestetilbyderens rutiner er tilstrekkelig betryggende.

Utvalgets mindretall, Sunde, er uenig i at det skal stilles krav om at politiet skal vurdere kvaliteten på tilbydernes rutiner for sikring av data når sikringspålegg begjæres. Politiet har ikke innsyn i tilbydernes rutiner og kan ikke gjøre denne vurderingen. Spørsmålet om krav til rutiner og kontroll hører inn under Samferdselsdepartementets ansvarsområde og skal følges opp av Post- og teletilsynet, eventuelt også av Datatilsynet og Nasjonal Sikkerhetsmyndighet. Dersom det hefter betenkeligheter ved visse tilbyderes rutiner, er dette dermed noe som de nevnte instanser skal ta fatt i.

Utvalgets flertall har etter dette kommet til at det bør trekkes et skille mellom trafikkdata og andre former for data. Selv om også trafikkdata kan gi opplysninger om forhold av privat karakter, vil nok et sikringspålegg som retter seg mot ulike former for innholdsdata, normalt utgjøre et større inngrep i den mistenktes personvern. Især gjelder dette om pålegget retter seg mot innholdet av en e-post, vedlegg til en e-post eller andre private forsendelser. Sikring av e-post hos en tjenestetilbyder kan langt på vei sammenliknes med det å åpne og ta kopi av brev på et postkontor. I straffeprosessloven §§ 211 og 212 er det gitt særlige regler om beslag av postsendinger som besittes av en postoperatør, og bygger på det syn at posthemmeligheten fortjener et særlig vern, jf. også Den europeiske menneskerettskonvensjon artikkel 8 nr. 1 som er inkorporert i norsk rett ved lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven) § 2. Flertallet antar derfor at adgangen til å sikre innholdsdata bør være noe snevrere enn adgangen til å sikre trafikkdata. Etter flertallets syn bør derfor sikring av andre data enn trafikkdata bare kunne skje ved mistanke om en straffbar handling med en høyere strafferamme enn fengsel i 6 måneder. Flertallet foreslår å gjøre unntak fra strafferammekravet ved mistanke om overtredelse av straffeloven § 390 a. Strafferammen i § 390 a er bøter eller fengsel inntil 6 måneder. Kravet til høyere strafferamme enn fengsel i 6 måneder er derfor ikke oppfylt. Flertallet mener at det likevel bør være adgang til å utferdige sikringspålegg ved mistanke om overtredelse av denne bestemmelsen. Sikringspålegg vil etter flertallets oppfatning være praktisk fordi overtredelser av § 390 a ofte skjer ved hjelp av et datasystem, for eksempel ved bruk av e-post.

Etter artikkel 16 nr. 2 skal et sikringspålegg innebære en plikt til å «maintain the integrity of that computer data for a period of time». Konvensjonen angir ikke på hvilken måte sikringen skal skje, såfremt dataene beskyttes mot «anything that would cause its current quality or condition to change or deterioate» for å unngå utilsiktet «modification, deteriotation or deletion», jf. den forklarende rapporten punkt 159. Sikring kan skje ved at det tas kopi av de dataene saken gjelder, eller ved at dataene gjøres utilgjengelige for andre enn den pålegget retter seg mot. Hvilken form for sikring som er mest hensiktsmessig, vil bero på omstendighetene og den tekniske utviklingen. Hensynet til teknologinøytralitet taler for at heller ikke den norske gjennomføringsbestemmelsen angir noe bestemt om hvordan dataene skal sikres. Den pålegget retter seg mot vil dermed selv kunne velge hvordan sikringen skal gjennomføres innenfor de muligheter som finnes, såfremt data-

enes integritet, tilgjengelighet og autensitet blir ivaretatt.

Utvalgets mindretall er uenig i det generelle vilkåret om 6 måneders strafferamme for bruk av sikringspålegg. Flertallets begrunnelse refererer seg til hensynet til posthemmeligheten. Vilkåret burde derfor vært begrenset til å gjelde sikringspålegg i e-post, og ikke gjelde data generelt. Reglene om sikringspålegg bør uansett ses i sammenheng med reglene om beslag og utleveringspålegg. En begrensning til e-post slik dette medlemmet foreslår, vil gi god sammenheng til beslagsregelen i straffeprosessloven § 211, som setter som vilkår for beslag i post (og e-post) at mistanken gjelder et straffbart forhold som etter loven kan medføre straff av fengsel i mer enn 6 måneder. For innholdsdata av annen art som for eksempel newsmeldinger, web-sider, ulovlig pornografi, opphavsrettslig beskyttet materiale, word-filer osv., gjelder det en generell beslagsadgang, jf. straffeprosessloven § 203. Harmonihensyn tilsier at det ikke bør gjelde strengere vilkår for bruk av sikringspålegg enn for beslag, siden sikringspålegg er et mindre inngripende tiltak enn beslag. Dette medlemmet kan heller ikke se at det er foreligger reelle grunner som i seg selv skulle begrunne et slikt strafferammevilkår i regelen om sikringspålegg. Dette medlemmet foreslår derfor at ny § 215 a første ledd i straffeprosessloven bør lyde:

> *Påtalemyndigheten kan gi pålegg om sikring av elektronisk lagrede data som antas å ha betydning som bevis. Sikringspålegg i e-post kan likevel bare tas ved mistanke om en straffbar handling som etter loven kan medføre en høyere straff enn fengsel i 6 måneder eller som rammes av straffeloven § 390 a.*

Videre har mindretallet en kommentarer av prinsipiell art. Dette medlemmet mener at flertallets vurderinger i for stor grad er knyttet opp til en forutsetning om at etterforskingen gjelder en bestemt mistenkt, mens reglene om sikringspålegg antakelig vil ha sin største betydning i saker med ukjent gjerningsperson, dvs. at man har holdepunkter for at en straffbar handling er begått, men man vet ikke av hvem. Dette er den typiske situasjon ved etterforsking av datainnbrudd, spredning og nedlasting av bilder av seksuelle overgrep mot barn via internett, sjikane og rasistiske ytringer ved bruk av elektroniske kommunikasjonstjenester, ulovlig distribusjon av opphavsrettslig beskyttet materiale mv. Flertallets merknader om underretning, spesifikasjon av mistanke og av data som skal kreves sikret, må leses med forbehold om at man ikke har tenkt på denne situasjonen.

Det neste spørsmålet som må avklares, er hvem som bør ha *kompetanse* til å beslutte sikring av lagrede data. Ved denne vurderingen er det naturlig å legge vekt på hvor inngripende tiltaket virker overfor den som rammes. Et sikringspålegg vil som nevnt være mindre inngripende enn både beslag etter § 203, utleveringspålegg etter § 210 og kommunikasjonskontroll etter §§ 216 a og 216 b, siden pålegget ikke innebærer noen løpende innhenting av opplysninger fremover i tid, og siden politiet ikke vil få tilgang til de dataene som omfattes av pålegget. Det er derfor neppe grunn til å kreve at beslutningen skal treffes av en domstol. Derimot vil det å legge kompetansen på politinivå være å gå for langt i motsatt retning, selv i hastetilfellene. Et sikringspålegg kan etter omstendighetene utgjøre et vesentlig inngrep i personvernet til den som opplysningene gjelder, samtidig som selve sikringen kan være både arbeids- og kostnadskrevende. Beslutningskompetansen bør derfor legges til påtalemyndigheten.

Et spørsmål for seg er om den som opplysningene knytter seg til, forutsatt at dette er en bestemt person, skal gis *underretning* om beslutningen, og når slik underretning i tilfelle skal gis. Dette spørsmålet har for øvrig nær tilknytning til spørsmålet om vedkommende bør kunne anvende rettsmidler mot sikringspålegget.

Ved bruk av tvangsmidler overfor en siktet i en straffesak er hovedregelen etter straffeprosessloven at vedkommende har krav på underretning *før* det aktuelle tiltaket settes i verk. Ved ransaking fremgår dette av straffeprosessloven § 200 første ledd, som også får anvendelse ved beslag, jf. straffeprosessloven § 205 første ledd siste punktum. Reglene om utleveringspålegg etter straffeprosessloven § 210 inneholder ikke noen tilsvarende henvisning, men et slikt pålegg vil naturlig nok ikke kunne gjennomføres uten at den det retter seg mot, blir gjort kjent med innholdet. Bakgrunnen for at den siktede har krav på underretning, er først og fremst hensynet til kontradiksjon. I vårt rettssystem regnes det som en sentral rettssikkerhetsgaranti at den siktede skal gjøres kjent med de anklager som rettes mot ham, og gis anledning til å ta til gjenmæle mot dem. For å sikre at påtalemyndigheten ikke anvender tvangsmidler i større utstrekning enn det loven åpner for, er det behov for regler om underretning, og for at underretning gis før det aktuelle tvangsmidlet iverksettes.

I enkelte tilfeller må imidlertid hensynet til den enkelte vike for hensynet til samfunnets kollektive interesse i å bekjempe kriminalitet. Etter straffeprosessloven §§ 200a om ransaking, 202e om båndlegging, 208a om beslag og 210a om utle-

veringspålegg kan retten ved kjennelse beslutte at underretning kan *utsettes* i inntil 8 uker om gangen, dersom det er strengt nødvendig av hensyn til etterforskningen. Gjelder det ransaking, er det et tilleggsvilkår at saken gjelder en handling eller forsøk på en handling som etter loven kan medføre straff av fengsel i 10 år eller mer, eller en av de andre alvorlige forbrytelsene loven nevner særskilt. Underretning kan bare *unnlates helt* i saker om overtredelse av straffeloven kapittel 8 og 9.

Etter utvalgets syn bør den som rammes av det opplysningene knytter seg til, underrettes om at det er utferdiget et sikringspålegg. Som tidligere nevnt, vil et sikringspålegg innebære at det innhentes og lagres opplysninger om den sikringen retter seg mot, uten at vedkommende har gitt sitt samtykke til lagringen. Mener den mistenkte at vilkårene for bruk av sikringspålegg ikke er oppfylt, taler rettssikkerhetshensyn for at han bør gis anledning til å ta til gjenmæle. De særlige hensyn som har begrunnet unntaket for saker om rikets sikkerhet, har ikke samme gjennomslagskraft når det gjelder mindre alvorlige former for kriminalitet.

Det er imidlertid ikke uten videre klart om underretning bør gis samtidig, slik utgangspunktet er ved beslag og ransaking mv., eller først på et senere tidspunkt, for eksempel når sikringsperioden utløper eller når straffesaken mot den mistenke er endelig avgjort. Hensynet til etterforskningen taler for at den mistenkte ikke bør ha krav på underretning allerede før sikringspålegget settes i verk. Den mistenkte bør heller ikke ha krav på underretning før eventuelle frister for utsatt underretning etter straffeprosessloven §§ 200a, 202e, 208a eller 210a har utløpt. I motsatt fall ville den mistenkte bli oppmerksom på at det pågår en etterforskning mot ham. Derimot kan det ikke være grunn til å vente helt til saken er endelig avgjort.

Etter utvalgets syn bør en mistenkt ha krav på underretning fra det tidspunkt han får status som siktet i saken, jf. straffeprosessloven § 82. Han vil dermed ha krav på underretning senest på det tidspunkt når påtalemyndigheten har erklært ham for siktet, når forfølging mot ham er innledet ved retten eller når det er besluttet eller foretatt pågripelse, ransaking, beslag eller lignende forholdsregler rettet mot ham. Er det besluttet utsatt underretning om et tvangsmiddel, inntrer stillingen som siktet først når underretning gis, jf. straffeprosessloven § 82 tredje ledd. I så fall skal den siktede samtidig gis underretning om sikringspålegget.

Det siste spørsmålet som må nevnes i denne forbindelse, er om en beslutning om bruk av sikringspålegg bør kunne gjøres til gjenstand for *rettslig prøving*. Etter utvalgets skjønn kan det ikke være tvilsomt at slike regler bør gis. For å sikre at påtalemyndigheten ikke anvender sikringspålegg i større utstrekning enn det loven åpner for, bør den opplysningene knytter seg til kunne be om en rettslig overprøving av påtalemyndighetens beslutning på samme måte som når det gjelder beslutninger om ransaking og beslag mv. Lovteknisk kan dette gjøres gjennom henvisning til straffeprosessloven § 208.

De dataene som er sikret gjennom et sikringspålegg, skal ikke tilflyte politiet. Slike data kan i utgangspunktet bare kreves utlevert innenfor rammen av straffeprosessloven § 210. Hensynet til etterforskningen taler imidlertid for at politiet straks bør få tilgang til de opplysninger som er nødvendige for å avdekke hvor de aktuelle dataene kom fra, og hvor de i tilfelle ble sendt til, jf. artikkel 17 nr. 1 bokstav b. En slik bestemmelse vil kunne bidra til å avdekke eventuelle bakmenn eller andre medvirkere. *Utvalgets flertall* har derfor fremmet forslag om en utvidet utleveringsplikt for slike opplysninger, jf. forslaget til ny § 215 a fjerde ledd.

Utvalgets mindretall mener at utleveringsplikten mht. trafikkdata, jf. utkastet til ny straffeprosessloven § 215 a siste ledd, bør skjerpes slik at tilbydere plikter å etterkomme utleveringspålegget «straks». Dette er i bedre samsvar med konvensjonens krav om «expeditious disclosure», jf. artikkel 17 nr. 1 bokstav b, og støtter også formålet med regelen, nemlig å tilrettelegge for det tempo i etterforskningen som er nødvendig for å spore opp gjerningspersoner via elektroniske data – før dataene forsvinner. Dette medlemmet mener derfor at siste ledd bør lyde:

> *Den pålegget retter seg mot, skal etter begjæring straks utlevere de trafikkdata som er nødvendige for å spore hvor dataene som omfattes av sikringspålegget kom fra og hvor de eventuelt ble sendt til.*

3.3 Utleveringspålegg – artikkel 18

3.3.1 Folkerettslige forpliktelser

Artikkel 18 omhandler utleveringspålegg («production order») og lyder:

> «1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
> a) a person in its territory to submit specified computer data in that person's pos-

session or control, which is stored in a computer system or a computer-data storage medium; and

b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
3. For the purpose of this article, the term «subscriber information» means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
   a) the type of communication service used, the technical provisions taken thereto and the period of service;
   b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
   c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.»

