

Førstestatsadvokat Inger Marie Sunde:

Forfatteropplysninger: Sunde er cand. jur. 1987, Master of Laws (Harvard) 1992; advflm/advokat ved advokatfirmaet BA-HR, dommerfullmektig ved Eidsvoll sorenskriverembete i 1990, førstestatsadvokat ved ØKOKRIM fra 1993; har ledet ØKOKRIMs Datakrimteamet siden januar 1998; konsultativt medlem i Næringslivets Sikkerhetsråd og medlem av arbeidsutvalget i Forum for IT-Sikkerhet.

CONVENTION ON CYBERCRIME

1 Innledning

Norge undertegnet nylig en viktig konvensjon på kriminalitetsbekjempelsens område, nemlig Convention on Cybercrime.¹ Konvensjonen er utferdiget av Europarådet, som i november 1996 oppnevnte ekspertgruppen som har utformet konvensjonsteksten. I ekspertgruppen deltok også 4 stater utenfor Europarådet, USA, Japan, Canada og Sør-Afrika. På denne måten sikret man seg allerede i utgangspunktet tilslutning fra teknologiledende land (i hvert fall gjelder det USA og Japan), som det er helt vesentlig å ha et effektivt samarbeide med i bekjempelsen av modernisert kriminalitet. Ekspertgruppens forslag ble godkjent av Europarådets Committee on Crime Problems (CDPC) i møte 18.-22. juni 2001. Den 23. november 2001 ble konvensjonen undertegnet av 26 Europarådsstater samt de nevnte fire statene. Konvensjonen trer i kraft etter at 5 stater har ratifisert, hvorav tre må være medlemmer av Europarådet.² Deretter kan konvensjonen tiltres av andre stater forutsatt at det foreligger en enstemmig invitasjon fra signaturstatene.³

Konvensjonen stiller minimumskrav til statenes materielle og prosessuelle lovgivning (Chapter II). Dertil etablerer den tiltak for internasjonalt samarbeide (Chapter III).

Konvensjonen supplerer gjeldende bi- og multilaterale avtaler og konvensjoner, herunder de viktige Europarådskonvensjonene om utlevering av 13. desember 1957, og om gjensidig bistand i straffesaker av 20. april 1959 og tilleggsprotokollen av 17. mars 1978.⁴

¹ Konvensjonsteksten og kommentarer til bestemmelsene (Explanatory Report) er tilgjengelig på <http://conventions.coe.int/Treaty/EN/projects/FinalCybercrime.htm>. Man kan også klikke seg frem til teksten via Europarådets hovedside på www.coe.int.

² Artikkel 36.

³ Artikkel 37.

2 *Formål og bakgrunn*

Formålet med konvensjonen er slik tittelen indikerer, å bekjempe datakriminalitet. Uttrykket datakriminalitet er dog for snevert. Konvensjonen legger faktisk opp til å effektivisere mulighetene for straffeforfølgning og internasjonalt samarbeide i *alle* straffesaker hvor dataetterforskning er relevant. Dette følger av de viktige bestemmelsene i artikkel 14 nr 2 a-c, hvor det fremgår at statene skal implementere prosessuelle regler, ikke bare for å bekjempe datakriminalitet, men også for å utnytte elektronisk informasjon som bevis ved enhver straffbar handling (artikkel 14 nr 2 c). Dette er fulgt opp i kapitlet om internasjonalt samarbeide, se artikkel 23. Dermed er konvensjonen gitt generell rekkevidde på kriminalitetsbekjempelsens område, og gjelder ikke bare for spesielt datakriminteresserte.

Dataetterforskning er å utnytte elektronisk informasjon for å oppklare straffesaker.

Informasjonen kan være lagret, f eks på harddisker eller minnekort, på PC-er, i personlige digitale assistenter ("PDA-er") eller i mobiltelefoner. For å få fatt i informasjonen må politiet som regel ransake og beslaglegge, eventuelt besørge utlevering fra tredje parter.

