RP 153/2006 rd

Regeringens proposition till Riksdagen med förslag om godkännande av Europarådets konvention om IT-relaterad brottslighet samt till lagar om sättande i kraft av de bestämmelser i konventionen som hör till området för lagstiftningen och om ändring av strafflagen, 4 kap. i tvångsmedelslagen, 27 och 28 § i förundersökningslagen och 15 och 23 § i lagen om internationell rättshjälp i straffrättsliga ärenden

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås att riksdagen godkänner den i Budapest den 23 november 2001 ingångna Europarådskonventionen om IT-relaterad brottslighet samt ger sitt samtycke till att vissa förklaringar och förbehåll görs med stöd av konventionen. Konventionen trädde i kraft internationellt den 1 juli 2004.

Samtidigt ändras lagstiftningen i överensstämmelse med kraven i rådets rambeslut 2005/222/RIF om angrepp mot informationssystem. Rambeslutet innehåller bestämmelser om samma frågor som konventionen.

I propositionen ingår ett förslag till lag om sättande i kraft av de bestämmelser i konventionen som hör till området för lagstiftningen.

I propositionen föreslås dessutom att i strafflagen, tvångsmedelslagen, förundersökningslagen och lagen om internationell rättshjälp i straffrättsliga ärenden görs de ändringar som föranleds av ikraftsättandet av konventionen och av genomförandet av rambeslutet samt en del ändringar som preciserar den gällande lagstiftningen. Enligt förslaget fogas till strafflagen nya straffbestämmelser om systemstörning, grov systemstörning och innehav av hjälpmedel vid nätbrott. Det föreslås också att i strafflagen tas in en bestämmelse om grovt dataintrång och att maximistraffet för skadegörelse höjs så som förutsätts i rådets rambeslut. När det gäller spridning av hjälpmedel vid nätbrott utvidgas den gällande regleringen till att omfatta förutom datavirus och andra motsvarande skadliga program också hjälpmedel och utrustning som används vid dataintrång. Försök till vissa av de brott som avses i konventionen kriminaliseras. Det föreslås att juridiska personers ansvar utvidgas så som konventionen förutsätter.

I tvångsmedelslagen föreslås nya bestämmelser om ett föreläggande att säkra data och en skyldighet för innehavare av informationssystem att lämna uppgifter. Till förundersökningslagen fogas en bestämmelse om skyldighet för ett vittne att vid förundersökningen lägga fram handlingar och annat bevismaterial som vittnet har i sin besittning. I lagen om internationell rättshjälp i straffrättsliga ärenden görs en ändring enligt vilken dubbel straffbarhet inte är ett krav för en begäran om rättslig hjälp som gäller ett föreläggande att säkra data. Dessutom föreslås i propositionen en del andra mindre ändringar som främst är av teknisk natur.

De föreslagna lagändringarna avses träda i kraft så snart som möjligt efter det att de har blivit stadfästa. Lagen om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i konventionen om IT-relaterad brottslighet avses dock träda i kraft samtidigt som konventionen träder i kraft för Finlands del, vid en tidpunkt som bestäms genom förordning av republikens president.

293278

INNEHÅLLFÖRTECKNING

ALLMÄN MOTIVERING

1. Inledning

Syftet med propositionen är att i Finland nationellt sätta i kraft den i Budapest den 23 november 2001 ingångna Europarådskonventionen om IT-relaterad brottslighet (ETS 185), nedan konventionen eller nätbrottskonventionen. Samtidigt ändras lagstiftningen så att den uppfyller kraven i Europeiska unionens råds rambeslut av den 24 februari 2005 om angrepp mot informationssystem (2005/222/RIF, EUT L 69/67, 16.3.2005), nedan rambeslutet. Rambeslutet innehåller bestämmelser om samma frågor som konventionen.

Med termen IT-relaterad brottslighet i konventionens namn avses detsamma som databrott. Med databrott avses dels brott som riktar sig mot informationssystem, dels brott som begås med hjälp av informationssystem. Gemensamt för dessa två brottstyper är således att de begås i en informationssystemmiljö och att brottens begående i allmänhet förutsätter något slags sakkunskap om hur dessa system fungerar.

Databrottsligheten orsakar stora ekonomiska skador. De samhälleliga grundfunktionerna är beroende av att informationssystemen och datanäten fungerar störningsfritt. Databrottsligheten orsakar därför också andra allvarliga skador än enbart de ekonomiska. Ett utmärkande drag för denna brottslighet är att den inte låter sig hejdas av gränser mellan länder. Dessa brott är svåra och ibland t.o.m. omöjliga att utreda utan internationellt samarbete.