Bestemmelsen pålegger statene å gi kompetent myndighet adgang til å utstede pålegg om utlevering av lagrede data og abonnementsinformasjon. Gjennomgående vil bruk av utleveringspålegg være et mindre inngripende virkemiddel enn for eksempel ransaking og beslag. Alminnelige forholdsmessighetsbetraktninger tilsier derfor bruk av utleveringspålegg dersom det er egnet for formålet.

Etter artikkel 18 nr. 1 skal regler om utleveringspålegg omfatte både elektronisk lagrede data i en persons besittelse eller kontroll, jf. bokstav a, og abonnementsdata hos en tjenestetilbyder uten hensyn til om disse er lagret elektronisk eller på andre måter, jf. bokstav b. Bestemmelsene gjelder bare data som rent faktisk eksisterer på tidspunktet for utferdigelsen av utleveringspålegget, og bare for personer som befinner seg innenfor den enkelte stats territorium.

Artikkel 18 gjelder bare spesifiserte lagrede data som en person besitter eller kontrollerer. En person anses for å besitte lagrede data dersom de fysisk sett er i den berørte personens besittelse. Kontrollerte data omfatter lagrede data som er fritt tilgjengelige for den berørte personen, uten at dataene fysisk er lagret hos vedkommende. Et typisk eksempel er data som er lagret på et annet geografisk sted enn der den personen pålegget er rettet mot befinner seg. Så lenge tilgangen kan skje faktisk og rettslig, vil kontrollalternativet normalt være oppfylt. Imidlertid innebærer ikke nødvendigvis det at en person har rett å få tilgang til en annens datasystem at dataene er underlagt førstnevntes kontroll. Det er uten betydning om lagringsmediet befinner seg i inn- eller utland.

Etter artikkel 18 nr. 1 bokstav b skal en tjenestetilbyder som tilbyr sine tjenester innenfor den enkelte stats territorium, kunne pålegges å utlevere abonnementsopplysninger underlagt dennes besittelse eller kontroll. Bestemmelsen gjelder bare abonnementsopplysninger som er relatert til den innenlandske virksomheten, jf. «related to such services».

Det følger av den forklarende rapporten punkt 175 at statene kan gi regler om taushetsplikt for dem utleveringspålegget rettes mot. Særlig praktisk vil det være i tilfeller hvor utleveringspålegget benyttes tidlig i etterforskningsfasen og før eventuelle andre tvangsmidler benyttes.

Begrepet «abonnementsopplysninger» («subscriber information») som er benyttet i artikkel 18 nr. 1 bokstav b, er definert i artikkel 18 nr. 3. Det er uten betydning om disse opplysningene er lagret elektronisk eller ikke. Begrepet omfatter all informasjon en tjenestetilbyder har som er knyttet til bruken eller brukere av sine tjenester, unntatt innholds- og trafikkdata, jf. den forklarende rapporten punkt 177 til 180. Bestemmelsen oppstiller ingen plikt for tjenestetilbydere til å registrere og oppbevare abonnementsopplysninger, jf. den forklarende rapporten punkt 181.

3.3.2 Gjeldende rett

I henhold til straffeprosessloven § 210 kan retten, eventuelt påtalemyndigheten, pålegge besitteren å utlevere ting som antas å ha betydning som bevis såfremt han plikter å vitne i saken. Begrepet «ting» omfatter også opplysninger som lagres på data, herunder bankutskrifter, registerte samtaler hos telefonoperatører osv., jf. Rt. 1992 s. 904 hvor Høyesterett uttaler:

> «Bestemmelsene i straffeprosesslovens kap 16 om beslag og utleveringspålegg av ting som antas å ha betydning som bevis er av generell karakter. Beslagsadgangen og utleveringsplikten omfatter ikke bare legemlige gjenstander, men også opplysninger lagret på data og som i tilfellet må gjøres tilgjengelig ved utskrifter, som for eksempel opplysninger om bankkonti.

> Begrensinger i lovens alminnelige adgang til beslag og krav om utlevering, ut over det som er fastsatt i straffeprosessloven, krever særskilt hjemmel».

Utleveringspålegg som virker fremover i tid reguleres av § 210b for så vidt gjelder ting, mens § 216b annet ledd bokstav c gjelder innhenting av fremtidige kommunikasjonsdata.

Formuleringen «antas å ha betydning som bevis» innebærer at en rimelig mulighet er tilstrekkelig, jf. Bjerke/Keiserud, *Straffeprosessloven - Kommentarutgave,* 3. utg. s. 725. Utleveringspålegget må spesifiseres slik at det er mulig for mottaker å vite hva han skal fremlegge, jf. Rt. 1997 s. 266 og Rt. 1999 s. 1944.

Det er bare personer med vitneplikt som har plikt til å etterkomme et utleveringspålegg. Hvis en person ikke har vitneplikt, må reglene om ransaking og beslag benyttes.

Bestemmelses annet ledd gir påtalemyndigheten adgang til å beslutte utleveringspålegg dersom det ved opphold er fare for at etterforskningen vil lide. Beslutningen skal i så fall snarest mulig oversendes retten til godkjennelse.

3.3.3 Utvalgets vurderinger

Det er ikke tvilsomt at begrepet «ting» også omfatter lagrede data. Derimot er det mulig at formuleringen «possesssion or control» i artikkel 18 nr. 1 rekker lengre enn begrepet «besittelse» i § 210.

Data som er lagret fysisk hos den pålegget rettes mot, er utvilsomt i vedkommendes besittelse i lovens forstand. Derimot kan det stilles spørsmål ved om det samme gjelder når dataene er lagret andre steder. Etter utvalgets oppfatning må det sondres mellom to ulike situasjoner. Den første situasjonen gjelder tilfeller hvor dataene befinner seg på et eksternt lagringsmedium uten noen form for nettverksforbindelse. I så fall er ikke dataene underlagt vedkommendes kontroll i konvensjonens forstand. Den andre situasjonen gjelder tilfeller hvor dataene befinner seg på et eksternt lagringsmedium med nettverksforbindelse. Etter utvalgets oppfatning må spørsmålet om det i slike tilfeller foreligger «besittelse» bero på råderetten til den pålegget retter seg mot, og ikke den fysiske plasseringen av lagringsmediet. Eierforholdet til lagringsmediet kan heller ikke være avgjørende. Man kan ikke omgå kravet til besittelse ved å lagre dataene hos en ekstern tjenestetilbyder, for eksempel på et såkalt Web-hotell. I slike tilfeller vil råderetten og tilgangen til dataene normalt være den samme som ved lagring på eget lagringsmedium. Utvalget er derfor av den oppfatning at formuleringen «possession or control» i forhold til lagrede data ikke rekker videre enn det som følger av begrepet «besittelse» i § 210.

Etter utvalgets oppfatning oppfyller straffeprosessloven § 210 forpliktelsene i artikkel 18. Det er derfor ikke behov for endringer i norsk rett.

3.4 Ransaking og beslag – artikkel 19

3.4.1 Folkerettslige forpliktelser

Artikkel 19 omhandler ransaking og beslag og lyder:

«1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
   a) a computer system or part of it and computer data stored therein; and
   b) a computer-data storage medium in which computer data may be stored in its territory.
2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
   a) seize or similarly secure a computer system or part of it or a computer-data storage medium;
   b) make and retain a copy of those computer data;
   c) maintain the integrity of the relevant stored computer data;
   d) render inaccessible or remove those computer data in the accessed computer system.
4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the

functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.»

Artikkel 19 nr. 1 og 2 gjelder ransaking, mens nr. 3 omhandler beslag. Formålet med bestemmelsen er å sørge for at nasjonale regler om ransaking og beslag blir tilpasset den teknologiske utviklingen. Gjeldende bestemmelser er i mange stater primært utarbeidet med fysiske objekter for øye. Ransaking med tanke på beslag av lagrede data forutsetter i slike tilfeller at man tar kontroll over selve lagringsmediet. Siktemålet med artikkel 19 er å sørge for at tilsvarende tvangsmidler kan benyttes overfor dataene i seg selv.

Etter artikkel 19 nr. 1 er statene forpliktet til å ha bestemmelser som gir kompetent myndighet adgang til å ransake både datasystemer og frittstående lagringsmedier, for eksempel CD-ROM og disketter.

Ettersom forpliktelsene i medhold av artikkel 19 bare gjelder lagrede data, oppstår det et spørsmål om uåpnet e-post som ligger mellomlagret hos en tjenestetilbyder, skal anses som lagrede data eller data under kommunikasjon. Spørsmålet har betydning for hvilke regelsett som kommer til anvendelse, idet tilgang til data under overføring reguleres av artikkel 20 og 21, og ikke av artikkel 19. Statene står imidlertid fritt til å velge den løsning som er best i samsvar med nasjonale prinsipper.

Artikkel 19 nr. 2 forplikter statene å ha bestemmelser som muliggjør umiddelbar utvidelse av ransakingen fra et datasystem eller en del av et datasystem til et datasystem eller en del av et datasystem som ikke er omfattet av ransakingsbeslutningen. Forpliktelsen omfatter tilfeller der det for det første er fyllestgjørende grunn til å anta at det andre systemet inneholder de ettersøkte dataene. Videre må datasystemene være tilknyttet hverandre. For det tredje må dataene i det eksternt plasserte systemet lovlig kunne innhentes fra det primære ransakingsobjektet. For det fjerde må det eksterne datasystemet befinne seg innen riket. Fremgangsmåten for en utvidet nettverksbasert ransaking er ikke gitt i konvensjonen, og er dermed opp til de enkelte statene selv å regulere.

I henhold til artikkel 19 nr. 3 er statene forpliktet til å ha bestemmelser som sikrer at data som er avdekket gjennom ransaking etter artikkel 19 nr. 1 og 2, kan beslaglegges. Siden lagrede data ikke kan eksistere uavhengig av et lagringsmedium, kan det tradisjonelle begrepet «beslag» virke noe upresist. Gjennomføringen av et beslag skjer indirekte ved at man tar med selve lagringsmediet, eller ved at dataene bli kopiert over på et eksternt lagringsmedium. Konvensjonen benytter derfor formuleringen «seize or similarily secure» som en fellesbetegnelse på mulige fremgangsmåter. Foruten beslag av selve lagringsmediet og kopiering av dataene, omfattes også tiltak som sikrer ivaretagelse av dataenes integritet og tiltak som muliggjør konfiskering eller utilgjengeliggjøring av dataene, jf. artikkel 19 nr. 3 bokstav a til d og den forklarende rapporten punkt 198 og 199.

Statene er etter artikkel 19 nr. 4 forpliktet til å sikre kompetent myndighet adgang til å pålegge systemadministrator eller andre å gi opplysninger som kan lette gjennomføringen av ransakingen. Opplysningsplikten rekker imidlertid ikke lenger enn det som er rimelig («reasonable»). Spørsmålet om hva som er rimelig, beror på en helhetsvurdering. Et relevant moment kan for eksempel være om datasystemet inneholder informasjon som faller inn under unntak fra vitneplikten i henhold til nasjonal rett, jf. den forklarende rapporten punkt 202.

Statene står fritt til å avgjøre om, og eventuelt i hvilken grad, den som blir utsatt for nettverksbasert ransaking og beslag, skal ha krav på underretning, jf. den forklarende rapporten punkt 204.

3.4.2 Gjeldende rett

Adgangen til *ransaking* fremgår av straffeprosessloven kapittel 15. Det skilles mellom husransaking og personransaking. Bare førstnevnte skal behandles her. Hovedregelen er gitt i straffeprosessloven § 192. Etter bestemmelsens første ledd kan det foretas ransaking av mistenktes bolig, rom eller oppbevaringssted dersom det foreligger skjellig grunn til mistanke om en handling som kan medføre frihetsstraff, og formålet med ransakingen er å søke etter bevis eller ting som kan beslaglegges. Videre er adgangen til å ransake hos tredjepersoner regulert i § 192 annet ledd. Det er ikke tvilsomt at ransakingsadgangen i § 192 omfatter datamaskiner og datalagringsmedier.

Kompetansen til å beslutte ransaking er i utgangspunktet tillagt retten, jf. § 197 første ledd. Påtalemyndigheten kan imidlertid selv beslutte ransaking dersom det er fare ved opphold, jf. § 197 annet ledd. Politiets begrensede adgang til å beslutte ransaking følger av § 198.

Adgangen til å ta *beslag* fremgår av straffepro-

sessloven kapittel 16. Hovedregelen fremkommer av § 203 hvor det heter at «ting som antas å ha betydning som bevis kan beslaglegges». I Rt. 1992 s. 904 berører Høyesteretts kjæremålsutvalg spørsmålet om hvorvidt data kan regnes som «ting» i straffeprosesslovens forstand:

> «Beslagsadgangen og utleveringsplikten omfatter ikke bare legemlige gjenstander, men også opplysninger som lagres på data og som i tilfelle må gjøres tilgjengelig ved utskrifter, som f eks opplysninger om bankkonti.»

Når det gjelder vilkårene for beslag følger det av bestemmelsen at alle ting som «antas å ha betydning som bevis», kan beslaglegges. «Antas» innebærer at rimelig mulighet er nok, jf. Bjerke/Keiserud, *Straffeprosessloven - Kommentarutgave,* 3. utgave s. 711.

Kompetansen til å beslutte beslag er lagt til påtalemyndigheten, jf. § 205 første punktum. Finner påtalemyndigheten at «særlige grunner foreligger», kan den bringe spørsmålet inn for retten. Politiets adgang til å ta beslag er regulert i § 206.

3.4.3 Utvalgets vurderinger

Som nevnt under punkt 3.3.2, er det ikke tvilsomt at straffeprosessloven kapittel 15 gir hjemmel til ransaking av datasystemer og datalagringsmedier. Vurderingstemaet for utvalget er dermed ikke hvorvidt man etter norsk rett har adgang til slik ransaking, men om dagens bestemmelser fullt ut dekker de folkerettslige forpliktelsene som følger av artikkel 19.

