DET KONGELIGE
JUSTIS- OG POLITIDEPARTEMENT

Ot.prp. nr. 40

(2004–2005)

Om lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjons-teknologi (lovtiltak mot datakriminalitet)

Særskilt vedlegg: NOU 2003: 27 Lovtiltak mot datakriminalitet

Innhold

DET KONGELIGE
JUSTIS- OG POLITIDEPARTEMENT

Ot.prp. nr. 40

(2004–2005)

Om lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet)

Tilråding fra Justis- og politidepartementet av 17. desember 2004, godkjent i statsråd samme dag.
(Regjeringen Bondevik II)

1 Proposisjonens hovedinnhold

I proposisjonen fremmer departementet forslag om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi, og om endringer i straffeloven og straffeprosessloven for å gjennomføre de forpliktelser som Norge vil påta seg ved ratifikasjonen.

For det første foreslår departementet et nytt straffebud som forbyr forskjellige former for urettmessig befatning med passord og andre tilgangsdata, og med dataprogrammer og andre innretninger som er særlig egnet til å begå straffbare handlinger rettet mot data eller datasystemer. Forslaget vil bl.a. ramme dem som uberettiget sprer passord, datavirus og hackerverktøy til andre. Straffen er foreslått å være bøter eller fengsel inntil 6 måneder eller begge deler. I grove tilfeller heves strafferammen til fengsel inntil 2 år.

For det annet foreslår departementet regler om midlertidig sikring av elektronisk lagrete data. Et sikringspålegg innebærer plikt til å sikre at dataenes integritet, tilgjengelighet og autensitet blir ivaretatt. Pålegget gjelder for et bestemt tidsrom, som ikke må være lengre enn nødvendig og høyst 90 dager om gangen. Dersom sikringen skjer etter anmodning fra fremmed stat, skal pålegget gjelde for minst 60 dager. Departementet understreker at det ikke er tale om noen generell plikt til å lagre trafikkdata. Om det er behov for en slik ordning, vil bli nærmere vurdert av Datakrimutvalget og deretter eventuelt fulgt opp i en særskilt proposisjon.

Det er bare data som antas å ha betydning som bevis i en straffesak som kan sikres. Gjelder sikringspålegget en e-post eller et vedlegg til en slik forsendelse, kan sikring bare pålegges dersom det er grunn til å tro at det er begått en straffbar handling.

Slike forslaget er utformet, vil den som har rådigheten over de dataene som omfattes av sikringspålegget, kunne bringe spørsmålet om sikringen skal opprettholdes inn for retten etter de samme regler som gjelder for beslag etter straffeprosessloven § 203.

Departementet går inn for å opprettholde vilkåret om at et forhold som strafforfølges av en annen stat, må være straffbart også i Norge for å kunne etterkomme anmodninger fra den utenlandske staten om å utferdige et sikringspålegg.

Det tredje forslaget innebærer at politiet, under ransaking av et datasystem, vil kunne pålegge enhver å gi de opplysninger som er nødvendige for å få tilgang til datasystemet.

Departementet vurderer i proposisjonen om det er grunn til å endre straffeloven § 145 annet ledd slik at det ikke lenger er et vilkår for å kunne straffes at en beskyttelse er brutt, men går inn for at spørsmålet bør utredes nærmere og ses i sammenheng med behovet for en ny regulering av ulovlig tilegnelse av elektronisk lagret informasjon. Departementet går imidlertid inn for en mindre straffskjerping ved overtredelser av bestemmelsen.

Ved siden av forslagene om lovendringer inneholder proposisjonen forslag om at Stortinget ved lov gir samtykke til ratifikasjon av konvensjonen, jf. Grunnloven § 26 annet ledd. Konvensjonen vil bidra til å styrke det internasjonale samarbeidet i saker av denne type. Departementet foreslår derfor at Norge sammen med de andre medlemsstatene slutter seg til konvensjonen.

På denne bakgrunn ber departementet om Stortingets samtykke til ratifikasjon av konvensjonen.

2 Bakgrunn

2.1 Arbeidet med konvensjonen

Arbeidet med Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi ble innledet i november 1996. Styringskomiteen for strafferettslige og straffeprosessuelle spørsmål (CDPC) vedtok da å opprette en ekspertgruppe som skulle utarbeide et utkast til en konvensjon om bekjempelse av datakriminalitet.

Bakgrunnen for initiativet var en erkjennelse av at samfunnet gradvis blir mer avhengig av datateknologi, og dermed mer sårbart for nye former for kriminalitet. Utviklingen i informasjons- og kommunikasjonsteknologien åpner også for at tradisjonelle former for kriminalitet kan begås på nye måter. Datakriminalitet har ofte et betydelig skadepotensial, og oppdagelsesrisikoen er gjerne lav. Styringskomiteen så derfor behov for en konvensjon med både strafferettslige og straffeprosessuelle bestemmelser, for å sikre at lovgivningen i medlemsstatene ble bedre tilpasset til den nye tids krav. Konvensjonen burde i tillegg legge til rette for et tett internasjonalt samarbeid.

Ekspertgruppen (PC-CY) ble formelt opprettet av Europarådets ministerkomité i vedtak 4. februar 1997, og startet sitt arbeid i april samme år. I arbeidsgruppen deltok både medlemmer av Europarådet (Belgia, Bulgaria, Estland, Finland, Frankrike, Hellas, Italia, Latvia, Makedonia, Nederland, Portugal, Sverige, Tjekkia og Tyskland) og enkelte observatørstater (USA, Canada og Japan). Under forhandlingene ble det avholdt i alt 28 møter. Norge var representert på de siste møtene i arbeidsgruppen.

Konvensjonen ble vedtatt 8. november 2001, og undertegnet av Norge 23. november samme år, jf. kgl. res. 16. november 2001. Det er i dag (pr. 17. november 2004) 30 stater som har undertegnet konvensjonen, og 8 stater som har ratifisert den. Blant konvensjonsstatene er ikke bare medlemmer av Europarådet, men også USA, Canada, Japan og Sør-Afrika.

Konvensjonen trådte i kraft 1. juli 2004.

Etter at arbeidet med konvensjonen ble avsluttet, er det i tillegg utarbeidet en tilleggsprotokoll om kriminalisering av rasistiske og fremmedfiendtlige handlinger som er begått ved hjelp av et datasystem. Protokollen rammer bl.a. spredning av rasistiske ytringer og rasistisk motiverte trusler. Tilleggsprotokollen ble vedtatt 28. januar 2003, men er foreløpig ikke undertegnet av Norge. Departementet går derfor foreløpig ikke inn på de spørsmål som denne protokollen reiser, men vil i tilfelle komme tilbake til disse i en senere proposisjon.

Det gjøres nærmere rede for konvensjonens innhold i punkt 2.5.

2.2 Datakrimutvalgets utredning (NOU 2003: 27 Lovtiltak mot datakriminalitet)

Regjeringen oppnevnte ved kongelig resolusjon 11. januar 2002 et utvalg for å utrede lovtiltak mot datakriminalitet (Datakrimutvalget). Den første delutredningen, NOU 2003: 27 Lovtiltak mot datakriminalitet, ble avgitt til departementet 2. november 2003. I utredningen fremmer utvalget i samsvar med sitt mandat forslag til gjennomføring av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (IKT) i norsk rett. Datakrimutvalget skal arbeide videre med en bredere gjennomgåelse av straffeloven og straffeprosessloven for å avdekke om det er behov for ytterligere lovendringer for å bekjempe datakriminalitet mer effektivt. Delutredningen om dette vil blant annet bli fulgt opp som ledd i departementets arbeid med den spesielle delen i en ny straffelov.

2.3 Departementets høringsbrev 2. februar 2004

Datakrimutvalgets utredning ble sendt på høring 2. februar 2004 med høringsfrist 3. mai 2004.

Datakrimutvalget anbefalte at Norge på noen punkter reserverer seg eller avgir en erklæring om at forpliktelsene i konvensjonen ikke vil bli gjennomført fullt ut. I høringsbrevet ga departementet uttrykk for at Norge ikke bør reservere seg på flere punkter enn strengt nødvendig. Departementet ba i lys av dette særskilt om høringsinstansenes syn på noen utvalgte problemstillinger.

Dette gjaldt for det første om anskaffelse av barnepornografi ved hjelp av et datasystem burde kriminaliseres uttrykkelig ved å føye til «anskaffelse» i gjerningsbeskrivelsen i straffeloven § 204 første ledd bokstav d. Departementet antok at det ikke var noe stort behov for en slik endring ettersom gjerningsbeskrivelsen i bokstav d allerede har et vidt nedslagsfelt, men at pedagogiske grunner likevel kunne tale for å endre loven. Dette forslaget er fulgt opp i en egen proposisjon med forslag til en straffebestemmelse som utelukkende retter seg mot barnepornografi. Forslaget til lovendring er utformet generelt slik at all anskaffelse av barnepornografi rammes, ikke bare anskaffelse ved hjelp av et datasystem.

For det annet spurte departementet i høringsbrevet om straffeloven § 145 annet ledd bør endres slik at vilkåret om beskyttelsesbrudd ble fjernet. I så fall vil det ikke være behov for å avgi en erklæring i tilknytning til artikkel 2, slik utvalget går inn for.

Et tredje spørsmål som ble reist i høringsbrevet, var om utleveringsloven § 24 bør endres slik at en begjæring fra utenlandske myndigheter om å utferdige et sikringspålegg, ikke er avhengig av at handlingen som strafforfølges i utlandet også er straffbar i Norge. I mangel av en slik lovendring vil Norge måtte reservere seg mot artikkel 29 nr. 4, slik utvalget går inn for.

Departementet ba særskilt om høringsinstansenes syn på kriminalisering av ulike former for befatning med utstyr som kan brukes til å begå nærmere bestemte straffbare handlinger som nevnt i konvensjonen artikkel 2 til 5, for eksempel ulovlig datainnbrudd.

På et punkt gikk departementet i høringsbrevet etter en foreløpig vurdering inn for at Norge i første omgang bør reservere seg, men at spørsmålet bør utredes nærmere av Datakrimutvalget. Dette gjaldt spørsmålet om å endre straffeloven § 216 b slik at trafikkdata kan innhentes som ledd i etterforskningen av flere straffbare forhold enn i dag.

2.4 Høringen

Utredningen ble sendt på høring til følgende adressater:
Departementene
Høyesterett
Lagmannsrettene
Oslo tingrett, Asker og Bærum tingrett, Bergen tingrett, Ryfylke tingrett, Sunnmøre tingrett, Nord-Troms tingrett
Domstoladministrasjonen
Riksadvokaten
Statsadvokatembetene
Politidirektoratet
Politiets sikkerhetstjeneste
ØKOKRIM
Generaladvokaten
Barneombudet
Forbrukerombudet
Datatilsynet
Konkurransetilsynet
Kredittilsynet
Amnesty International Norge
Det juridiske fakultet, UiB
Det juridiske fakultet, UiO
Det juridiske fakultet, UiTø
Den Norske Advokatforening
Den Norske Dataforening
Den norske Dommerforening
Det kriminalitetsforebyggende råd (KRÅD)
Forbrukerrådet
Forsvarergruppen av 1977
Institutt for rettsinformatikk, UiO
Juridisk rådgivning for kvinner (JURK)
Juss Hjelpa i Nord-Norge
Juss-Buss
Jussformidlingen i Bergen
Kontor og Datateknisk Landsforening
Kommunenes Sentralforbund (KS)
Landsorganisasjonen i Norge (LO)
NetCom GSM AS
Norges Juristforbund
Norges Lensmannslag
Norsk forening for Jus og EDB
Norsk forening for kriminalreform (KROM)
Norsk Senter for Menneskerettigheter
Norsk Tele- og Informasjonsbrukerforening
Næringslivets Hovedorganisasjon (NHO)
Politiembetsmennenes Landsforening
Politiets fellesforbund
Rettspolitisk forening
Redd Barna
Statsadvokatenes forening
Straffedes organisasjon i Norge (SON)
Telenor
Tele2 Norge AS

Følgende instanser har kommet med realitetsmerknader til høringen:
Barne- og familiedepartementet
Nærings- og handelsdepartementet
Samferdselsdepartementet
Utenriksdepartementet
Barneombudet
Riksadvokaten

Politidirektoratet
Datatilsynet
Konkurransetilsynet
ØKOKRIM
Den norske Dommerforening
Den Norske Advokatforening

Vedlagt høringsuttalelsen fra Politidirektoratet er uttalelser fra KRIPOS, Politiets data- og materielltjeneste og følgende politidistrikter: Oslo, Asker og Bærum, Gudbrandsdal, Haugaland og Sunnhordland, Sør-Trøndelag og Troms.

Generaladvokaten tiltrer i det alt vesentligste utvalgets forslag. Direktoratet for samfunnsberedskap og sikkerhet har ingen innvendinger mot departementets vurderinger i høringsbrevet.

Følgende høringsinstanser har opplyst at de ikke har merknader til høringsbrevet:
Arbeids- og administrasjonsdepartementet
Forsvarsdepartementet
Helsedepartementet
Kommunal- og regionaldepartementet
Sosialdepartementet
Utdannings- og forskningsdepartementet
Høyesterett
Politiets sikkerhetstjeneste
Forbrukerrådet
Nasjonal sikkerhetsmyndighet
Det juridiske fakultet, Universitetet i Oslo
Landsorganisasjonen i Norge (LO)

Innholdet i høringsuttalelsene blir behandlet i tilknytning til de enkelte lovforslagene. Hovedinntrykket etter høringen er at høringsinstansene er positive til forslagene om lovendringer som gjør det mulig for Norge å ratifisere konvensjonen. Høringsinstansene er mer delt i synet på hvilke punkter Norge bør reservere seg mot konvensjonsforpliktelsene.

2.5 Nærmere om Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (IKT)

2.5.1 Innledning

I det følgende gis en kort oversikt over hovedinnholdet i konvensjonen. Konvensjonen i engelsk originaltekst og norsk oversettelse er inntatt som trykt vedlegg til proposisjonen. På de punktene hvor det er eller kan være aktuelt å endre loven, blir det gitt en mer detaljert gjennomgåelse av de aktuelle konvensjonsbestemmelsene, jf. punkt 3.2.1 (artikkel 2), 3.3.1 (artikkel 6) og 4.2.1 (artikkel 16 og 17) nedenfor. Mer utfyllende merknader til konvensjonen går frem av utvalgets utredning og av den forklarende rapporten til konvensjonen, som er tilgjengelig på Europarådets nettsider (http://conventions.coe.int/Treaty/en/Reports/Html/185.htm).

2.5.2 Hovedinnholdet i konvensjonen

I *fortalen* uttrykker partene sin felles bekymring for utviklingen av IKT-kriminalitet, og understreker behovet for nye lovtiltak og styrket internasjonalt samarbeid.

Artikkel 1 definerer uttrykkene «computer system», «computer data», «service provider» og «traffic data».

Artikkel 2 – 10 pålegger partene å kriminalisere ulike former for samfunnskadelig bruk av informasjons- og kommunikasjonsteknologi, blant annet
- datainnbrudd (*artikkel 2*),
- dataavlytting (*artikkel 3*),
- dataskadeverk (*artikkel 4*),
- systemskadeverk (*artikkel 5*),
- besittelse og spredning av tilgangsmidler, hackerprogramvare mv. (*artikkel 6*),
- datarelatert falsk (*artikkel 7*),
- datarelatert bedrageri (*artikkel 8*),
- befatning med barnepornografi (*artikkel 9*),
- immaterialrettskrenkelser (*artikkel 10*).

Artikkel 11 pålegger partene å kriminalisere forsøk på og medvirkning til forbrytelsene som er nevnt i artikkel 2 – 10.

Artikkel 12 pålegger partene å gi regler som gjør det mulig å holde foretak ansvarlig for handlinger begått av ledende ansatte som handler på vegne av foretaket, og for handlinger begått av underordnete som følge av manglende tilsyn eller kontroll.

Artikkel 13 pålegger partene å sørge for at de forbrytelsene som konvensjonen nevner, skal kunne straffes på en effektiv, proporsjonal og avskrekkende måte, blant annet ved bruk av frihetsstraff.

Artikkel 14 angir rekkevidden av de prosessuelle bestemmelsene. Konvensjonen skal ikke bare gjelde under etterforskningen av de forbrytelser som er nevnt i artikkel 2 – 11, men også ved etterforskning av andre forbrytelser som er begått ved hjelp av et datasystem eller i saker hvor bevis kan være lagret i elektronisk form.

Artikkel 15 slår fast at de tvangsmidlene som

konvensjonen gir anvisning på, skal utformes og gjennomføres på en måte som er forenelig med statspartenes interne straffeprosess og med nærmere angitte traktatbestemmelser om menneskerettigheter.

Artikkel 16 pålegger partene å gi regler om midlertidig sikring av lagrede data.

Artikkel 17 pålegger partene å sørge for at reglene om midlertidig sikring kan anvendes uten hensyn til hvor mange tjenestetilbydere som var involvert i dataoverføringen. I tillegg pålegges partene å sørge for at myndighetene uten videre skal kunne få utlevert de trafikkdataene som er nødvendige for å spore hvor dataene kom fra, og hvor de eventuelt ble sendt til.

Artikkel 18 pålegger partene å gi regler om utlevering av elektronisk lagrede data. Slike utleveringspålegg skal kunne rettes mot både privatpersoner og tjenestetilbydere.

Artikkel 19 pålegger partene å gi regler om ransaking og beslag av datasystemer og lagringsmedier.

Artikkel 20 pålegger partene å gi regler om avlytting av trafikkdata i sanntid, dvs. mens bruken skjer.

Artikkel 21 pålegger partene å åpne for avlytting av innholdsdata under etterforskningen av alvorlige forbrytelser.

Artikkel 22 gir regler om jurisdiksjon.

Artikkel 23 slår fast at konvensjonsstatene skal samarbeide i så stor utstrekning som mulig under etterforskningen av saker om IKT-kriminalitet.

Artikkel 24 slår bl.a. fast at de forbrytelsene som er nevnt i artikkel 2 – 11, skal gi grunnlag for utlevering såfremt de har en strafferamme på fengsel i minst ett år.

Artikkel 25 slår bl.a. fast at partene så langt det er mulig, skal yte hverandre bistand under etterforskningen av saker om IKT-kriminalitet.

Artikkel 26 slår fast at partene uoppfordret kan sende hverandre informasjon som kan komme til nytte under en pågående etterforskning i en annen stat. Den stat som sender informasjon fra seg, kan kreve at opplysningene behandles konfidensielt og kan knytte vilkår til overføringen.

Artikkel 27 gir regler om saksbehandlingen i saker om gjensidig bistand, som skal gjelde hvor annet ikke er avtalt mellom partene.

Artikkel 28 gir den anmodede stat rett til å kreve at de opplysninger den gir fra seg, skal behandles konfidensielt og ikke brukes i andre saker enn den henvendelsen gjaldt.

Artikkel 29 bestemmer at en stat kan anmode en annen stat om å sikre data midlertidig. Begjæringen kan avslås hvis den gjelder et politisk lovbrudd, eller hvor begjæringen strider mot den anmodede stats suverenitet, sikkerhet, *ordre public* eller andre grunnleggende hensyn, jf. artikkel 29 nr. 5. Begjæringen kan også avslås om den gjelder et forhold som ikke er straffbart etter vedkommende lands rett, med mindre det er tale om en handling som nevnt i artikkel 2 til 11.

Artikkel 30 innebærer at en stat kan anmode en annen stat som har vært involvert i en kommunikasjonsoverføring, å utlevere nok trafikkdata til å kunne avgjøre hvilken tjenestetilbyder som ble benyttet. Begjæringen kan bare avslås hvis den gjelder et politisk lovbrudd, eller strider mot den anmodede stats suverenitet, sikkerhet, *ordre public* eller andre grunnleggende hensyn.

Artikkel 31 innebærer at en stat kan anmode en annen stat om å ransake, beslaglegge og utlevere data som er lagret i den anmodede stat, inkludert data som er sikret i medhold av artikkel 29.

Artikkel 32 slår fast at en stat bare kan skaffe seg tilgang til data som er lagret på en annen stats territorium hvis dataene enten er åpent tilgjengelige for offentligheten, eller hvis vedkommende stat har innhentet samtykke fra den som har rådigheten over dataene.

Artikkel 33 forplikter statspartene til å bistå hverandre ved innhenting av trafikkdata i sanntid.

Artikkel 34 innebærer at statspartene skal bistå hverandre ved avlytting av innholdsdata i sanntid.

Artikkel 35 pålegger partene å opprette et kontaktpunkt som skal være tilgjengelig 24 timer i døgnet, 7 dager i uken (24/7-nettverk), og som skal bistå med tekniske råd, sikring av data etter artikkel 29 og 30, innsamling av bevis mv.

Artikkel 36 slår fast at konvensjonen kan tiltres både av stater som er medlemmer av Europarådet og av stater som ikke er det. Bestemmelsen gir også nærmere regler om når konvensjonen trer i kraft.

Artikkel 37 regulerer adgangen til å tiltre konvensjonen etter at den har trådt i kraft. Etter denne bestemmelsen kan Ministerkomiteen, med enstemmig samtykke fra konvensjonsstatene, etter nærmere regler invitere stater som ikke er medlemmer av Europarådet til å slutte seg til konvensjonen.

Artikkel 38 gir partene anledning til å angi det territorium eller de territorier konvensjonen skal gjelde for.

Artikkel 39 regulerer forholdet mellom konvensjonen og enkelte andre folkerettslige instrumenter.

Artikkel 40 gir regler om hvordan partene skal gå frem om de ønsker å avgi erklæringer i tilknytning til enkelte av bestemmelsene i konvensjonen.