I allmänhet finns bevismaterialet i dessa fall nästan enbart i elektronisk form. Det går synnerligen lätt att ändra eller utplåna materialet. Det är därför av avgörande betydelse att undersökningsåtgärderna kan vidtas snabbt. Av samma orsaker bör även ett snabbt internationellt samarbete vara möjligt.

Nätbrottskonventionen är den första konventionen som gäller databrott. Syftet med konventionen och det nationella ikraftsättandet av den är att förenhetliga och utvidga de straffbestämmelser som gäller denna typ av brottslighet samt effektivera utredningen av brott och det internationella rättsliga samarbetet så att samhället kan skyddas mot dessa brott och de skador de orsakar.

Konventionen har undertecknats av Europarådets medlemsstater och dessutom av Kanada, Japan, Sydafrika och Förenta staterna. Även andra stater kan senare tillträda konventionen. Meningen är inte att konventionen skall vara heltäckande och helt fristående, utan syftet med den är att komplettera de redan befintliga konventionerna med bestämmelser om databrott och utredning av dessa brott. Med tanke på konventionens syften är det viktigt att så många stater som möjligt tillträder den. Konventionen trädde i kraft internationellt den 1 juli 2004.

Konventionen har bifogats denna proposition. Europarådets ministerkommitté antog dessutom den 8 november 2001 en förklarande rapport till konventionen, nedan den förklarande rapporten. Innehållet i den förklarande rapporten behandlas i motiveringen till de enskilda artiklarna i propositionen. Det bör noteras att tolkningsrekommendationerna i den förklarande rapporten inte är bindande. Vid beredningen av propositionen har man i datatekniska frågor använt sig av populariserade framställningar inom området (se Tietoturva & Yksityisyys, Petteri Järvinen, Borgå 2002 med källor).

2. Nuläge

2.1. Inledning

Den gällande lagstiftningen och dess förhållande till konventionen behandlas i allt väsentligt i motiveringen till de olika artiklarna i propositionen i fråga om strafflagen, tvångsmedelslagen och förundersökningslagen. Det är därför inte ändamålsenligt att gå in på dem i detta avsnitt.

Den internationella rättsliga hjälpen samt utlämningen för brott och den internationella rättsliga hjälpen i brottmål grundar sig i Finland på ett flertal parallella bestämmelser och internationella avtal. För att ge en helhetsbild

av saken behandlas regleringssystemen i det följande på ett mera allmänt plan. Dessutom innehåller motiveringen till respektive artikel en redogörelse för de gällande bestämmelserna i fråga om den.

2.2. Utlämning för brott

2.2.1. Lagstiftning

Utlämning för brott regleras i Finland både i den nationella lagstiftningen och i internationella överenskommelser. I Finland gäller en allmän lag om utlämning för brott samt speciallagar om utlämning för brott mellan de nordiska länderna och mellan EU:s medlemsstater. Finland är part i ett flertal konventioner om utlämning för brott och även i bilaterala fördrag.

Den allmänna lagen som reglerar utlämning av förbrytare är lagen om utlämning för brott (456/1970, nedan utlämningslagen). Merparten av bestämmelserna i lagen avser utlämning från Finland. Lagen innehåller endast några få bestämmelser om förfarandet vid utlämning till Finland. Vid utlämning från en annan stat till Finland iakttas lagstiftningen i den stat från vilken utlämning sker och de avtal som gäller saken.

Enligt utlämningslagen kan utlämning från Finland komma i fråga trots att det inte finns något avtal om utlämning. I praktiken iakttas reciprocitetsprincipen i utlämningsärenden trots att lagen inte uttryckligen förutsätter detta. En förutsättning för att utlämning från Finland skall kunna ske är i allmänhet att maximistraffet för brottet i Finland är minst ett års fängelse. Efter att EU:s råd den 13 juni 2002 antog rambeslutet om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna (EGT L 190, 18.7.2002, s. 1) har situationen mellan EU:s medlemsstater dock förändrats. Det finns inte längre några krav gällande straffets maximilängd.