3.4.3.1 Ransaking

Konvensjonens bestemmelser om ransaking skaper stort sett ingen problemer i forhold til norsk rett. Et spørsmål som imidlertid må avklares, er om gjeldende rett tilfredsstiller konvensjonens krav om hurtig utvidelse av ransakingen til et datasystem eller en del av et datasystem som ikke er omfattet av ransakingsbeslutningen, jf. artikkel 19 nr. 2. Hvilke datasystemer som lovlig kan ransakes, beror i utgangspunktet på utformingen av den beslutningen som gir grunnlag for ransakingen. Spørsmålet om hurtig utvidelse av ransakingen fra ett datasystem til et annet, uavhengig av om den er ment å gjøres via nettet eller ikke, oppstår derfor først i de tilfellene hvor den opprinnelige ransakingsbeslutningen ikke rekker langt nok. Utvalget legger til grunn at konvensjonens krav om hurtig utvidelse («expeditiously extention») innebærer at tidsløpet som går fra behovet om utvidelse oppstår til ransakingen kan settes i verk, må være kort. Innhenting av en ny ransakingsbeslutning fra retten, jf. straffeprosessloven § 197 første ledd, vil etter utvalgets oppfatning lett kunne ta for lang tid. Utvalget legger imidlertid til grunn at påtalemyndighetens hastekompetanse i straffeprosessloven § 197 annet ledd vil dekke konvensjonens krav, også fordi beslutningen kan gis muntlig, jf. straffeprosessloven § 197 tredje ledd.

Ransaking av e-post som er mellomlagret hos en tjenestetilbyder i påvente av mottakerens nedlasting, er etter utvalgets oppfatning omfattet av reglene om ransaking hos tredjemann i § 192 annet ledd.

Det er etter utvalgets oppfatning ikke behov for lovendringer for å kunne ratifisere konvensjonens bestemmelser om ransaking i artikkel 18 nr. 1 og nr. 2.

3.4.3.2 Særlig om plikten til å gi opplysninger i forbindelse med ransaking

I henhold til artikkel 19 nr. 4 er statene forpliktet til å gi kompetent myndighet adgang til å pålegge en systemadministrator eller andre med kjennskap til et bestemt datasystem, å bistå under ransakingen ved å gi opplysninger. Det finnes ingen slik generell hjemmel i norsk rett. Straffeprosessloven § 216a fjerde ledd annet punktum gir riktignok politiet hjemmel til å pålegge en eier eller tilbyder av nett eller tjeneste å yte den bistanden som er nødvendig for gjennomføring av kommunikasjonsavlytting. Bestemmelsen er gitt tilsvarende anvendelse i forhold til innhenting av trafikkdata i sanntid, jf. straffeprosessloven § 216b tredje ledd. Bestemmelsens anvendelsesområde er imidlertid svært begrenset, og kan ikke tolkes slik at den gir politiet tilsvarende hjemmel i forbindelse med ransaking. Det er tale om inngrep i borgernes rettssfære som av hensyn til legalitetsprinsippet krever hjemmel i lov. Etter utvalgets oppfatning er det derfor påkrevd med lovendring.

Vernet mot selvinkriminering

Pålegg om å gi opplysninger i forbindelse med en ransaking kan tenkes å komme i konflikt med vernet mot selvinkriminering som Den europeiske menneskerettsdomstol (EMD) har innfortolket i EMK artikkel 6. Et tilsvarende forbud finnes i blant annet i SP artikkel 14 nr. 3 g.

Individet er vernet mot selvinkriminering i forbindelse med behandling av en straffsiktelse i rettsapparatet, det vil si et hvert forhold som anses for å

være en straffsiktelse i henhold til EMK artikkel 6. Begrepet «straffsiktelse» i artikkel 6 er autonomt. Det er derfor ikke uten videre avgjørende om en person regnes som siktet etter nasjonal rett. I henhold til praksis fra EMD foreligger det i alle tilfeller en siktelse hvis vedkommende er siktet i henhold til nasjonal rett. Videre vurderer EMD om anklagens art eller arten og alvorligheten av den straffen som vil kunne idømmes, tilsier at det dreier seg om en straffsiktelse.

Et pålegg om å bidra med de opplysningene som er nødvendige for å gjennomføre ransaking av et datasystem, innebærer ikke en straffsiktelse i seg selv. Vedkommende vil ikke få stilling som siktet etter norsk rett, jf. straffeprosessloven § 82. En opplysningsplikt i forbindelse med ransaking har lite til felles med virkemidler som pågripelse, ransaking eller beslag.

Utvalget kjenner ikke til praksis fra EMD som gjelder pålegg om å gi opplysninger under en politietterforskning. Derimot mener utvalget at praksis fra EMD som gjelder kontrollstadiet i forvaltningssaker kan tjene som illustrasjon. Begge tilfellene gjelder en straffesanksjonert opplysningsplikt som pålegges en person som på det tidspunktet ikke er siktet i EMKs forstand. Videre er det i begge typene saker en mulighet for at den personen som pålegges opplysningsplikt, vil bli siktet senere i prosessen. Praksis som gjelder hvorvidt en person kan pålegges opplysningsplikt på kontrollstadiet i en forvaltningssak, kan derfor ha overføringsverdi.

EMD har i nyere praksis kommet til at vernet mot selvinkriminering på visse vilkår kan bli utløst allerede på kontrollstadiet, i forbindelse med ileggelse av bøter for overtredelse av en opplysningsplikt, jf. J. B.-saken.[1)] I saken ble J. B. en rekke ganger pålagt å utlevere dokumenter til skattemyndighetene. Klageren ble ilagt fire bøter på grunn av overtredelse av påleggene, men var ikke siktet i henhold til nasjonal rett. EMD kom likevel til at det forelå en straffsiktelse, og at J. B.'s rett til frihet fra selvinkriminering var krenket. Man kan neppe trekke den slutning fra dommen at det gjelder et generelt forbud mot straffesanksjonert opplysningsplikt. Retten synes å legge vekt på at myndighetene tok sikte på en mulig sanksjonssak da de påla J. B. å utlevere dokumenter, og at informasjonen som ble krevd utlevert, ville være relevant for denne saken:

> «The Court observes that, in the present case, the proceedings served the various purposes of establishing the taxes due by the applicant and, if the conditions therefor were met, of imposing on him a supplementary tax and a fine for tax evasion. Nevertheless, the proceedings were not expressly classified as constituting either supplementary-tax proceedings or tax-evasion proceedings.
>
> The Court furthermore considers, and this was not in dispute between the parties, that from the beginning and throughout the proceedings the tax authorities could have imposed a fine on the applicant on account of the criminal offence of tax evasion. According to the settlement reached on 28 November 1996, the applicant did indeed incur such a fine amounting to CHF 21,625.95. The penalty was not, however, intended as pecuniary compensation; rather, it was essentially punitive and deterrent in nature. Moreover, the amount of the fine incurred was not inconsiderable. Finally, there can be no doubt that the fine was 'penal' in character (see the A.P., M.P. and T.P. v. Switzerland cited above).
>
> In the Court's opinion, whatever other purposes served by the proceedings, by allowing the imposition of such a fine on the applicant, the proceedings amounted in the light of the Court's case-law to the determination of a criminal charge.
>
> As a result, the Court finds that Article 6 is applicable under its criminal head.»[2)]

Dermed vil neppe en opplysningsplikt pålagt en person som politiet ikke har til hensikt å strafforfølge, utløse vernet mot selvinkrimiering. Det følger også av begrunnelsen for selvinkrimineringsvernet slik EMD formulerte det i for eksempel Saunders-saken:

> «Their rationale lies, inter alia, in the protection of the accused against improper compulsion by the authorities thereby contributing to the avoidance of miscarriages of justice and to the fulfilment of the aims of Article 6 … The right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused.»[3)]

Vernet mot selvinkriminering vil komme inn i de tilfellene der den opplysningsplikten er rettet mot,

1) J. B. mot Sveits 3. mai 2001, sak 31827/96.

2) J. B. mot Sveits 3. mai 2001, sak 31827/96, avsnitt 47 til 50.

3) Saunders mot Storbritannia 17 desember 1996, sak 19187/92 avsnitt 68.

regnes som straffsiktet av andre årsaker. Utvalget har utformet forslaget til bestemmelse om opplysningsplikt slik at plikten bare kan pålegges den som plikter å vitne i saken. I henhold til straffeprosessloven § 123 kan et vitne nekte å svare på spørsmål som vil kunne utsette vitnet eller nærstående for straff eller tap av borgerlig aktelse. En siktet vil derfor ikke kunne pålegges plikt til å hjelpe politiet med å fremskaffe opplysninger som kan brukes mot ham i en senere straffesak. Utvalget forutsetter at denne begrensningen i bestemmelsens anvendelsesområde vil hindre krenkelser av vernet mot selvinkriminering. Videre vil politiet uansett ikke kunne pålegge opplysningsplikt i strid med vernet mot selvinkriminering, jf. straffeprosessloven § 4 og menneskerettsloven §§ 2 og 3.

Nærmere om utformingen av bestemmelsen

Ved utformingen av en lovbestemmelse om opplysningsplikt for systemadministratorer og andre med kjennskap til et bestemt datasystem, må flere spørsmål avklares. Det gjelder omfanget av opplysningsplikten, hvem opplysningsplikten kan påhvile, hvem som skal ha kompetanse til å pålegge en opplysningsplikt og hvilke sanksjoner som skal gjelde dersom opplysningsplikten ikke overholdes.

Etter utvalgets oppfatning bør ikke opplysningsplikten gis et større *omfang* enn det artikkel 19 nr. 4 forplikter oss til. En opplysningsplikt under ransaking av et datasystem innebærer et brudd med den alminnelige retten til å nekte å forklare seg overfor politiet, jf. straffeprosessloven § 230. Derfor bør opplysningsplikten begrenses til det som er nødvendig for å gi *tilgang* til det aktuelle datasystemet. Med tilgang til et datasystem menes tilgang til dataene som er lagret i systemet. Slik tilgang kan for eksempel kreve at politiet gis opplysninger om eventuelle tilgangskoder.

Det bør derimot ikke kunne kreves annen og mer omfattende bistand av den personen som opplysningsplikten pålegges. Etter lovutkastet kan for eksempel ikke politiet kreve at vedkommende skal finner frem til konkrete opplysninger som politiet søker.

En person kan bare pålegges av gi «nødvendige» opplysninger. Avgjørende er dermed hvilke opplysninger som er påkrevd for at politiet skal få tilgang til datasystemet. Begrensningen innebærer for eksempel at det ikke kan gis pålegg om å gi opplysninger som ikke berører det datasystemet som er omfattet av ransakingsbeslutningen.

Videre begrenses adgangen til å pålegge opplysningsplikt av det alminnelige forholdsmessighetsprinsippet i straffeprosessloven § 170a. For å konkretisere forholdsmessighetsvurderingen kan det være illustrerende å legge til grunn en tredelt vurdering, slik det ofte gjøres i europeisk rett:[4] For det første må man vurdere hvorvidt tiltaket er egnet for å nå målet. Videre må alternative, mindre inngripende virkemidler vurderes. For det tredje må man spørre seg om tiltaket står i et rimelig forhold til viktigheten av det man ønsker å oppnå.

Det tredje punktet innebærer en interesseavveining av flere ulike hensyn, herunder hensynet til den opplysningsplikten rettes mot, hensynet til etterforskningen og hensynet til dem opplysningene knytter seg til (proporsjonalitet i snever forstand). I denne helhetsvurderingen kan man for eksempel legge vekt på hvor inngripende opplysningsplikten vil være for den personen som plikten pålegges. Et annet relevant moment vil være om datasystemet inneholder sensitive opplysninger eller opplysninger som besitteren ikke plikter å forklare seg om, jf. den forklarende rapporten punkt 202.

Når det gjelder spørsmålet om *hvem som kan pålegges å gi opplysninger*, følger det av konvensjonen at plikten i utgangspunktet skal kunne pålegges enhver person («any person»). En begrensning følger av vernet mot selvinkriminering som redegjort for ovenfor. Plikten til å gi opplysninger kan ikke gjelde personer som er fritatt fra plikten til å vitne, jf. straffeprosessloven § 123. Politiet kan følgelig ikke pålegge en mistenkt å bistå med å fremskaffe bevis som kan bli benyttet mot ham i en senere straffesak. Det samme gjelder personer som kan nekte å forklare seg, jf. straffeprosessloven § 122 første og annet ledd. Personer som kan fritas fra vitneplikten, jf. straffeprosessloven §§ 121, 122 tredje ledd og 123 første ledd annet punktum og annet ledd, er i utgangspunktet forpliktet til å etterkomme et pålegg om å gi opplysninger så lenge det ikke er gitt fritak. Påberoper en person en vitnefritaksbestemmelse som grunnlag for ikke å etterkomme et pålegg, vil politiet være forpliktet til å ta hensyn til det inntil en eventuell rettslig avklaring foreligger. Er det av ulike årsaker ikke tid til å innhente rettens beslutning, må politiet frafalle pålegget eller eventuelt rette det mot en annen.

Konvensjonen stiller statene fritt i spørsmålet om hvem som skal gis *kompetanse* til å pålegge opplysningsplikten, jf. «competent authority». Valget står derfor mellom domstolene, påtalemyndig-

[4] En slik inndeling ble for eksempel lagt til grunn i Ot.prp. nr. 109 (2001-2002), se s. 29-30.

heten og politiet. Ved valget mellom disse alternativene må man foreta en avveining av de kryssende interessene som gjør seg gjeldende. På den ene siden vil et pålegg om å gi opplysninger innebære et brudd med den alminnelige retten til å nekte å forklare seg overfor politiet, jf. straffeprosessloven § 230. Dette grunnleggende straffeprosessuelle prinsippet kan tale for ikke å legge kompetansen til politiet, men til domstolene eller eventuelt påtalemyndigheten. Praktiske hensyn taler på den andre siden imot en slik løsning. Behovet for bistand vil etter all sannsynlighet oppstå på selve ransakingsstedet. Retten vil i liten grad ha anledning til å forutse et slikt behov i forkant, og langt mindre ha forutsetning for å vurdere hvem et slikt pålegg eventuelt skal kunne rettes mot. Tidstapet som følge av at et pålegg om å gi opplysninger måtte besluttes av retten, ville også kunne skade etterforskningen.

Utvalget har funnet det hensiktsmessig å legge kompetansen til politiet. Ved vurderingen har utvalget særlig lagt vekt på at dersom en plikt til å gi opplysinger av den karakter det her er tale om skal være effektiv, må pålegget kunne gis når behovet oppstår. Dernest følger det av straffeprosessloven § 216a fjerde ledd at kompetansen til å utløse bistandsplikt i forbindelse med kommunikasjonsavlytting er lagt til politiet. I og med at det i slike tilfeller er tale om å yte bistand som rekker lenger enn det å gi opplysninger, vil det etter utvalgets oppfatning gi dårlig sammenheng i regelverket å legge kompetansen til å pålegge opplysningsplikt til et høyere organ.