Artikkel 41 gir enkelte særregler for forbundsstater.

Artikkel 42 gir regler om hvordan partene skal gå frem dersom de ønsker å ta forbehold mot enkelte av bestemmelsene i konvensjonen.

Artikkel 43 slår fast at en part kan trekke tilbake hele eller deler av en reservasjon ved å underrette Generalsekretæren.

Artikkel 44 innebærer at Ministerkomiteen etter nærmere regler kan endre konvensjonen etter forslag fra en konvensjonsstat.

Artikkel 45 gir regler om tvisteløsning.

Artikkel 46 pålegger partene å gjennomføre periodiske konsultasjoner med sikte på å utveksle erfaringer, vurdere om det er behov for endringer mv.

Artikkel 47 gir regler om hvordan partene skal gå frem dersom de ønsker å tre ut av konvensjonen.

Artikkel 48 angir enkelte forhold som Europarådet skal underrette statspartene om.

3 Konvensjonens straffebestemmelser

3.1 Innledning

Norsk strafferett er i det alt vesentlige i samsvar med de krav konvensjonen stiller. *Datakrimutvalget* la således til grunn at det ikke var behov for andre lovendringer enn dem som artikkel 6 gjør nødvendig, noe *høringsinstansene* har sluttet seg til. Departementet er enig i dette. Forpliktelsene i artikkel 3 til 5 er allerede gjennomført i straffeloven § 145 annet ledd og §§ 291 og 292, mens artikkel 7, 8 og 10 er gjennomført i straffeloven § 182, § 270 første ledd nr. 2 og åndsverkloven § 54. Når det særskilt gjelder skadeverk, er for øvrig utvalgets lovforståelse i samsvar med det syn Høyesterett bygger på i kjennelse 17. oktober 2004 (HR-2004-01807-A). Artikkel 9 om barnepornografi er som nevnt fulgt opp i en egen proposisjon. En nærmere gjennomgåelse av konvensjonens straffebestemmelser og av de tilsvarende norske straffebestemmelsene, er gitt i utredningens punkt 2.

Departementet kommer nærmere tilbake til artikkel 6 i punkt 3.3 nedenfor. Aller først er det naturlig å drøfte om det er grunn til å følge opp forslaget i høringsbrevet om å endre straffeloven § 145 annet ledd om datainnbrudd, jf. artikkel 2.

3.2 Datainnbrudd

3.2.1 Konvensjonsforpliktelsen

Konvensjonen artikkel 2 gjelder datainnbrudd og lyder slik:

> «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.»

Bestemmelsen pålegger konvensjonsstatene å sette straff for den som rettsstridig skaffer seg tilgang til hele eller deler av et datasystem, uavhengig av om vedkommende har gjort seg kjent med innholdet av de data som datainnbruddet har gitt tilgang til. Det skal være uten betydning for straffbarheten om innbruddet retter seg mot en enkeltstående datamaskin eller en maskin i et nettverk, jf. definisjonen av «computer system» i artikkel 1 bokstav a.

Konvensjonen rammer som nevnt bare den som urettmessig skaffer seg tilgang til et datasystem, jf. «without right». Den som etter avtale med eieren begår eller forsøker å begå et datainnbrudd for å teste sikkerheten, faller dermed utenfor bestemmelsens virkeområde, iallfall i den utstrekning han ikke går lenger enn avtalen forutsetter. Utenfor faller dermed også det å skaffe seg tilgang til de delene av et datasystem som er ment å være åpne for allmennheten. Den som leser en nettavis, rammes naturligvis ikke av artikkel 2.

Det er overlatt til statspartene selv å bestemme om straffansvar skal være betinget av at det er brutt en beskyttelse, at handlingen er begått i en bestemt hensikt eller at den retter seg mot en datamaskin i et nettverk.

3.2.2 Gjeldende rett

Datainnbrudd rammes av straffeloven § 145 annet ledd, som lyder:

> «Det samme gjelder som ved å bryte en beskyttelse eller på lignende måte uberettiget skaffer seg adgang til data eller programutrustning som er lagret eller som overføres ved elektroniske eller tekniske hjelpemidler.»

Uttrykket «data» skal forstås vidt, og omfatter all slags maskinlesbar informasjon, f.eks. om personlige, tekniske eller økonomiske forhold. Det kreves ikke at informasjonen i seg selv er av konfidensiell art, jf. Ot.prp. nr. 35 (1986–87) s. 20. Med «programutrustning» menes instruksjonene til en datamaskin, altså dataprogrammer. Alternativet er strengt tatt overflødig ved siden av alternativet «data», siden et dataprogram nødvendigvis består av data.

Bestemmelsen rammer bare den som «ved brytе en beskyttelse eller på lignende måte uberettiget skaffer seg adgang til data eller programutrust-

ning». I forarbeidene begrunnes dette slik, jf. NOU 1985: 31 Datakriminalitet s. 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 praktisk form for «beskyttelse» vil være bruk av passord. Den som uberettiget gjør bruk av en annens passord, har ikke brutt en beskyttelse, men vil etter omstendighetene kunne rammes av alternativet «på annen tilsvarende måte» dersom handlingen fremstår som «kvalifisert uberettiget», jf. Ot.prp. nr. 35 (1986–87) s. 20.

Det er ikke et vilkår for straff at gjerningspersonen har gjort seg kjent med dataene eller programutrustningen. Etter bestemmelsen er det tilstrekkelig at hun eller han har skaffet seg adgang til dem.

Bestemmelsen rammer både data som er lagret, og data som er under overføring. Det siste vil kunne være aktuelt ved avlytting.

Strafferammen er bøter eller fengsel inntil 6 måneder, jf. § 145 første ledd. Skyldkravet er forsett, jf. § 40. Forsøk og medvirkning er straffbart, jf. straffeloven § 49 og § 145 fjerde ledd.

3.3.2 Utvalgets forslag

Utvalget drøfter forholdet mellom artikkel 2 og straffeloven § 145 annet ledd på side 14–15 i utredningen. Utvalget mener for det første at anvendelsesområdet til straffeloven § 145 er tilstrekkelig vidt til å dekke kravene i artikkel 2. Det drøfter deretter om strafferammen i § 145 er streng nok, og går inn for å endre bestemmelsen slik at overtredelser kan straffes med fengsel inntil 6 måneder eller bøter *eller begge deler*.

Utvalget peker på at dersom vilkåret i § 145 om beskyttelsesbrudd skal videreføres, slik utvalget går inn for, må Norge avgi en erklæring om dette i henhold til konvensjonen artikkel 40 jf. artikkel 2 annet punktum.

3.2.4 Høringsbrevet

I høringsbrevet ber departementet høringsinstansene vurdere om det fremdeles bør være et vilkår for straff at det foreligger et beskyttelsesbrudd. Departementet peker blant annet på at den tilsvarende bestemmelsen i den danske straffeloven ikke oppstiller noe slikt krav, og at den kraftige økningen i bruk av datasystemer til kommunikasjon gjør at muligheten for å skaffe seg uberettiget adgang til data er større nå enn i 1985, da spørsmålet sist ble vurdert i Norge.

3.2.5 Høringsinstansenes syn

De fleste høringsinstansene som har uttalt seg om spørsmålet, gir uttrykk for at det ikke lenger bør være et vilkår for straff at det foreligger et beskyttelsesbrudd. Dette gjelder *Nærings- og handelsdepartementet, Utenriksdepartementet, Politidirektoratet, ØKOKRIM, Asker og Bærum politidistrikt, Troms politidistrikt, Haugaland og Sunnhordland politidistrikt* og *Datatilsynet.*

Nærings- og handelsdepartementet viser til at også privatpersoner som ikke beskytter sine data har behov for et strafferettslig vern, og at man ved å fjerne beskyttelsesvilkåret i § 145 vil kunne oppnå at elektronisk kommunikasjon i mindre grad blir misbrukt. Nærings- og handelsdepartementet mener kravet om forsett vil føre til at en slik endring ikke vil lede til at straffansvaret rekker for vidt:

> «Vi legger ... til grunn at forsettkravet vil medføre at dersom en bruker tilfeldigvis, og uten viten og vilje, kommer inn på et datasystem som ikke er det han vanligvis benytter, vil ikke denne handlingen medføre strafferettslig ansvar så lenge brukeren trer tilbake straks han oppdager at han er inne på et system som han kan ha rimelig grunn til å tro at han ikke har tilgang til.»

Også *Utenriksdepartementet* anbefaler at vilkåret om beskyttelsesbrudd fjernes fra straffeloven § 145 for å styrke enkeltpersoners strafferettslige vern av privat kommunikasjon. *Asker og Bærum politidistrikt* gjør gjeldende at bestemmelsen om datainnbrudd bør verne også dem som ikke har ressurser til å installere sikkerhetstiltak:

> «Dette vil sørge for at det også oppnås et strafferettslig vern for 'de små' private innehavere av dataanlegg (de som ikke ser seg i stand til å benytte ressurser til beskyttelsestiltak).»

Flere høringsinstanser støtter forslaget under henvisning til bestemmelsene om tyveri, som ikke krever at den fornærmede har truffet spesielle beskyttelsestiltak. *ØKOKRIM* uttaler blant annet:

> «Straffeloven har relativt liten beskyttelse mot 'tyveri' av informasjon. Bestemmelsene om forretnings-, drifts- og bedriftshemmeligheter i straffeloven §§ 294 nr. 2 og 405 a har begrenset anvendelsesområde og/eller relativt lave straffer, iallfall sammenlignet med tyveri av gjenstander. Misbruksbestemmelsene i straffeloven §§ 261 og 391 rammer den som utnytter data-

maskinressurser hos andre, og ikke direkte det å skaffe eller tilegne seg informasjon/data. Åndsverksloven regulerer åndsverk og nærstående rettigheter og gir kun eneretter til eksemplarfremstilling og tilgjengeliggjøring for allmennheten. Straffeloven §§ 291 og 292 kan ramme endring eller sletting av data, men ikke det at informasjon/data kopieres eller tilegnes. Straffeloven §§ 275 og 276 om utroskap er i utgangspunktet begrenset til personer med en lederstilling eller en viss posisjon.

ØKOKRIM ... har registrert en økning i henvendelser som gjelder 'tyveri' av informasjon ved hjelp av en datamaskin, men hvor det vanskelig kan sier å foreligge brudd på en beskyttelse. Et typeeksempel er en utro tjener i en bedrift som uberettiget kopierer ut informasjon til en konkurrent.

I en tid hvor man tillegger IKT-tjenester stadig større verdi, bør det strafferettslige vern om data i hvert fall være på linje med det man har for gjenstander, og som kjent stilles det ikke noe vilkår om at en gjenstand skal være beskyttet for at det skal være tale om tyveri.

Etter vår oppfatning bør straffeloven inneholde en regel om rettsstridig adgang til data som er lagret eller som er under overføring. Beskyttelsesbrudd, skadeforvoldelse eller vinnings hensikt bør være straffskjerpende omstendigheter, sml. utformingen av strl § 258 om grovt tyveri.

[...]

Bestemmelsen om informasjonstilegnelse gjelder en handling som er beslektet med tyveri. Bestemmelsen bør derfor inntas i strl kap 24. Regelen om beskyttelsesbrudd gjelder handlinger som rammer datasikkerheten som sådan. Dette kan sammenlignes med et skadeverk (kap 28), men er primært anslag mot det samfunnsmessige behov for et sikkert system for informasjonsutveksling. Plassering i kapitlet om almenfarlige forbrytelser (kap 13) som i dag, er derfor antakelig korrekt plassering. Her er også regelen om fysisk innbrudd plassert (strl § 147).

Vi mener også at strl § 262 om beskyttelsesbrudd overfor betalingsbelagte tjenester i form av data som overføres (vernede tjenester), burde integreres i den nye bestemmelsen om informasjonstilegnelse. Det at krenkelsen skjer ved beskyttelsesbrudd og i vinnings hensikt er dermed skjerpende omstendigheter. I dag inneholder straffeloven to bestemmelser som slår ned på beskyttelsesbrudd overfor data som overføres, nemlig strl § 145 annet ledd og strl § 262. Den tekniske fremgangsmåten for å oppnå den uberettigede tilgangen er avgjørende for subsumsjonen. Er det tale om privatdekoding av en film på TV hjemme i stuen, skal strl § 262 anvendes, mens strl § 145 annet ledd skal anvendes dersom tilgangen skaffes ved innbrudd i en database på internett. Denne fragmenteringen av regelverket virker ikke velgrunnet og leder til uklarhet om rekkevidden av bestemmelsene.»

Politidirektoratet slutter seg til disse synspunktene, og tilføyer at det forutsetter en viss datakyndighet å sette opp beskyttelse mot datainnbrudd.

Også *Datatilsynet* støtter forslaget, og begrunner sitt syn med at den som behandler personopplysninger med elektroniske hjelpemidler bør ha et strafferettslig vern selv om datasystemet ikke sikres slik personopplysningsloven krever. Det peker på at personopplysningene som noen uberettiget tilegner seg, ofte gjelder andre enn den som har forsømt å beskytte systemet.

Oslo politidistrikt går imot forslaget og begrunner det med at det er enkelt å beskytte datasystemer mot misbruk.

Også *Den Norske Advokatforening* er kritisk til forslaget, og ber om at Datakrimutvalget vurderer spørsmålet som ledd i arbeidet med den andre delutredningen. Synspunktet støttes av *Den norske Dommerforening*.

Politidirektoratet støtter for øvrig utvalgets forslag om å heve strafferammen til «bøter eller fengsel inntil 6 måneder eller begge deler», slik at tvangsmidler kan benyttes i henhold til konvensjonens artikkel 14 nr. 2.

3.2.6 Departementets syn

I lys av høringen er det etter departementets syn naturlig å se spørsmålet om å endre straffeloven § 145 annet ledd i sammenheng med reglene om uberettiget tilegnelse av informasjon, selv om disse regelsettene retter seg mot ulike stadier av et hendelsesforløp og heller ikke fullt ut varetar de samme hensyn. Ulike former for «informasjonstyveri» synes å utgjøre et økende samfunnsmessig problem, som det kan være grunn til å møte med nye lovtiltak. På bakgrunn av særlig ØKOKRIMs høringsuttalelse, som får støtte av Politidirektoratet, ser departementet et klart behov for å utrede nærmere om data i dag har et for svakt strafferettslig vern sammenlignet med for eksempel vernet mot tyveri av fysiske gjenstander. Å vurdere dette og eventuelt utforme en helt ny bestemmelse som rammer urettmessig tilegnelse av informasjon, slik ØKOKRIM foreslår, er imidlertid en oppgave av en slik art at det er naturlig å la den gå inn i Datakrimutvalgets videre arbeid. Det synes med andre ord som om reformbehovet innenfor dette feltet strekker seg utover en eventuell endring av straffeloven

§ 145 annet ledd slik som skissert i høringsbrevet. Spørsmålet blir da om det er et mer akutt behov for å følge opp forslaget i høringsbrevet (å fjerne beskyttelsesvilkåret) allerede nå, eller om også dette mer avgrensede spørsmålet best kan følges opp i Datakrimutvalgets andre delutredning, slik Advokatforeningen og Dommerforeningen foreslår.

Selv om de fleste høringsinstansene som har uttalt seg om spørsmålet går inn for å fjerne vilkåret om beskyttelsesbrudd, underbygger ikke høringen at det er noe påtrengende behov for foreslå en slik lovendring nå. Det vil være en fordel at problemstillingen blir vurdert i en bredere sammenheng. Departementet foreslår derfor ikke nå å fjerne dette vilkåret i straffeloven § 145 annet ledd. Dette innebærer i tilfelle at det må avgis en erklæring i samsvar med artikkel 40, jf. punkt 5 nedenfor.

Departementet er enig med utvalget og Politidirektoratet i at straffen for overtredelsen av bestemmelsen bør skjerpes noe, og tiltrer utvalgets forslag. Dette vil sikre at det kan brukes straffeprosessuelle tvangsmidler i den utstrekning konvensjonen krever.

3.3 Ulovlig spredning av tilgangsdata – artikkel 6

3.3.1 Konvensjonsforpliktelsen

Artikkel 6 gjelder besittelse og spredning av visse dataprogrammer, tilgangsdata mv. («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 nr. 1 bokstav a (i) pålegger konvensjonsstatene å sette straff for produksjon, salg, kjøp, import, distribusjon og andre former for spredning av dataprogrammer og andre innretninger som er utformet eller tilpasset for å kunne begå straffbare handlinger som nevnt i artikkel 2 til 5. I underpunkt ii rammes tilsvarende former for befatning med passord, tilgangskoder og lignende data som er egnet til å gi tilgang til hele eller deler av et datasystem. Plikten til å straffesanksjonere gjelder likevel bare overfor den som har til hensikt å begå en av de handlingene som er nevnt i artikkel 2 til 5.

Artikkel 6 nr. 1 bokstav b rammer den som besitter tilgangsmidler eller innretninger som nevnt i bokstav a (i) og (ii), i den hensikt å begå en straffbar handling som nevnt i artikkel 2 til 5.

Artikkel 6 nr. 2 gjentar at konvensjonsstatene ikke har noen plikt til å kriminalisere den som besitter eller sprer hackerverktøy eller tilgangsmidler mv. uten å ha til hensikt å begå en straffbar handling. Etter artikkel 6 nr. 3 kan en konvensjonsstat reservere seg mot å gjennomføre enkelte av forpliktelsene i artikkel 6 nr. 1. Reservasjonsadgangen omfatter imidlertid ikke salg, distribusjon og andre former for spredning av tilgangsdata, jf. artikkel 6 nr. 1 bokstav a (ii).

3.3.2 Gjeldende rett

I norsk lovgivning finnes det ingen straffebestemmelse som fullt ut dekker de handlingene som er beskrevet i artikkel 6. Straffeloven § 317 om heleri og § 262 om dekodingsinnretninger dekker deler av gjerningsinnholdet. Det samme gjør åndsverklo-

ven § 54 a. I tillegg vil flere av handlingene som er beskrevet i artikkel 6, etter omstendighetene 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», jf. Ot.prp. nr. 53 (1992–93) s. 24–25. I Rt. 1995 s. 1872 la Høyesterett til grunn at også en PIN-kode vil kunne være utbytte i lovens forstand dersom koden «har økonomisk betydning og er egnet til å bli disponert over». Tilsvarende må antakelig gjelde passord og andre former for tilgangskoder.

Også *straffeloven § 262* kan få anvendelse på enkelte av handlingene som omfattes av artikkel 6. Etter første ledd rammes den som besitter eller sprer en dekodingsinnretning i den hensikt å skaffe noen uautorisert tilgang til en vernet tjeneste, for eksempel kodete radio- og fjernsynssignaler. Uttrykket «dekodingsinnretning» er definert i tredje ledd. Etter forarbeidene vil både PIN-koder og andre data som gir tilgang til vernede tjenester, kunne være dekodingsinnretninger i lovens forstand, jf. Ot.prp. nr. 51 (2000–2001) s. 14.

Åndsverkloven § 54 a jf. § 54 setter straff for «omsetning av, eller besittelse i ervervsøyemed av et hvilket som helst middel hvis eneste formål er å gjøre det lettere ulovlig å fjerne eller omgå tekniske innretninger til beskyttelse av et datamaskinprogram».

Disse straffebestemmelsene må suppleres med 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 (Bergen 1999) s. 239–240. Det samme gjelder hvor et dataprogram eller et passord legges ut på internett, selv om vedkommende på gjerningstidspunktet ikke vet med sikkerhet om programmet eller passordet vil bli brukt til å begå skadeverk eller datainnbrudd, 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 dersom medvirkerens bidrag ikke sto i noe medvirkende årsaksforhold til det etterfølgende skadeverket, vil medvirkeren etter omstendighetene kunne straffes for forsøk på medvirkning.

3.3.3 Er det behov for lovendringer?

Datakrimutvalget la til grunn at artikkel 6 gjør det nødvendig med lovendringer, jf. NOU 2003: 27 s. 19. Det viste til at straffeloven § 317 bare gjelder utbytte av straffbare handlinger. Bestemmelsen rammer ikke den som tilfeldigvis har funnet eller gjettet seg frem til et passord, og som deretter sprer det til andre. Straffeloven § 262 gjelder bare passord som gir tilgang til vernete tjenester. Bestemmelsen rammer ikke passord som gir tilgang til andre former for data, for eksempel bedriftshemmeligheter eller sensitive personopplysninger.

Ingen av *høringsinstansene* er uenige med Datakrimutvalget på dette punkt.

Etter departementets syn kan det ikke være tvilsomt at artikkel 6 gjør det nødvendig med lovendringer, slik også Straffelovkommisjonen la til grunn i 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.

3.3.4 Bør reservasjonsadgangen benyttes?

3.3.4.1 Utvalgets forslag

I NOU 2003: 27 blir spørsmålet om og i tilfelle i hvilken utstrekning Norge bør benytte reservasjonsadgangen i artikkel 6 nr. 3 drøftet på s. 19–21. Utvalget tar utgangspunkt i at man i Norge har vært tilbakeholdende med å sette straff for forberedelseshandlinger, jf. utredningen side 20:

> «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.»