Det sistnämnda rambeslutet har i Finland satts i kraft genom lagen om utlämning för brott mellan Finland och de övriga medlemsstaterna i Europeiska unionen (1286/2003). I lagens 2 och 3 § bestäms om de allmänna förutsättningarna för utlämning. I 2 § förutsätts det att den gärning som ligger till grund för framställningen om utlämning utgör brott enligt finsk lag och att det strängaste straffet för gärningen enligt den ansökande medlemsstatens lagstiftning är ett frihetsstraff på minst ett år. Enligt 3 § 1 mom. skall utlämning beviljas oberoende av om den gärning som ligger till grund för framställningen utgör brott enligt finsk lag eller inte, om gärningen enligt den ansökande medlemsstatens lagstiftning är en sådan gärning som avses i 2 mom. i samma paragraf och det strängaste straffet för gärningen enligt lagstiftningen i medlemsstaten i fråga är ett frihetsstraff på minst tre år. Paragrafens 2 mom. innehåller en förteckning över 32 brott och brottstyper. Förteckningen upptar även IT-brottslighet.

I fråga om utlämning mellan Finland och de övriga nordiska länderna gäller lagen om utlämning för brott Finland och de övriga nordiska länderna emellan (270/1960), nedan den nordiska utlämningslagen. Den nordiska utlämningslagen grundar sig inte på någon överenskommelse mellan de nordiska länderna, men lagar med samma sakinnehåll finns dock i de andra nordiska länderna. Den nordiska utlämningslagen är i vissa avseenden lindrigare än utlämningslagen. En förutsättning för utlämning från Finland är att fängelse enligt lagen i den ansökande staten kan följa på brottet. Det krävs inte dubbel straffbarhet (4 §). En finsk medborgare får inte utlämnas, om inte personen i fråga i minst två år stadigvarande har vistats i det land till vilket utlämning begärs eller det strängaste föreskrivna straffet för brottet enligt finsk lag är minst fyra års fängelse (2 §).

2.2.2. Internationella konventioner

Den centrala konventionen som reglerar utlämning för brott är Europeiska konventionen om utlämning för brott (FördrS 32/1971), nedan Europeiska utlämningskonventionen, och det andra tilläggsprotokollet till den (FördrS 15/1985).

Finland är dessutom part i en del konventioner som även innehåller bestämmelser om utlämning för brott. Sådana konventioner är t.ex. Europeiska konventionen om bekämpande av terrorism (FördrS 16/1990)och Förenta Nationernas konvention mot olaglig hantering av narkotika och psykotropa ämnen (FördrS 44/1994).

2.2.3. Bilaterala fördrag

Finland har ingått bilaterala överenskommelser om utlämning med en del stater. De viktigaste av dessa är i praktiken avtalen med Förenta staterna, Kanada och Australien. Förenta staterna och Kanada har även undertecknat den konvention som sätts i kraft genom denna proposition. I riksdagen behandlas som bäst också en regeringsproposition som gäller godkännandet av avtal om utlämning och rättslig hjälp mellan Europeiska unionen och Förenta staterna (RP 86/2005 rd).

Bestämmelserna i konventionen och den gällande rätten i Finland behandlas också i motiveringen till artikel 24.

2.3. Internationell rättslig hjälp

2.3.1. Lagstiftning

Internationell rättslig hjälp i brottmål regleras i Finland både i den nationella lagstiftningen och i internationella överenskommelser. I Finland gäller en allmän lag om rättslig hjälp i brottmål samt vissa speciallagar. Finland är part i ett flertal konventioner om rättslig hjälp i brottmål och även i bilaterala fördrag.

Den allmänna lagen som reglerar den internationella rättsliga hjälpen i brottmål är lagen om internationell rättshjälp i straffrättsliga ärenden (4/1994), nedan lagen om straffrättslig rättshjälp. Lagen är ett enhetligt regelverk om internationell straffrättslig hjälp utifrån vilket de finska myndigheterna kan begära rättslig hjälp av myndigheterna i en annan stat och lämna dessa rättslig hjälp. Principen i lagen är att de finska myndigheterna omedelbart med stöd av den skall kunna lämna myndigheterna i en annan stat rättslig hjälp, oberoende av om det finns ett fördrag mellan Finland och den stat som begärt hjälpen eller inte. Dubbel straffbarhet förutsätts endast om begäran om rättslig hjälp gäller eller förutsätter användning av tvångsmedel. Det krävs inte heller att den stat som framställt begäran skulle lämna Finland motsvarande hjälp. De finska myndigheterna kan således redan med stöd av lagen om straffrättslig rättshjälp lämna myndigheterna i en annan stat rättslig hjälp. En bestämmelse om ovillkorliga grunder för förvägrande av rättshjälp finns i lagens 12 §. Enligt paragrafens 1 mom. lämnas rättshjälp inte om lämnandet av hjälpen kunde kränka Finlands suveränitet eller äventyra Finlands säkerhet eller andra väsentliga intressen. Enligt 2 mom. lämnas rättshjälp inte heller om lämnandet av hjälpen strider mot principerna om de mänskliga rättigheterna och grundläggande friheterna eller om lämnandet av hjälpen annars strider mot grundprinciperna för Finlands rättsordning. I 13 § i lagen om straffrättslig rättshjälp finns dessutom bestämmelser om sådana grunder för förvägrande som är beroende av prövning. Enligt paragrafen kan rättshjälp förvägras bl.a. om begäran hänför sig till en gärning som skall betraktas som ett politiskt brott. Paragrafen innehåller dessutom andra grunder för förvägrande vilka hänför sig till preskription av åtalsrätten, anhängiga rättegångar och andra motsvarande omständigheter. Lagen om straffrättslig rättshjälp innehåller dessutom bestämmelser om framställande av en begäran om rättshjälp till en annan stat. Till dessa delar gäller bestämmelserna främst frågan om vilken myndighet i Finland som har rätt att vidta åtgärder i saken. Med stöd av lagen om straffrättslig rättshjälp har utfärdats förordningen om internationell rättshjälp i straffrättsliga ärenden (13/1994). Förordningen utgör en komplettering till lagen och innehåller detaljerade bestämmelser om hur rättslig hjälp skall begäras och lämnas.