Etter utvalgets oppfatning bør unnlatelse av å etterkomme et pålegg *straffesanksjoneres*. Effektivitetsbetraktninger tilsier at unnlatelse bør sanksjoneres. Personer som gis pålegg om å bidra med opplysninger vil kunne komme i en lojalitetskonflikt der hensynet til arbeidsgiver står mot forpliktelsen til å gi informasjon til politiet. For å sikre at pålegg overholdes, antar utvalget at det vil være nødvendig å innføre en straffetrussel. Videre tilsier hensynet til sammenheng i regelverket at unnlatelse av å etterkomme et pålegg bør straffesanksjoneres. Unnlatelse av å etterkomme et utleveringspålegg, jf. straffeprosessloven § 210, straffes med bøter, jf. domstolsloven § 206.

3.4.3.3 Beslag

Når det gjelder beslag, følger det av redegjørelsen for gjeldende rett i kapittel 18.2 at data som sådan kan beslaglegges. Beslag kan for eksempel tas i form av dokumentutskrifter eller ved kopiering til et eksternt lagringsmedium. Iverksettelsen av skritt for å sikre dataenes integritet, jf. artikkel 19 nr. 3 bokstav c, vil være en naturlig del av denne prosessen, og krever etter utvalgets syn ingen særskilt hjemmel. Det samme gjelder konvensjonens krav om at de beslaglagte dataene må kunne gjøres utilgjengelige eller fjernes fra det aktuelle datasystemet, jf. artikkel 19 nr. 3 bokstav d. Ved beslag av fysiske objekter vil beslagsgjenstanden normalt bli fjernet fra innehaverens rådighet. Selv om kopiering eller utskrift til papir vil innebære at dataene blir værende i systemet, antar utvalget at det ikke er noe i veien for at dataene fjernes eller gjøres utilgjengelige for den berørte. Det alminnelige forholdsmessighetsprinsippet, jf. straffeprosessloven § 170a, kan begrense adgangen til å fjerne eller gjøre data utilgjengelige.

Det er etter utvalgets oppfatning ikke behov for lovendringer for å kunne ratifisere konvensjonens bestemmelser om beslag i artikkel 18 nr. 3.

3.5 Innhenting av trafikkdata – artikkel 20

3.5.1 Folkerettslige forpliktelser

Artikkel 20 gjelder innhenting av trafikkdata i sanntid og lyder:

«1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
   a) collect or record through the application of technical means on the territory of that Party, and
   b) compel a service provider, within its existing technical capability:
      i. to collect or record through the application of technical means on the territory of that Party; or
      ii. to co-operate and assist the competent authorities in the collection or recording of,

   traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory,

through the application of technical means on that territory.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.»

Bestemmelsen pålegger statene å sørge for regler som gir kompetent myndighet adgang til å innhente trafikkdata i sanntid («real-time»). Med sanntid mener utvalget signaloverføring som er slik at det ikke er tid til å manipulere dataene.

Forpliktelsen i artikkel 20 gjelder innhenting av trafikkdata for konkrete kommunikasjonsoverføringer («specified communications»). Kravet til spesifisering innebærer at statene ikke er forpliktet til å åpne for innhenting av trafikkdata ut ifra rene etterretningsformål. Begrepet «communications» er benyttet fordi det kan være nødvendig å innhente trafikkdata fra flere kommunikasjonsmidler for å avdekke kilden eller destinasjonen til en eller flere konkrete kommunikasjonsoverføringer.

Det følger av artikkel 20 nr. 1 bokstav a at statene er forpliktet til å gi kompetent myndighet adgang til å innhente trafikkdata. Videre er statene også forpliktet til å åpne for at trafikkdata kan innhentes med bistand fra tjenestetilbyder, jf. artikkel 20 bokstav b. Bokstav b fastsetter to alternative måter å gjennomføre innhentingen med bistand fra tjenestetilbyder på. Etter det første alternativet kan statene gi kompetent myndighet adgang til å pålegge tjenestetilbydere å innhente trafikkdataene, jf. underpunkt i. I henhold til det andre alternativet kan statene gi kompetent myndighet adgang til å pålegge tjenestetilbyderen å yte den nødvendig bistand i forbindelse med innhentingen av trafikkdataene, jf. underpunkt ii. Bistandsplikten er begrenset til det som er tekniske mulig ut ifra tjenestetilbyderens forutsetninger og utstyr («within its technical existing capability»). Det oppstilles med andre ord ingen plikt til ytterligere investeringer.

Bestemmelsen gjelder bare kommunikasjonsoverføringer som finner sted på den enkelte stats territorium. En kommunikasjonsoverføring anses å finne sted innen territoriet dersom en av de involvert i kommunikasjonen, eller utstyret som kommunikasjonen er rutet via, befinner seg der. Det er uten betydning om virksomheten er administrert fra utlandet, jf. den forklarende rapporten punkt 222.

Stater som på grunn av begrensninger i intern rett ikke har anledning til å gjennomføre tiltak som beskrevet i artikkel 20 nr. 1 bokstav a, kan benytte en alternativ fremgangsmåte, jf. artikkel 20 nr. 2. I stedet for at kompetent myndighet utfører kontrollen med eget utstyr, kan disse statene gi regler som gir kompetent myndighet adgang til å pålegge tjenestetilbyder å stille utstyr til disposisjon for de som skal gjennomføre kontrollen.

Etter artikkel 20 nr. 3 er statene forpliktet til å ha regler som åpner for at tjenestetilbydere kan pålegges taushetsplikt om iverksatt innhenting av trafikkdata og om opplysninger knyttet til innhentingen.

3.5.2 Gjeldende rett

Adgangen til innhenting av trafikkdata i sanntid er regulert i straffeprosessloven § 216b annet ledd bokstav c, som er plassert i straffeprosessloven kapittel 16a om kommunikasjonskontroll. Paragrafen gir også hjemmel til å innstille eller avbryte kommunikasjon og til å stenge et kommunikasjonsanlegg, jf. § 216b annet ledd bokstavene a og b. Bestemmelsens virkeområde må avgrenses mot avlytting av innholdet av en kommunikasjonsoverføring, jf. § 216a.

I henhold til § 216b annet ledd har politiet anledning til å innhente opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom settes i forbindelse med telefoner, datamaskiner eller andre kommunikasjonsanlegg, og andre data knyttet til kommunikasjonen. Begrepet «andre kommunikasjonsanlegg» tolkes vidt, slik at valget av kommunikasjonsform er uten betydning, jf. Bjerke/Keiserud, *Straffeprosessloven - Kommentarutgave,* 3. utg. s. 745. Det følger av ordlyden at identifikasjon av hvilke anlegg som har kommunisert med hverandre i et bestemt tidsrom, er omfattet. Det samme gjelder fremtidig kommunikasjon.

De materielle vilkårene for å beslutte kommunikasjonskontroll er for det første at det må foreligge «skjellig grunn til mistanke», jf. første ledd. Mistanken må dernest gjelde en handling som kan medføre fengsel i minst 5 år, jf. første ledd bokstav a, eller rammes av en av de uttrykkelig nevnte straffebestemmelsene i første ledd bokstav b. Av særlig interesse her er straffeloven § 145 annet ledd (datainnbrudd) og § 204 første ledd bokstav d (barnepornografi).

I tillegg til vilkårene som følger av § 216b, må også de alminnelige vilkårene i 216c være oppfylt. I henhold til § 216c kan kommunikasjonskon-

troll bare tillates dersom den vil være av vesentlig betydning for å oppklare saken, og oppklaring ellers i vesentlig grad vil bli vanskeliggjort. Følgelig kan kommunikasjonskontroll bare benyttes dersom de tradisjonelle etterforskningsmetodene antas å komme til kort, jf. Ot.prp. nr. 10 (1976-77) s. 6. I begrepet «antas» ligger det et krav om noe mer enn en ren formodning, men ikke så mye som sannsynlighetsovervekt, jf. Bjerke/Keiserud, *Straffeprosessloven - Kommentarutgave,* 3. utg. s. 748. Videre kan ikke innhentingen av trafikkdata være et uforholdsmessig inngrep, jf. § 170a.

Kompetansen til å beslutte kommunikasjonskontroll er som hovedregel tillagt retten, jf. straffeprosessloven § 216b første ledd. Påtalemyndigheten er imidlertid gitt kompetanse dersom det er stor fare for at etterforskningen vil lide, jf. § 216d. I følge Bjerke/Keiserud, *Straffeprosessloven - Kommentarutgave,* 3. utg. s. 750, bør det antakelig kreves sannsynlighetsovervekt for at det er stor fare og at det er viktig for etterforskningen.

Henvisningen til straffeprosessloven § 216a fjerde ledd i § 216b tredje ledd, innebærer at politiet kan pålegge en tjenestetilbyder å bistå i forbindelse med gjennomføringen av kommunikasjonskontrollen.

Det følger av § 216i at alle som har kjennskap til at det er eller vil bli gjennomført kommunikasjonskontroll, har plikt til å bevare taushet om dette. Det samme gjelder de opplysingene som fremkommer ved kontrollen. Brudd på taushetsplikten er straffbar i medhold av straffeloven § 121.

3.5.3 Utvalgets vurderinger

Som redegjørelsen for gjeldende rett viser, er ikke norsk rett i samsvar med forpliktelsene i konvensjonen når det gjelder det saklige anvendelsesområdet for kommunikasjonskontroll. Konvensjonen krever i utgangspunktet at statene skal tillate kommunikasjonskontroll i forbindelse med samtlige straffebud fastsatt i samsvar med artikkel 2 til 11, jf. artikkel 14 nr. 2 bokstav a. De norske bestemmelsene som samsvarer med artikkel 6, 7 og 10, oppfyller ikke kravet til 5 års strafferamme i straffeloven § 216b første ledd bokstav a. De er heller ikke uttrykkelig nevnt i § 216b første ledd bokstav b. Spørsmålet blir derfor om man bør inkludere de aktuelle straffebestemmelsene i opplistingen i § 216b første ledd bokstav b eller benytte reservasjonsadgangen som statene er gitt i artikkel 14 nr. 3 bokstav a.

Etter utvalgets oppfatning bør Norge benytte reservasjonsadgangen på dette punktet. Det skyldes at avveiningen av hvilke straffbare handlinger som skal kunne kvalifisere for bruk av kommunikasjonskontroll, er basert på en grundig vurdering av de kryssende hensyn som gjør seg gjeldende. Utvalget finner derfor ikke grunn til å foreslå endringer i bestemmelsen i denne omgang, men vil kunne komme tilbake til spørsmålet som ledd i fase to av sitt arbeid.

Reservasjonsadgangen i artikkel 14 nr. 3 bokstav a er undergitt et vilkår. Begrensninger i anvendelsesområdet for innhenting av trafikkdata kan ikke være mer vidtrekkende enn ved avlytting av innholdsdata. Det vil si at det minst må være anledning til å innhente trafikkdata i forbindelse med overtredelser av straffebud som anses som «serious offences» etter artikkel 21. Ettersom straffeprosessloven § 216b har et videre anvendelsesområde enn § 216a, er vilkåret oppfylt. Norge står derfor fritt til å benytte reservasjonsadgangen i artikkel 14 nr. 3 bokstav a.

Et annet spørsmål som må vurderes, er hvilken rolle tjenestetilbydere skal spille ved innhenting av trafikkdata, jf. artikkel 20 nr. 1 bokstav b. Som beskrevet under punkt 3.5.1, står valget mellom å gi regler som åpner for at tjenestetilbyderne selv kan gjennomføre kontrollen etter pålegg fra kompetent myndighet, og å gi regler som gir kompetent myndighet hjemmel til å pålegge en tjenestetilbyder å samarbeide i forbindelse med kontrollen. Politiet har anledning til å pålegge en tjenestetilbyder å yte nødvendig teknisk bistand, jf. straffeprosessloven § 216b tredje ledd, jf. § 216a fjerde ledd. Videre er tilbydere av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste forpliktet til å tilrettelegge nett og tjeneste slik at lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon sikres, jf. lov om elektronisk kommunikasjon § 2-8 første ledd. Det er derfor etter utvalgets oppfatning klart at norsk rett dekker konvensjonens krav på dette punktet. En ordning der tjenestetilbyderne gjennomfører selve innhentingen, jf. artikkel 20 nr. 1 bokstav b underpunkt i, er etter utvalgets oppfatning verken nødvendig eller ønskelig.

3.6 Avlytting av innholdsdata – artikkel 21

3.6.1 Folkerettslige forpliktelser

Artikkel 21 omhandler avlytting av innholdsdata og lyder:

«1. Each Party shall adopt such legislative and

other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and
b) compel a service provider, within its existing technical capability:
   i. to collect or record through the application of technical means on the territory of that Party, or
   ii. to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.»

Artikkel 21 pålegger statene å sørge for regler som gir kompetent myndighet adgang til å avlytte innholdsdata («content data»). Begrepet «content data» er ikke definert i konvensjonen. Det følger imidlertid av den forklarende rapporten punkt 229 at begrepet er negativt avgrenset til å omfatte alle data som ikke er trafikkdata. Begrepet «trafikkdata» er definert i artikkel 1 bokstav d.

Avlytting av innholdsdata representerer et mer inngripende virkemiddel enn innhenting av trafikkdata. I konvensjonen kommer forskjellen klart til uttrykk ved at bruken av dette virkemidlet kan forbeholdes etterforskning av alvorlige straffbare handlinger («serious offences»). Statene står imidlertid fritt til å avgjøre hva som skal regnes som en alvorlig straffbar handling. Virkemidlets inngripende karakter gjør det naturlig at bruken underlegges strengere vilkår enn det som er vanlig for andre tvangsmidler, herunder innhenting av trafikkdata, jf. den forklarende rapporten punkt 215 og 231.

Artikkel 21 er med noen få unntak utformet på samme måte som artikkel 20. Redegjørelsen for de folkerettslige forpliktelsene er derfor begrenset til det som særpreger avlytting av innholdsdata sammenliknet med innhenting av trafikkdata.