Etter å ha gjort rede for sitt prinsipielle syn på kriminalisering av forberedelseshandlinger, går utvalget over til å drøfte om besittelse av innretninger

som nevnt i artikkel 6 nr. bokstav a (i) bør kriminaliseres. Utvalget peker på at det er en latent risiko for at den som besitter skadevoldende dataprogrammer vil spre dem til andre, også uforvarende, men mener at denne risikoen ikke kan begrunne at besittelsen kriminaliseres. Det legger dessuten vekt på at grensen for hva som er straffbart i for stor grad vil bero på subjektive forhold, og at en slik «sinnelagsstrafferett» er uheldig. I samme retning trekker at en straffebestemmelse som rammer besittelse av slike dataprogrammer indirekte vil øke kontrollnivået i den private sfære, fordi en slik bestemmelse vil åpne for bruk av tvangsmidler. På denne bakgrunn mener utvalget at Norge bør reservere seg mot å oppstille straffansvar for besittelse av visse dataprogrammer. Utvalget går heller ikke inn for å kriminalisere det å gjøre slike innretninger tilgjengelige for andre, og legger blant annet vekt på at slike handlinger ofte vil kunne rammes av reglene om straffbar medvirkning og forsøk.

3.3.4.2 Høringsinstansenes syn

Følgende høringsinstanser uttrykker generell støtte til utvalgets forslag om å benytte reservasjonsadgangen etter artikkel 6 nr. 3 fullt ut: *Den Norske Advokatforening, Oslo politidistrikt, Asker og Bærum politidistrikt* og *Nærings- og handelsdepartementet.*

Oslo politidistrikt begrunner sitt syn slik:

> «Oslo politidistrikt viser til utvalgets begrunnelse, og er enig i at man bør benytte reservasjonsadgangen i artikkel 6. Kriminalisering av hardware/software som kan tenkes å skulle brukes til straffbare handlinger eller er egnet til dette, er betenkelig. En kriminalisering på dette feltet vil kunne hindre utvikling og vil medføre økt kontroll (også fra private aktører med opphavsrettsinteresser) og mistenkeliggjøring av borgerne.»

Enkelte høringsinstanser gir uttrykk for at Norge i denne omgang bør reservere seg, slik utvalget har foreslått, men at spørsmålet bør vurderes på ny som ledd i Datakrimutvalgets videre arbeid. Dette gjelder *Politidirektoratet, Troms politidistrikt* og *Datatilsynet* .

ØKOKRIM gir for sin del uttrykk for at «forholdet til art 6 bør vurderes på nytt», og uttaler videre:

> «Det bør i større grad enn Datakrimutvalget har gjort, fokuseres på den skaderisiko som datavirus, hackerverktøy og liknende dataprogrammer innebærer for samfunnet. Produksjon, spredning og bruk av slik programvare er et misbruk av datateknologiens iboende svakheter (som skaper sårbarheter). Gjerningene påfører samfunnet enorme kostnader og underminerer blant annet den tillit som er nødvendig for realisering av den politiske målsetting om utvikling av ehandel. Parallellen til for eksempel sprengstoff (utredningen s 20, 1. sp), hvor besittelse er gjort straffbar i straffeloven § 161, er nærliggende. Datavirus, hackerverktøy og liknende dataprogrammer kan betraktes som 'elektronisk sprengstoff'. Bruken av dem representerer et enormt samfunnsmessig problem, og det er derfor overraskende at Datakrimutvalget ikke har vurdert konvensjonen artikkel 6 mer grundig på dette punkt.
>
> ØKOKRIMs erfaring er at det er nødvendig å kunne gjøre straffansvar gjeldende overfor dem som tilgjengeliggjør hackerverktøy m.v. Medvirknings- og forsøksreglene gir ikke klare grenser for rekkevidden av straffansvaret i dag og har vist seg utstrekkelige i praksis. Det er behov for et klarere regelverk på området, hvor grensen for det straffbare tydelig markeres. Det antas at klare regler i seg selv vil kunne ha en preventiv effekt i forhold til tilgjengeliggjøring, siden en del av denne aktiviteten sannsynligvis er basert på at gjerningspersonene opplever at de opererer i et straffritt område, i høyden en juridisk gråsone, slik at risikoen for strafforfølgning er minimal.»

3.3.4.3 Departementets syn

Artikkel 6 innebærer en forpliktelse til å kriminalisere forberedelseshandlinger. I Ot.prp. nr. 90 (2003–2004) Om lov om straff (straffeloven) s. 104 har departementet gitt uttrykk for enkelte prinsipielle synspunkter når det kriminalisering av slike handlinger.

En forberedende handling ligger som oftest lenger fra den umiddelbart samfunnskadelige handling enn et straffbart forsøk på en slik handling. Dette gjør forberedelseshandlingene mindre straffverdige. Den forbryterske vilje har normalt ikke manifestert seg så sterkt at det bør føre til straff. Forberedelsene kan være begått før gjerningspersonen har bestemt seg for om han vil begå lovbruddet eller ikke. Og selv om han har bestemt seg, er sannsynligheten for at han vil ombestemme seg når hemninger og motforestillinger melder seg, større enn ved forsøk. Risikoen for at handlingen krenker beskyttelsesverdige interesser er derfor mindre. Dette taler for å kreve en tungtveiende begrunnelse for å sette straff for forberedelseshandlinger. I samme retning trekker ønsket om ikke å knytte grensen for det straffbare i for stor grad til rent subjektive forhold. Mange handlinger, som for eksempel et innkjøp i en jernvarehandel, kan være en del av forberedelsene til en alvorlig straffbar handling, men er sannsynligvis en forberedelse til lovlige ak-

tiviteter. Forskjellen ligger på det subjektive plan: Det blir avgjørende for straffbarheten om gjerningspersonen har til hensikt eller iallfall forsett om å begå en senere straffbar handling som innkjøpet er en forberedelse til. At grensen mellom forberedelse til samfunnsskadelige handlinger og forberedelser til helt uskyldige handlinger i stor grad beror på sinnelaget til personen som begår dem, taler generelt med tyngde imot at slike handlinger skal kriminaliseres.

Dette synspunktet får imidlertid mer begrenset bærekraft når den aktuelle forberedelseshandlingen i større utstrekning enn helt hverdagslige handlinger bidrar til å kaste lys over gjerningspersonens forsett. Det vil eksempelvis kunne være tilfelle dersom en person anskaffer seg et dataprogram eller en annen innretning som har et meget begrenset lovlig bruksområde. Mens en tapetkniv og andre verktøy har et vell av lovlige bruksområder, er situasjonen en annen når det gjelder ulike former for hackerverktøy mv. som er særlig egnet til å begå straffbare handlinger. Et straffebud som retter seg mot det å besitte slike innretninger, vil dermed være mer treffsikkert enn et straffebud som retter seg mot mer dagligdagse handlinger. Heller ikke når det gjelder besittelse av passord og andre tilgangsmidler, vil rent subjektive forhold få avgjørende betydning. Departementet antar at tilknytningsforholdet mellom den som har passordet i sin besittelse og den som disponerer det datasystemet som passordet knytter seg til, ofte vil kunne gi en viss veiledning ved vurderingen. Er det ingen rimelig og fornuftig grunn til at den mistenkte har passordet, kan det ofte tyde på at han allerede har begått eller er i ferd med å planlegge en straffbar handling.

Også andre momenter gjør det forsvarlig å kriminalisere de forberedelseshandlingene som omfattes av artikkel 6. Innretninger av den type som det her er tale om, kan brukes til å begå alvorlige straffbare handlinger. Den som sprer et datavirus kan lett forvolde betydelig skade, især dersom det sprer seg ukontrollert. Den som benytter et passord eller et hackerverktøy til å begå et datainnbrudd, vil i prinsippet kunne skaffe seg tilgang til opplysninger av betydning for rikets sikkerhet, eller til datasystemer av betydning for samfunnets energiforsyning, samferdsel eller muligheter for elektronisk kommunikasjon. Også i andre tilfeller kan et datainnbrudd krenke viktige samfunnsmessige eller private interesser, uavhengig av om det ledsages av et etterfølgende skadeverk eller av andre straffbare handlinger. Et datainnbrudd overfor en virksomhet eller en tilfeldig privatperson kan avsløre bedriftshemmeligheter eller sensitive personopplysninger. Og selv om inntrengeren logger seg av straks innbruddet er fullbyrdet, vil selve inntrengningen kunne gjøre det nødvendig å gjennomgå hele eller deler av datasystemet av sikkerhetsmessige grunner, som vil i sin tur vil legge beslag på ressurser hos den fornærmede. Som allerede disse eksemplene viser, knytter det seg et betydelig skadepotensiale til det å besitte innretninger av denne type.

De skadevirkningene som departementet hittil har pekt på, berører ikke utelukkende dem som rammes av den straffbare handlingen, men har også en side mot folks tillit til og bruk av elektronisk kommunikasjon. Dersom det fester seg et inntrykk av at elektronisk kommunikasjon er mindre trygt enn det reelt sett er, vil det i sin tur kunne få forskjellige negative konsekvenser, bl.a. for fremveksten av e-handelen og for annen teknologiavhengig verdiskaping i samfunnet.

Departementet viser videre til at oppdagelsesrisikoen ved datainnbrudd og annen datakriminalitet foreløpig ser ut til å være relativt lav. Dette har antakelig ikke bare sammenheng med at etterforskningen av disse sakene kan være teknisk komplisert, men også at politiet vil kunne ha behov for opplysninger og bistand fra andre lands politimyndigheter. Det forekommer også at handlingen er begått fra utlandet. Mange datainnbrudd blir for øvrig aldri oppdaget, mens andre blir ikke anmeldt – enten fordi den fornærmede ikke finner det bryet verd, eller av frykt for tap av omdømme. Disse forholdene bidrar til å svekke den preventive virkningen av eksisterende straffebud.

Etter departementets syn taler både det betydelige skadepotensialet, hensynet til tilliten til elektronisk kommunikasjon som kommunikasjonsform og den tilsynelatende lave oppdagelsesrisikoen for at det bør det være straffbart å besitte hackerverktøy og andre tilsvarende innretninger. En slik straffebestemmelse lar seg ikke bare forsvare ut fra de prinsippene for kriminalisering som det er redegjort for i Ot.prp. nr. 90 (2003–2004) s. 88 flg. Det vil også lette det internasjonale samarbeidet i saker som gjelder datakriminalitet, især hvor samarbeidet er betinget av at den handlingen som det er tale om, er straffbar også etter norsk rett. Departementet nevner for øvrig, uten at det har vært avgjørende, at slike handlinger allerede er straffbare etter dansk rett.

Et mulig argument mot en kriminalisering er at det foreløpig er usikkert om den straffbare handling som planlegges, vil bli gjennomført. Mange vil føle en viss psykologisk barriere mot å bevege seg fra et forberedende stadium til å begå selve den straffbare handlingen. Overfor dem som aldri skrider til verket, kan det hevdes at det å sette straff for

besittelsen av hensyn til skadepotensialet ved handlinger han ikke har begått, i en viss utstrekning vil fortone seg som straff for ugjort gjerning. Etter departementets syn er det imidlertid grunn til å tro at den psykologiske barrieren mot å begå datakriminalitet normalt vil være mindre enn når det gjelder andre former for kriminalitet. Dette henger dels sammen med den måten slike forbrytelser blir begått på, men også at det ikke alltid knytter seg noen sosial fordømmelse til det å begå straffbare handlinger over nettet. I enkelte miljøer kan det tvert om knytte seg status til det å begå et datainnbrudd eller et dataskadeverk. Slike forhold kan bidra til at gjerningspersonen lettere enn ellers realiserer sin plan. Det kan også forekomme at gjerningspersonen ikke er klar over at handlingen er straffbar etter norsk rett, især når den retter seg mot datamaskiner i utlandet. I så fall vil heller ikke straffens preventive virkning avholde ham eller henne fra å begå handlingen.

Departementet har på denne bakgrunn kommet til at det bør settes straff for besittelse av passord og hackerverktøy mv.

Departementet går så over til å drøfte spørsmålet om det bør settes straff for *å gjøre slike innretninger tilgjengelige for andre*.

I Datakrimutvalgets utredning ble det foreslått at heller ikke slike handlinger kriminaliseres. Etter departementets syn har de momentene som det er vist til i drøftelsen ovenfor, minst like stor gjennomslagskraft i spredningstilfellene. Som også utvalget viser til, innebærer spredningen at den som sender et passord eller et hackerverktøy til en annen eller legger det ut på et nettsted som er åpent for allmennheten, selv mister kontrollen over hva dataene brukes til. Informasjon på internett kan når som helst lastes ned av hvem som helst hvor som helst i verden, herunder av organiserte kriminelle grupper eller terrorister. Skadepotensialet ved en slik handling er derfor betydelig, samtidig som oppdagelsesrisikoen vil være beskjeden ved dataangrep fra utlandet. Også spredning bør derfor kriminaliseres. Siden slike handlinger ofte er straffbare allerede etter reglene om forsøk og medvirkning, vil en slik utvidelse innebære en forholdsvis beskjeden nykriminalisering.

3.3.5 Nærmere om utformingen av bestemmelsen

3.3.5.1 Utvalgets forslag

I utredningen forslås det at artikkel 6 nr. 1 bokstav a (ii) blir gjennomført i en ny straffebestemmelse, jf. side 19 flg.:

> «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.»

Utvalget foreslår at bestemmelsens objektive gjerningsinnhold utformes slik at den «ikke begrenses til å gjelde passord, men må gjelde alle former for data som kan gi tilgang til hele eller deler av et datasystem». Til spørsmålet om hvilke former for befatning med tilgangsdata som bør omfattes, uttaler utvalget:

> «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.»

Ved drøftelsen av skyldkravet, går utvalget inn på spørsmålet om det bør kreves en bestemt form for hensikt, eller om det bør være tilstrekkelig med alminnelig forsett. Utvalget legger avgjørende vekt på at også forsettlige overtredelser er straffverdige:

> «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.»

Utvalget foreslår at strafferammen i normaltilfellene bør settes til bøter eller fengsel inntil 6 måneder eller begge deler, men med straff av fengsel inntil 2 år ved grove overtredelser.

Endelig foreslår utvalget at bestemmelsen bør føyes til på listen over straffebud som nevnes i straffeloven § 12 nr. 3. Begrunnelsen er særlig at datakriminalitet ofte har et internasjonalt preg.

3.3.5.2 Høringsinstansenes syn

Den eneste høringsinstansen som direkte berører forslaget til gjennomføringen av artikkel 6 er *ØKOKRIM*, som fremhever at forslaget materielt sett ikke rekker langt nok, og at en «ny bestemmelse bør kunne baseres nokså direkte på teksten i konvensjonen art 6».

3.3.5.3 Departementets syn

Departementet er enig med utvalget i at artikkel 6 bør gjennomføres i en ny straffebestemmelse, som foreslås som ny § 145 b i straffeloven. Det finnes ingen bestemmelse som fra før rammer tilsvarende forhold som det konvensjonen retter seg mot. Især gjelder dette dersom konvensjonsbestemmelsen blir gjennomført fullt ut, slik departementet går inn for. Siden det er et nært slektskap mellom de enkelte elementene i artikkel 6, holder departementet fast ved at det er naturlig å samle reglene i ett straffebud. Også pedagogiske hensyn taler for en slik løsning.

Når det gjelder bestemmelsens *objektive gjerningsinnhold*, må man først ta stilling til hvordan objektet for den straffbare handling skal utformes.

Artikkel 6 nr. 1 bokstav a (i) rammer ulike former for befatning med «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». Det fremgår av bestemmelsen at uttrykket «device» iallfall omfatter dataprogrammer, f.eks. ulike former for hackerverktøy. Mer tvilsomt er det om artikkel 6 også omfatter fysiske innretninger, f.eks. innretninger til bruk for avlytting av data som overføres til en datamaskin fra et tastatur eller som overføres til andre over nettet. Antakelig omfatter konvensjonen enhver logisk eller fysisk innretning som er særlig egnet ved overtredelse av artikkel 2 til 5. For å sikre at Norge lojalt oppfyller sine folkerettslige forpliktelser er lovutkastet utformet i samsvar med det.

Artikkel 6 nr. 1 bokstav a (ii) rammer ulike former for befatning med «a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed». Departementet er enig med utvalget i at bestemmelsen må utformes slik at den gjelder alle former for data som kan gi tilgang til hele eller deler av et datasystem, typisk et passord. Det bør være uten betydning om tilgangsdataene er bærere av tall, symboler eller bokstaver, om disse i kombinasjon er meningsbærende, og om dataene er kryptert. Bestemmelsen bør heller ikke være begrenset til å gjelde data som brukeren selv taster inn i datasystemet, men bør også omfatte data som genereres maskinelt ved irisavlesning, avlesning av fingeravtrykk eller stemmeregistrering.

Det neste spørsmålet er hvilke befatningsformer som skal rammes. Etter artikkel 6 nr. 1 bokstav a må straffebudet iallfall ramme det «the production, sale, procurement for use, import, distribution or otherwise making available of» de aktuelle tilgangsdataene eller innretningene. Etter bokstav b skal dessuten «possession» rammes. Flere av kategoriene overlapper hverandre. Etter departementets syn vil det være tilstrekkelig om den norske gjennomføringsbestemmelsen rammer befatningsformene fremstille, anskaffe, besitte eller gjøre tilgjengelig for andre.

Straffansvar kan bare komme på tale der den aktuelle befatningsformen er uberettiget. Har anskaffelsen, fremstillingen, besittelsen eller spredningen tilstrekkelig hjemmel i lov, avtale eller annet rettsgrunnlag, skal den ikke rammes av straffebestemmelsen. En datasikkerhetsansvarlig vil derfor straffritt kunne være i besittelse av et hackerverktøy, selv om verktøyet vil være særlig egnet til å begå datainnbrudd. Det samme gjelder innretninger man lovlig kan besitte i henhold til utkastet til ny § 53 a i åndsverkloven.

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. Departementet er enig med utvalget i at også rent forsettlige overtredelser av bestemmelsen er straffverdige. Det bør derfor ikke kreves at handlingen er begått med en bestemt hensikt, jf. også NOU 2002: 4 Ny straffelov s. 175–176.

Datakrimutvalget foreslo å sette *strafferammen* til bøter eller fengsel i 6 måneder eller begge deler. For grove tilfeller foreslo utvalget en strafferamme på fengsel i 2 år. Departementet slutter seg til utvalgets vurderinger på dette punkt. Forslaget innebærer at strafferammen for overtredelse av utkastet til ny § 145 b normalt ikke vil overstige strafferammen for noen av de lovbrudd som forberedelseshandlingen knytter seg til, men den kan etter omstendighetene være lavere. Bakgrunnen for det er at en forberedelseshandling er mindre straffverdig enn en fullbyrdet forbrytelse. Både hensynet til for-

holdsmessighet mellom lovbrudd og straff (proporsjonalitet) og hensynet til forholdsmessighet mellom straffen for ulike lovbruddstyper (ekvivalens) taler derfor for en slik løsning.

Når det gjelder bestemmelsens *stedlige virkeområde*, er departementet enig med utvalget i at bestemmelsen bør føyes til straffeloven § 12 nr. 3, og kan i den forbindelse slutte seg til utvalgets begrunnelse. Datakriminaliteten er utpreget grenseløs. Tilføyelsen vil innebære at utkastet til ny § 145 b vil kunne ramme handlinger som er begått i utlandet av norske statsborgere eller andre som er hjemmehørende i Norge.

4 Konvensjonens bestemmelser om straffeprosessuelle spørsmål

4.1 Innledning

Norsk straffeprosess er på de fleste punkter i samsvar med de krav konvensjonen stiller. *Datakrimutvalget* la således til grunn at det ikke var behov for andre lovendringer enn dem som artikkel 16, 17 nr. 1 bokstav b og 19 nr. 4 gjør nødvendig, noe *høringsinstansene* har sluttet seg til. Departementet er enig i dette. Forpliktelsene i artikkel 18 til 21 er allerede gjennomført i straffeprosessloven kapittel 15 (ransaking), kapittel 16 (beslag og utleveringspålegg) og kapittel 16 a (avlytting og annen kontroll av kommunikasjonsanlegg). En nærmere gjennomgåelse av konvensjonens straffeprosessuelle bestemmelser og av de tilsvarende norske bestemmelsene, er gitt i utredningens punkt 3.

I det følgende går departementet først inn på bestemmelsene om sikringspålegg i artikkel 16 og 17, jf. punkt 4.2 nedenfor. Bestemmelsen om opplysningsplikt under ransaking i artikkel 19 nr. 4, blir behandlet i punkt 4.3.

4.2 Midlertidig sikring av lagrete data (sikringspålegg)

4.2.1 Konvensjonsforpliktelsen

4.2.1.1 Artikkel 16

Artikkel 16 gjelder midlertidig sikring av elektronisk lagrede data og lyder slik:

«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.»

Bestemmelsen gir regler om midlertidig sikring av data som antas å ha betydning som bevis i en straffesak. Et pålegg om sikring vil kunne sikre at viktig bevismateriale ikke går tapt, men gir ikke rett til å få dataene utlevert. Størst praktisk betydning får bestemmelsen derfor for data som foreløpig ikke kan kreves utlevert. Regler om utleveringspålegg er gitt i artikkel 18.

Bestemmelsen omfatter alle former for data som er elektronisk lagret, både trafikkdata og innholdsdata. Et sikringspålegg kan imidlertid bare rette seg mot data som er lagret på sikringstidspunktet. Konvensjonen forplikter ikke til å innføre generelle regler om lagringsplikt, og heller ikke til å sikre fremtidige data. Pålegget må dessuten være spesifisert og rette seg mot nærmere angitte data. Artikkel 16 åpner ikke for sikring av alle de data som den pålegget retter seg mot, har i sin besittelse eller har kontroll over. Data som er under overføring faller utenfor bestemmelsens virkeområde. Regler om innhenting av slike data er gitt i artikkel 20 og 21.