Informasjonen kan også være under overføring, f eks som tale eller som bombardering med datapakker (elektronisk skadeverk⁵). I slike tilfelle må politiet vurdere muligheten for bruk av metoder for kommunikasjonsavlytting og overvåking. Informasjonen kan være direkte meningsbærende som tekst, lyd eller bilde. Den kan også bestå i programutrustning. Også informasjon om informasjonen (metainformasjon) er interessant. Typiske eksempler er sporingsinformasjon, trafikkdata og logger av forskjellig slag. Informasjonen kan også være om abonnentene, dvs såkalte abonnementsdata. Dette er data som normalt fremgår av telefonkatalogen, eller av WHOIS-databasene på Internett. Ofte er politiet henvist til å innhente dataene fra tele- og tjenestetilbyderne. Forespørsler vil typisk gjelde identiteten til innehavere av såkalt anonyme telefonnumre eller brukere av oppringt linje til Internett.

3 *Utviklingstrekk: Økningen i bruken av elektroniske bevis, nye kriminalitetsformer og internasjonalisering av kriminaliteten*

Utnyttelsen av elektronisk informasjon i etterforskning økte kraftig på slutten av forrige århundre. Betydningen av denne informasjonen vil selvfølgelig bare fortsette å øke i takt med

⁴ Se artikkel 39.

⁵ Såkalt Denial of Service eller DOS-angrep.

økningen i avhengigheten av elektroniske tjenester. Elektroniske bevis spiller en helt sentral rolle ved etterforskning av den nye datakriminalitet som datainnbrudd, DOS-angrep og databedragerier. Men i tillegg spiller elektroniske bevis stor rolle i all annen type kriminalitet. Vi har etter hvert mange eksempler fra norske straffesaker hvor slike bevis har stått sentralt. Det er tale om utpresning, narkotikakriminalitet, drapssaker og økonomiske straffesaker. Det samme gjelder selvfølgelig det meget alvorlige problemet med seksuelle overgrep mot barn, overgrep som ofte filmes, hvoretter filmene spres til barnepornomarkedet via Internett.

Bruk av Internett og teletjenester gjør at offer og gjerningsperson stadig oftere befinner seg i forskjellige land. Dette er vanlig i databedragerisaker og dataangrep via Internett. Videre kan kriminelle miljøer enkelt organisere seg internasjonalt og sørge for effektiv transport av narkotika, barn / kvinner til sexmarkedet og annen menneskesmugling på tvers av landegrensene. Internett- og teletjenester lar seg enkelt utnytte til å hvitvaske økonomisk utbytte fra kriminell aktivitet. Dette kan gjøres transnasjonalt slik at gjerningspersonen er i ett land, hvitvaskingsoperasjonen foregår i et annet, mens den tilsynelatende legitime fortjeneste oppstår i et tredje land. I den individuelle frihets og personvernets navn er det utviklet avanserte krypteringsverktøy som inngår som standardtjeneste i vanlige operativsystem, og det tilbys anonymiseringstjenester for kommunikasjon. Det vil si at tjenestetilbyderen ikke har kunnskap om identiteten til sine egne kunder. Tjenestetilbyderen kan slike tilfelle ikke utlevere informasjon om sine kunder selv om han får rettslig pålegg om det, simpelthen fordi han ikke har noen slik informasjon. Selvfølgelig er det ikke bare lovlige borgere som benytter disse tjenestene. Tjenestene er særdeles velegnede for kriminelle miljøer som ikke ønsker å bli sporet opp av politiet. Sted og tidspunkt for å begå datakriminalitet, eller organisere annen kriminalitet, spiller ingen rolle. Man kan logge seg på når som helst hvor som helst. Alle vet at landegrensene har mistet sin betydning som hemmende faktor for kriminalitet. Politi- og rettsvesenets territoriale kompetanse, og begrensning, fremstår derimot som en alvorlig hindring for effektiv straffeforfølgning. Disse forhold søker Cybercrime-konvensjonen å avbøte ved å etablere ”*a common criminal policy aimed at the protection of society against cybercrime*”.⁶

4 Konvensjonens tilnærming til problemene

⁶ Se konvensjonens fortale (“*preamble*”) 4. avsnitt.