3.6.2 Gjeldende rett

Adgangen til å avlytte datakommunikasjon er regulert i straffeprosessloven § 216a som er plassert i straffeprosessloven kapittel 16a om kommunikasjonskontroll. Paragraf 216a gir politiet hjemmel til å avlytte samtaler og annen form for kommunikasjon til og fra kommunikasjonsanlegg. Det er uten betydning om kommunikasjonen skjer via telefon, datamaskin eller andre kommunikasjonsanlegg, jf. tredje ledd. Avlyttingsadgangen gjelder imidlertid bare anlegg som den mistenkte «besitter eller antas å ville bruke». Det innebærer at det bare er avlytting av anlegg den mistenkte antas å ville benytte *selv,* som er omfattet. Avlytting av anlegg den mistenkte antas å ville kontakte, men som han ikke har tilgang til, faller utenfor bestemmelsens anvendelsesområde. I følge departementet ville en slik adgang være for inngripende, jf. Ot.prp. nr. 64 (1998-99) s. 157. Bruken av begrepet «kommunikasjon» innebærer at det kun er signalstrømmen mellom avsender og mottaker som kan avlyttes. Avlytting av data som ikke kommuniseres, for eksempel fjernavlesning av et skjermbilde og avlytting av signalstrømmen mellom en datamaskin og en skriver, faller utenfor bestemmelsens anvendelsesområde, jf. Ot.prp. nr. 64 (1998-99) s. 156.

Vilkårene for bruk og kompetansereglene er stort sett de samme som for innhenting av trafikkdata, jf. § 216b. Det vises derfor til redegjørelsen under punkt 3.5.2. En vesentlig forskjell ligger imidlertid i kravet til strafferamme. Det følger av § 216a første ledd bokstav a at det må foreligge skjellig grunn til mistanke om en handling som etter loven kan medføre straff av fengsel i 10 år eller mer. Kravet om 10 års strafferamme er ikke absolutt idet første ledd bokstav b gjør unntak for enkelte overtredelser. Oppregningen skiller seg fra § 216b første ledd ved at henvisningene til straffeloven §§ 204 første ledd bokstav d, 145 annet ledd og 390a er tatt ut, og eksportkontrolloven § 5 er tatt inn i stedet. Adgangen til å gjennomføre avlytting av innholdsdata er klart snevrere enn adgangen til å innhente trafikkdata. Det skyldes at avlytting av innholdsdata er et langt mer inngripende virkemiddel.

3.6.3 Utvalgets vurderinger

Ettersom konvensjonen overlater vurderingen av hvilke straffebud som skal anses som «serious offences» til statene, skaper ikke dette problemer for gjennomføringen av forpliktelsene.

Når det gjelder spørsmålet om hvorvidt tjenestetilbydere skal gis adgang til å gjennomføre selve kommunikasjonsavlyttingen etter pålegg fra kompetent myndighet, jf. artikkel 21 nr. 1 bokstav b underpunkt i, vises det til drøftelsen under punkt 3.5.3. I dag kan politiet pålegge tjenestetilbydere å bistå med den tekniske gjennomføringen av kontrollen. Derimot foretar politiet selve avlyttingen. Utvalget mener at denne løsningen er hensiktsmessig og at det verken er nødvendig eller ønskelig at tjenestetilbydernes rolle skal endres.

For øvrig er det utvalgets oppfatning at norsk rett fullt ut dekker konvensjonens forpliktelser. Det er derfor ikke behov for å endre norsk rett på dette punktet

3.7 Jurisdiksjon – artikkel 22

3.7.1 Folkerettslige forpliktelser

Artikkel 22 gjelder jurisdiksjon og lyder:

«1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
   a) in its territory; or
   b) on board a ship flying the flag of that Party; or
   c) on board an aircraft registered under the laws of that Party; or
   d) by one of its nationals, if the offence is punishable under criminal law where it was committed or it f the offence is committed outside the territorial jurisdiction of any State.
2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.»

Bestemmelsen oppstiller krav til det stedlige virkeområdet til straffebud som er nevnt i artikkel 2 til 11 i konvensjonen.

Artikkel 22 nr. 1 bokstav a forplikter statene til å gjennomføre territorialprinsippet. Dette innebærer at statene må kunne strafforfølge handlinger som er begått i eget territorium. En handling anses å være begått i en stats territorium når gjerningspersonen og objektet for den straffbare handlingen (datasystemet) befinner seg der. Det samme gjelder når hele eller deler av det datasystemet som berøres av den straffbare handling, er plassert i territoriet, selv om gjerningspersonen ikke er det, jf. den forklarende rapporten punkt 233.

Det følger av artikkel 22 nr. 1 bokstav b at statene også skal kunne strafforfølge handlinger som begås på skip som seiler under statens flagg. Det samme gjelder handlinger som begås på luftfartøy som er registrert i henhold til statens lover, jf. artikkel 22 nr. 1 bokstav c.

Etter artikkel 22 nr. 1 bokstav d skal statene også kunne strafforfølge handlinger begått i utlandet av egne statsborgere forutsatt at handlingen også var straffbar i det landet den ble begått, eller at handlingen ikke ble begått innenfor territoriet til en stat.

I artikkel 22 nr. 2 er statene gitt adgang til å reservere seg mot å gjennomføre artikkel 22 nr. 1 bokstav b til d.

I henhold til artikkel 22 nr. 3 er statene forpliktet til å gjennomføre prinsippet «extradite or prosecute». Prinsippet innebærer at dersom en stat nekter å utlevere egen borger etter å ha mottatt begjæring om det i henhold til artikkel 24 nr. 1, plikter staten selv å strafforfølge vedkommende dersom handlingen er straffbar etter nasjonal rett.

Bestemmelsene i artikkel 22 er ikke til hinder for at statene etablerer en mer vidtrekkende jurisdiksjon enn det som følger av konvensjonen, jf. artikkel 22 nr. 4.

Etter artikkel 22 nr. 5 skal statene, dersom det er hensiktsmessig, konsultere hverandre når en straffbar handling får virkning i flere stater.

Dersom en handling etter omstendighetene

dekkes av flere staters jurisdiksjon, skal statene så langt det er hensiktsmessig konsultere hverandre om hvor handlingen skal strafforfølges.

3.7.2 Gjeldende rett

Det følger av straffeloven § 12 første ledd nr. 1 at norsk straffelov får anvendelse på handlinger som er foretatt i riket. Når det gjelder forståelsen av begrepet «i riket» vises det til Ruud/Ulfstein, *Innføring i folkerett*, 2. utg. kapittel 7. Straffeloven er gitt anvendelse på norske skip og luftfartøy som befinner seg utenfor territorialgrensene, jf. § 12 første ledd nr. 1 bokstav d og e.

Det følger av straffeloven § 12 første ledd nr. 3 at norske statsborgere i visse tilfeller kan strafforfølges i Norge for handlinger de har begått i utlandet. Med «utlandet» menes alle områder som etter § 12 første ledd nr. 1 og 2 ikke regnes som «riket». Blant annet kan norske borgere strafforfølges når handlingen er straffbar etter det lands lov hvor handlingen er foretatt, jf. § 12 første ledd nr. 3 bokstav c.

3.7.3 Utvalgets vurderinger

Det følger av redegjørelsen for gjeldende rett at straffeloven § 12 første ledd nr. 1 dekker konvensjonens forpliktelser for så vidt gjelder handlinger begått på norsk territorium, samt handlinger som er begått om bord på et norsk skip eller luftfartøy, jf. artikkel 22 nr. 1 bokstav a til c.

Når det gjelder spørsmålet om hvorvidt norsk rett oppfyller konvensjonens krav om adgang til å strafforfølge egne borgere for handlinger som er begått utenfor territoriet, er det behov for å nyansere. Det følger av straffeloven § 12 første ledd nr. 3 bokstav c at straffeloven kommer til anvendelse på handlinger som også er straffbare i det landet der handlingen ble foretatt. I disse tilfellene dekker norsk rett konvensjons krav.

Et spørsmål er imidlertid om norske borgere, i henhold til norsk rett, kan strafforfølges for handlinger begått i områder som ikke er underlagt noen stats territorialhøyhet, jf. artikkel 22 nr. 1 bokstav d. Er handlingen begått om bord på norskregistrerte skips- og luftfartøyer, følger det av § 12 nr. 2 at handlingen kan strafforfølges etter norsk rett. Er handlingen begått om bord på utenlandsregistrerte fartøy som befinner seg i områder som nevnt, vil norske myndigheters adgang til å strafforfølge handlingen bero på om handlingen omfattes av oppregningen i § 12 nr. 3 bokstav a. I og med at de norske bestemmelser som samsvarer med konvensjonen artikkel 2, 3, 6 og 10 ikke er nevnt, kan slike handlinger i utgangspunktet ikke strafforfølges i Norge. Det er mulig at straffeloven § 12 annet ledd kan komme til anvendelse i slike tilfeller dersom virkningen av en handling er inntrådt eller tilsiktet fremkalt i Norge. Rekkevidden av denne bestemmelsen er imidlertid etter utvalgets oppfatning usikker, se for eksempel RG 2001 s. 219. Denne usikkerheten, kombinert med hensynet til å sikre en lojal etterlevelse av konvensjonens forpliktelser, taler for at Norge bør vurdere en lovendring. Alternativt kan Norge benytte reservasjonsadgangen som er gitt i artikkel 22 nr. 2.

Utvalget er av den oppfatning at Norge bør endre straffeloven § 12 nr. 3 for å sikre at overtredelse av bestemmelsene kan straffes i Norge uavhengig av om forbrytelsen er begått i Norge eller i utlandet. Derimot går ikke utvalget inn for at en handling begått i utlandet av en utlending skal kunne straffes i Norge.

Bakgrunnen for forslaget er at datakriminalitet ofte har et internasjonalt preg. Handlingen kan være begått på tvers av landegrenser eller i samvirke mellom personer i flere land til samme tid. Undertiden kan det også være vanskelig å fastslå i hvilket land den straffbare handlingen er begått. Fordi norske statsborgere ikke kan utleveres til land utenfor Norden, jf. utleveringsloven § 2, er det dessuten viktig å sikre at nordmenn som begår slike forbrytelser i utlandet, kan pådømmes i Norge.

Når det gjelder den gjensidige konsultasjonen, skal statene praktisere den dersom det etter forholdene fremstår som hensiktsmessig, jf. artikkel 22 nr. 5. Utvalget legger til grunn at norsk rett er dekket for så vidt gjelder de statene som har ratifisert Europarådets konvensjon om gjensidig hjelp i straffesaker 20. april 1959. I forhold til stater som ikke har tiltrådt denne konvensjonen, kunne det tenkes at konsultasjonsadgangen ville blitt begrenset av den taushetsplikten som påhviler politi og påtalemyndighet i kraft av straffeprosessloven § 61a. Utvalget legger imidlertid til grunn at unntaket fra taushetsplikten i straffeprosessloven § 61c nr. 5 vil kunne avhjelpe dette. Bestemmelsen åpner for at utenlandske rettshåndhevende myndigheter kan gjøres kjent med taushetsbelagte opplysninger.

Kapittel 4
Internasjonalt samarbeid

4.1 Innledende bemerkninger

I artikkel 23 til 35 er det fastsatt bestemmelser om internasjonalt samarbeid ved bekjempelse av datakriminalitet og sikring av elektroniske bevis i alle typer straffesaker. Kapitlet er delt i to: Den første delen gjelder generelle prinsipper for internasjonalt samarbeid. Her er det fastsatt overordnede prinsipper, prinsipper for utlevering og internasjonalt rettslig samarbeid og prosedyrer for anmodninger om bistand i de tilfellene der det ikke finnes anvendelige internasjonale instrumenter. Del to etablerer enkelte særskilte mekanismer for internasjonalt samarbeid i saker som gjelder datakriminalitet og elektroniske bevis. Mekanismene gjelder blant annet sikring av lagrede data, avdekking av trafikkdata, tilgang til lagrede data og offentlig tilgjengelige data, innhenting av trafikkdata i sanntid, avlytting av innholdsdata og etablering av et 24/7-nettverk.

Ved fremforhandlingen av konvensjonen var deltagerstatene enige om at det ikke burde utarbeides et særskilt regime for gjensidig bistand i konvensjonen. I stedet skal statene anvende eksisterende regimer med tillegg av de spesielle mekanismene som er etablert i konvensjonen kapittel 3. Flertallet av bestemmelsene er følgelig av supplerende karakter.

Bestemmelsene bygger i hovedsak på gjeldende traktater og konvensjoner, herunder Europarådskonvensjon 13. desember 1957 om utlevering av lovbrytere med tilleggsprotokoller, samt Europarådskonvensjon 20. april 1959 om gjensidig hjelp i straffesaker med tilleggsprotokoller. Disse konvensjonene er gjennomført i norsk rett blant annet ved lov 13. juni 1975 nr. 39 om utlevering av lovbrytere (utleveringsloven). Utlevering og andre former for rettslig samarbeid i Norden er regulert særskilt i lov 3. mars 1961 nr. 1 om utlevering av lovbrytere til Danmark, Finland, Island og Sverige.

4.2 Folkerettslige forpliktelser og utvalgets vurderinger

4.2.1 Generelle prinsipper

4.2.1.1 Generelle prinsipper for internasjonalt samarbeid

Artikkel 23 fastsetter tre grunnleggende prinsipper for internasjonalt samarbeid. Statene skal for det første samarbeide i så stor grad som mulig ved etterforskning og strafforfølgning av datakriminalitet. For det andre er statene forpliktet til å samarbeide i forbindelse med straffbare handlinger som gjelder datasystemer og data og sikring av elektroniske bevis. Forpliktelsen til å samarbeide om sikring av elektroniske bevis gjelder alle typer straffbare handlinger. For det tredje skal statene i sitt samarbeid overholde både bestemmelsene i konvensjonens kapittel om internasjonalt samarbeid, andre internasjonale instrumenter om internasjonalt rettslig samarbeid i straffesaker og nasjonal lovgivning. Det tredje prinsippet innebærer at konvensjonens bestemmelser om internasjonalt samarbeid ikke erstatter bestemmelser i andre internasjonale instrumenter.

Etter utvalgets oppfatning reiser bestemmelsen ingen spørsmål om lovendringer i norsk rett. Oppfyllelsen av forpliktelsen vil skje ved gjennomføringen og praktiseringen av de øvrige bestemmelsene om internasjonalt samarbeid.

4.2.1.2 Utlevering

Artikkel 24 regulerer utlevering for forbrytelser som er omfattet av artikkel 2 til 11. Det er fastsatt to vilkår for plikten til å utlevere lovbrytere. For det første kreves det dobbelt straffbarhet. For det andre må strafferammen for overtredelsen i begge stater være fengsel i minst ett år.