Et sikringspålegg vil innebære en plikt til å sikre integriteten av dataene. Konvensjonsstatene står fritt til å velge hvordan dataene praktisk sett skal sikres. Dataene kan fryses slik at brukeren ikke får tilgang til dem, eller det kan tas en sikringskopi. Konvensjonen er ikke til hinder for at brukeren gis tilgang til dataene eller kopier av dem under sikringsperioden.

Et sikringspålegg skal ikke gjelde for et lengre

tidsrom enn nødvendig, og uansett ikke for mer enn 90 dager om gangen, jf. artikkel 16 nr. 2. Det er opp til konvensjonsstatene å avgjøre om et sikringspålegg skal kunne forlenges ved utløpet av en sikringsperiode.

Besluttes et sikringspålegg etter anmodning fra en fremmed stat, følger det av artikkel 29 nr. 7 at dataene skal sikres i minst 60 dager. Formålet er å gi den anmodende stat tid og anledning til å ta de nødvendige skritt for å skaffe seg tilgang til dataene.

Etter artikkel 16 nr. 3 er partene forpliktet til å gi bestemmelser som pålegger den som sikringspålegget retter seg mot, taushetsplikt om at det har vært foretatt midlertidig sikring av data. Dersom det er en tredjeperson som har sørget for sikring, skal taushetsplikten hvile også på ham. Bestemmelsen varetar dels personvernhensyn, og dels hensynet til den videre etterforskningen.

4.2.1.2 Artikkel 17

Artikkel 17 gir særregler om 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 nr. 1 bokstav a innebærer at trafikkdata må kunne sikres midlertidig også i de tilfeller hvor flere tjenestetilbydere er involvert i en kommunikasjonsoverføring. Slik sikring vil kunne lette arbeidet med å spore hvor dataene kom fra, og hvor de eventuelt ble sendt til. Uttrykket «trafikkdata» skal tolkes i samsvar med definisjonen i artikkel 1 bokstav d.

Et sikringspålegg innebærer som nevnt ikke at myndighetene får tilgang til dataene. Vedkommende myndighet vil derfor ikke vite om andre tjenestetilbydere har vært involvert i dataoverføringen, og hvilke tilbydere det i tilfelle er tale om. Siden trafikkdata ofte blir slettet etter relativt kort tid, kan det føre til at viktige bevis går tapt. Artikkel 17 nr. 1 bokstav b åpner derfor for at myndighetene umiddelbart skal gis tilgang til trafikkdata i den utstrekning det er nødvendig for å avklare om andre tjenestetilbydere har vært involvert.

4.2.2 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 det er tvilsomt om denne bestemmelsen har noen praktisk betydning i denne sammenheng, og den er uansett ikke i seg selv tilstrekkelig til å oppfylle konvensjonens forpliktelser. Heller ikke § 211 annet ledd, som gjelder pålegg til styrer av post- eller telegrafstasjon om å holde sendinger tilbake inntil en uke, er på noen måte tilstrekkelig i forhold til konvensjonen.

Når det derimot gjelder artikkel 17 nr. 1 bokstav b om utlevering av trafikkdata, antar departementet at konvensjonsforpliktelsen i utgangspunktet dekkes 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 rettes mot 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. Lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (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 politiet eller påtalemyndigheten om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse, jf. ekomloven § 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 kompetansen til Post- og teletilsynet. En tilbyder har dermed plikt til å utlevere elektronisk lagrede data etter straffeprosessloven § 210 i den utstrekning Post- og teletilsynet samtykker.

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

4.2.3 Er det behov for lovendringer?

Datakrimutvalget la til grunn i sin utredning at straffeprosessloven § 216 ikke fullt ut oppfyller forpliktelsene i artikkel 16 og 17 nr. 1 bokstav a, og at det derfor uten videre er klart at konvensjonens bestemmelser om midlertidig sikring av data gjør det nødvendig med lovendringer.

Derimot var utvalget mer i tvil 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 som nevnt betinget av at Post- og teletilsynet gir fritak fra taushetsplikten etter ekomloven § 2–9 første ledd. Skal denne ordningen videreføres, vil tilsynet i tilfelle måtte gi fritak i alle de saker som faller innenfor artikkel 17 nr. 1 bokstav b, og det vil innbære at tilsynsfunksjonen blir uten realitet. Etter utvalgets syn er det lite å vinne på en slik ordning, og det foreslo i stedet en egen bestemmelse om utlevering av visse trafikkdata.

Ingen av *høringsinstansene* er uenige i utvalgets vurderinger på dette punkt.

Etter departementets syn er det ikke tvilsomt at artikkel 16 og 17 nr. 1 bokstav a gjør det nødvendig med lovendringer i norsk rett. Departementet er videre enig med utvalget i at det bør gis en særskilt bestemmelse om utlevering av trafikkdata som nevnt i artikkel 17 nr. 1 bokstav b. Departementet understreker at det her ikke er tale om å innføre noen generell lagringsplikt for trafikkdata. Om det er behov for en slik ordning, vil bli nærmere vurdert som et ledd i Datakrimutvalgets arbeid med en ny delutredning.

4.2.4 Nærmere om utformingen av bestemmelsen

4.2.4.1 Utvalgets forslag

I utredningen forslås det at artikkel 16 og 17 bør gjennomføres i en ny bestemmelse i straffeprosessloven, jf. side 37 flg.

Utvalget drøfter først hvilke former for data som bestemmelsen skal omfatte, og konkluderer med at alle former for data, inkludert e-post og andre former for innholdsdata, bør med.

Utvalget vurderer om det skal kreves mistanke om en straffbar handling for at sikringspålegget skal kunne utferdiges, eventuelt om mistankekravet skal være kvalifisert (for eksempel i form av «skjellig» grunn til mistanke). Utvalget kommer til at det bør oppstilles et mistankekrav, og understreker at mistanken må bygge på objektive holdepunkter. Noe kvalifisert mistankekrav går utvalget imidlertid ikke inn for.

Et særlig spørsmål er om adgangen til å utferdige sikringspålegg bør variere avhengig av om pålegget retter seg mot innholdsdata eller trafikkdata, jf. utredningen side 38:

> «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. [...] 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.»

Utvalgets flertall mener på denne bakgrunn 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.»

Utvalgets mindretall (Sunde) foreslår for sin del at strafferammekravet bare bør knyttes til midlertidig sikring av e-post:

«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 news-meldinger, web-sider, ulovlig pornografi, opphavsrettslig beskyttet materiale, wordfiler 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.»

I tillegg til disse konkrete bemerkningene, føyer hun til en mer generell refleksjon:

«Videre har mindretallet en kommentar 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.»

Utvalget går inn for at påtalemyndigheten bør få kompetanse til å pålegge sikring, jf. utredningen side 39. Det er ikke behov for noen domstolsavgjørelse fordi pålegget ikke medfører at politiet får tilgang til dataene som er sikret.

Spørsmålet om hvilke plikter som følger av et gyldig sikringspålegg, kommenteres slik av utvalget:

«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 dataenes integritet, tilgjengelighet og autensitet blir ivaretatt.»

Utvalget går inn for at den som opplysningene knytter seg til, forutsatt at dette er en bestemt person, skal gis underretning om sikringspålegget, jf. utredningen side 40:

«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. [...] Hensynet til etterforskningen taler [imidlertid] 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. Utvalget

går også inn for at en beslutning om bruk av sikringspålegg bør kunne prøves av domstolene, jf. utredningen side 40.

Når det gjelder bestemmelsen om utlevering av visse trafikkdata etter artikkel 17 nr. 1 bokstav b, foreslår utvalgets flertall at forpliktelsen gjennomføres slik at politiet etter en særskilt bestemmelse skal få tilgang til opplysninger som er nødvendige for å avdekke hvor de aktuelle dataene kom fra eller ble sendt til. Utvalgets mindretall (Sunde) mener at utleveringsplikten bør skjerpes slik at tilbydere plikter å etterkomme utleveringspålegget «straks», jf. utredningen side 40, siden dette er i bedre samsvar med konvensjonen.

4.2.4.2 Høringsinstansenes syn

De eneste instansene som uttaler seg om hvordan den norske gjennomføringsbestemmelsen bør utformes, er *Den Norske Advokatforening* og *Oslo politidistrikt*. Begge er kritiske til utvalgets forslag om hvilke vilkår sikringen skal være betinget av.

Den Norske Advokatforening går imot et skille mellom innholdsdata og trafikkdata, og vil heller ikke ha særregler om e-post. Foreningen går i stedet inn for at mistankekravet kvalifiseres slik at det kreves «skjellig grunn» til mistanke før sikringspålegg kan gis:

> «Et slikt krav vil imøtese de personvernmessige hensyn som foreligger. Etter vår oppfatning er 'skjellig grunn' er rettslig standard, og innholdet i dette kravet vil variere noe ut fra om det er tale om pålegg om sikring eller andre tvangsmidler så som beslag. Det må således legges til grunn at selv om man benytter den samme rettslige standarden, vil terskelen for sikringspålegg i praksis være lavere. Videre er standarden godt kjent og godt egnet til å ta opp i seg de vurderingene som måtte ligge bak ønskene om å særbehandle innholdsdata og profesjonelle aktører.
>
> [...]
>
> Advokatforeningen finner videre at det bør gjelde en strafferamme på mer enn 6 måneder for sikringspålegg.»

Oslo politidistrikt slutter seg til forslaget fra mindretallet i utvalget.

4.2.4.3 Departementets syn

Etter departementets syn må de nye reglene om sikringspålegg utformes i lys av reglene om beslag i §§ 203 flg. Reglene har til felles at de tar sikte på sikre bevis til bruk i en etterfølgende straffesak. Til forskjell fra beslag får imidlertid påtalemyndigheten ikke rådighet over dataene, og dette gjør sikringspålegg til et mindre inngripende tvangsmiddel enn beslag. For at de nye reglene skal få noen selvstendig betydning ved siden av beslagsinstituttet, må vilkårene forutsetningsvis være mindre strenge.

Det første spørsmålet som oppstår, er *hvilke former for data* hjemmelen for sikringspålegg skal omfatte. Slik artikkel 16 nr. 1 er formulert, legger departementet til grunn at bestemmelsen må omfatte alle former for data, inkludert e-post og andre kategorier av innholdsdata.

Spørsmålet om *hvilke vilkår* et sikringspålegg av blant annet rettssikkerhetsmessige grunner bør gjøres betinget av, er overlatt til konvensjonsstatene å avgjøre, jf. artikkel 16 nr. 4 sammenholdt med artikkel 15. Flere løsninger kan i prinsippet være aktuelle.

Tar man utgangspunkt i straffeprosessloven § 203, krever loven tilsynelatende ikke annet enn at den aktuelle gjenstanden kan antas å ha betydning som bevis. Det er ikke noe vilkår at noen med skjellig grunn kan mistenkes for handlingen, eller at en bestemt person er mistenkt. Det er et mer åpent spørsmål om det må foreligge skjellig grunn til mistanke om at det er begått en straffbar handling, jf. Andenæs: Norsk straffeprosess, bind II (3. utgave, Oslo 2000) s. 188 med videre henvisninger. Antakelig må et slikt krav innfortolkes, jf. Rt. 1998 s. 1838, men uklarheten taler for at mistankekravet uansett bør reguleres særskilt i sikringsbestemmelsen.

Departementet er enig med utvalget i at det vil neppe være i strid med konvensjonen å kreve at det må foreligge skjellig grunn til mistanke, slik straffeprosessloven ofte krever for bruk av tvangsmidler. *Den Norske Advokatforening* går inn for et slikt krav i sin høringsuttalelse. Departementet er imidlertid enig med utvalget i at terskelen for bruk av sikringspålegg bør ligge lavere enn det, og kan slutte seg til utvalgets begrunnelse. Et krav om skjellig grunn ville innebære at reglene ville bli uten praktisk betydning. Dersom mistanken først er så sterk, må det antas at politiet normalt vil foretrekke å beslaglegge de aktuelle dataene i medhold av straffeprosessloven § 203 eller kreve dem utlevert i medhold av straffeprosessloven § 210, i den utstrekning Post- og teletilsynet gir fritak fra taushetsplikten etter ekomloven § 2–9.

Spørsmålet blir etter dette om det bør kreves at det foreligger mistanke om at det er begått en straffbar handling, slik utvalget foreslår, eller om det i stedet bør være tilstrekkelig at dataene kan antas å ha betydning som bevis. Den sistnevnte løsningen vil ikke innebære at sikringspålegg kan besluttes uten noen som helst tilknytning til en mulig

straffbar handling, ettersom etterforskning bare kan foretas dersom det foreligger anmeldelse eller andre omstendigheter som gir rimelig grunn til å undersøke om det foreligger et straffbart forhold, jf. straffeprosessloven § 224 første ledd.

Etter departementets oppfatning bør det i utgangspunktet være tilstrekkelig at dataene kan ha betydning som bevis. Slik reglene om sikringspålegg foreslås utformet, vil den midlertidige sikringen utgjøre et forholdsvis beskjedent inngrep. Å bygge på et generelt mistankekrav ville dessuten lede til et unødig finmasket og komplisert system. Hensynet til den som opplysningene knytter seg til, vil være tilstrekkelig varetatt ved det alminnelige forholdsmessighetsprinsippet i straffeprosessloven § 170 a. Det følger av denne bestemmelsen at midlertidig sikring bare kan foretas dersom det er tilstrekkelig grunn til det, og dersom sikringen etter sakens art og forholdene ellers ikke utgjør et uforholdsmessig inngrep. Ved vurderingen vil det her bl.a. måtte legges vekt på hvor sensitive opplysninger det er tale om å sikre. Dersom politiet har kjennskap til forhold som gir grunn til å tro at opplysningene ikke vil bli sikret på en betryggende måte, vil det dessuten måtte tas hensyn til det, slik utvalgets flertall påpeker.

Når det særskilt gjelder elektroniske postsendinger, kan det spørres om sammenhengen med reglene i straffeprosessloven som varetar posthemmeligheten, gjør at det her bør kreves noe mer enn at det er grunnlag for etterforskning og at de aktuelle dataene må antas å ha betydning som bevis. Departementet går inn for at pålegg til en tjenestetilbyder om å sikre e-post og eventuelle vedlegg bør være betinget av at det er grunn til å tro at det er begått en straffbar handling. En slik løsning er best i samsvar med reglene om beslag av brev og andre postsendinger i straffeprosessloven §§ 211 og 212, som bygger på det syn at posthemmeligheten fortjener et særlig vern. Også EMK artikkel 8 om vern av korrespondanse, som ble inkorporert i norsk rett ved lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven) § 2, taler for en slik begrensning. Uttrykket «grunn til å tro» skal forstås på samme måte som det tilsvarende uttrykket i straffeprosessloven § 222 a første ledd om besøksforbud.

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 deteriorate» for å unngå utilsiktet «modification, deterioration or deletion», jf. den forklarende rapporten punkt 159. Sikringen kan dermed skje på flere måter. Departementet er enig med utvalget i at bestemmelsen bør utformes teknologinøytralt, og at det derfor ikke bør sies noe bestemt i loven om hvordan dataene skal sikres. Den pålegget retter seg mot bør selv kunne velge hvordan sikringen praktisk sett skal gjennomføres innenfor de muligheter som til enhver tid finnes, såfremt dataenes integritet, tilgjengelighet og autensitet blir ivaretatt.

Det neste spørsmålet som må avklares, er hvem som skal ha *kompetanse* til å beslutte midlertidig sikring av data. Departementet er enig med utvalget i at kompetansen bør ligge hos påtalemyndigheten, også i hastetilfellene, og viser til utvalgets begrunnelse.

Den som besitter de data som skal sikres – typisk en tjenestetilbyder – må naturligvis få *underretning* om pålegget om midlertidig sikring for at dette skal bli gjennomført. Et annet spørsmål er om den som eventuelt er mistenkt for en handling som pålegget skal sikre bevis for, skal ha krav på underretning. Departementet er enig med utvalget i at en mistenkt bør ha krav på underretning fra det tidspunkt han får status som siktet i saken, men bare dersom sikringspålegget gjelder data som den siktede selv har lovlig tilgang til. En tjenestetilbyder blir for eksempel pålagt å sikre data som knytter seg til den mistenktes e-postkonto eller hans hjemmeside på internett. I slike tilfeller vil han 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, jf. straffeprosessloven § 82 første ledd. Er det besluttet utsatt underretning om et tvangsmiddel, blir vedkommende først siktet når underretning gis, jf. straffeprosessloven § 82 tredje ledd. I slike tilfeller skal det samtidig gis underretning om sikringspålegget.

Departementet har vurdert om andre enn den mistenkte bør gis underretning om at det er foretatt sikring av data som vedkommende har rådigheten over. Utvalget har ikke tatt stilling til spørsmålet, og høringsinstansene har heller ikke kommentert det. Etter departementets syn taler de beste grunner for at også den som er utenfor mistanke, bør få underretning i samme utstrekning som den mistenkte. En slik løsning har ikke bare reelle grunner for seg, men er også best i samsvar med straffeprosesslovens system ved bruk av andre tvangsmidler. Ved husransaking hos andre enn den mistenkte skal politiet som hovedregel underrette den som beslutningen retter seg mot, jf. straffeprosessloven § 200 første ledd. Tilsvarende gjelder ved beslag, jf.

§ 205 første ledd. Hensynet til diskresjon omkring etterforskningen bør til gjengjeld varetas gjennom regler om taushetsplikt, slik også utvalget har foreslått.

Etter departementets syn er det derimot neppe grunn til å gi den mistenkte underretning om at det er sikret data som han ikke selv har lovlig tilgang til, for eksempel andres e-post, men som inneholder opplysninger om vedkommende. Straffeprosesslovens regler om underretning gjelder bare overfor den tvangsmidlet retter seg mot. Et sikringspålegg er ikke så inngripende at det er naturlig å gå lenger her. Også praktiske hensyn taler for en slik løsning. Siden politiet ikke uten videre får tilgang til dataene, vil man ikke kunne fastslå hvem som i tilfelle omtales i de dataene som omfattes av sikringspålegget.

Det siste spørsmålet som knytter seg til selve saksbehandlingen, er om en beslutning om bruk av sikringspålegg bør kunne gjøres til gjenstand for *rettslig prøving* . Utvalget har foreslått at det bør være adgang til rettslig overprøving, og departementet er enig i det. Også sikringspålegg er en form for myndighetsutøvelse som bør kunne etterkontrolleres. Lovteknisk kan dette gjennomføres ved en henvisning til straffeprosessloven § 208, slik utvalget har foreslått.

Data som er sikret gjennom et sikringspålegg, 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. Departementet foreslår derfor at en begjæring om utlevering av slike data skal etterkommes så snart som mulig.

4.2.5 Sikringspålegg som ledd i internasjonalt samarbeid i straffesaker

Etter lov 13. juni 1975 nr. 39 om utlevering av forbrytere mv. § 24 nr. 3 er det et vilkår for å yte rettshjelp til andre stater, at handlingen som forfølgningen gjelder også er straffbar i Norge. *Konvensjonen* artikkel 29 pålegger på sin side statspartene å etterkomme en anmodning om å utferdige et sikringspålegg selv om forholdet ikke er straffbart i staten som anmodes om å yte bistand. Artikkel 29 nr. 4 gir imidlertid stater som Norge, som har dobbel straffbarhet som et vilkår for å yte rettshjelp, mulighet til å reservere seg mot forpliktelsen til å utferdige sikringspålegg i saker som gjelder forhold som ikke er straffbare i Norge.

Utvalget går inn for at Norge benytter seg av denne muligheten, jf. utredningen side 37 flg. Utvalget viser særlig til at kravet om dobbel straffbarhet er et fast innarbeidet prinsipp i norsk rett.

Utvalget får støtte fra et flertall av *høringsinstansene* som har uttalt seg om spørsmålet, som ble løftet særskilt frem i høringsbrevet. *Nærings- og handelsdepartementet, Utenriksdepartementet, ØKOKRIM* og *Konkurransetilsynet* slutter seg alle til utvalgets vurdering. *Politidirektoratet* mener derimot at Norge ikke bør reservere seg, og begrunner det med at et sikringspålegg er et lite inngripende tvangsmiddel.

Også departementet har kommet til at kravet i utleveringsloven § 24 nr. 3 bør opprettholdes for anmodninger om sikringspålegg. Prinsippet om dobbel straffbarhet sikrer at Norge ikke yter rettshjelp i saker som sett fra et norsk ståsted ikke bør gi grunnlag for bruk av tvangsmidler. Konvensjonens pålegg om kriminalisering av en rekke datarelaterte og samfunnsskadelige handlinger vil imidlertid lede til at vilkåret om dobbel straffbarhet vil være oppfylt i flere saker enn i dag.

4.3 Opplysningsplikt under ransaking

4.3.1 Konvensjonsforpliktelsen

Artikkel 19 nr. 4 gjelder opplysningsplikt under ransaking og lyder:

> «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 applies 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.»

Bestemmelsen pålegger konvensjonsstatene å gi regler om opplysningsplikt under ransaking av et datasystem. Opplysningsplikten skal i rimelig utstrekning omfatte forhold som er nødvendige for å kunne gjennomføre ransakingen, typisk opplysning om tilgangskoder.

4.3.2 Gjeldende rett

I norsk rett finnes det ingen generell regel om opplysningsplikt av den type som artikkel 19 forutsetter. Straffeprosessloven § 216 a fjerde ledd annet punktum gir politiet hjemmel til å pålegge en eier eller tilbyder av det nett eller den tjeneste som brukes ved samtalen eller kommunikasjonen å yte den

bistanden som en nødvendig for å gjennomføre avlyttingen. Bestemmelsen er gitt tilsvarende anvendelse når det gjelder innhenting av trafikkdata i sanntid, jf. § 216 b tredje ledd. Det må antas at disse bestemmelsene i en viss utstrekning gir politiet hjemmel til å kreve opplysninger, men verken § 216 a eller § 216 b gir hjemmel for noen opplysningsplikt i forbindelse med ransaking etter §§ 192 flg. For å gjennomføre konvensjonsforpliktelsen er det derfor nødvendig med en ny lovbestemmelse.