På denne bakgrunn har ekspertgruppen særlig konsentrert seg om følgende problemstillinger:

- Nye kriminalitetsformer har dukket frem. Dette har skapt problemer i forhold til prinsippet om *dual criminality* ved bistand til bruk av tvangsmidler. Når den anmodede stat ikke anser handlingen som straffbar etter sin nasjonale rett, vil den normalt avvise bistand til bruk av tvangsmidler også.⁷ Varianter av dataangrep og databedragerier er eksempler på nye kriminalitetsformer hvor internasjonalt etterforskingssamarbeid av den grunn har vært vanskelig. Det samme gjelder befatning med bilder av seksuelle overgrep mot barn. Her kan man heldigvis registrere en internasjonal holdningsendring, men inntil nylig hadde mange land ikke strafferegler mot dette. Problemet med overgrep mot barn er imidlertid blitt så veldokumentert gjennom det store utbudet av bilder på Internett at det nå skjer en stor motmobilisering innen FN⁸, EU⁹ og nå også via Cybercrime-konvensjonen, se artikkel 9. Konvensjonens krav til statenes materielle straffelovgivning skal forebygge at krav om *dual criminality* skal hindre internasjonalt samarbeide om bekjempelse av nye kriminalitetsformer.¹⁰
- Elektronisk informasjon kan sies å være u håndgripelig. Politiet er interessert i informasjonen, men må beslaglegge lagringsmediet. Er det kurant? F eks benytter straffeprosessloven ordet ”ting” i beslagsbestemmelsen i § 203. Men politiet er jo ikke interessert i harddisken som sådan (i så fall bare i eventuelle fingeravtrykk), bare i informasjonen lagret på den. Dette kan sammenlignes med å kreve beslag i bokstavene i en bok, dvs forlange ”storyen”, men ikke arkene den er skrevet på.¹¹ Mange stater har erfart usikkerhet om i hvilken grad beslagsreglene kan anvendes i dataverdenen. Ikke minst gjelder det ved beslag i elektroniske nettverk. Klare konsepter og regler er derfor

⁷ Prinsippet om *dual criminality* er bl a nedfelt i bistandskonvensjonen av 1959 art 5 nr 1 a. Norge har reservert seg mot å yte bistand til ransaking og beslag dersom ikke kravet til *dual criminality* er tilfredsstillt.

⁸ FN har utferdiget en tilleggsprotokoll til Barnekonvensjonen av 20. november 1989, om salg av barn, barneprositusjon og barnepornografi. Tilleggsprotokollen er datert 25. mai 2000. Norge har undertegnet og ratifisert og protokollen trer i kraft 18. januar 2002. Tilleggsprotokollen er tilgjengelig på <http://untreaty.un.org/English/TreatyEvent2001/index.htm>. Se også St.prp. nr 58 (2000-2001) om samtykke til ratifikasjon av tilleggsprotokollen.

⁹ EUs ministerråd vedtok den 29. mai 2000 en tiltaksplan mot barneporno på Internett (2000/375/JHA). Videre tok EU kommisjonen et nytt initiativ ved å fremme forslag om en Council Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography av 22.1.2001 (COM 2000/854).

¹⁰ Se konvensjonens Chapter II artikkel 2-13, og den supplerende samarbeidsbestemmelse i artikkel 25 nr 5.

¹¹ Eksemplet er fra et foredrag av Jon Bing.

nødvendig for å bistå hverandre. Dette søker konvensjonen å etablere gjennom de straffeprosessuelle reglene i Chapter II, section 2.¹²

- Videre er elektronisk informasjon særdeles sårbar i sin natur. Som det ofte uttrykkes: ”Et tastetrykk er nok til å slette vitale spor”. Kravet til tempo i etterforskningen er derfor meget fremtredende i forhold til å sikre databevis. Problemet består selvfølgelig delvis i at de kriminelle selv raskt kan slette sine spor. Men like mye handler problemet, sett fra politiets side, om for kort lagring eller manglende lagringsrutiner for sporingsinformasjon og trafikkdata, og tilbud av anonymitetstjenester fra tjenestetilbyderne. Politiet vil regelmessig være avhengig av en rettslig beslutning (til ransaking eller et utleveringspålegg i forhold til taushetsbelagt informasjon) for å få tilgang til dataene.¹³ Internasjonalt har man ikke hatt noe instrument for rask informasjonsinnhenting i slike tilfeller. Man har vært henvist til bruk av rettsanmodninger, noe som går altfor sent i forhold til etterforskningens behov.¹⁴ Konvensjonen søker å etablere raske prosedyrer for bevissikring, slik at data kan ”fryses” til de formelle bistandsrutiner er gjennomført.¹⁵ Videre søker man i Chapter III *International Co-operation*, å etablere mekanismer for raskere internasjonalt samarbeide i straffeforfølgningen.