Stater som er forhindret fra å utlevere egne borgere til fremmed stat, skal etter artikkel 24 nr. 6 vurdere strafforfølgning dersom den anmodende stat ber om det. Det samme gjelder dersom en utleveringsanmodning blir avslått under henvisning til at forholdet hører inn under nasjonal jurisdiksjon.

Strafforfølgning av slike saker skal vurderes på lik linje med øvrige nasjonale saker.

Utleveringsforpliktelsene i artikkel 24 er etter utvalgets mening dekket av utleveringsloven og lov om utlevering av lovbrytere til Danmark, Finland, Island og Sverige.

4.2.1.3 Gjensidig bistand i straffesaker

I *artikkel 25* er det fastsatt generelle prinsipper for gjensidig bistand. Statene er forpliktet til å bistå hverandre i så stor grad som mulig i forbindelse med strafforfølgning av datakriminalitet og elektronisk bevissikring.

I saker hvor tidsmomentet er av særlig betydning, skal statene kunne fremme rettsanmodninger raskt og enkelt, for eksempel via faks eller e-post. Den anmodede stat skal i slike tilfeller besvare henvendelsen på samme måte. Rettsanmodningen kan i så fall kreves verifisert gjennom regulære kanaler dersom den anmodede stat ber om det. Plikten til å kunne kommunisere hurtig gjelder imidlertid bare i den utstrekning det anses forsvarlig av sikkerhetsmessige årsaker. Det er overlatt til statene selv å bli enige om den praktiske gjennomføringen.

De generelle prinsippene for gjensidig bistand i artikkel 25 kan etter utvalgets oppfatning gjennomføres ved en eventuell omlegging av interne retningslinjer og instrukser, og nødvendiggjør ingen lovendringer.

Etter *artikkel 26* kan statene uoppfordret gi opplysninger til en annen konvensjonsstat dersom den antar opplysningene vil avdekke straffbare forhold i vedkommende stat eller kunne komme til nytte under en pågående strafforfølgning. Bestemmelsen er ikke bindende og kan gjennomføres innenfor rammene av eksisterende nasjonal lovgivning.

Nasjonale regler om taushetsplikt kan tenkes å sette skranker for spontan informasjonsutveksling i medhold av artikkel 26. Etter straffeprosessloven § 61a har tjenestemenn i politi og påtalemyndighet en vidtrekkende taushetsplikt om det de får kjennskap til i sitt arbeid. Taushetsplikten er imidlertid underlagt en rekke unntak. Av betydning i denne sammenhengen er § 61c første ledd nr. 5 som gjør unntak for opplysninger som formidles for å forebygge lovovertredelser. Bestemmelsen er antatt ikke å være begrenset til overtredelser som retter seg mot norske interesser, jf. Tor-Geir Myhrer, *Personvern og samfunnsforsvar*, s. 458 flg. Forfatteren drøfter her rekkevidden av § 61c første ledd nr. 5, sammenholdt med politiloven § 24 fjerde ledd nr. 2 og strafferegistreringsloven § 7 annet ledd. Konklusjonen er at taushetsbelagte opplysninger kan oversendes utenlandske myndigheter til deres interne bruk dersom opplysningene kan være egnet til å forebygge mulige lovovertredelser. Etter Myhrers oppfatning kan opplysningenes karakter og de politiske forholdene i mottakerlandet tale for å utvise forsiktighet med å overlevere opplysninger i visse tilfeller. Utvalget slutter seg til Myhrers vurdering.

Gjelder opplysningene en konkret straffesak, er det unntaket i straffeprosessloven § 61c første ledd nr. 2 som kommer til anvendelse. Vilkår knyttet til utlevering av taushetsbelagte opplysninger følger av reglene i § 61d.

Etter utvalgets oppfatning kan artikkel 26 fullt ut gjennomføres ved en eventuell omlegging av interne retningslinjer og instrukser. Det er derfor ikke behov for lovendringer i norsk rett.

4.2.1.4 Prosedyrer for anmodninger i fravær av anvendelige internasjonale instrumenter

Ved utarbeidelsen av konvensjonen kom man frem til at det ikke burde utarbeides et særskilt regime for gjensidig bistand i konvensjonen. I stedet skal statene anvende eksisterende regimer med tillegg av de spesielle mekanismene som er etablert i konvensjonen kapittel 3. *Artikkel 27* regulerer gjensidig bistand i de tilfellene som ikke allerede er omfattet av internasjonale instrumenter eller samarbeidsavtaler. Den anmodede stat vil, dersom den har ratifisert denne konvensjonen, være forpliktet til å behandle anmodningen i tråd med prinsippene i artikkel 27.

Etter utvalgets oppfatning krever artikkel 27 ingen endringer i norsk rett. Dette skyldes at vilkårene i utleveringsloven §§ 24 og 25 gjelder uavhengig av om den anmodende staten har inngått en samarbeidsavtale med Norge. Som utgangspunkt behandles alle anmodninger likt, og kan etterkommes dersom vilkårene i utleveringsloven er oppfylt. Bestemmelsen kan imidlertid ha selvstendig betydning for Norge i visse tilfeller, for eksempel hvis Norge retter en anmodning til en stat som krever traktatgrunnlag for å kunne etterkomme anmodningen. I slike tilfelle kan Norge kreve at en anmodet stat som har sluttet seg til konvensjonen, behandler rettsanmodningen etter prinsippene i artikkel 27.

Artikkel 28 gjelder taushetsplikt og begrensninger for bruken av informasjon som oversendes som følge av en rettsanmodning, i de tilfellene som ikke allerede er omfattet av internasjonale instrumenter eller samarbeidsavtaler. Etter utvalgets oppfatning krever ikke gjennomføringen av artikkelen lovendringer. Adgangen til å utlevere infor-

masjon til bruk for etterforskning og strafforfølgning i en annen stat er underlagt bestemmelsene om taushetsplikt i straffeprosessloven § 61a flg. Bestemmelsene er generelle og gjelder uavhengig av om Norge har en samarbeidsavtale med den anmodende stat. Mottar Norge en henvendelse om utlevering av slik informasjon, vil vedkommende myndighet være forpliktet til å orientere om taushetsplikten som gjelder, jf. § 61d. Samme bestemmelse gir også hjemmel til å kreve skriftlig erklæring fra den som får tilgang til taushetsbelagte opplysninger, om at vedkommende kjenner og vil respektere reglene.

4.2.2 Særskilte bestemmelser

Artikkel 29 forplikter statene til å sikre lagrede data, jf. artikkel 16, hvis en statspart anmoder om det. En anmodning kan avslås hvis den gjelder en politisk forbrytelse eller av hensyn til statens suverenitet, sikkerhet eller *ordre public*. Derimot kan en konvensjonsstat som utgangspunkt ikke sette dobbelt straffbarhet som et vilkår for å etterkomme anmodninger. Men i artikkel 29 nr. 4 er stater som har dobbel straffbarhet som vilkår for å etterkomme rettsanmodninger om bruk av tradisjonelle tvangsmidler, som for eksempel ransaking og beslag, gitt anledning til å reservere seg. Statene kan reservere seg mot forpliktelsen til å etterkomme rettsanmodninger om sikring av lagrede data dersom det på tidspunktet for gjennomføringen er grunn til å anta at kravet om dobbel straffbarhet ikke kan anses oppfylt. Reservasjonsadgangen gjelder ikke handlinger som nevnt i artikkel 2 til 11 ettersom det forutsettes at disse handlingene er kriminalisert.

Videre følger det av artikkel 29 nr. 7 at dataene skal sikres i minimum 60 dager. Minimumstiden er nødvendig for at den anmodende stat skal få anledning til å fremsette en rettsanmodning om bruk av andre tvangsmidler, for eksempel ransaking og beslag.

Det fremgår av utleveringsloven § 24 at norske myndigheter etter begjæring fra fremmed stat kan anvende blant annet de tvangsmidlene som er nevnt i straffeprosessloven kapittel 16. Utkastet til ny bestemmelse om sikring av lagrede data er foreslått plassert i dette kapitlet. Forutsatt at de øvrige vilkårene i loven er oppfylt, vil det derfor være adgang til å gi sikringspålegg etter begjæring fra en konvensjonsstat.

Det fremgår av utleveringsloven § 24 nr. 3 at en rettsanmodning bare kan etterkommes dersom den handlingen forfølgningen gjelder er straffbar etter norsk lov. I henhold til artikkel 29 nr. 3 kan ikke statene oppstille dobbelt straffbarhet som et vilkår for å etterkomme en anmodning. Konvensjonen åpner som nevnt for at statene kan forbeholde seg retten til ikke å etterkomme en anmodning dersom forfølgningen gjelder andre forhold enn dem som er nevnt i artikkel 2 til 11 og det samtidig er grunn til å tro at vilkåret om dobbel straffbarhet ikke er oppfylt, jf. artikkel 29 nr. 4.

Etter utvalgets oppfatning bør Norge benytte seg av reservasjonsadgangen i artikkel 29 nr. 4. Det skyldes at dobbelt straffbarhet som vilkår for utlevering og annen bistand, har en fast og innarbeidet forankring i norsk rett. Med unntak av de reglene som gjelder for utlevering av lovbrytere i Norden, jf. lov 3. mars 1961 nr. 1, gjelder prinsippet så langt utvalget har kunnet konstatere, absolutt.

Utvalget kan ikke se at det foreligger tilstrekkelig gode grunner til å fravike prinsippet om dobbelt straffbarhet. Det er etter utvalgets mening heller ikke nødvendig av hensyn til det internasjonale samarbeidet. En begjæring om sikringspålegg som er begrunnet i handlinger som faller inn under konvensjonen artikkel 2 til 11, vil som hovedregel oppfylle kravet til dobbel straffbarhet. I tillegg skal ikke ulik terminologi eller kategorisering av straffebud være til hinder for at vilkåret om dobbelt straffbarhet anses for å være oppfylt, jf. den forklarende rapporten punkt 259. Kravet til dobbel straffbarhet vil derfor sjelden være til hinder for å yte bistand. Videre er det ingen grunn til å utsette den berørte for et sikringspålegg dersom man på sikringstidspunktet har grunn til å anta at en etterfølgende rettsanmodningen om beslag eller lignende vil bli avvist fordi kravet til dobbel straffbarhet ikke vil være oppfylt.

Artikkel 30 gjelder hurtig avdekking av sikrede trafikkdata. Bestemmelsen gjelder tilfeller hvor trafikkdata har blitt sikret på grunnlag av en anmodning etter artikkel 29. Dersom den anmodede stat i slike tilfeller avdekker at en utenlandsk tjenestetilbyder har vært involvert i en bestemt kommunikasjonsoverføring, plikter staten umiddelbart å gi den anmodende stat tilgang til nødvendige trafikkdata for å kunne spore kommunikasjonsoverføringen og identifisere tjenestetilbyderen.

Tilgang til slike trafikkdata kan bare holdes tilbake dersom den anmodede stat anser overtredelsen for å være et politisk lovbrudd eller dersom det å etterkomme anmodningen vil kunne true statens suverenitet, sikkerhet, *ordre public* eller andre vesentlige interesser.

Forpliktelsen i artikkel 30 krever etter utvalgets oppfatning ikke ytterligere lovendringer. Etter forslaget til ny straffeprosesslov § 215 a fjerde ledd

kan den sikringspålegget retter seg mot, pålegges å utlevere nødvendige trafikkdata for å spore hvor de sikringspålagte dataene kom fra og hvor de eventuelt ble sendt til. Dersom en annen stat fremmer en rettsanmodning om å få utlevert trafikkdata som nevnt, jf. artikkel 30, følger det av utleveringsloven § 24 nr. 1, at en slik begjæring kan følges opp av påtalemyndigheten dersom de øvrige vilkårene i loven er oppfylt.

Artikkel 31 omhandler bistand til ransaking, beslag og utlevering av lagrede data etter anmodning fra en annen konvensjonsstat. Det følger av artikkel 31 nr. 3 at den anmodede staten plikter å reagere hurtig dersom det er grunn til å tro at dataene kan bli slettet eller forringet. Det samme gjelder dersom instrumenter og lover som nevnt i artikkel 23 gir anvisning på hurtig reaksjon.

Rettsanmodninger i medhold av artikkel 31 om bistand til ransaking, beslag og utlevering av lagrede data skal behandles etter reglene i utleveringsloven § 24. Henvisningen til straffeprosessloven kapittel 15 og 16 i utleveringsloven § 24 nr. 1 innebærer at bistand kan ytes dersom vilkårene for øvrig er oppfylt. Når det gjelder plikten til å handle raskt ved fare for at data kan gå tapt, jf. artikkel 31 nr. 3, legger utvalget til grunn at forpliktelsene kan oppfylles ved endring av interne retningslinjer for behandling av slike saker. Derfor er det etter utvalgets oppfatning ikke nødvendig med lovendringer.

Artikkel 32 gjelder grenseoverskridende tilgang til lagrede data. Formålet med artikkel 32 er å klargjøre at konvensjonsstatene skal kunne skaffe seg tilgang til offentlig tilgjengelige data lagret i en annen konvensjonsstat uten å måtte innhente tillatelse. Tillatelse fra en annen stat skal heller ikke være påkrevd dersom den som rettmessig kontrollerer dataene, gir samtykke til slik tilgang. Bestemmelsen endrer ikke prinsippet om at den enkelte konvensjonsstatens politi har full suverenitet på eget territorium.

Det følger forutsetningsvis av straffeprosessloven § 225 at politiet har enerett til å drive etterforskning i Norge. Spørsmålet blir derfor om dette utgangspunktet er til hinder for at politiet i en fremmed stat, via nettet, innhenter offentlig tilgjengelige data lagret på norsk territorium. Etter utvalgets oppfatning må dette besvares benektende. Slik innhenting det her er tale om må sidestilles med ordinær surfing på nettet. Hvorvidt dette gjøres som ledd i en konkret etterforskning eller av andre grunner, kan etter utvalgets syn ikke være avgjørende.

Når det gjelder spørsmålet om norsk rett er til hinder for at en fremmed stat innhenter data på norsk territorium på grunnlag av et samtykke fra den som har råderetten til dataene, stiller dette seg etter utvalgets oppfatning på samme måte. Så lenge innhentingen skjer via nettet, og uten bruk av tvangsmidler, må det legges til grunn at norsk territorialhøyhet ikke blir krenket. Etter utvalgets oppfatning er det derfor ikke behov for endringer i norsk rett.