4.3.3 Utvalgets forslag

Utvalget mener at artikkel 19 nr. 4 gjør det påkrevd å endre straffeprosessloven. Utvalget fremhever samtidig at pålegg om å gi opplysninger i forbindelse med en ransaking kan tenkes å komme i konflikt med vernet mot selvinkriminering som er innfortolket i Den europeiske menneskerettskonvensjon (EMK) artikkel 6, jf. også FN-konvensjonen om sivile og politiske rettigheter (SP) artikkel 14 nr. 3 bokstav g (utredningen side 44–46).

Utvalget peker på at et pålegg om å bidra med opplysninger ikke innebærer noen straffsiktelse i seg selv, men at selvinkrimineringsvernet etter EMDs praksis kan bli utløst på kontrollstadiet i en forvaltningssak dersom myndighetene tar sikte på å ilegge personen sanksjoner allerede da pålegget om å gi opplysninger ble gitt. Derimot kan et pålegg om opplysningsplikt ikke antas å utløse vernet mot selvinkriminering dersom det retter seg mot en person som politiet ikke har til hensikt å strafforfølge. Vernet gjør seg med andre ord gjeldende «i de tilfellene der den opplysningsplikten er rettet mot, regnes som straffsiktet av andre årsaker», jf. utredningen side 45–46. På denne bakgrunnen foreslår utvalget at opplysningsplikten 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.»

Når det gjelder selve utformingen av bestemmelsen, går utvalget inn for at opplysningsplikten ikke bør gis et større omfang enn konvensjonen artikkel 19 nr. 4 krever. Opplysningsplikten bør med andre ord begrenses til det som er nødvendig for å gi tilgang til det aktuelle datasystemet, for eksempel i form av tilgangskoder. Politiet skal derimot ikke kunne kreve at vedkommende skal finne frem til konkrete opplysninger som politiet måtte være interessert i.

Utvalget slår fast at rekkevidden av den foreslåtte opplysningsplikten i tillegg vil begrenses av kravet til nødvendighet og forholdsmessighet i straffeprosessloven § 170 a.

Etter utvalgets syn bør kompetansen til å kreve opplysninger ligge hos politiet, og legger vekt på at dette vil gi en praktisk løsning.

Utvalget går inn for at plikten til å gi opplysninger bør være straffesanksjonert for å sikre at pålegget etterleves.

4.3.4 Høringsinstansenes syn

Den eneste høringsinstansen som kommenterer utvalgets forslag er *Konkurransetilsynet*, som ut fra sin erfaring mener det åpenbart er behov for en slik bestemmelse. Tilsynet slutter seg til utvalgets vurderinger av forholdet til EMK.

4.3.5 Departementets syn

Departementet vil peke på at konvensjonsforpliktelsen etter artikkel 19 nr. 4 bare omfatter opplysninger som trengs for å gi tilgang til det datasystemet som skal ransakes. Slike opplysninger vil i seg selv neppe være egnet til å utsette angiveren for straff. Allerede av den grunn anser departementet det lite sannsynlig at vernet mot selvinkriminering vil innebære noen begrensning for å kreve opplysninger etter artikkel 19 nr. 4. I tillegg kommer at rekkevidden av det folkerettslige vern mot selvinkriminering til dels er uklar. I konvensjonen artikkel 15 nr. 1 er det pekt på at gjennomføringen av konvensjonen må ta hensyn til menneskerettighetene som er nedfelt i EMK og SP. En opplysningsplikt som angitt i artikkel 19 nr. 4 faller ikke naturlig inn under ordlyden i SP artikkel 14 nr. 3 bokstav g. Selvinkrimineringsvernet etter EMK må etter departementets mening på sin side forstås i lys av den europarådskonvensjon som proposisjonen her tar sikte på å gjennomføre.

Departementet ser på denne bakgrunn ingen grunn til å begrense rekkevidden av opplysningsplikten om tilgang til datasystemer slik den går frem av konvensjonen artikkel 19 nr. 4. Departementet er på den annen side enig med utvalget i at opplysningsplikten ikke bør gis et større omfang enn konvensjonen krever. Det vises til forslaget til

straffeprosessloven § 199 a er gitt i punkt 6.2 nedenfor. Brudd på opplysningsplikten kan straffes med bøter, jf. straffeloven § 339 nr. 1. Slik departementets forslag er utformet, vil imidlertid ikke en siktet kunne straffes i medhold av denne bestemmelsen. En tilsvarende avveining ligger til grunn for straffeloven § 132 tredje ledd. Om dette er en hensiktsmessig avgrensning av straffansvaret, kommer departementet tilbake til som ledd i arbeidet med ny straffelov.

5 Bør Norge ratifisere konvensjonen?

Samfunnet blir gradvis mer avhengig av datateknologi. Denne avhengigheten gjør oss sårbare for nye former for kriminalitet (f.eks. spredning av datavirus). Utviklingen åpner også for at gamle former for kriminalitet kan begås på nye måter (f.eks. spredning av barnepornografi). Felles for de ulike formene for datakriminalitet er at de ofte har stort skadepotensial, samtidig som oppdagelsesrisikoen er lav. Dette stiller samfunnet overfor nye utfordringer. For å 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. De lovforslagene som fremmes i denne proposisjonen og som springer ut av konvensjonen, utgjør etter departementets syn et viktig bidrag i den forbindelse.

Men et godt lovverk ikke i seg selv tilstrekkelig. Datakriminalitet er ofte grenseoverskridende, samtidig som den nasjonale rettshåndhevelsen er bundet til statsterritoriet. Ved etterforskningen av denne type kriminalitet er man derfor ofte nødt til å samarbeide med politimyndigheter i andre land. Slikt samarbeid kan av praktiske og rettslige grunner være vanskelig, og tar gjerne lang tid. Disse vanskelighetene forsterkes når flere land er involvert.

Departementet er ikke i tvil om at konvensjonen vil bidra til å styrke det internasjonale samarbeidet i saker av denne type. Konvensjonen er det første forpliktende internasjonale initiativet på området, og har som nevnt fått tilslutning fra flere teknologisk ledende stater utenfor Europa, herunder USA. Det er viktig at Norge sammen med de andre medlemsstatene følger opp og slutter seg til konvensjonen.

På enkelte punkter åpner konvensjonen for at statene kan reservere seg, mens på andre er det anledning til å erklære at man ønsker å gjennomføre konvensjonsforpliktelsene på en bestemt måte, jf. artikkel 40 og 42. Datakrimutvalget foreslår at Norge bør reservere seg mot deler av artikkel 6 (ulovlige innretninger), 9 (barnepornografi) og 20 (innhenting av trafikkdata i sanntid), jf. NOU 2003: 27 s. 21, 25 og 49. Utvalget foreslår dessuten at det bør avgis to erklæringer i samsvar med artikkel 40. For det første forslås det at Norge bør opprettholde kravet til beskyttelsesbrudd i straffeloven § 145 annet ledd om datainnbrudd, jf. artikkel 2. For det annet foreslås det at Norge ikke bør åpne for midlertidig sikring av data etter anmodning fra fremmed stat med mindre den handlingen som etterforskes er straffbar også etter norsk rett, jf. artikkel 29.

Slik lovforslaget er utformet i proposisjonen her, vil det ikke være behov for å reservere seg mot noen del av artikkel 6 og 9. Gjennomføringen av artikkel 6 er drøftet i punkt 3.3 ovenfor. Når det gjelder artikkel 9, vil det som nevnt bli fremmet en egen proposisjon med forslag til ny barnepornografibestemmelse som fullt ut oppfyller de krav konvensjonen stiller. Derimot er departementet enig med utvalget i at Norge ikke bør åpne for innhenting av trafikkdata i sanntid i mindre alvorlige straffesaker, jf. artikkel 20. Det bør dessuten avgis erklæringer i tilknytning til artikkel 2 og 29, slik utvalget foreslår. Departementet viser i den forbindelse til punkt 3.2.6 og 4.3.5. I tillegg må Norge avgi erklæringer i tilknytning til artikkel 24 og 27.

På denne bakgrunn ber departementet om Stortingets samtykke til ratifikasjon av konvensjonen med den reservasjon og de erklæringer som nevnt ovenfor.

6 Økonomiske og administrative konsekvenser

De foreslåtte lovendringene vil neppe få større økonomiske eller administrative konsekvenser.

Forslaget til ny § 145 b vil innebære en viss nykriminalisering, men utvidelsen vil antakelig bare i beskjeden utstrekning legge beslag på ressurser hos politiet og påtalemyndigheten. Som oftest vil overtredelser av forslaget til en ny straffebestemmelse bli avdekket under etterforskningen av andre straffbare handlinger og av den grunn kreve lite merarbeid.

Forslaget til regler om midlertidig lagring av elektronisk lagrete data vil kunne få visse økonomiske konsekvenser, uten at det er mulig å tallfeste disse. Departementet understreker at det ikke er tale om å innføre noen generell lagringsplikt, men en plikt til i å sikre nærmere bestemte data etter pålegg fra påtalemyndigheten. De økonomiske konsekvensene av dette blir etter departementets mening begrensete og vil bli dekket av staten etter prinsippet i ekomloven § 2–8 annet ledd.

Forslaget om en begrenset opplysningsplikt under ransaking av et datasystem vil kunne lette politiets arbeid under etterforskningen, og i så fall lede til visse besparelser. Sett under ett vil lovforslagene kunne bidra til bekjempelsen av datakriminalitet. I den utstrekning omfanget av slik kriminalitet reduseres, vil også de kostnadene som kriminaliteten påfører samfunnet og den enkelte, reduseres.

Forslaget om å ratifisere konvensjonen vil i seg selv ikke ha nevneverdig økonomiske eller administrative konsekvenser.

7 Merknader til de enkelte bestemmelsene

7.1 Til endringene i straffeloven

Til § 12

Forslaget innebærer at § 145 annet ledd og ny § 145 b tas med i oppregningen i § 12 første ledd nr. 3 bokstav a.

Endringene innebærer at overtredelser av disse bestemmelsene som er begått i utlandet av norske statsborgere eller andre som er hjemmehørende i Norge, vil kunne strafforfølges i Norge.

Til § 145

Strafferammen for brevbrudd og datainnbrudd foreslås hevet til bøter eller fengsel inntil 6 måneder eller begge deler. Om bakgrunnen for forslaget vises det til punkt 3.2.

Endringen i strafferammen vil åpne for bruk av tvangsmidler etter straffeprosessloven, herunder pålegg om midlertidig sikring av elektroniske postsendinger etter forslaget til ny § 215 a i straffeprosessloven.

Til ny § 145 b

Utkastet til *første ledd bokstav a* rammer forskjellige former for befatning med «passord eller andre data som kan gi tilgang til et datasystem». Uttrykket er funksjonelt avgrenset, og omfatter alle data som kan gi tilgang til ulike 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 som brukeren selv taster inn i datasystemet, men omfatter også data som genereres maskinelt ved for eksempel irisavlesning, avlesning av fingeravtrykk eller stemmeregistrering.

Første ledd *bokstav b* rammer forskjellige former for befatning med «dataprogrammer og andre innretninger som er særlig egnet til å begå straffbare handlinger som retter seg mot data eller datasystemer». Bestemmelsen vil typisk ramme forskjellige former for datavirus og hackerverktøy. Uttrykket «innretninger» skal imidlertid forstås vidt, og omfatter enhver logisk eller fysisk innretning som er særlig egnet til å begå straffbare handlinger som retter seg mot data eller datasystemer. I uttrykket «særlig egnet» legger ikke bare et krav til at innretningen funksjonelt sett må være spesielt godt egnet til å begå straffbare handlinger av den type lovutkastet nevner, men også at dette må fremstå som innretningens mest fremtredende egenskap.

Det fremgår innledningsvis av bestemmelsen at loven rammer den som «fremstiller, anskaffer, besitter eller gjør tilgjengelig for andre» tilgangsdata eller innretninger som nevnt i bokstavene a eller b. Alternativet «fremstiller» vil bl.a. omfatte den som lager dataprogrammer av den typen som loven nevner. Alternativet «anskaffer» vil få selvstendig betydning ved siden av alternativet «besitter» i de tilfeller hvor en innretning er bestilt, men ennå ikke levert, eller hvor en nedlasting fra nettet mislykkes, jf. straffeloven § 49 første ledd. Uttrykket «gjør tilgjengelig» omfatter både det å overlate tilgangsdata eller hackerverktøy til en annen (for eksempel via e-post), og det å gjøre slike data eller programmer tilgjengelig for en 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.

Utkastet til første ledd krever at den aktuelle befatningsformen må være «uberettiget». Har fremstillingen, anskaffelsen, besittelsen eller spredningen tilstrekkelig hjemmel i lov, avtale eller annet rettsgrunnlag, rammes den ikke av bestemmelsen. En datasikkerhetsansvarlig vil derfor straffritt kunne være i besittelse av et hackerverktøy, selv om verktøyet vil være særlig egnet til å begå datainnbrudd. Det samme gjelder innretninger man lovlig kan besitte i henhold til utkastet til ny § 53 a i åndsverkloven.

Skyldkravet er forsett, jf. straffeloven § 40. Den som uforvarende kommer i skade for å spre et datavirus som en følge av at hans egen datamaskin er infisert, vil dermed ikke kunne straffes for selve spredningen.

Utkastet til *annet ledd* skjerper strafferammen i grove tilfeller til fengsel inntil 2 år. Ved avgjørelsen av om overtredelsen er grov, nevner lovutkastet tre forhold det særlig skal legges vekt på i vurderingen. For det første vil det være av betydning om tilgangsdataene kan gi tilgang til sensitive opplysninger, for eksempel opplysninger av betydning for rikets sikkerhet, enkelte bedriftsinterne opplysninger og visse personopplysninger, inkludert personopplysninger som nevnt i personopplysningsloven § 2 nr. 8. Slike opplysninger har et særskilt krav på vern, og vil derfor ofte være undergitt lovbestemt eller instruksfastsatt taushetsplikt. Ved anvendelsen av annet ledd vil det imidlertid være tilstrekkelig at opplysningen etter sin art og sammenhengen den inngår i 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 eller begår skadeverk mv. For det tredje vil det ha betydning om handlingen skaper fare for betydelig skade. Både økonomiske og ikke-økonomiske skadevirkninger skal tas i betraktning.

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

Medvirkning er straffbart, jf. utkastet til *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 å laste ned hackerverktøy eller spre datavirus, vil dermed kunne straffes dersom straffbarhetsvilkårene for øvrig er oppfylt.

7.2 Til endringene i straffeprosessloven

Til § 199 a

Forslaget gir politiet adgang til å pålegge enhver som har befatning med et datasystem å bistå med opplysninger i forbindelse med ransakingen av datasystemet. 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 utkastet til *første ledd* at opplysningsplikt kan pålegges enhver som har befatning med datasystemet. Ved ransaking av datasystemer til virksomheter med eget IT-personale vil det være naturlig å rette pålegget mot disse personene. Personkretsen som kan pålegges opplysningsplikt er imidlertid ikke begrenset til bestemte profesjonsgrupper.

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 å gi «nødvendige» opplysninger, dvs. opplysninger som er påkrevd for at politiet skal få tilgang til datasystemet.

Videre begrenses opplysningsplikten av det alminnelige forholdsmessighetsprinsippet i straffeprosessloven § 170 a. 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 kan etter omstendighetene forutsette en avveining 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. I normaltilfellene vil imidlertid pålegg om opplysningsplikt være så lite tyngende at det ikke kan anses uforholdsmessig.

Brudd på opplysningsplikten kan straffes med bøter, jf. straffeloven § 339 nr. 1. Slik departementets forslag er utformet, vil imidlertid ikke en siktet kunne straffes i medhold av denne bestemmelsen. En tilsvarende avveining ligger til grunn for straffeloven § 132 tredje ledd.

Til ny § 215 a

Forslaget til denne nye bestemmelsen gir hjemmel for midlertidig sikring av elektronisk lagrede data som ledd i etterforskningen av straffesaker. Om bakgrunnen for bestemmelsen, se punkt 4.2.1. En regel om sikringspålegg har en viss innholdsmessig sammenheng med reglene i straffeprosessloven § 216, og bør etter departementets syn plasseres rett foran denne.

Det fremgår av utkastet til *første ledd* at påtalemyndigheten kan gi pålegg om sikring av elektronisk lagrede data som antas å ha betydning som bevis. Det er et grunnvilkår at sikringspålegget skjer som ledd i etterforskning, slik at vilkårene i § 224

forutsettes å være oppfylt. Dette går frem av sammenhengen i loven, men er sagt uttrykkelig for ordens skyld.

Med «sikring» menes ethvert tiltak som ivaretar de aktuelle dataenes integritet, tilgjengelighet og autentisitet. Sikring kan skje ved at det tas kopi av de data saken gjelder, eller ved at de aktuelle 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 «data», uten hensyn til om de er bærere av tall, symboler eller bokstaver, om disse i kombinasjon er meningsbærende og om dataene er kryptert. Bestemmelsen omfatter dermed både trafikkdata og innholdsdata, herunder filer med lyd, bilder eller tekst. Det er imidlertid et vilkår at de aktuelle dataene foreligger i elektronisk lagret form på det tidspunkt 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 med tilknytning til saken. Det er et vilkår at dataene «antas å ha betydning som bevis» i en straffesak. 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.

Utkastet til *annet ledd* gjelder pålegg om sikring som retter seg mot en tilbyder av tilgang til elektronisk kommunikasjonsnett eller elektronisk kommunikasjonstjeneste, og som gjelder innholdet av en elektronisk postsending eller et vedlegg til en slik sending, jf. de tilsvarende begrepene i straffeprosessloven § 211 første ledd. Om begrunnelsen for særregelen vises til punkt 4.2.4.3 ovenfor. I slike tilfeller er det et vilkår for sikring at det er grunn til å tro at det er begått en straffbar handling. Uttrykket «grunn til å tro» skal forstås på samme måte som det tilsvarende uttrykket i straffeprosessloven § 222 a første ledd om besøksforbud. Dette innebærer at det ikke kreves sannsynlighetsovervekt for at en slik handling er begått, jf. Ot.prp. nr. 109 (2001–2002) s. 44. Mistanken må imidlertid bygge på visse objektive holdepunkter i det konkrete saksforholdet, og kan derfor ikke utelukkende forankres i rent subjektive forestillinger.

Det fremgår av utkastet til *tredje ledd* at en mistenkt skal gis underretning om beslutningen straks dataene er sikret og 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.

Retter sikringspålegget seg mot en annen enn den mistenkte, skal underretning gis straks pålegget er gjennomført.

Et sikringspålegg gjelder for et bestemt tidsrom, som ikke må være lengre enn nødvendig, jf. utkastet til *fjerde ledd*. Sikringsperioden kan høyst utgjøre 90 dager om gangen. Dersom beslutningen treffes etter begjæring fra fremmed stat, skal sikringsperioden etter *annet punktum* 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. I tillegg foreslås taushetsplikt etter § 216 i.

Etter utkastet til *femte 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. 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.

7.3 Til forslaget om å ratifisere konvensjonen

For at Norge skal kunne ratifisere konvensjonen, er det nødvendig å innhente Stortingets samtykke, jf. Grunnloven § 26 annet ledd og lovforslaget del III. Departementet foreslår at Norge bør reservere seg mot å åpne for innhenting av trafikkdata i sanntid i mindre alvorlige straffesaker, jf. artikkel 20 og 14 nr. 3. I tillegg forslås det at Norge avgir to erklæringer i medhold av artikkel 40. For det første forslås

det at Norge opprettholder kravet til beskyttelsesbrudd i straffeloven § 145 annet ledd om datainnbrudd, jf. artikkel 2. For det annet foreslås det at Norge ikke åpner for midlertidig sikring av data etter anmodning fra fremmed stat med mindre den handlingen som etterforskes er straffbar også etter norsk rett, jf. artikkel 29 nr. 4.

7.4 Til regelen om ikraftsetting

Det går frem av lovforslaget del IV at lovendringene gjelder fra det tidspunktet loven er sanksjonert.

Justis- og politidepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet).

Vi HARALD, Norges Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjøre vedtak til lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet) i samsvar med et vedlagt forslag.

Forslag

til lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet)

I

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

I § 12 første ledd nr. 3 bokstav a føyes §§ *145 annet ledd og 145 b* til i opplistingen.

§ 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 fremstiller, anskaffer, besitter eller gjør tilgjengelig for andre

a) passord eller andre data som kan gi tilgang til et datasystem, eller

b) dataprogrammer eller andre innretninger som er særlig egnet til å begå straffbare handlinger som retter seg mot data eller datasystemer straffes med bøter eller fengsel inntil 6 måneder eller begge deler.

Grove overtredelser straffes med fengsel inntil 2 år. Ved avgjørelsen av om overtredelsen er grov, skal det blant annet legges vekt på om dataene kan gi tilgang til sensitive opplysninger, om spredningen er omfattende og om handlingen skaper fare for betydelig skade.

Medvirkning straffes på samme måte.

II

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 har befatning med datasystemet å gi nødvendige opplysninger for å gi tilgang til datasystemet.

Brudd på opplysningsplikten som begås av andre enn den siktede, straffes etter straffeloven § 339 nr. 1.