5 *Grenser i cyberspace?*

Konvensjonen legger ikke opp til å utvide statenes territorielle kompetanse. Man kan bare etterforske og straffeforfølge i eget territorium. Ekspertgruppen har imidlertid diskutert spørsmålet om territorielle grenser på Internett. Er det eller er det ikke grenser i cyberspace? I stedet for å utforme bestemmelser som forholder seg spørsmålet om slike grenser, baserer konvensjonen seg på andre kriterier: Man forholder seg til *lagret* informasjon.

¹² Problemstillingen kan anses som litt søkt. Beslag i datalagret informasjon bør jo ikke vurderes som mer problematisk enn å beslaglegge dokumentmapper. I et videre kjæremål fra 1999, hvor politiet i en barnepornosak hadde bedt om sporingsinformasjon fra en tjenestetilbyder, gjorde tilbyderen gjeldende at man ikke var pliktig til å etterkomme utleveringspålegget, jf strpl § 210. Grunnen var at opplysningene var lagret i datalogger og dermed ikke kunne anses som ”ting”. Anførselen ble imidlertid trukket før saken kom opp for Høyesterett. Vi har ellers rettspraksis for at *utskrifter* med trafikkdata anses som ”ting”, jf strpl § 210, se Rt 1992 s 904 og 928 og Rt 1997 s 470.

¹³ I Norge avhenger behovet for rettslig beslutning noe av hvilken betydning tjenestetilbyderen tillegger et fritak for taushetsplikten i teleloven § 9-3, gitt av Post- og Teletilsynet, jf strpl § 118 første ledd. Noen baserer seg på PTs fritak, mens andre krever et utleveringspålegg i tillegg. I visse tilfelle, slik som ved innhenting av trafikkdata i sann tid, er rettslig utleveringspålegg utvilsomt nødvendig, jf strpl § 216b annet ledd bokstav c.

¹⁴ Regulært tar det flere måneder å få svar på en rettsanmodning utenom Norden. Det betyr at tempoet i det internasjonale rettslige samarbeidet er helt i utakt med tempoet i den kriminelle aktivitet som skal bekjempes.

¹⁵ Se artikkel 16 og 17.

Avlyttingsmetoder overfor informasjon *under overføring*, kan politiet ikke benytte på egen hånd utenfor sitt territorium, men må basere seg på assistanse fra den anmodede stat.¹⁶ For lagret informasjon er det spørsmål om informasjonen er åpent tilgjengelig eller ei, dvs om det er tale om såkalt "*open source computer data*". Dersom den er åpent tilgjengelig for allmennheten er den også åpent tilgjengelig for politiet, uavhengig av påloggingspunkt eller hvor på Internett informasjonen finnes. Politiet kan derfor surfe like fritt på Internett som den vanlige borger. Med et gyldig samtykke kan politiet også innhente annen lagret informasjon fra server i utlandet. Spørsmålene er regulert i artikkel 32 *Trans-border access to stored computer data*.¹⁷

6 *Effektivitet kontra rettssikkerhet?*

Effektivitetshensynet brytes ofte mot hensynet til rettssikkerheten til dem som kommer i politiets søkelys. Det har vært viktig for Europarådet å markere at man opprettholder respekten for de tradisjonelle rettssikkerhetsgarantier. For det første inneholder det 10. avsnittet i fortalet en henvisning til den Europeiske Menneskerettighetskonvensjon av 1950 og til FNs erklæring om sivile og politiske rettigheter av 1966. Henvisningen er gjentatt i konvensjonens artikkel 15 *Conditions and safeguards*. Mer konkret fastslår artikkel 15 også at implementering av konvensjonens prosessuelle regler kan gjøres betinget av de rettssikkerhetsgarantier som ellers følger av den nasjonale lovgivning. For norsk rett betyr det blant annet at vi kan opprettholde kravet til domstolskontroll og forholdsmessighet ved bruk av tvangsmidler, samt kravet til skjellig grunn til mistanke ved ransaking. Vi kan også begrense bruken av visse inngripende etterforskningsmetoder til bestemte alvorlige forbrytelser, slik det f eks følger av reglene om kommunikasjonskontroll i straffeprosessloven kapittel 16 a.¹⁸ Videre inneholder bestemmelsene om internasjonalt samarbeide de vanlige reservasjoner i forhold politiske forbrytelser og ordre public.