Artikkel 33 omhandler bistand i forbindelse med innhenting av trafikkdata i sanntid. Plikten til å bistå gjelder bare spesifikke kommunikasjonsoverføringer, og prosedyrene og vilkårene for gjennomføringen skal være i tråd med den anmodede stats nasjonale rett. Statene skal som et minimum åpne for bistand i forbindelse med overtredelser som ville gitt grunnlag for kommunikasjonskontroll etter nasjonal rett.

Rettsanmodninger om bistand til innhenting av trafikkdata i sanntid skal behandles etter reglene i utleveringsloven § 24. Henvisningen til straffeprosessloven kapittel 16a i utleveringsloven § 24 nr. 1 innebærer at bistand kan ytes dersom vilkårene for øvrig er oppfylt. Statene er bare forpliktet til å åpne for bistand i forbindelse med overtredelser som ville gitt grunnlag for innhenting av trafikkdata i en nasjonal sak. Etter utvalgets oppfatning er det derfor ikke behov for endringer i norsk rett.

Artikkel 34 gjelder avlytting av innholdsdata. Formålet med bestemmelsen er å sikre statene anledning til å anmode om bistand til avlytting av innholdsdata i en annen konvensjonsstat. Plikten til å bistå gjelder bare spesifikke kommunikasjonsoverføringer og prosedyrene og vilkårene for gjennomføringen skal være i tråd med den anmodede stats nasjonale rett.

Rettsanmodninger i medhold av artikkel 34 skal behandles etter reglene i utleveringsloven § 24. På samme måte som ved innhenting av trafikkdata i sanntid, innebærer henvisningen til straffeprosessloven kapittel 16a i utleveringsloven § 24 nr. 1 at bistand kan ytes dersom lovens øvrige vilkår er oppfylt. Begrensingene i straffeprosessloven § 216a første ledd gjelder tilsvarende i forhold til rettsanmodninger fra fremmede stater. Ettersom statene bare er forpliktet til å yte bistand i de tilfellene kommunikasjonskontroll er tillatt etter nasjonal rett, dekker norsk rett etter utvalgets oppfatning forpliktelser i konvensjonen.

Artikkel 35 omhandler opprettelsen av et døgnkontinuerlig kontaktnett mellom statene. Bestemmelsens formål er å styrke samarbeidet om bekjempelsen av datakriminalitet ved å opprette et kontaktpunkt i alle konvensjonsstatene. Kontaktpunktet skal være tilgjengelig til enhver tid, og skal raskt kunne bistå andre stater med blant annet

tekniske råd, sikring av lagrede data, jf. artikkel 29 og 30, innhenting av bevis og sporing av mistenkte personer. Videre skal kontaktpunktet være i stand til å gi eller fremskaffe relevant juridisk informasjon vedrørende forutsetninger for bistand og hvilke prosedyrer som skal følges.

Hvorvidt den konkrete oppfølgingen og bistanden foretas direkte av den enkelte statens kontaktpunkt, eller indirekte gjennom tilrettelegging for kompetente myndigheter, er opp til konvensjonsstatene. Følges sistnevnte fremgangsmåte skal kommunikasjonen mellom kontaktpunktet og statens kompetente myndigheter kunne skje raskt og direkte. Det samme gjelder kontaktpunktene statene i mellom. Videre plikter statene å sørge for at kontaktpunktene til enhver tid er bemannet av kompetent og velutstyrt personell.

Forpliktelsen til å opprette et 24/7-nettverk i artikkel 35 krever ikke lovendringer. Det er ikke nødvendig å gi kontaktpunktet kompetanse til å utføre aktuelle tiltak, all den tid kontaktpunktet legger til rette for bistand. Det vil derfor være tilstrekkelig med interne instrukser og opplæring av personer som kan fylle funksjonen.

Kapittel 5
Økonomiske og administrative konsekvenser av lovforslagene

Utvalget foreslår enkelte endringer i straffeloven og straffeprosessloven som kan ha økonomiske og administrative konsekvenser.

For det første foreslår utvalget en ny straffebestemmelse som kriminaliserer det å gjøre passord og andre tilgangsdata tilgjengelig for andre, se punkt 2.6. Lovendringen fører til at flere handlinger blir straffbare. Avhengig av påtalemyndighetens prioriteringer kan forslaget dermed øke påtalemyndighetens arbeidsbyrde. Utvalget mener likevel at endringen neppe vil medføre nevneverdige økonomiske eller administrative konsekvenser.

Videre foreslår utvalget hjemmel for politiet til å pålegge personer opplysningsplikt i forbindelse med ransaking av et datasystem, se punkt 3.4. Utvalget antar at en slik opplysningsplikt vil kunne lette politiets arbeid under etterforskningen, og følgelig kunne lede til visse besparelser. Samtidig vil de personene som pålegges opplysningsplikt bli påført et visst merarbeid. Utvalget tar ikke stilling til hvem som bør dekke merutgiftene for den sistnevnte gruppen, men peker på at kostnadene kan bli betydelige.

For det tredje foreslår utvalget en bestemmelse i straffeprosessloven som gir påtalemyndigheten adgang til å pålegge sikring av elektronisk lagrede data som antas å ha betydning som bevis, se punkt 3.2. Utvalget antar at anvendelsen av det nye virkemidlet vil kunne føre til en viss økning i politiets og påtalemyndighetens ressursbruk. Videre vil adgangen til å pålegge private aktører å sikre elektronisk lagrede data kunne påføre disse aktørene utgifter til investeringer, støtte og drift. Utvalget tar ikke stilling til hvem som bør dekke merutgiftene, men peker på at kostnadene kan bli betydelige.

Både endringene i straffeloven og straffeprosessloven vil kunne føre til at justissektoren vil måtte yte bistand i forbindelse med etterforskning i utlandet. Utvalget finner det vanskelig å anslå omfanget av de administrative og økonomiske konsekvensene av en økning i antallet anmodninger om rettslig bistand, og kan ikke utelukke at utgiftene vil øke.

Ettersom utvalget mener at opprettelsen av et 24/7-nettverk ikke krever lovendringer, har ikke utvalget vurdert de administrative og økonomiske konsekvensene av opprettelsen av et slikt nettverk. Utvalget vil likevel peke på at en slik beredskap trolig vil føre til økte utgifter både for private aktører og det offentlige, avhengig av utformingen og praktiseringen av ordningen.

Utvalget antar at lovforslagene sett under ett vil kunne føre til samfunnsmessige besparelser. Datakriminalitet påfører i dag både det offentlige og privatpersoner store utgifter. Lovforslagene er utarbeidet med sikte på å effektivisere bekjempelsen av datakriminalitet, noe som forhåpentligvis vil ha en preventiv virkning. Utvalget antar at forslagene derfor vil kunne bidra til å redusere omfanget av datakriminalitet og de kostnadene denne kriminalitetsformen bringer med seg.

Kapittel 6
Merknader til de enkelte bestemmelsene

6.1 Til endringene i straffeloven

Til § 12

Datakrimutvalget foreslår at § 145 annet ledd og ny § 145 b tas med i oppregningen i § 12 første ledd nr. 3 bokstav a. I tillegg foreslår utvalget å ta inn en henvisning til § 54 i lov om vern av åndsverk i ny bokstav i.

Endringene fører til at overtredelse av bestemmelsene i konvensjonen artikkel 2, 3, 6 og 10 begått i utlandet av en norsk statsborger eller noen i Norge hjemmehørende person kan strafforfølges i Norge. Begrunnelsen for endringen er at datakriminalitet ofte har et internasjonalt preg. Handlingen kan være begått på tvers av landegrenser eller i samvirke mellom flere personer.

Til § 145

Utvalget foreslår at strafferammen for brevbrudd og datainnbrudd heves til bøter eller fengsel inntil 6 måneder *eller begge deler*. Om bakgrunnen for forslaget vises det til punkt 2.2.

Endringen i strafferammen har blant annet den prosessuelle virkningen at personer som mistenkes for overtredelse av bestemmelsen, vil kunne pågripes fordi strafferammekravet i straffeprosessloven dermed er oppfylt. Videre vil påtalemyndigheten kunne gi pålegg om sikring av elektronisk lagrede data som antas å ha betydning som bevis, jf. utvalgets forslag til ny § 215 a i straffeprosessloven.

Til ny § 145 b

Bestemmelsen retter seg mot det å gjøre passord og andre data som kan gi tilgang til et datasystem, tilgjengelig for andre, jf. *første ledd*.

Gjenstanden for den straffbare handlingen er «passord og andre data». Uttrykket er funksjonelt avgrenset, og omfatter alle data som kan gi tilgang til fysiske eller logiske nivåer i et datasystem. Det er uten betydning om tilgangsdataene er bærere av tall, symboler eller bokstaver, om disse i kombinasjon er meningsbærende, og om dataene er kryptert. Bestemmelsen er ikke begrenset til å gjelde data brukeren selv taster inn i datasystemet, men omfatter også data som genereres maskinelt ved bruk av for eksempel irisavlesning, avlesning av fingeravtrykk eller stemmeregistrering.

Uttrykket «gjør tilgjengelig» omfatter både det å overlate tilgangsdata til en annen (for eksempel via e-post), og det å gjøre slike data tilgjengelig for en større eller ubestemt krets av personer (for eksempel på Internett). Spredningen kan skje direkte, ved at selve passordet sendes til en annen, eller indirekte, ved at man sprer URL-adresser eller lenker til nettsteder hvor passordet finnes eller som angir på hvilket nettsted opplysningen ligger tilgjengelig. Det er uten betydning hvor mange ledd man i tilfelle må igjennom. Spredningen kan for øvrig skje mot eller uten vederlag. Loven omfatter også det å gjøre tilgangsdata kjent for andre på en mer indirekte måte, for eksempel ved å legge ut passord på en hjemmeside.

Loven krever at spredningen må være «uberettiget». Den som har tilstrekkelig hjemmel for å spre en tilgangskode, for eksempel i lov, avtale eller annet rettsgrunnlag, rammes dermed ikke av bestemmelsen.

Skyldkravet er forsett, jf. straffeloven § 40.

Bestemmelsens *annet ledd* skjerper strafferammen for grov spredning av tilgangsdata til fengsel inntil 2 år. Ved avgjørelsen av om spredningen er grov, nevner lovutkastet tre forhold det særlig skal legges vekt på ved vurderingen. For det første vil det være av betydning om dataene kan gi tilgang til sensitive opplysninger, for eksempel opplysninger av betydning for rikets sikkerhet, enkelte bedriftsinterne opplysninger og visse personopplysninger. Slike opplysninger har et særskilt krav på vern, og vil derfor ofte være undergitt lovbestemt eller instruksfastsatt taushetsplikt. I denne sammenhengen vil det imidlertid være tilstrekkelig at opplysningen etter sin art har en sensitiv karakter. For det annet skal det legges vekt på om spredningen er omfattende, siden dette vil øke risikoen for at noen skaffer seg uberettiget tilgang. For det tredje vil det ha betydning om handlingen skaper fare for betydelig skade. Både økonomiske og ikkeøkonomiske skadevirkninger vil her måtte tas i betraktning.

Oppregningen i annet ledd er ikke uttømmende. Også andre momenter vil derfor etter omstendighetene kunne få betydning, for eksempel om spredningen er skjedd mot vederlag eller som ledd i organisert kriminalitet.

Medvirkning er straffbart, jf. *tredje ledd*. Den som for eksempel stiller datautstyr til disposisjon for en annen og som samtidig regner det for sikkert eller overveiende sannsynlig at utstyret skal brukes til spredning av tilgangskoder, vil dermed kunne straffes dersom straffbarhetsvilkårene for øvrig er oppfylt.

Det fremgår av *fjerde ledd* at offentlig påtale ikke finner sted uten fornærmedes begjæring, med mindre allmenne hensyn krever påtale. Bakgrunnen for dette er at det i mindre alvorlige saker kan være naturlig at påtalespørsmålet ligger i den fornærmedes hånd, med mindre allmenne hensyn gjør det nødvendig å forfølge saken. Både prosessøkonomiske hensyn og hensynet til den fornærmede selv, som av private eller forretningsmessige grunner ikke nødvendigvis ønsker offentlighet om saken, taler for en slik løsning.

6.2 Til endringene i straffeprosessloven

Til § 199 a

Bestemmelsen gir politiet adgang til å pålegge personer med vitneplikt å bistå med opplysninger i forbindelse med ransakingen av et datasystem. I disse ransakingssituasjonene er det et spesielt stort behov for bistand for at politiet skal kunne gjennomføre ransakingen. Bestemmelsen er teknologinøytral. Om begrepet «datasystem», se punkt 1.4.

Det følger at *første ledd* at opplysningsplikten bare gjelder personer med vitneplikt. Hovedregelen om vitneplikt følger av straffeprosessloven § 108 og unntakene av §§ 117 flg. Hensynet til vernet mot selvinkriminering tilsier at en mistenkt ikke kan pålegges å gi opplysninger som kan utsette vedkommende for straffansvar, jf. § 123. Videre begrenses opplysningsplikten av vernet mot selvinkriminering slik det er fastlagt i EMK, jf. straffeprosessloven § 4 og menneskerettsloven § 2.

Etter ordlyden kan enhver person med vitneplikt pålegges å gi opplysninger. Ved ransaking av datasystemer til virksomheter med eget IT-personale, vil det være naturlig å rette pålegget mot disse personene. Personkretsen er imidlertid ikke begrenset til bestemte profesjonsgrupper. Behovet for bistand i form av opplysninger kan også tenkes å oppstå på steder som ikke har eget IT-personale, eller hvor slikt personale ikke er tilgjengelig.

Omfanget av opplysningsplikten er begrenset til det som er nødvendig for å gi tilgang til datasystemet. Med tilgang til datasystemet menes også tilgang til data som er lagret i systemet. Slik tilgang kan for eksempel kreve at politiet gis opplysninger om tilgangskoder.

En person kan bare pålegges av gi «nødvendige» opplysninger. Avgjørende er dermed hvilke opplysninger som er påkrevd for at politiet skal få tilgang til datasystemet. Begrensningen innebærer for eksempel at det ikke kan gis pålegg om å gi opplysninger som ikke berører det datasystemet som er omfattet av ransakingsbeslutningen.