Ny § 215 a skal lyde:

Påtalemyndigheten kan som ledd i etterforskning gi pålegg om sikring av elektronisk lagrede data som antas å ha betydning som bevis.

Pålegg om sikring av data i en sending som besittes av en tilbyder av tilgang til elektroniske kommunikasjonsnett eller elektronisk kommunikasjonstjeneste, kan bare gis dersom vilkårene i første ledd er oppfylt og det er grunn til å tro at det er begått en straffbar handling.

Den som har rådigheten over de data som omfattes av sikringspålegget, skal underrettes om pålegget. En mistenkt skal underrettes straks dataene er sikret og han får status som siktet i saken. For øvrig skal underretning gis straks dataene er sikret.

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

III

Samtykke til ratifikasjon

Stortinget samtykker til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi.

IV

Ikraftsetting

Loven trer i kraft straks.

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

Konvensjon om datakriminalitet Budapest, 23.11.2001

Innledning

Medlemsstatene i Europarådet og de andre statene som har undertegnet denne konvensjon,

som tar i betraktning Europarådets mål om å oppnå større enhetlighet mellom sine medlemmer,

som erkjenner verdien av å fremme samarbeidet med de andre statene som er part i denne konvensjon,

som er overbevist om nødvendigheten av å føre og å prioritere en felles kriminalpolitikk som tar sikte på å beskytte samfunnet mot datakriminalitet, blant annet ved å vedta hensiktsmessige lover og å fremme internasjonalt samarbeid,

som er seg bevisst de gjennomgripende forandringer som digitaliseringen, tilnærmingen og den stadige globaliseringen av datanettene har medført,

som er bekymret over faren for at datanettverk og elektroniske data også kan bli brukt til å begå straffbare handlinger og at bevis knyttet til slike handlinger kan lagres og overføres av slike nettverk,

som erkjenner behovet for samarbeid mellom stater og privat industri for å bekjempe datakriminalitet, samt behovet for å beskytte rettmessige interesser i forbindelse med bruk og utvikling av informasjonsteknologi,

som mener at en effektiv kamp mot datakriminalitet krever et sterkere, raskere og mer effektivt internasjonalt samarbeid i straffesaker,

som er overbevist om at denne konvensjon er nødvendig for å forebygge handlinger rettet mot datasystemenes, nettverkenes og dataenes konfidensielle karakter, integritet og tilgjengelighet, samt misbruk av slike systemer, nettverk og data, ved å sørge for kriminalisering av aktivitet som beskrevet i denne konvensjon, samt innføre tilstrekkelig myn-

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;

dighet til å bekjempe slike straffbare handlinger effektivt, ved å tilrettelegge for avdekking, etterforskning og rettslig forfølgning av slike straffbare handlinger både nasjonalt og internasjonalt, og ved å sørge for ordninger som muliggjør et raskt og pålitelig internasjonalt samarbeid,

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;

som er seg bevisst behovet for å sikre tilstrekkelig balanse mellom hensynet til håndhevelse av loven og overholdelse av de grunnleggende menneskerettigheter, nedfelt i Europarådets konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter av 1950, De forente nasjoners internasjonale konvensjon om sivile og politiske rettigheter av 1966, samt andre internasjonale traktater om menneskerettigheter som får anvendelse og som bekrefter ethvert menneskes rett til fritt å kunne ha sine egne meninger, samt retten til ytringsfrihet, herunder frihet til å søke, motta og meddele opplysninger og ideer av alle slag, uavhengig av grenser, samt retten til respekt for privatlivets fred,

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;

som også er seg bevisst retten til vern av personopplysninger, nedfelt i Europarådets konvensjon om personvern i forbindelse med elektronisk databehandling av personopplysninger av 1981,

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

som tar i betraktning De forente nasjoners konvensjon om barnets rettigheter av 1989 og Den internasjonale arbeidsorganisasjonens konvensjon om de verste former for barnearbeid av 1999,

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;

som tar hensyn til Europarådets eksisterende konvensjoner om samarbeid på det strafferettslige området samt liknende traktater inngått mellom Europarådets medlemsstater og andre stater, og som understreker at denne konvensjon er ment å utfylle de nevnte konvensjonene med det mål å gjøre strafferettslig etterforskning og forfølgning mer effektiv samt gjøre det mulig å innhente elektroniske bevis i forbindelse med straffbare handlinger,

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;

som gleder seg over utviklingen i den senere tid, som ytterligere fremmer internasjonal forståelse og samarbeid når det gjelder bekjempelse av datakriminalitet, herunder tiltak truffet av De forente nasjoner, OECD, Den europeiske union og 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,

som minner om anbefaling nr. R (85) 10 om den praktiske håndhevelse av Den europeiske konvensjon om gjensidig samarbeid i straffesaker når det gjelder rettsanmodninger om overvåking av telekommunikasjon, anbefaling nr. R (88) 2 om pirat-

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 particular 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;

virksomhet knyttet til opphavsrett og beslektede rettigheter, anbefaling nr. R (87) 15 om regulering av bruk av personopplysninger innenfor politisektoren, anbefaling nr. R (95) 4 om beskyttelse av personopplysninger innenfor telekommunikasjonstjenester, særlig telefontjenester, samt anbefaling nr. R (89) 9 om kriminalitet knyttet til datamaskiner, som gir retningslinjer for definering av visse typer datakriminalitet i nasjonal rett, og anbefaling nr. R (95) 13 om problemer i straffeprosesslovgivningen knyttet til informasjonsteknologi,

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;

som viser til resolusjon nr. 1 vedtatt av de europeiske justisministrene under deres 21. konferanse (Praha, juni 1997), som anbefalte Ministerkomiteen å støtte arbeidet med datakriminalitet i Den europeiske komité for kriminalspørsmål (CDPC) for å få til en tilnærming av bestemmelsene i de ulike nasjonale straffelovgivninger, samt tillate bruk av effektive midler i etterforskning av slike straffbare handlinger, samt resolusjon nr. 3, vedtatt under de europeiske justisministrenes 23. konferanse (London, juni 2000), som oppfordret forhandlingspartene til å fortsette arbeidet for å finne egnede løsninger, slik at et størst mulig antall stater kan bli part i konvensjonen, og som erkjente behovet for en rask og effektiv internasjonal samarbeidsordning, der det tas behørig hensyn til de særlige krav som stilles i kampen mot datakriminalitet,

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;

som også tar i betraktning handlingsplanen vedtatt av Europarådets stats- og regjeringssjefer under deres annet toppmøte (Strasbourg, 10. og 11. oktober 1997), for å finne fram til felles mottiltak basert på Europarådets normer og verdier for å møte utviklingen av ny informasjonsteknologi,

Have agreed as follows:

er blitt enige om følgende:

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;

Kapittel I – Termbruk

Artikkel 1 – Definisjoner

I forbindelse med denne konvensjon betyr:

a) «datasystemer»: enhver innretning eller gruppe innretninger som er koplet sammen eller som hører sammen, hvorav en eller flere utfører programmert, automatisk behandling av data,
b) «elektroniske data»: enhver framstilling av fakta, informasjon eller begrep i en form som er egnet for behandling i et datasystem, herunder et program som kan få et datasystem til å utføre en funksjon,

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;

c) «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.

c) «tjenesteyter»:
   i. en offentlig eller privat virksomhet som gir brukere av sine tjenester muligheten til å kommunisere ved hjelp av et datasystem, og
   ii. enhver annen virksomhet som behandler eller lagrer elektroniske data på vegne av en slik kommunikasjonstjeneste eller brukere av slike tjenester.

d) «trafikkdata»: alle elektroniske data knyttet til en kommunikasjon via et datasystem som er blitt produsert av et datasystem som inngikk i kommunikasjonskjeden, og som angir kommunikasjonens opphavssted, bestemmelsessted, rute, klokkeslett, dato, omfang, varighet eller type underliggende tjeneste.

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,

Kapittel II – Tiltak som skal iverksettes nasjonalt

Avsnitt 1 – Materiell strafferett

Del 1 – Straffbare handlinger som rammer datasystemers og dataenes fortrolige karakter, integritet og tilgjengelighet

Artikkel 2 – Ulovlig tilgang

Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå forsettlig, urettmessig tilgang til hele eller deler av et datasystem som straffbar handling etter nasjonal rett. En part kan stille som vilkår at den straffbare handlingen er begått ved brudd på sikkerhetstiltak i den hensikt å få tak i elektroniske data eller i annen uredelig hensikt, eller i forbindelse med et datasystem som er knyttet til et annet datasystem.

Artikkel 3 – Ulovlig oppfanging av data

Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå som straffbar handling etter nasjonal rett, forsettlig, urettmessig oppfanging av elektroniske data med tekniske midler i forbindelse med ikke offentlig tilgjengelige overføringer til, fra eller innenfor et datasystem, herunder elektromagnetisk stråling fra datasystemer som inneholder slike elektroniske data. En part kan stille som vilkår at den straffbare handlingen er begått med uredelig hensikt, eller i forbindelse med et datasystem som er knyttet til et annet datasystem.

Artikkel 4 – Inngrep i dataenes integritet

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå forsettlig ødeleggelse, sletting, forringelse, en-

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.

dring eller fjerning av elektroniske data som straffbare handlinger etter nasjonal rett.

2. En part kan forbeholde seg retten til å stille som vilkår at handlingen beskrevet i nr. 1 medfører alvorlig skade.

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.

Artikkel 5 – Inngrep i driften av et datasystem

Hver part skal vedta de lover og andre tiltak som er nødvendige for å fastslå at følgende forsettlige, urettmessige og alvorlige handlinger, som forhindrer et datasystems drift, er straffbare handlinger etter nasjonal rett: tilførsel, overføring, ødeleggelse, sletting, forringelse og endring eller fjerning av 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.

Artikkel 6 – Misbruk av innretninger og tilgangsdata

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå følgende forsettlige og urettmessige handlinger som straffbare handlinger etter nasjonal rett:
   a) produksjon, salg, erverv for bruk, import, distribusjon eller tilgjengeliggjøring på annen måte av:
      i. en innretning, herunder et dataprogram, utviklet eller tilpasset hovedsakelig i den hensikt å begå en av de straffbare handlingene fastslått i samsvar med artikkel 2 til 5,
      ii. et passord, adgangskode eller liknende data som gir tilgang til hele eller deler av et datasystem,

      i den hensikt å bruke det til å begå en av de straffbare handlingene fastslått i artikkel 2 til 5, og
   b) besittelse av utstyr og adgangskoder omhandlet i bokstav a) i) eller ii) ovenfor i den hensikt å bruke det for å begå de straffbare handlingene fastslått i artikkel 2 til 5. En part kan i sin nasjonale rett stille vilkår om besittelse av slikt utstyr eller slike adgangskoder i et visst omfang før det får strafferettslige følger.
2. Denne artikkel skal ikke tolkes slik at produksjon, salg, erverv for bruk, import, distribusjon eller tilgjengeliggjøring på annen måte eller besittelse omhandlet i nr. 1 i denne artikkel medfører strafferettslig ansvar når det ikke skjer i den hensikt å begå en straffbar handling fastslått i samsvar med artikkel 2 til 5 i denne konvensjon, som autorisert testing og beskyttelse av et datasystem.

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.

3. Hver part kan forbeholde seg retten til ikke å anvende nr. 1 i denne artikkel, forutsatt at forbeholdet ikke gjelder salg, distribusjon eller tilgjengeliggjøring på annen måte av utstyret og adgangskodene omhandlet i nr. 1 bokstav a) ii).

Title 2 – Computer-related offences

Del 2 – Straffbare handlinger knyttet til datamaskiner

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.

Artikkel 7 – Datarelatert falsk

Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå som straffbare handlinger etter nasjonal rett, forsettlig, urettmessig tilførsel, endring, sletting eller fjerning av elektroniske data som fører til ugyldige data, i den hensikt at de skal anses som eller brukes i rettslig sammenheng som om de var ekte, enten de er direkte lesbare og forståelige eller ikke. En part kan stille som vilkår at det må foreligge svikaktig eller annen uredelig hensikt før straffansvar pådras.

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.

Artikkel 8 – Datarelatert bedrageri

Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå som straffbare handlinger etter nasjonal rett, forsettlige, urettmessige handlinger som påfører andre tap av eiendom gjennom:

a) innlegging, endring, sletting eller utilgjengeliggjøring av elektroniske data,
b) inngrep som forstyrrer et datasystems drift,

i den svikaktige eller uredelige hensikt å skaffe seg selv eller andre urettmessig økonomisk vinning.

Title 3 – Content-related offences

Del 3 – Straffbare handlinger knyttet til innhold

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;

Artikkel 9 – Straffbare handlinger knyttet til barnepornografi

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå følgende forsettlig og urettmessig aktivitet som straffbar handling etter nasjonal rett:

   a) å produsere barnepornografi for distribusjon via et datasystem,

   b) å tilby eller gjøre barnepornografi tilgjengelig via et datasystem,
   c) å distribuere eller formidle barnepornografi via et datasystem,

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.

d) å skaffe til veie barnepornografi til seg selv eller andre via et datasystem,
e) å være i besittelse av barnepornografi lagret i et datasystem eller på et annet datalagringsmedium.

2. Uttrykket «barnepornografi» i nr. 1 ovenfor skal omfatte pornografisk materiale som gir en visuell framstilling av:
a) en mindreårig som er involvert i eksplisitt seksuell aktivitet,
b) en person som ser ut som en mindreårig som er involvert i eksplisitt seksuell aktivitet,
c) realistiske bilder som framstiller en mindreårig som er involvert i eksplisitt seksuell aktivitet.

3. Uttrykket «mindreårig» i nr. 2 ovenfor skal omfatte alle personer under 18 år. En part kan imidlertid oppstille en lavere aldersgrense, som ikke skal være under 16 år.

4. Hver part kan forbeholde seg retten til ikke å anvende hele eller deler av nr. 1 d) og e), samt nr. 2 b) og 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 Organi-

Del 4 – Straffbare handlinger knyttet til krenkelser av opphavsrett og nærstående rettigheter

Artikkel 10 – Straffbare handlinger knyttet til krenkelse av opphavsrett og nærstående rettigheter

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å kunne fastslå som straffbar handling etter nasjonal rett, en krenkelse av opphavsretten slik den er definert i vedkommende parts rett i samsvar med de forpliktelser parten har påtatt seg etter Parisakten av 24. juli 1971 til Bernkonvensjonen for vern av litterære og kunstneriske verk, Avtalen om handelsrelaterte sider ved immaterielle rettigheter og WIPO-traktaten om opphavsrett, med unntak av enhver åndsrett fastsatt i disse konvensjonene, når slike handlinger begås med forsett, i et kommersielt omfang og ved hjelp av et datasystem.
2. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå som straffbar handling etter nasjonal rett, en krenkelse av nærstående rettigheter slik de er definert i vedkommende parts rett i samsvar med de forpliktelser parten har påtatt seg etter Den internasjonale konvensjon om vern for utøvende kunstnere, fonogramprodusenter og kring-

sations (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;

kastingsinstitusjoner (Romakonvensjonen), Avtalen om handelsrelaterte sider ved immaterielle rettigheter og WIPO-traktaten om kunstneriske framføringer og fonogrammer, med unntak av enhver åndsrett fastsatt i disse konvensjonene, når slike handlinger begås med forsett, i et kommersielt omfang og ved hjelp av et datasystem.

3. En part kan forbeholde seg retten til ikke å ilegge strafferettslig ansvar etter nr. 1 og 2 i begrensede tilfeller, forutsatt at det finnes andre effektive rettsmidler, og at slikt forbehold ikke innskrenker partens internasjonale forpliktelser i henhold til de internasjonale instrumentene nevnt i nr. 1 og 2 i denne artikkel.

Del 5 – Andre former for ansvar og straffereaksjoner

Artikkel 11 – Forsøk og medvirkning

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå som straffbar handling etter nasjonal rett, forsettlig medvirkning til en handling etter artikkel 2 til 10 i denne konvensjon når slik medvirkning skjer i den hensikt å begå slik handling.

2. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå som en straffbar handling etter nasjonal rett, forsettlig forsøk på å begå en av de straffbare handlingene omhandlet i artikkel 3 til 5, 7, 8, 9 nr. 1 a) og c) i denne konvensjonen

3. Hver part kan forbeholde seg retten til ikke å anvende i sin helhet eller delvis nr. 2 i denne artikkel.

Artikkel 12 – Juridiske personers ansvar

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å sikre at en juridisk person kan holdes ansvarlig for straffbare handlinger fastsatt i samsvar med denne konvensjon, som er begått til den juridiske personens fordel av en fysisk person som opptrer enten på egen hånd eller som en del av et organ tilhørende vedkommende juridiske person, og som har en ledende stilling i henhold til:
   a) fullmakt til å representere den juridiske personen,
   b) myndighet til å treffe beslutninger på vegne av den juridiske personen, eller

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.

c) myndighet til å utøve kontroll innenfor den juridiske personen,

2. I tillegg til de tilfeller som er fastsatt i nr. 1, skal hver part treffe nødvendige tiltak for å sikre at en juridisk person kan holdes ansvarlig dersom manglende tilsyn eller kontroll fra en fysisk persons side nevnt i nr. 1 har gjort det mulig å begå en straffbar handling fastsatt i samsvar med denne konvensjon til fordel for den juridiske personen.
3. Avhengig av partens rettsprinsipper, kan den juridiske personens ansvar være strafferettslig, sivilrettslig eller administrativt.
4. Slikt ansvar skal ikke berøre det strafferettslige ansvar som påhviler fysiske personer som har begått den straffbare handlingen.

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.

Artikkel 13 – Straffereaksjoner og tiltak

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å sikre at straffbare handlinger fastsatt i samsvar med artikkel 2 til 11 kan straffes med effektive, forholdsmessige og forebyggende straffereaksjoner, som også omfatter frihetsstraff.
2. Hver part skal sikre at juridiske personer som holdes ansvarlig i samsvar med artikkel 12, skal kunne straffes med effektive, forholdsmessige og avskrekkende straffereaksjoner eller ikke-strafferettslige sanksjoner, herunder økonomiske sanksjoner.

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.

Avsnitt 2. Prosesslovgivning

Del 1 – Felles bestemmelser

Artikkel 14 Prosessbestemmelsenes virkeområde

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å innføre de fullmakter og prosedyrer som er fastsatt i dette avsnittet med henblikk på en bestemt strafferettslig etterforskning eller forfølgning.
2. Med unntak for de tilfeller som er særskilt angitt i artikkel 21, skal hver part anvende fullmaktene og prosedyrene nevnt i nr. 1 i forbindelse med:
   a) straffbare handlinger fastsatt i samsvar med artikkel 2 til 11 i denne konvensjon,
   b) andre straffbare handlinger begått ved hjelp av et datasystem, og
   c) innhenting av elektroniske bevis for en straffbar handling.

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.

3. a) Hver part kan forbeholde seg retten til å anvende tiltakene nevnt i artikkel 20 bare for de straffbare handlingene eller kategoriene straffbare handlinger som er angitt i forbeholdet, forutsatt at spekteret av slike straffbare handlinger eller kategorier straffbare handlinger ikke er mer begrenset enn spekteret av straffbare handlinger som parten anvender tiltakene nevnt i artikkel 21 på. Hver part skal overveie å begrense et slikt forhold slik at tiltaket nevnt i artikkel 20 kan få videst mulig anvendelse.
   b) Når en part på grunn av begrensninger i sin lovgivning på det tidspunkt denne konvensjon blir vedtatt ikke er i stand til å anvende tiltakene nevnt i artikkel 20 og 21 for kommunikasjoner som overføres med et datasystem tilhørende en tjenesteyter,

      i. som drives til fordel for en lukket brukergruppe, og
      ii. som ikke bruker offentlige kommunikasjonsnett og ikke er tilknyttet et annet, verken offentlig eller privat datasystem,

   kan denne parten forbeholde seg retten til ikke å anvende disse tiltakene for slike kommunikasjoner. Hver part skal overveie å begrense et slikt forbehold slik at tiltakene nevnt i artikkel 20 og 21 kan få videst mulig anvendelse.

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.

Artikkel 15 – Vilkår og rettssikkerhetsgarantier

1. Hver part skal sikre at innføringen, iverksettelsen og anvendelsen av fullmaktene og prosedyrene fastsatt i dette avsnitt er underlagt vilkårene og rettssikkerhetsgarantiene fastsatt i partens nasjonale rett, som skal sikre tilstrekkelig beskyttelse av menneskerettighetene og frihetene, herunder rettighetene som følger av de forpliktelser parten har påtatt seg etter Europarådets konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter av 1950, De forente nasjoners internasjonale konvensjon om sivile og politiske rettigheter av 1966 og andre internasjonale menneskerettighetsinstrumenter, og som skal omfatte forholdsmessighetsprinsippet.
2. Dersom det er hensiktsmessig ut fra den berørte prosedyren eller fullmaktens karakter, skal slike vilkår og garantier blant annet omfatte rettslig og annet uavhengig tilsyn, grunner som rettferdiggjør anvendelse og begrensning av omfanget eller gyldighetstiden for slike fullmakter eller prosedyrer.

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

3. I den utstrekning det er forenlig med allmennhetens interesser, særlig forsvarlig rettspleie, skal en part vurdere hvilken virkning fullmaktene og prosedyrene i dette avsnittet vil få på tredjeparters rettigheter, ansvar og legitime interesser.

Del 2 – Hurtig sikring av lagrede, elektroniske data

Artikkel 16 – Hurtig sikring av lagrede, elektroniske data

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å gjøre sine kompetente myndigheter i stand til å beordre eller på annen måte sørge for hurtig sikring av nærmere angitte elektroniske data, herunder trafikkdata, som er blitt lagret i et datasystem, særlig når det er grunn til å tro at de elektroniske dataene er spesielt utsatt for tap eller endring.