¹⁶ Se artikkel 34 jf artikkel 21.

¹⁷ Selvfølgelig vil det lett oppstå tvilstilfelle ved praktiseringen av bestemmelsen, f eks dersom politiet ønsker å infiltrere kriminelle miljøer på Internett. Explanatory Report punkt 293-294 inneholder noen veiledende synspunkter, men slår ellers fast at "*it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules*".

¹⁸ Dette er for øvrig også presisert i artikkel 14 nr 3a, i forhold til utnyttelse av trafikkdata i sann tid og avlytting, jf konvensjonens artikkel 20 og 21.

7 *Data og personvern*

Data knyttet til elektroniske tjenester, hva enten det er e-post, surfing på web-sider, taleoverføring eller bruk av on-line banktjenester, oppfattes som særlig sensitive. Det hersker en viss frykt for at ubegrenset registrering og systematisering av slike data vil kunne lede til en uønsket overvåking av borgernes liv og være i strid med grunnleggende personvern hensyn. Sett fra politiets side er det imidlertid ønskelig at logger over bruk av kommunikasjonstjenester genereres og at data lagres så lenge at de kan være til praktisk nytte ved etterforskning. Uten slike elektroniske spor kan politiet ikke avdekke hvem som har stått bak et datainnbrudd, et databedrageri eller deltatt i et pedofilt nettverk på Internett. Utviklingen av anonymitetstjenester¹⁹ undergraver dermed politiets mulighet til å oppklare alvorlig kriminalitet. Det er ikke dermed sagt at politiets tilgang til dataene må være ubegrenset eller at dataene skal oppbevares for alltid. Personvernere uten ansvar for kriminalitetsbekjempelsen har imidlertid vektlagt overvåkingsfaren i en slik grad at man har sørget for å påby sletting av alle personrelaterte data som refererer seg til bruk av telekommunikasjonstjenester, med mindre dataene behøves som faktureringsgrunnlag.²⁰ Kriminalpolitisk må dette være en uønsket utvikling. Personverndebatten har også preget ekspertgruppens arbeide. Særlig har debatten vært ført i relasjon til bestemmelsene om "preservation of data", dvs artikkel 16 og 17. Ekspertgruppen valgte *ikke* å ta stilling til spørsmålet om tjenestetilbyderne skulle være forpliktet til å registrere data som gjør det mulig å spore opp brukerne av tjenestene ("data retention"). Spørsmålet om anonymiseringstjenester er det dermed opp til statene selv å regulere. Derimot har ekspertgruppen laget regler som forplikter dem som besitter data til å oppbevare dataene ("data preservation"), *vel og merke hvis de allerede har dem når de får ordre om "preservation"*. Dermed sikrer man disse sårbare dataene inntil politiet får vurdert behovet for dem og eventuelt innhentet nødvendige utleveringspålegg.

8 *Kort om konvensjonens strafferettslige regler*

¹⁹ Se punkt 3 ovenfor

²⁰ EUs Telekommunikasjonsdirektiv (97/66) går langt i å oppfordre til utvikling av anonyme tjenester og til å forlange sletting av trafikkdata, se artikkel 6. Direktivet gjelder imidlertid ikke på kriminalitetsbekjempelsens område, jf artikkel 1 nr 3, og ifølge artikkel 14 har medlemslandene adgang til å vedta regler om generering og lagring av data såfremt tiltakene er nødvendige for å bekjempe kriminalitet og ikke fremstår som uforholdsmessige. Bestemmelsen anvender samme språk som EMK artikkel 8 nr 2. Datatilsynets standardkonsejson til telekommunikasjonsnæringen av 23.10.2000, baserer seg på direktivets hovedregler om sletting og anonymisering, men har i motsetning til direktivet, *ikke* åpnet for unntak begrunnet i hensynet til kriminalitetsbekjempelsen.