Videre begrenses adgangen til å pålegge opplysningsplikt av det alminnelige forholdsmessighetsprinsippet i straffeprosessloven § 170a. Om forholdsmessighetsvurderingen, se punkt 3.4.3.3. Opplysningsplikt kan bare pålegges dersom det er tilstrekkelig grunn til det. Bruk av opplysningsplikt kan som utgangspunkt bare sies å være velbegrunnet dersom plikten er egnet til å gi den ønskede virkningen, det vil si lette gjennomføringen av ransakingen, og det ikke finnes mindre inngripende, alternative virkemidler som er like egnede. Dernest må forholdsmessigheten av bruk av opplysningsplikt vurderes. Forholdsmessighetsvurderingen innebærer en interesseavveining av flere ulike hensyn, som for eksempel hensynet til den opplysningsplikten rettes mot, hensynet til etterforskningen og hensynet til besitteren av opplysningene eller den opplysningene gjelder.

Henvisningen til domstolsloven § 206 i *annet ledd* innebærer at unnlatelse av å etterkomme et pålegg om å gi opplysninger kan straffes med rettergangsbot.

Til ny § 215 a

Bestemmelsen gjelder midlertidig sikring av elektronisk lagrede data som ledd i etterforskningen av straffesaker. Om bakgrunnen for bestemmelsen, se punkt 3.2.

Det fremgår av *første ledd* at påtalemyndigheten på nærmere vilkår kan gi pålegg om sikring av elektronisk lagrede data som antas å ha betydning som bevis. Med «sikring» menes ethvert tiltak som ivaretar de aktuelle dataenes integritet, tilgjengelighet og autensitet. Sikring kan skje ved at det tas kopi av de dataene saken gjelder, eller ved at dataene gjøres utilgjengelige for andre enn den pålegget retter seg mot. Det vil kunne variere hvilken form for sikring som er mest hensiktsmessig i det enkelte tilfellet.

Et sikringspålegg kan omfatte alle former for elektroniske «data», uten hensyn til om dataene er bærere av tall, symboler eller bokstaver, om disse i kombinasjon er meningsbærende og om dataene er kryptert. Bestemmelsen omfatter dermed både trafikkdata og andre former for data, herunder e-post og filer med lyd, bilder eller tekst. Det er imidlertid et vilkår at de aktuelle dataene foreligger i elektronisk lagret form på det tidspunktet sikringspålegget utferdiges. Et sikringspålegg kan dermed ikke gis virkning fremover i tid, i motsetning til en beslutning om kommunikasjonskontroll etter straffeprosessloven §§ 216 a og 216 b.

Bestemmelsen gir ikke uten videre hjemmel til å sikre alle elektronisk lagrede data som tilhører den mistenkte. Det er et vilkår at dataene «antas å ha betydning som bevis» i straffesaken mot vedkommende. Dette vilkåret skal tolkes på samme måte som det tilsvarende vilkåret i straffeprosessloven § 203 om beslag. Rettspraksis og andre rettskildefaktorer i tilknytning til § 203 vil dermed være av betydning ved tolkningen av utkastet til ny § 215 a.

De materielle vilkårene for å beslutte sikring varierer etter hvilke data sikringspålegget retter seg mot: Terskelen er lavest når det gjelder sikring av *trafikkdata.* Vilkåret er her at det at foreligger «mistanke» om en straffbar handling. Dette kravet vil være oppfylt dersom det foreligger visse objektive holdepunkter for at den mistenkte har begått den handlingen saken gjelder. En helt løs mistanke vil derimot ikke være tilstrekkelig. Utkastet til ny § 215 a krever derimot ikke at det foreligger skjellig grunn til mistanke. Terskelen er av personvernhensyn noe høyere når det gjelder sikring av *andre former for data*. I slike tilfeller er det et vilkår for sikring at mistanken gjelder en straffbar handling som etter loven kan medføre en høyere straff enn fengsel i 6 måneder, jf. første ledd. Det er gjort unntak fra strafferammekravet for straffeloven § 390 a. Ved vurderingen av om strafferammekravet er oppfylt, kommer forhøyelse av maksimumsstraffen ved gjentakelse eller sammenstøt av forbrytelser ikke i betraktning.

Det fremgår av *annet ledd* at en mistenkt skal gis underretning om beslutningen straks har får status som siktet i saken, jf. straffeprosessloven § 82. Han vil dermed ha krav på underretning senest på det tidspunkt når påtalemyndigheten har erklært ham for siktet, når forfølging mot ham er innledet ved retten eller når det er besluttet eller foretatt pågripelse, ransaking, beslag eller lignende forholdsregler rettet mot ham. Er det besluttet utsatt underretning om et tvangsmiddel, inntrer stillingen som siktet først når underretning gis, jf. straffeprosessloven § 82 tredje ledd. I så fall skal den siktede samtidig gis underretning om sikringspålegget.

Et sikringspålegg gjelder for et bestemt tidsrom, som ikke må være lengre enn nødvendig, jf. *tredje ledd*. Sikringsperioden kan høyst utgjøre 90 dager om gangen. Dersom beslutningen treffes etter begjæring fra fremmed stat, skal sikringsperioden være minst 60 dager, jf. artikkel 29 nr. 7.

Det følger av henvisningen til straffeprosessloven § 197 tredje ledd at sikringspålegget så vidt mulig skal være skriftlig og opplyse om hva saken gjelder, formålet med sikringen og hva den skal omfatte. En muntlig beslutning skal snarest mulig nedtegnes. Enhver som rammes av sikringspålegget kan straks eller senere kreve brakt inn for retten spørsmålet om det skal opprettholdes, jf. henvisningen til § 208 første og tredje ledd. Praktisk sett vil det først bli spørsmål om rettslig overprøving etter at den mistenkte har fått status som siktet, jf. ovenfor.

Etter *fjerde ledd* skal den sikringspålegget retter seg mot, etter begjæring utlevere opplysninger som er nødvendige for å avdekke hvor de aktuelle dataene kom fra, og hvor de i tilfelle ble sendt til. Slik utlevering krever ikke at det foreligger skjellig grunn til mistanke. På dette punktet rekker lovutkastet lengre enn straffeprosessloven § 210. Utleveringsplikten omfatter imidlertid ikke andre data enn trafikkdata, og heller ikke alle de trafikkdataene som tjenestetilbydere har sikret. Politiet har bare krav på å få de dataene som kan bidra til å spore en bestemt kommunikasjonsoverføring.

Kapittel 7
Lovutkast

7.1 Endringer i straffeloven

Lov 22. mai 1902 nr. 10 Almindelig borgerlig Straffelov (straffeloven) endres slik:

I § 12 første ledd nr. 3 gjøres følgende endringer:
I bokstav a blir §§ *145 annet ledd og 145 b* føyd til i opplistingen.

I bokstav g går ordet «eller» ut.

Bokstav h avsluttes med komma i stedet for semikolon og blir tillagt «eller».

Ny bokstav i skal lyde:
i) er straffbar etter lov 12. mai 1961 nr. 2 § 54 om vern av åndsverk;

§ 145 første ledd skal lyde:

Den som uberettiget bryter brev eller annet lukket skrift eller på liknende måte skaffer seg adgang til innholdet, eller baner seg adgang til en annens låste gjemmer, straffes med bøter eller med fengsel inntil 6 måneder *eller begge deler.*

Ny § 145 b skal lyde:

Den som uberettiget gjør tilgjengelig passord eller andre data som kan gi tilgang til et datasystem, straffes for spredning av tilgangsdata med bøter eller fengsel inntil 6 måneder eller begge deler.

Grov spredning av tilgangsdata straffes med fengsel inntil 2 år. Ved avgjørelsen av om spredningen er grov, skal det særlig legges vekt på om dataene kan gi tilgang til sensitive opplysninger, om spredningen er omfattende og om handlingen for øvrig skaper fare for betydelig skade.

Medvirkning straffes på samme måte.

Offentlig påtale finner ikke sted uten fornærmedes begjæring med mindre allmenne hensyn krever påtale.

7.2 Endringer i straffeprosessloven

Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven) endres slik:

Ny § 199 a skal lyde:

Ved ransaking av et datasystem kan politiet pålegge enhver som plikter å vitne i saken, å gi nødvendige opplysninger for å gi tilgang til datasystemet.

Reglene i domstolloven § 206 gjelder tilsvarende.

Ny § 215 a skal lyde:

Ved mistanke om en straffbar handling som etter loven kan medføre en høyere straff enn fengsel i 6 måneder eller som rammes av straffeloven § 390 a, kan påtalemyndigheten gi pålegg om sikring av elektronisk lagrede data som antas å ha betydning som bevis. Forhøyelse av maksimumsstraffen ved gjentakelse eller sammenstøt av forbrytelser kommer ikke i betraktning. Trafikkdata kan kreves sikret selv om strafferammekravet ikke er oppfylt.

En mistenkt skal underrettes om beslutningen straks han får status som siktet i saken.

Sikringspålegget gjelder for et bestemt tidsrom, som ikke må være lengre enn nødvendig og høyst 90 dager om gangen. Dersom sikringspålegges gis etter anmodning fra fremmed stat, gjelder pålegget for minst 60 dager. § 197 tredje ledd, § 208 første og tredje ledd og § 216i gjelder tilsvarende.

Den pålegget retter seg mot, skal etter begjæring utlevere de trafikkdata som er nødvendige for å spore hvor dataene som omfattes av sikringspålegget kom fra og hvor de eventuelt ble sendt til.

Vedlegg 1

Convention on Cybercrime, Budapest, 23.11.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, *No. R (87) 15* regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with par-

ticular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a) «computer system» means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
b) «computer data» means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
c) «service provider» means:
   i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
   ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service;
d) «traffic data» means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
   a) the production, sale, procurement for use, import, distribution or otherwise making available of:
      i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
      ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

   with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
   b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
a) any input, alteration, deletion or suppression of computer data;
b) any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
   a) producing child pornography for the purpose of its distribution through a computer system;
   b) offering or making available child pornography through a computer system;
   c) distributing or transmitting child pornography through a computer system;
   d) procuring child pornography through a computer system for oneself or for another person;
   e) possessing child pornography in a compu-

ter system or on a computer-data storage medium.
2. For the purpose of paragraph 1 above, the term «child pornography» shall include pornographic material that visually depicts:
   a) a minor engaged in sexually explicit conduct;
   b) a person appearing to be a minor engaged in sexually explicit conduct;
   c) realistic images representing a minor engaged in sexually explicit conduct.
3. For the purpose of paragraph 2 above, the term «minor» shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.
3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:
   a) a power of representation of the legal person;
   b) an authority to take decisions on behalf of the legal person;
   c) an authority to exercise control within the legal person.
2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible

the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.
3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.
2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
   a) the criminal offences established in accordance with Articles 2 through 11 of this Convention;
   b) other criminal offences committed by means of a computer system; and
   c) the collection of evidence in electronic form of a criminal offence.
3. a) Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
   b) Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
      i. is being operated for the benefit of a closed group of users, and
      ii. does not employ public communications networks and is not connected with another computer system, whether public or private,

   that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:
   a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
   b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.
2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
   a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
   b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.
2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
3. For the purpose of this article, the term «subscriber information» means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
   a) the type of communication service used, the technical provisions taken thereto and the period of service;
   b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
   c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
   a) a computer system or part of it and computer data stored therein; and

b) a computer-data storage medium in which computer data may be stored

in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
   a) seize or similarly secure a computer system or part of it or a computer-data storage medium;
   b) make and retain a copy of those computer data;
   c) maintain the integrity of the relevant stored computer data;
   d) render inaccessible or remove those computer data in the accessed computer system.
4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
   a) collect or record through the application of technical means on the territory of that Party, and
   b) compel a service provider, within its existing technical capability:
      i. to collect or record through the application of technical means on the territory of that Party; or
      ii. to co-operate and assist the competent authorities in the collection or recording of,

   traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:
   a) collect or record through the application of technical means on the territory of that Party, and
   b) compel a service provider, within its existing technical capability:
      i. to collect or record through the application of technical means on the territory of that Party, or
      ii. to co-operate and assist the competent authorities in the collection or recording of,

   content data, in real-time, of specified communications in its territory transmitted by means of a computer system.
2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
   a) in its territory; or
   b) on board a ship flying the flag of that Party; or
   c) on board an aircraft registered under the laws of that Party; or
   d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1. a) This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.
   b) Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.
2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.
3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may

consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.
5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.
6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.
7. a) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.
   b) The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.
3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.
4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.
5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.
2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such requ-

est, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance request in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
2. a) Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.
   b) The central authorities shall communicate directly with each other;
   c) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;
   d) The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.
3. Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.
4. The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
   a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
   b) it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.
5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.
6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.
7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.
8. The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
9. a) In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.
   b) Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).
   c) Where a request is made pursuant to subparagraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.
   d) Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting

Party to the competent authorities of the requested Party.

e) Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
2. The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:
   a) kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or
   b) not used for investigations or proceedings other than those stated in the request.
3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.
4. Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.
2. A request for preservation made under paragraph 1 shall specify:
   a) the authority seeking the preservation;
   b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
   c) the stored computer data to be preserved and its relationship to the offence;
   d) any available information identifying the custodian of the stored computer data or the location of the computer system;
   e) the necessity of the preservation; and
   f) that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.
3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.
4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.
5. In addition, a request for preservation may only be refused if:
   a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
   b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.
6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform

the requesting Party, which shall then determine whether the request should nevertheless be executed.

7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.
2. Disclosure of traffic data under paragraph 1 may only be withheld if:
   a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or
   b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.
2. The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.
3. The request shall be responded to on an expedited basis where:
   a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
   b) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance in the real-time collection of traffic data

1. The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.
2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1. Each Party shall designate a point of contact

available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a) the provision of technical advice;
b) the preservation of data pursuant to Articles 29 and 30;
c) the collection of evidence, the provision of legal information, and locating of suspects.

2. a) A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
   b) If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.
3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.
2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.
4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.
2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.
2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.
3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:
   - the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
   - the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
   - the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).
2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.
3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1. A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.
2. When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.
3. With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.
2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.
3. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.
2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.
3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.
4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.
5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.
2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:
   a) the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;
   b) the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;
   c) consideration of possible supplementation or amendment of the Convention.
2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.
3. The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.
4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.
5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.
2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a) any signature;
b) the deposit of any instrument of ratification, acceptance, approval or accession;

c) any date of entry into force of this Convention in accordance with Articles 36 and 37;
d) any declaration made under Article 40 or reservation made in accordance with Article 42;
e) any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.