2. Når en part iverksetter nr. 1 ovenfor ved å gi ordre til en person om å sikre nærmere angitte lagrede elektroniske data som denne personen har i sin besittelse eller har kontroll over, skal parten vedta slike lover og andre tiltak som eventuelt er nødvendige for å pålegge denne personen å sikre og beskytte disse dataenes integritet i det tidsrom som er nødvendig, inntil 90 dager maksimum, slik at de kompetente myndigheter skal ha mulighet til å be om at de utleveres. En part kan sørge for at et slikt pålegg siden forlenges.
3. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å pålegge den som oppbevarer dataene eller annen person som skal utføre sikring, taushetsplikt med hensyn til iverksettelsen av slike prosedyrer i det tidsrom som partens nasjonale rett gir hjemmel for.
4. Fullmaktene og prosedyrene omhandlet i denne artikkel skal være underlagt artikkel 14 og 15.

Artikkel 17 – Hurtig sikring og delvis utlevering av trafikkdata

1. Hver part skal med hensyn til trafikkdata som skal sikres i henhold til artikkel 16, vedta de lover og andre tiltak som eventuelt er nødvendige for å:
   a) sikre at slik hurtig sikring av trafikkdata er mulig uansett om en eller flere tjenesteytere var involvert i overføringen av den aktuelle kommunikasjon,

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.

b) sikre hurtig utlevering til partens kompetente myndighet eller til en person utpekt av denne myndighet av en tilstrekklig mengde data til at parten kan identifisere tjenesteyterne og kommunikasjonsruten.

2. Fullmaktene og prosedyrene omhandlet i denne artikkel skal være underlagt artikkel 14 og 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.

Del 3 – Pålegg om utlevering av data

Artikkel 18 – Pålegg om utlevering av data

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å gi sine kompetente myndigheter fullmakt til å pålegge:
   a) en person som befinner seg på dens territorium, å utlevere nærmere angitte elektroniske data som denne personen har i sin besittelse eller har kontroll over, og som ligger lagret i et datasystem eller på et datalagringsmedium, og
   b) en tjenesteyter som tilbyr sine tjenester på partens territorium, å framlegge abonnentopplysninger knyttet til slike tjenester som denne tjenesteyteren har i sin besittelse eller har kontroll over.
2. Fullmaktene og prosedyrene omhandlet i denne artikkel skal være underlagt artikkel 14 og 15.
3. «Abonnentopplysninger» i denne artikkel betyr enhver opplysning i form av elektroniske data eller annen form som en tjenesteyter har i sin besittelse og som gjelder abonnentene av slike tjenester, unntatt data som gjelder trafikk eller innhold som gjør det mulig å fastslå:

   a) hvilke type kommunikasjonstjeneste som er benyttet, hvilke tekniske tiltak som er truffet i den forbindelse og tjenestens varighet,
   b) abonnentens identitet, postadresse eller geografiske adresse, telefonnummer og andre numre for tilgang, opplysninger om fakturering og betaling som er tilgjengelige i henhold til inngått kontrakt eller ordning angående tjenesten,
   c) enhver annen opplysning på stedet der kommunikasjonsutstyret er installert, som er tilgjengelig i henhold til inngått kontrakt eller ordning angående tjenesten.

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.

Del 4 – Ransaking og beslag av lagrede, elektroniske data

Artikkel 19 – Ransaking og beslag av lagrede, elektroniske data

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å gi sine kompetente myndigheter fullmakt til å ransake eller på annen måte få tilgang til:
   a) et datasystem eller del av slikt datasystem, samt elektroniske data lagret i datasystemet, og
   b) datalagringsmedium der elektroniske data kan lagres,
   på partens territorium.
2. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å sikre at dets myndigheter, når de ransaker eller på annen måte får tilgang til et bestemt datasystem eller del av det i samsvar med nr. 1 a) og har grunn til å tro at de ettersøkte dataene er lagret i et annet datasystem eller del av det på sitt territorium, og disse data er lovlig tilgjengelige fra eller for det første systemet, har mulighet til raskt å utvide ransakingen eller annen tilgang til dette andre systemet.
3. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å gi sine kompetente myndigheter fullmakt til å beslaglegge eller på annen måte sikre elektroniske data som de har fått tilgang til i samsvar med nr. 1 eller 2. Disse tiltakene skal omfatte fullmakt til å:
   a) beslaglegge eller på annen måte sikre et datasystem eller del av det, eller et datalagringsmedium,
   b) lage eller beholde et kopi av disse elektroniske dataene,
   c) bevare de relevante, elektronisk lagrede dataenes integritet, og
   d) gjøre utilgjengelige eller fjerne disse elektroniske dataene i det aktuelle datasystem.
4. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å gi sine kompetente myndigheter fullmakt til å pålegge en person som har kjennskap til driften av et datasystem eller tiltak som anvendes for å beskytte de elektroniske data i systemet, i rimelig utstrekninig å gi de nødvendige opplysninger som gjør det mulig å iverksette tiltakene omhandlet i nr. 1 og 2.
5. Fullmaktene og prosedyrene omhandlet i denne artikkel skal være underlagt artikkel 14 og 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

Del 5 – Innhenting av elektroniske data i sanntid

Artikkel 20 – Innhenting av trafikkdata i sanntid

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å gi sine kompetente myndigheter fullmakt til å:
   a) innhente eller lagre ved hjelp av tekniske midler på denne partens territorium, og

   b) pålegge en tjenesteyter, så langt tjenesteyterens eksisterende tekniske midler tillater, å:
      i. innhente eller lagre ved hjelp av tekniske midler på denne partens territorium, eller
      ii. å samarbeide og hjelpe de kompetente myndigheter å innhente eller lagre.

   i sanntid trafikkdata som er knyttet til bestemte kommunikasjoner på partens territorium og som er overført ved hjelp av et datasystem.
2. Når en part som følge av etablerte prinsipper i sitt nasjonale rettssystem ikke kan innføre tiltakene omhandlet i nr. 1 a), kan den i stedet vedta de lover og andre tiltak som eventuelt er nødvendige for å sikre innhenting eller lagring i sanntid av trafikkdata knyttet til bestemte kommunikasjoner på sitt territorium ved hjelp av tekniske midler på dette territorium.

3. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å pålegge en tjenesteyter taushetsplikt med hensyn til iverksettelsen av tvangsmidlene fastsatt i denne artikkel, samt enhver opplysning i denne sammenheng.
4. Fullmaktene og prosedyrene omhandlet i denne artikkel skal være underlagt artikkel 14 og 15.

Artikkel 21 – Oppfanging av data knyttet til innhold

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å gi sine kompetente myndigheter fullmakt i forbindelse med et spekter av alvorlige straffbare handlinger som defineres i partens nasjonale rett, til i sanntid å:
   a) innhente eller lagre ved hjelp av tekniske midler på denne partens territorium, og
   b) pålegge en tjenesteyter, så langt tjenesteyterens eksisterende tekniske midler tillater, å:
      i. innhente eller lagre ved hjelp av tekniske midler på denne partens territorium, eller

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.

ii. samarbeide og hjelpe de kompetente myndigheter å innhente eller lagre

data knyttet til innholdet i bestemte kommunikasjoner på partens territorium, og som er overført ved hjelp av et datasystem.

2. Når en part som følge av etablerte prinsipper i sitt nasjonale rettssystem ikke kan innføre tiltakene omhandlet i nr. 1 a), kan den i stedet vedta de lover og andre tiltak som eventuelt er nødvendige for å sikre innhenting eller lagring i sanntid av data knyttet til innholdet i bestemte kommunikasjoner på sitt territorium ved hjelp av tekniske midler på dette territorium.
3. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å pålegge en tjenesteyter taushetsplikt med hensyn til iverksettelsen av fullmaktene fastsatt i denne artikkel, samt enhver opplysning i denne sammenheng.
4. Fullmaktene og prosedyrene omhandlet i denne artikkel skal være underlagt artikkel 14 og 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

Avsnitt 3 – Jurisdiksjon

Artikkel 22 – Jurisdiksjon

1. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å etablere jurisdiksjon med hensyn til enhver straffbar handling fastslått i samsvar med artikkel 2 til 11 i denne konvensjon, når den straffbare handlingen er begått:
   a) på denne partens territorium, eller
   b) om bord på et skip som fører denne partens flagg, eller
   c) om bord på et luftfartøy som er registrert etter denne partens rett, eller
   d) av en borger av denne part dersom handlingen kan straffes på det sted handlingen ble begått, eller dersom den straffbare handlingen er begått utenfor enhver stats territoriale jurisdiksjon.
2. Hver stat kan forbeholde seg retten til ikke å anvende eller til bare å anvende i bestemte tilfeller eller på bestemte vilkår reglene om jurisdiksjon fastsatt i nr. 1 b) til d) i denne artikkel eller deler av disse.
3. Hver part skal vedta de lover og andre tiltak som eventuelt er nødvendige for å fastslå jurisdiksjon med hensyn til de straffbare handlingene omhandlet i artikkel 24 nr. 1 i denne konvensjon, når den antatte gjerningsmann befinner seg på partens territorium og parten ikke utle-

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.

verer vedkommende til en annen part utelukkende av hensyn til vedkommendes nasjonalitet, etter en anmodning om utlevering.

4. Denne konvensjon utelukker ikke strafferettslig jurisdiksjon som utøves i samsvar med nasjonal rett.
5. Når mer enn en part gjør krav på jurisdiksjon med hensyn til en påstått straffbar handling fastslått i samsvar med denne konvensjon, skal de berørte parter, når det er hensiktsmessig, rådføre seg med hverandre for å bestemme hvilken jurisdiksjon som er best egnet til å gjennomføre rettsforfølgningen.

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.

Kapittel III – Internasjonalt samarbeid

Avsnitt 1 – Generelle prinsipper

Del 1 – Generelle prinsipper angående internasjonalt samarbeid

Artikkel 23 – Generelle prinsipper angående internasjonalt samarbeid

Partene skal samarbeide i samsvar med bestemmelsene i dette kapittel og ved å anvende de relevante internasjonale instrumentene om internasjonalt samarbeid i straffesaker, ordninger basert på felles eller gjensidig lovgivning og nasjonal rett, i størst mulig utstrekning med henblikk på etterforskning eller forfølgning av straffbare handlinger knyttet til datasystemer og data, eller for innhenting av elektroniske bevis for en straffbar handling.

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

Del 2 – Prinsipper angående utlevering

Artikkel 24 – Utlevering

1. a) Denne artikkel gjelder utlevering mellom partene som følge av straffbare handlinger fastslått i samsvar med artikkel 2 til 11 i denne konvensjon, forutsatt at de etter begge de berørte partenes rett kan straffes med en maksimum frihetsstraff på minst ett år, eller med en strengere straff.

   b) Dersom det kreves en annen minimumsstraff i henhold til en ordning basert på en felles eller gjensidig lovgivning eller en utleveringsavtale, herunder Den europeiske konvensjon om utlevering (ETS nr. 24), inngått mellom to eller flere parter, skal minstestraffen fastsatt i et slik ordning eller avtale få anvendelse.
2. De straffbare handlingene beskrevet i nr. 1 i denne artikkel skal anses å inngå blant de straff-

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.

bare handlinger som gir grunnlag for utlevering i enhver eksisterende utleveringsavtale mellom to eller flere parter. Partene forplikter seg til å inkludere slike straffbare handlinger blant straffbare handlinger som gir grunnlag for utlevering i enhver utleveringsavtale som vil bli inngått mellom to eller flere parter.

3. Dersom en part som stiller som vilkår for utlevering at det foreligger en avtale, mottar en anmodning om utlevering fra en annen part som den ikke har noen utleveringsavtale med, kan den betrakte denne konvensjon som rettslig grunnlag for utlevering for straffbare handlinger nevnt i nr. 1 i denne artikkel.
4. Parter som ikke stiller som vilkår for utlevering at det foreligger en avtale, skal anerkjenne de straffbare handlingene nevnt i nr. 1 i denne artikkel som straffbare handlinger som gir grunnlag for utlevering mellom dem.
5. Utlevering skal skje på de vilkår som er fastsatt i den anmodede parts rett eller i gjeldende utleveringsavtaler, herunder de grunner den anmodede part kan påberope seg for å avslå utlevering.
6. Dersom utlevering for en straffbar handling nevnt i nr. 1 i denne artikkel avslås utelukkende på grunnlag av den ettersøkte personens nasjonalitet, eller fordi den anmodede part mener at den har jurisdiksjon med hensyn til den straffbare handlingen, skal den anmodede part, etter anmodning fra den anmodende part, forelegge saken for sine kompetente myndigheter med henblikk på rettslig forfølgning, og skal innen rimelig tid avgi rapport om det endelige resultatet til den anmodende part. Disse myndighetene skal treffe sin avgjørelse og utføre sin etterforskning og rettslige forfølgning på samme måte som ved enhver annen straffbar handling av tilsvarende karakter etter denne partens rett.
7. a) Hver part skal ved undertegning eller ved deponering av sitt ratifikasjons-, godtakelses-, godkjennings- eller tiltredelsesdokument meddele Europarådets generalsekretær navnet og adressen på hver myndighet som har ansvaret for å oversende eller motta en anmodning om utlevering eller midlertidig pågripelse dersom det ikke foreligger noen avtale.
   b) Europarådets generalsekretær skal sette opp og holde oppdatert et register over myndigheter som slik er utpekt av partene. Hver part skal sikre at opplysningene i registeret til enhver tid er riktige.

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 anot-

Del 3 – Generelle prinsipper angående gjensidig hjelp

Artikkel 25 – Generelle prinsipper angående gjensidig hjelp

1. Partene skal gi hverandre gjensidig hjelp i størst mulig utstrekning i forbindelse med etterforskning eller rettslig forfølgning av straffbare handlinger knyttet til datasystemer og data, eller med innhenting av elektroniske bevis for en straffbar handling.
2. Hver part kan også vedta de lover og andre tiltak som eventuelt er nødvendige for å gjennomføre forpliktelsene fastsatt i artikkel 27 til 35.
3. Hver part kan i hastetilfeller sende anmodninger om gjensidig hjelp eller meddelelser om slik hjelp ved hjelp av raske kommunikasjonsmidler, herunder faks eller e-post, i den utstrekning slike midler gir tilstrekkelig sikkerhet og autentifisering (herunder bruk av kryptering der det er nødvendig), med ettersendelse av formell bekreftelse dersom den anmodede part krever det. Den anmodede part skal godta og besvare anmodningen som oversendes med slike raske kommunikasjonsmidler.
4. Unntatt når annet er spesielt angitt i artiklene i dette kapittel, skal gjensidig hjelp være underlagt vilkårene fastsatt i den anmodede parts rett eller i gjeldende avtaler om gjensidig hjelp, herunder de grunner den anmodede part eventuelt påberoper seg for å avslå samarbeid. Den anmodede part skal ikke bruke retten til å avslå gjensidig hjelp i forbindelse med de straffbare handlingene nevnt i artikkel 2 til 11 utelukkende på grunnlag av at anmodningen gjelder en straffbar handling som den anser som en fiskal forbrytelse.
5. Dersom den anmodede part i samsvar med bestemmelsene i dette kapittel har adgang til å stille som vilkår for gjensidig hjelp at det foreligger dobbel straffbarhet, skal dette vilkåret anses oppfylt, uansett om partens lover plasserer den straffbare handlingen i samme kategori straffbare handlinger eller bruker samme betegnelse for den straffbare handlingen som den anmodende part eller ikke, dersom atferden som ligger til grunn for forbrytelsen som det søkes om hjelp for, er en straffbar handling etter denne partens lover.

Artikkel 26 – Uoppfordret formidling av opplysninger

1. En part kan i den grad nasjonal rett tillater og uten å ha mottatt anmodning om det på forhånd

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

oversende en annen part opplysninger den har mottatt i forbindelse med egen etterforskning når den mener at kjennskap til slike opplysninger kan hjelpe mottakerparten med å innlede eller gjennomføre etterforskning eller rettslig forfølgning av straffbare handlinger etter denne konvensjon, eller kan føre til, en anmodning fra den andre parten om samarbeid i henhold dette kapittel.

2. Parten som oversender slike opplysninger, kan før oversendelse kreve at opplysningene skal behandles fortrolig eller bare brukes på bestemte vilkår. Dersom mottakerparten ikke kan etterkomme en slik anmodning, skal den underrette parten som oversender opplysningene, som så skal avgjøre om opplysningene likevel bør oversendes. Dersom mottakerparten mottar opplysningene på bestemte vilkår, skal den være bundet av vilkårene.

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

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

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation 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 regis-

Del 4 – Framgangsmåter ved anmodning om gjensidig bistand når det ikke foreligger gjeldende internasjonale avtaler

Artikkel 27 – Framgangsmåter ved anmodning om gjensidig hjelp når det ikke foreligger gjeldende internasjonale avtaler

1. Dersom det ikke foreligger noen avtale eller ordning om gjensidig bistand basert på gjeldende felles eller gjensidig lovgivning mellom den anmodende og den anmodede part, skal bestemmelsene i nr. 2 til 10 i denne artikkel gjelde. Bestemmelsene i denne artikkel får ikke anvendelse når en slik avtale, ordning eller lovgivning finnes, med mindre de berørte partene bestemmer å anvende i stedet hele eller deler av resten av denne artikkel.
2. a) Hver part skal utpeke en sentral myndighet eller sentrale myndigheter som skal ha ansvaret for å oversende og svare på anmodninger om gjensidig bistand, å gjennomføre slike anmodninger, eller videreformidle dem til de kompetente myndigheter for gjennomføring.

   b) De sentrale myndigheter skal kommunisere med hverandre direkte.

   c) Hver part skal ved undertegning eller ved deponering av sitt ratifikasjons-, godtakelses-, godkjennelses- eller tiltredelsesdokument meddele Europarådets generalsekretær navnet og adressen til myndighetene utpekt i henhold til dette nummer.

   d) Europarådets generalsekretær skal sette opp og holde oppdatert et register over sen-

ter 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,

trale myndigheter som er utpekt av partene. Hver part skal sikre at opplysningene i registeret til enhver tid er riktige.

3. Anmodninger om gjensidig bistand etter denne artikkel skal gjennomføres i samsvar med framgangsmåtene angitt av den anmodende part, unntatt når de er uforenlige med den anmodede parts rett.
4. I tillegg til grunnene for avslag fastsatt i artikkel 25 nr. 4, kan den anmodede part avslå bistand dersom:
   a) anmodningen gjelder en straffbar handling som den anmodede part anser som en straffbar handling av politisk karakter eller knyttet til en straffbar handling av politisk karakter, eller
   b) den mener at gjennomføringen av en anmodning vil kunne krenke dens suverenitet, sikkerhet, *ordre public* eller andre vesentlige interesser.
5. Den anmodede part kan utsette iverksettelsen av skritt i henhold til en anmodning dersom dette kan skade etterforskningen eller den rettslige forfølgningen iverksatt av dens myndigheter.
6. Den anmodede part skal før den avslår eller utsetter sin hjelp og eventuelt etter å ha rådført seg med den anmodende part, vurdere om anmodningen kan etterkommes delvis eller på de vilkår den anser nødvendig.

7. Den anmodede part skal straks underrette den anmodende part om utfallet av gjennomføringen av en anmodning om hjelp. Dersom anmodningen avslås eller utsettes, skal grunnene til slikt avslag eller slik utsettelse oppgis. Den anmodede part skal også informere den anmodende part om eventuelle grunner som gjør det umulig å gjennomføre anmodningen eller som kan forsinke gjennomføringen betraktelig.
8. Den anmodende part kan be den anmodede part om fortrolig behandling av og innhold i en anmodning framsatt i henhold til dette kapittel, unntatt i den utstrekning det er nødvendig for å gjennomføre anmodningen. Dersom den anmodede part ikke kan etterkomme kravet om fortrolig behandling, skal den umiddelbart underrette den anmodende part, som så skal avgjøre om anmodningen likevel bør etterkommes.
9. a) Dersom saken haster, kan anmodninger om gjensidig hjelp eller meddelelser knyttet til slike anmodninger oversendes av de judisielle myndigheter i den anmodende part direkte til de tilsvarende myndigheter i den anmodede part. I slike tilfeller skal en kopi

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 sub-paragraph 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.

samtidig oversendes til den sentrale myndighet i den anmodede part via den sentrale myndighet i den anmodende part.

b) En anmodning eller en meddelelse etter dette nummer kan framsettes gjennom Den internasjonale kriminalpolitiorganisasjonen (Interpol).

c) Når en anmodning framsettes i henhold til bokstav a) og myndigheten ikke er kompetent til å behandle anmodningen, skal den henvise anmodningen til den kompetente nasjonale myndighet og underrette den anmodende part direkte om dette.

d) Anmodninger eller meddelelser framsatt i henhold til dette nummer som ikke innebærer tvangstiltak, kan oversendes av de kompetente myndigheter i den anmodende part direkte til de kompetente myndigheter i den anmodede part.

e) Hver part kan ved undertegning eller ved deponering av sitt ratifikasjons-, godtakelses-, godkjennings- eller tiltredelsesdokument, meddele Europarådets generalsekretær at anmodninger framsatt i henhold til dette nummer, av effektivitetshensyn, skal rettes til dens sentrale myndighet.