Finska statens internationella förpliktelser när det gäller att lämna andra stater rättslig hjälp och Finlands rätt att få rättslig hjälp av andra stater bestäms på basis av internationella överenskommelser. I 30 § i lagen om straffrättslig rättshjälp sägs att internationell rättshjälp i straffrättsliga ärenden utan hinder av bestämmelserna i nämnda lag lämnas också enligt vad som särskilt har avtalats eller bestämts om lämnande av rättshjälp. Lagen om straffrättslig rättshjälp och de internationella överenskommelserna tillämpas således parallellt.

Merparten av bestämmelserna i lagen om straffrättslig rättshjälp gäller villkoren för när de finska myndigheterna kan lämna myndigheterna i andra stater rättslig hjälp. Förutsätt-

ningarna för att lämna rättslig hjälp är sinsemellan mycket olika i andra stater och kan inte bestämmas i lagen om straffrättslig rättshjälp. Förutsättningarna för att lämna rättslig hjälp kan vara olika också hos parterna i en och samma överenskommelse. Detta beror på att parterna kan göra förbehåll till överenskommelserna, och dessutom kan den nationella lagstiftningen i de stater som tillträtt en överenskommelse avvika från bestämmelserna i överenskommelsen. När de finska myndigheterna begär rättslig hjälp är de tvungna att följa den internationella överenskommelse som gäller mellan Finland och den främmande staten i fråga. I dessa situationer räcker det i allmänhet inte att de finska myndigheterna enbart tillämpar bestämmelserna i lagen om straffrättslig rättshjälp.

Bestämmelser om internationell rättslig hjälp finns förutom i lagen om straffrättslig rättshjälp också i bl.a. rättegångsbalken, tvångsmedelslagen (450/1987), lagen om immunitet i vissa fall för personer som deltar i rättegång och förundersökning (11/1994), lagen om behörighet för och rättshjälp till tribunalen som behandlar brott som begåtts i det forna Jugoslavien (12/1994) samt lagen om ikraftträdande av de bestämmelser som hör till området för lagstiftningen i Romstadgan för Internationella brottmålsdomstolen och om tillämpning av stadgan (1284/2000).

2.3.2. Internationella konventioner

Den centrala konventionen om rättslig hjälp i brottmål som är i kraft i Finland är den europeiska konventionen om inbördes rättshjälp i brottmål (FördrS 30/1981) och dess tilläggsprotokoll (FördrS 14/1985). Finland undertecknade det andra tilläggsprotokollet den 9 oktober 2003.

Lagen om straffrättslig rättshjälp uppfyller beträffande sakinnehållet kraven i den europeiska konventionen om inbördes rättslig hjälp i brottmål. De finska myndigheterna kommer därför i praktiken till ett slutresultat som överensstämmer med den nämnda konventionen genom att tillämpa enbart den finska lagstiftningen. Den jämförelse av kraven enligt konventionen och bestämmelserna i lagen om straffrättslig rättshjälp som görs i motiveringen till de enskilda artiklarna i denna proposition innefattar i praktiken också den europeiska konventionen om inbördes rättshjälp i brottmål. Lagen om straffrättslig rättshjälp går visserligen till vissa delar utöver den nämnda konventionen. Enligt den nämnda lagen kan rättslig hjälp lämnas vid teleövervakning och teleavlyssning trots att den europeiska konventionen inte förutsätter detta.