Konvensjonen krever bare anvendelse av straff ved de forsettlige handlinger, jf bruken av ordet ”*intentionally*”, og ordet ”*wilfully*” i artikkel 10.²¹ Det betyr at norsk strafferett på flere punkter er strengere enn det som er påkrevet.²² Som i norsk rett baserer reglene seg også på en generell rettsstridsreservasjon ved bruk av uttrykket ”*without right*”. Det er f.eks. ikke meningen at en datasikkerhetsansvarlig skal straffes for datainnbrudd når han har trengt inn i datasystemet til arbeidsgiveren for å teste om sikkerhetsnivået er tilfredsstillende.

Bestemmelsene i artiklene 2 til 6 er de såkalte ”*CIA-offences*”, dvs. handlinger som rammer konfidensialiteten, integriteten og tilgjengeligheten til data og datasystemer. De tre hensynene er grunnleggende i forhold til påliteligheten til data og datasystemer. Konfidensialitets- og tilgjengelighetshensynet kan sies å stå i et visst spenningsforhold til hverandre. Poenget er at eierne/brukerne av informasjons- og kommunikasjonstjenester skal kunne stole på at man virkelig kommuniserer fortrolig når systemet legger opp til det. Videre at data bare skal gjøres tilgjengelig på det tidspunkt og på den måte som eieren/forvalteren av dataene bestemmer. I det siste tilfellet kan det være like uheldig om data *ikke* eksponeres når de skal (brudd på tilgjengeligheten), som at de eksponeres for tidlig/i strid med forvalterens vilje (brudd på konfidensialiteten). Også integritetshensynet gjelder påliteligheten til dataene og datasystemene. For eksempel anses datainnbrudd som farlig, ikke nødvendigvis bare fordi det kan medføre informasjonslekkasjer, men fordi gjerningspersonen kan endre/manipulere data eller installere uønsket programvare som medfører systemfeil. Fordi eieren ikke lenger kan stole på systemet sitt rammer datainnbrudd bestandig integriteten.

Konvensjonen straffbelegger uautorisert tilgang til lagrede data (artikkel 2) og til data under overføring (artikkel 3). Statene kan gjøre straff betinget av at gjerningspersonen har brutt en beskyttelse, jf uttrykket ”*infringing security measures*” i artikkel 2. Sammenligningsvis setter straffeloven på visse vilkår straff både for den ulovlige bruk, jf strl §§ 261 og 393, og for datainnbrudd og uautorisert avlytting av datatrafikk, jf strl § 145 annet ledd.²³ Videre etablerer

²¹ Bestemmelsen gjelder opphavsrettslig vern og følger språkbruken til TRIPS-avtalen.

²² Dette gjelder bl.a. uaktsomt grovt skadeverk som er straffbart jf strl § 291 tredje ledd, uaktsom befatning med barnepornografi, jf strl § 204 første ledd d jf tredje ledd og uaktsom overtredelse av bestemmelsene i åndsverkloven kap. 1 og 2, jf åvl § 54 første ledd. Videre er uforsettlige skadefølger av et datainnbrudd en straffeskjerpene omstendighet, jf strl § 145 tredje ledd.

²³ Her bør det skje en samordning med strl § 145 a nr 1, som rammer avlytting av telefonsamtaler. Straffebud mot avlytting bør ikke skjelve mellom hvilken overføringsteknologi som benyttes. Videre bør nok også straffeloven modernisere strukturen med en oppsplitting mellom regler til vern om lagret informasjon og informasjon under overføring.

konvensjonen straff for skadeverk mot data (artikkel 4) og mot datasystemer (artikkel 5). Etter norsk rett greier vi oss, i hvert fall foreløpig, med én straffebestemmelse som anses å omfatte alle varianter av skadeverk, nemlig strl § 291. Bestemmelsen kan anvendes ved uberettiget endring/sletting av data og skadeverk mot datasystemer, typisk virusangrep og DOS-angrep²⁴. Artikkel 6 har vært den mest kontroversielle bestemmelsen. I punkt 1a (i), jf punkt 1b, slår den ned på all befatning med gjenstander, informasjon, programsnutter (scripts, exploits osv) laget for å begå ”CIA-offences”. Etter norsk rett vil dette eventuelt kreve innføring av et nytt straffebud. Det er imidlertid adgang til å reservere seg mot regelen, jf artikkel 6 nr 3. Bestemmelsens nr 1 a (ii) jf punkt 1b, rammer også uberettiget befatning med passord og tilgangskoder til datasystemer. Etter omstendighetene kan dette rammes av strl § 145 tredje ledd og heleribestemmelsen i § 317.²⁵

Artikkel 7 og 8 retter seg mot dokumentfalsk og databedrageri. Straffeloven § 270 første ledd nr 2 inneholder allerede en spesialbestemmelse mot databedrageri. Derimot mangler vi spesielle bestemmelser for falske data, og her kan det nok være behov for en vurdering av om straffeloven lever opp til konvensjonens krav på en tilfredsstillende måte.