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

Artikkel 28 – Fortrolig behandling og begrensing i bruk

1. Når det ikke foreligger noen avtale eller ordning om gjensidig hjelp basert på gjeldende felles eller gjensidig lovgivning mellom den anmodende og den anmodede part, skal bestemmelsene i denne artikkel gjelde. Bestemmelsene i denne artikkel får ikke anvendelse når en slik avtale, ordning eller lovgivning finnes, med mindre de berørte partene bestemmer å anvende i stedet hele eller deler av resten av denne artikkel.
2. Den anmodede part kan formidle opplysninger eller materiale som svar på en anmodning under den forutsetning av at slike opplysninger eller slikt materiale:
   a) behandles fortrolig når anmodningen om gjensidig hjelp ikke ville kunne etterkommes uten et slikt vilkår, eller
   b) ikke brukes til annen etterforskning eller rettslig forfølgning enn det som er angitt i anmodningen.
3. Dersom den anmodende part ikke kan oppfylle vilkåret nevnt i nr. 2, skal den omgående underrette den annen part, som så skal avgjøre om opplysningene likevel skal formidles. Når den

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.

anmodende part godtar vilkåret, skal den være bundet av det.

4. En part som formidler opplysninger eller materiale på et vilkår angitt i nr. 2, kan kreve at den annen part redegjør for bruken av slike opplysninger eller slikt materiale i forhold til det nevnte vilkår.

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

Avsnitt 2 – Særlige bestemmelser

Del 1 – Gjensidig bistand i forbindelse med midlertidige tiltak

Artikkel 29 – Hurtig sikring av lagrede, elektroniske data

1. En part kan anmode en annen part om å beordre eller på annen måte sørge for hurtig sikring av elektroniske data som er lagret i et datasystem på territoriet til denne annen part, og for hvilke den anmodende part akter å framsette en anmodning om gjensidig bistand med sikte på ransaking eller liknende tilgang, beslag eller liknende forvaring, eller avdekking av data.
2. En anmodning om sikring framsatt etter nr. 1 skal angi:
   a) myndigheten som ber om sikring,
   b) den straffbare handling som er gjenstand for etterforskning og rettslig forfølgning samt en kort beskrivelse av de faktiske forhold i saken,
   c) de lagrede elektroniske data som skal sikres og deres sammenheng med den straffbare handlingen,
   d) alle tilgjengelige opplysninger for å kunne identifisere administrator av de elektroniske data eller stedet der datasystemet er plassert,
   e) nødvendigheten av sikring, og
   f) at parten akter å framsette en anmodning om gjensidig bistand med henblikk på ransaking eller liknende tilgang, beslag eller liknende forvaring, eller avdekking av de lagrede elektroniske data.
3. Når den anmodede part mottar anmodningen fra den annen part, skal den treffe alle egnede tiltak for raskt å sikre de angitte data i samsvar med sin nasjonale rett. For å kunne etterkomme en slik anmodning skal dobbelt straffbart forhold ikke være et vilkår for å foreta slik sikring.
4. En part som stiller som vilkår at det foreligger dobbelt straffbart forhold for å etterkomme en anmodning om gjensidig bistand med sikte på ransaking eller liknende tilgang, beslag eller

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.

liknende forvaring, eller avdekking av data, kan for andre straffbare handlinger enn de som er fastslått i samsvar med artikkel 2 til 11 i denne konvensjon, forbeholde seg retten til å avslå en anmodning om sikring etter denne artikkel dersom den har grunn til å tro at vilkåret om dobbelt straffbart forhold ikke kan oppfylles på avdekkingstidspunktet.

5. For øvrig kan en anmodning om sikring bare avslås dersom:
   a) anmodningen gjelder en straffbar handling som den anmodede part anser som en straffbar handling av politisk karakter eller knyttet til en straffbar handling av politisk karakter, eller
   b) den anmodede part mener at gjennomføringen av anmodningen kan krenke dens suverenitet, sikkerhet, *ordre public* eller andre vesentlige interesser.
6. Dersom den anmodede part mener at sikring ikke er noen garanti for at dataene vil være tilgjengelige i framtiden eller at det vil true den fortrolige behandlingen under den anmodende partens etterforskning eller på annen måte kan skade den, skal den straks gi underretning om dette til den anmodende part, som så skal avgjøre om anmodningen likevel bør gjennomføres.
7. All sikring utført for å etterkomme anmodningen omhandlet i nr. 1, skal vare minst 60 dager, slik at den anmodende part skal ha mulighet til å framsette en anmodning om ransaking eller liknende tilgang, beslag eller liknende forvaring, eller avdekking av data. Etter at en slik anmodning er mottatt, skal sikringen av data fortsette i påvente av en avgjørelse angående anmodningen.

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

Artikkel 30 – Hurtig utlevering av sikrede trafikkdata

1. Dersom den anmodede part i løpet av gjennomføringen av en anmodning framsatt etter artikkel 29 om sikring av data knyttet til overføringen av en bestemt kommunikasjon oppdager at en tjenesteyter i en annen stat var involvert i overføringen av kommunikasjonen, skal den anmodede part raskt gi den anmodende part en tiltrekkelig mengde trafikkdata for å kunne identifisere vedkommende tjenesteyter og kommunikasjonsruten.
2. Utlevering av trafikkdata i henhold til nr. 1 kan bare avslås dersom:
   a) anmodningen gjelder en handling som den anmodede part anser som en straffbar hand-

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 com-

ling av politisk karakter eller knyttet til en straffbar handling av politisk karakter, eller

b) den anmodede part mener at gjennomføringen av anmodningen kan krenke dens suverenitet, sikkerhet, *ordre public* eller andre vesentlige interesser.

Del 2 Gjensidig hjelp med hensyn til etterforskningsmyndighet

Artikkel 31 – Gjensidig hjelp for å få tilgang til lagrede, elektroniske data

1. En part kan anmode en annen part om ransaking eller liknende tilgang, beslag eller liknende forvaring, eller avdekking av data som er lagret i et datasystem som befinner seg på den anmodede parts territorium, herunder data som er blitt sikret i henhold til artikkel 29.
2. Den anmodede part skal etterkomme anmodningen ved å anvende de internasjonale instrumentene, ordningene og lovgivningene nevnt i artikkel 23, og i samsvar med andre relevante bestemmelser i dette kapittel.
3. Anmodningen skal etterkommes omgående dersom:
   a) det er grunn til å tro at relevante data er spesielt utsatt for tap eller endring, eller
   b) instrumentene, ordningene og lovgivningene nevnt i nr. 2 inneholder annen bestemmelse om raskt samarbeid.

Artikkel 32 – Grenseoverskridende tilgang til lagrede, elektroniske data, med samtykke eller når de er offentlig tilgjengelige

En part kan uten å innhente tillatelse fra en annen part:

a) skaffe seg tilgang til offentlig tilgjengelige, lagrede data (åpne kilder), uansett hvor dataene befinner seg geografisk, eller
b) skaffe seg tilgang til eller motta via et datasystem på sitt territorium lagrede, elektroniske data som befinner seg i en annen stat, dersom parten innhenter lovlig og frivillig samtykke fra den person som har rettmessig myndighet til å avdekke data til parten via dette datasystemet.

Artikkel 33 – Gjensidig bistand i forbindelse med innhenting av trafikkdata i sanntid

1. Partene skal yte hverandre gjensidig bistand i forbindelse med innhenting av trafikkdata i sanntid som er knyttet til bestemte kommunikasjoner på deres territorium, og som er overført

puter 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.

ved hjelp av et datasystem. Med forbehold for nr. 2 skal bistanden reguleres av de vilkår og prosedyrer som er fastsatt i nasjonal rett.

2. Hver part skal i det minste yte slik bistand i tilfeller der det i tilsvarende saker nasjonalt ville være adgang til innhente trafikkdata i sanntid.

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.

Artikkel 34 – Gjensidig bistand i forbindelse med oppfanging av data knyttet til innhold

Partene skal yte hverandre gjensidig bistand i forbindelse med innhenting eller registering i sanntid av data knyttet til innholdet i bestemte kommunikasjoner overført ved hjelp av et datasystem, i den utstrekning det gis adgang til det etter deres gjeldende avtaler og nasjonale rett.

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.

Del 3 – 24/7 nettverk

Artikkel 35 – 24/7 nettverk

1. Hver part skal utpeke et kontaktpunkt som er tilgjengelig 24 timer i døgnet, 7 dager i uken for å sikre omgående hjelp til etterforskning eller rettslig forfølgning av straffbare handlinger forbundet med datasystemer og data, eller for innhenting av elektroniske bevis for straffbare handlinger. Slik hjelp skal omfatte tilrettelegging for eller, dersom partens nasjonale rett og praksis tillater det, direkte :
   a) formidling av tekniske råd,
   b) sikring av data i henhold til artikkel 29 og 30, og
   c) innhenting av bevis, juridisk rådgivning og lokalisering av mistenkte.
2. a) En parts kontaktpunkt skal ha mulighet til å kommunisere med en annen parts kontaktpunkt etter en hasteprosedyre.
   b) Dersom kontaktpunktet utpekt av en part ikke er en del av denne partens myndighet eller myndigheter som har ansvaret for internasjonal gjensidig bistand eller utlevering, skal kontaktpunktet påse at det er i stand til å samordne sitt arbeid med slik myndighet eller slike myndigheter etter en hasteprosedyre.
3. Hver part skal sørge for å ha tilgjengelig personell med nødvendig opplæring og utstyr for å lette nettverkets arbeid.

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, accep-

Kapittel IV – Sluttbestemmelser

Artikkel 36 – Undertegning og ikrafttredelse

1. Denne konvensjon skal være åpen for undertegning av Europarådets medlemsstater og ikke-medlemsstater som har deltatt i utarbeidelsen av konvensjonen.
2. Denne konvensjon skal ratifiseres, godtas eller godkjennes. Ratifikasjons-, godtakelses- eller godkjenningsdokumentene skal deponeres hos Europarådets generalsekretær.
3. Denne konvensjon skal tre i kraft den første dagen i måneden etter utløpet av et tidsrom på tre måneder regnet fra den dag fem stater, hvorav minst tre medlemsstater i Europarådet, har gitt sitt samtykke til å være bundet av konvensjonen i samsvar med bestemmelsene i nr. 1 og 2.
4. For en signatarstat som på et senere tidspunkt gir sitt samtykke til å være bundet av konvensjonen, skal konvensjonen tre i kraft den første dagen i måneden etter utløpet av et tidsrom på tre måneder regnet fra den dag den har gitt sitt samtykke til å være bundet av konvensjonen i samsvar med bestemmelsene i nr. 1 og 2.

Artikkel 37 – Tiltredelse

1. Etter at denne konvensjon er trådt i kraft, kan Europarådets ministerkomité etter å ha rådført seg med konvensjonsstatene og innhentet deres enstemmige samtykke, invitere en stat som ikke er medlem av Europarådet og som ikke har deltatt i utarbeidelsen av konvensjonen, til å tiltre denne konvensjon. Beslutningen skal treffes med det flertall som er fastsatt i artikkel 20 bokstav d) i Europarådets vedtekter, og ved enstemmighet blant representantene for de konvensjonsstater som har rett til å delta i ministerkomiteen.
2. For en stat som tiltrer konvensjonen etter nr. 1 ovenfor, skal den tre i kraft den første dag i måneden som følger etter utløpet av et tidsrom på tre måneder regnet fra den dag tiltredelsesdokumentet er deponert hos Europarådets generalsekretær.

Artikkel 38 – Territorial anvendelse

1. En stat kan ved undertegning eller deponering av sitt ratifikasjons-, godtakelses-, godkjen-

tance, 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.

nings- eller tiltredelsesdokument nærmere angi det eller de territorier som denne konvensjon får anvendelse på.

2. En stat kan på ethvert senere tidspunkt ved erklæring rettet til Europarådets generalsekretær utvide denne konvensjonens anvendelse til ethvert annet territorium som angis i erklæringen. For slikt territorium skal konvensjonen tre i kraft den første dag i måneden som følger etter utløpet av et tidsrom på tre måneder regnet fra den dag Generalsekretæren mottok slik erklæring.
3. En erklæring avgitt i henhold til de to foregående numre kan trekkes tilbake for et territorium angitt i slik erklæring ved underretning til Europarådets generalsekretær. Tilbaketrekkingen får virkning den første dagen i måneden som følger etter utløpet av et tidsrom på tre måneder regnet fra den dag Generalsekretæren mottok slik underretning.

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.

Artikkel 39 – Konvensjonens virkninger

1. Formålet med denne konvensjon er å utfylle eksisterende multilaterale eller bilaterale avtaler eller ordninger som får anvendelse mellom partene, herunder bestemmelsene i:
   - Den europeiske konvensjon om utlevering åpnet for undertegning i Paris 13. desember 1957 (ETS nr. 24),
   - Den europeiske konvensjon om gjensidig bistand i straffesaker åpnet for undertegning i Strasbourg 20. april 1959 (ETS nr. 30),
   - Tilleggsprotokoll til Den europeiske konvensjon om gjensidig bistand i straffesaker åpnet for undertegning i Strasbourg 17. mars 1978 (ETS nr. 99).
2. Dersom to eller flere parter allerede har inngått en avtale eller en traktat om spørsmål omhandlet i denne konvensjon eller på annen måte har etablert sine forbindelser i slike spørsmål, eller vil gjøre det i framtiden, skal de også ha rett til å anvende slik avtale eller traktat eller regulere slike forbindelser i samsvar med disse. Dersom partene imidlertid etablerer forbindelser som gjelder spørsmål omhandlet i denne konvensjon på annen måte enn det som er fastsatt i denne konvensjon, skal dette gjøres på en måte som ikke er uforenlig med denne konvensjonens mål og prinsipper.
3. Ingen bestemmelse i denne konvensjon skal berøre en parts øvrige rettigheter, restriksjoner, forpliktelser og ansvar.

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.

Artikkel 40 – Erklæringer

En stat kan ved undertegning eller ved deponering av sitt ratifikasjons-, godtakelses-, godkjennings eller tiltredelsesdokument og ved skriftlig underretning til Europarådets generalsekretær erklære at den benytter seg av adgangen til å stille tilleggsvilkårene fastsatt i artikkel 2, artikkel 3, artikkel 6 nr. 1 b), artikkel 7, artikkel 9 nr. 3 og artikkel 27 nr. 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.

Artikkel 41 – Forbundsstatsklausul

1. En forbundsstat kan forbeholde seg retten til å påta seg forpliktelser etter kapittel II i denne konvensjon i overensstemmelse med dens grunnleggende prinsipper som regulerer forholdet mellom dens sentrale regjering og delstatene eller andre liknende territoriale enheter, forutsatt at den fremdeles er i stand til å samarbeide etter kapittel III.
2. Når en forbundsstat framsetter et forbehold i henhold til nr. 1, kan den ikke anvende vilkårene i et slikt forbehold til å utelukke eller i vesentlig grad innskrenke sine forpliktelser til å sørge for tiltak fastsatt i kapittel II. Den skal i hovedsak sørge for å ha omfattende og effektive midler til rådighet for å håndheve de nevnte tiltakene.
3. Med hensyn til bestemmelser i denne konvensjon hvis anvendelse hører inn under jurisdiksjonen til en delstat eller liknende territorial enhet som etter forbundsstatens konstitusjonelle system ikke er forpliktet til å treffe lovtiltak, skal den føderale regjeringen informere de kompetente myndigheter i disse statene om de nevnte bestemmelser og gi sin positive uttalelse, samt oppmuntre dem til å treffe hensiktsmessige tiltak for å iverksette dem.

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.

Artikkel 42 – Forbehold

En stat kan ved undertegning eller ved deponering av sitt ratifikasjons-, godtakelses-, godkjennings- eller tiltredelsesdokument, erklære ved skriftlig underretning til Europarådets generalsekretær om at den ønsker å ta ett eller flere av forbeholdene fastsatt i artikkel 4 nr. 2, artikkel 6 nr. 3, artikkel 9 nr. 4, artikkel 10 nr. 3, artikkel 11 nr. 3, artikkel 14 nr. 3, artikkel 22 nr. 2, artikkel 29 nr. 4 og artikkel 41 nr. 1. Det kan ikke tas andre forbehold.

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).

Artikkel 43 – Status og tilbaketrekking av forbehold

1. En part som har tatt et forbehold i samsvar med artikkel 42, kan helt eller delvis trekke forbeholdet tilbake ved underretning til Europarådets generalsekretær. Tilbaketrekkingen får virkning den dag generalsekretæren mottar underretningen. Dersom det i underretningen er oppgitt at tilbaketrekkingen av et forbehold skal få virkning på en angitt dato, og denne dato inntreffer senere enn den dag generalsekretæren mottar underretningen, skal underretningen tre i kraft på en slik senere dato.
2. En part som har tatt et forbehold i samsvar med artikkel 42, skal trekke forbeholdet tilbake helt eller delvis så snart omstendighetene tillater det.
3. Europarådets generalsekretær kan regelmessig rette en forespørsel til partene som har tatt ett eller flere forbehold i samsvar med artikkel 42 om utsiktene for tilbaketrekking av disse forbehold.

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.

Artikkel 44 – Endringer

1. Enhver part kan foreslå endringer i denne konvensjon, og Europarådets generalsekretær skal oversende dem til Europarådets medlemsstater, til enhver ikke-medlemsstat som har deltatt i utarbeidelsen av denne konvensjon, samt til enhver stat som har tiltrådt eller som er blitt invitert til å tiltre konvensjonen i samsvar med bestemmelsene i artikkel 37.
2. Enhver endring som foreslås av en part, skal oversendes Europarådets komité for kriminalspørsmål (CDPC), som skal legge fram en uttalelse for Ministerkomiteen om endringsforslaget.
3. Ministerkomiteen skal behandle endringsforslaget og uttalelsen fra CDPC, og kan vedta endringen etter å ha rådført seg med ikke-medlemsstater som er part i denne konvensjon.
4. Den endringstekst som vedtas av Ministerkomiteen i samsvar med nr. 3 i denne artikkel, skal oversendes partene for godtakelse.
5. En endring som vedtas i samsvar med nr. 3 i denne artikkel, skal tre i kraft den trettiende dag etter at alle parter har underrettet generalsekretæren om at de godtar endringen.

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.

Artikkel 45 – Tvisteløsning

1. Europarådets komité for kriminalspørsmål (CDPC) skal holdes underrettet om tolkningen og anvendelsen av denne konvensjon.

2. Dersom det oppstår en tvist mellom partene om tolkningen eller anvendelsen av denne konvensjon, skal de søke å løse tvisten ved forhandling eller andre fredelige midler etter eget valg, herunder henvisning av tvisten til CDPC, til en voldgiftsrett hvis avgjørelser skal være bindende for partene, eller til Den internasjonale domstol, etter overenskomst mellom de berørte parter.

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.

Artikkel 46 – Konsultasjoner mellom partene

1. Partene skal etter behov regelmessig konsultere hverandre for å tilrettelegge for:
   a) effektiv bruk og gjennomføring av denne konvensjon, herunder påpeke problemer i denne forbindelse, samt følgene av en erklæring avgitt eller et forbehold framsatt i henhold til denne konvensjon,
   b) utveksling av opplysninger om rettslig, politisk eller teknologisk utvikling av betydning for datakriminalitet og innhenting av elektroniske bevis,
   c) vurdering av eventuelle tilføyelser eller endringer i konvensjonen.
2. Europarådets komité for kriminalspørsmål (CDPC) skal holdes løpende informert om resultatene av konsultasjoner omhandlet i nr. 1.

3. CDPC skal ved behov tilrettelegge for konsultasjoner omhandlet i nr. 1 og treffe de nødvendige tiltak for å bistå partene i deres anstrengelser for å utfylle eller endre konvensjonen. Senest tre år etter at denne konvensjon er trådt i kraft skal Europarådets komité for kriminalspørsmål (CDPC) i samarbeid med partene foreta en gjennomgang av alle bestemmelsene i konvensjonen og om nødvendig anbefale hensiktsmessige endringer.

4. Utgifter som påløper i forbindelse med gjennomføringen av bestemmelsene i nr. 1, skal, med mindre Europarådet påtar seg slike utgifter, bæres av partene på den måten de bestemmer.
5. Europarådets sekretariat skal bistå partene i forbindelse med utføringen av deres oppgaver i henhold til denne artikkel.

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.

Artikkel 47 – Oppsigelse

1. En part kan til enhver tid si opp denne konvensjon ved underretning til Europarådets generalsekretær.
2. Slik oppsigelse får virkning den første dag i måneden etter utløpet av et tidsrom på tre måneder regnet fra den dag Generalsekretæren mottok underretningen.

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.

Artikkel 48 – Underretninger

Europarådets generalsekretær skal underrette Europarådets medlemsstater, de ikke-medlemsstatene som har deltatt i utarbeidelsen av denne konvensjon, samt enhver stat som har tiltrådt eller som er blitt invitert til å tiltre konvensjonen, om:

a) enhver undertegning
b) deponering av ethvert ratifikasjons-, godtakelses-, godkjennings- eller tiltredelsesdokument,
c) enhver ikrafttredelsesdato for denne konvensjon i samsvar med artikkel 36 og 37,
d) enhver erklæring avgitt i henhold til artikkel 40 eller forbehold tatt i samsvar med artikkel 42,
e) enhver annen handling, underretning eller meddelelse som gjelder denne konvensjon.

Til bekreftelse på dette har de undertegnede, som har fått behørig fullmakt til det, undertegnet denne konvensjon.

Utferdiget i Budapest, den 23. november 2001 på engelsk og fransk, med samme gyldighet for begge tekster, i ett eksemplar som skal deponeres i Europarådets arkiver. Europarådets generalsekretær skal oversende bekreftede kopier til hver medlemsstat i Europarådet, til de ikke-medlemsstater som har deltatt i utarbeidelsen av denne konvensjon, og til enhver stat som er blitt invitert til å tiltre konvensjonen.