Artikkel 9 rammer all befatning med barneporno. Dette føyer seg som nevnt inn i rekken av internasjonale initiativ i kampen mot seksuelle overgrep mot barn.²⁶ Man bør for øvrig merke seg passusen i Explanatory Report punkt 98, hvor det står at ”*An effective way to curtail the production of child pornography is to attach criminal consequences to the conduct of each participant in the chain from production to possession*”. Lovgivningsmessig ligger Norge bra an med utformingen av strl § 204 første ledd bokstav d. Utfordringen for oss er å oppnå tilstrekkelig strenge domstolsreaksjoner som reflekterer alvoret i å etterspørre bilder som dokumenterer seksuelle overgrep mot barn.²⁷

²⁴ Norgeshistoriens første dom for DOS-angrep ble avsagt av Ringerike herredsrett den 21. desember 2001 (sak nr 01-00552M). To 19-åringer ble domfelt for grovt skadeverk, og idømt samfunnstjeneste på 90 og 120 dager, inndragning av datautstyr og erstatning til fornærmede. Saken er i skrivende stund ikke rettskraftig.

²⁵ I Rt 1995 s 1872 har Høyesterett slått fast at § 317 kan anvendes ved såkalt informasjonsheleri. Det gjaldt en PIN-kode som gjerningspersonen mente var stjålet. Han ble dømt for forsøk på informasjonsheleri ved tilegnelse av denne koden.

²⁶ Se punkt 4 om dette.

²⁷ Nå kan det synes som om domstolene er på glid i retning av en strengere straffeutmåling. I Oslo byretts dom av 26. november 2001 (sak 01-03802 M/59) ble det idømt 7 måneders fengselsstraff for besittelse av barneporno, hvorav 5 måneder betinget. Påtalemyndigheten har anket til Høyesterett, jf strpl § 8. Videre har Nord-Troms herredsrett i en dom av 21. desember 2001 (sak nr 01-91M) utmålt en straff på ett år og tre måneder for besittelse og spredning av barneporno, se merknadene i premissene på s 17. Dommen er ikke rettskraftig.

Artikkel 10 gir strafferettslig vern for opphavsrettigheter. Åndsverklovens straffebestemmelse i § 54 går faktisk lenger enn påkrevd, siden konvensjonen bare krever straff når krenkelsen skjer ”on a commercial scale”. For øvrig må man nærmere vurdere om det saklige området for § 54 og § 54 a er så vidt som konvensjonen krever.

Title 5 inneholder regler om forsøk, medvirkning, foretaksstraff og sanksjoner.

9 Kort om konvensjonens prosessuelle regler

Reglene i Chapter II *Procedural law* tar sikte på rask og effektiv bevissikring. Artikkene 16 og 17 om *Expedited preservation of stored computer data* og *Preservation and partial disclosure of traffic data* forholder seg til at det kan være behov for å fryse dataene raskt i påvente av et utleveringspålegg. Dersom dataene skal innhentes internasjonalt går det ofte lang tid og dataene kan være forspilt på utleveringstidspunktet. En myndighet utpekt nasjonalt som ”competent authority” skal kunne gi slik preservation order. Et slikt system mangler vi klare regler for etter norsk rett, så her ligger det an til at vi må foreta en viss regelutvikling.²⁸

Artikkel 17 er særlig interessant fordi den åpner for et mer effektivt samarbeide tjenestetilbyderne imellom og i forhold til politiet. Der flere tjenestetilbydere er involvert i en sak, skal de kunne gi informasjon om det til politiet og identifisere de øvrige tjenestetilbyderne politiet kan henvende seg til for å få nødvendig informasjon om gjerningsperson osv. Det åpnes for at ett pålegg om ”preservation” og ”disclosure of traffic data” skal kunne gjøres suksessivt gjeldende overfor *alle* de impliserte tjenestetilbyderne, slik at de på eget initiativ kan ”videresende” pålegget til neste tjenestetilbyder i kjeden. På dette punkt bør statene virkelig bestrebe seg på å utforme gode nasjonale regler slik konvensjonen inviterer til, fordi det innebærer et meget stort effektiviseringspotensiale i den internasjonale straffeforfølgning.

Artikkel 18 inneholder en regel om utleveringspålegg. Her er norsk rett godt dekket gjennom strpl §§ 210-210c, 216 b og teleloven § 9-3 tredje jf fjerde ledd²⁹.

²⁸ På dette punkt er norske regler neppe helt tilfredsstillende. Påtalemyndighetens primærkompetanse til å kreve data utlevert i hastetilfelle, jf strpl § 210 annet ledd og § 216 d, kan ikke anses å dekke konvensjonens krav.

²⁹ Slik bestemmelsen er fortolket av Høyesterett i avgjørelsene inntatt i Rt 1999 s 1944 og 2000 s 169.

Artiklene 19-21 inneholder regler om ransaking og beslag i lagrede data (jf strpl § 192 flg), kommunikasjonskontroll i sann tid (se strpl § 216 b annet ledd bokstav c, om kommunikasjonsanlegg som skal settes i forbindelse med hverandre) og kommunikasjonsavlytting (se strpl § 216 a).

10 Internasjonalt samarbeide

Chapter III om *International Co-operation*, inneholder på vanlig måte en generell oppfordring om å yte assistanse ”to the widest extent possible”, dvs at forskjellige formalkrav ikke skal være til hinder for samarbeide. Essensen er at statene forventes å ha et effektivt opplegg for å assistere ved bevissikring etter de metoder som er beskrevet i de prosessuelle reglene.³⁰

Hensynet til tempo og effektivitet er tydelig vektlagt ved at hver stat forutsettes å opprette et kontaktpunkt som er operativt døgkontinuerlig hele uken, jf artikkel 35. Det stilles krav til at de ansatte har relevant kompetanse og er tilstrekkelig teknisk utstyrt. Man skal kunne bistå med tekniske råd, sørge for bevissikring, innhente bevis, oppspore gjerningspersoner m.v.³¹ Videre skal kontaktpunktet ha kompetanse til å kommunisere med andre kontaktpunkt i nettverket ”on an expedited basis”. Konvensjonen åpner for bruk av enkle og uformelle kommunikasjonsmetoder som fax og e-mail ved ”urgent circumstances”³², jf artikkel 25 nr 3. Slike kommunikasjonsmetoder er selvfølgelig for lengst vanlig praktisert mellom politi i forskjellige land, men konvensjonen gir det en mer formell berettigelse. Dessuten innebærer bestemmelsen at også påtalemyndigheten kan utveksle bistandsanmodninger på slik måte, med ettersendelse på formelt vis dersom den anmodede stat krever det. Dette kan vise seg å bli en vesentlig lettelse for samarbeidet.

11 Sluttkommentar

Jeg tror konvensjonens største betydning er at den virkelig har satt effektivisering på dagsorden, samt at den bidrar til en nødvendig modernisering og harmonisering av

³⁰ Se korrespondansen mellom artikkel 29 og artikkel 16 (expedited preservation), artikkel 30 og artikkel 17 (expedited disclosure of traffic data), artikkel 31 og artikkel 19 (accessing of stored computer data), artikkel 33 og 20 (real-time collection of traffic data) og mellom artikkel 34 og artikkel 21 (interception).

³¹ Norge ligger bra an i internasjonal sammenheng gjennom satsingen på Politiets Datakrimcenter ved ØKOKRIM.

³² Reservasjonen ”urgent circumstances” må anses overflødig når det er tale om sikring av databevis, siden dette alltid er ”urgent”, jf det som er sagt om sårbarhet, jf punkt 4 ovenfor.

lovgivningen i de stater som tiltrer konvensjonen. I lys av den tross alt begrensede erfaring som ekspertgruppen må ha hatt med de relativt nye kriminalitetsformer og etterforskningsmetoder som konvensjonen regulerer, må den roses for å ha kommet frem til gode praktiske løsninger. Så vil fremtiden vise om konvensjonen virkelig bringer oss et stykke fremover ved håndteringen av de utfordringer vi står overfor.