Finland har dessutom tillträtt ett flertal andra konventioner som även innehåller bestämmelser om internationell rättslig hjälp i brottmål. De viktigaste av dem är Schengenkonventionen (FördrS 23/2001), konventionen om penningtvätt, efterforskning, beslag och förverkande av vinning av brott (FördrS 53/1994) och Förenta Nationernas konvention mot olaglig hantering av narkotika och psykotropa ämnen (FördrS 44/1994).

Medlemsstaterna i Europeiska unionen ingick den 29 maj 2000 en konvention om ömsesidig rättslig hjälp i brottmål (EGT C 197, 12.7.2000). Konventionen kompletterar den europeiska konventionen om inbördes rättshjälp i brottmål, och den innehåller bestämmelser om bl.a. kontakterna mellan de rättsliga myndigheterna, förhör med vittnen genom videokonferens och dessutom omfattande bestämmelser om telefonavlyssning. Finland har ratificerat konventionen, och den trädde i kraft internationellt den 23 augusti 2005 (FördrS 88/2005). Protokollet till konventionen mellan Europeiska unionens medlemsstater trädde i kraft den 5 oktober 2005 (FördrS 94/2005).

2.3.3. Det nordiska samarbetet

Finland, Danmark, Island, Norge och Sverige ingick 1974 en överenskommelse om inbördes rättshjälp genom delgivning och bevisupptagning (FördrS 26/1975). Närmare bestämmelser om tillämpningen av konventionen har utfärdats genom förordningen om inbördes rättshjälp mellan de nordiska länderna genom delgivning och bevisupptagning (470/1975). I Finland gäller dessutom lagen om skyldighet att i vissa fall inställa sig vid domstol i annat nordiskt land (349/1975). Lagen bygger på samnordisk lagstiftning. Dessa bestämmelser som gäller det nordiska

samarbetet har i Finland ansetts ha en sådan ställning att de finska myndigheterna kan tillämpa dem parallellt med den europeiska konventionen om inbördes rättshjälp i brottmål och lagen om straffrättslig rättshjälp.

2.3.4. Bilaterala fördrag

Finland har med en del stater ingått bilaterala fördrag om internationell rättslig hjälp i brottmål och sådana överenskommelser om brottsbekämpning eller annat samarbete som innehåller bestämmelser om internationell rättslig hjälp i brottmål. Dylika stater är t.ex. Australien, Estland, Lettland, Litauen, Polen, Ryssland, Ukraina och Ungern. Med undantag av Australien har dessa stater även undertecknat den konvention som skall sättas i kraft genom denna proposition. Bestämmelser om rättslig hjälp ingår också i den regeringsproposition, 86/2005 rd, som riksdagen behandlar som bäst och som gäller ikraftsättandet av avtal mellan Europeiska unionen och Förenta staterna om utlämning för brott och rättslig hjälp.

Bestämmelserna i konventionen och den gällande rätten i Finland behandlas också i motiveringen till de enskilda artiklarna.

3. Målsättning och de viktigaste förslagen

Syftet med propositionen är att nationellt sätta i kraft konventionen i Finland och att genomföra rambeslutet. Genom konventionen och rambeslutet försöker man skydda samhället mot databrottslighet och de skador denna brottslighet orsakar.

I propositionen föreslås att riksdagen skall godkänna konventionen och ge sitt samtycke till att vissa förklaringar och förbehåll görs med stöd av den. Propositionen innehåller ett lagförslag om sättande i kraft av de bestämmelser i konventionen som hör till området för lagstiftningen.

I propositionen föreslås att i strafflagen, tvångsmedelslagen, förundersökningslagen och lagen om internationell rättshjälp i straffrättsliga ärenden görs de ändringar som följer av konventionens ikraftträdande.

I strafflagen föreslås nya bestämmelser om systemstörning och innehav av hjälpmedel vid nätbrott. Den gällande regleringen utvidgas när det gäller spridning av hjälpmedel vid nätbrott. I strafflagens 38 kap. föreslås en ny 7 a §, enligt vilken den skall dömas för systemstörning som genom att mata in data eller på något annat sätt som anges i bestämmelsen hindrar ett informationssystems funktion eller orsakar allvarliga störningar i det. I 7 b § finns en bestämmelse om en grov gärningsform av brottet. Det föreslås att bestämmelsen om orsakande av fara för informationsbehandling i 34 kap. 9 a § i strafflagen ändras så att den utöver spridning av datavirus och motsvarande skadliga program även omfattar spridning av andra hjälpmedel vid nätbrott, såsom program och utrustning som används vid dataintrång samt lösenord. I kapitlets nya 9 b § kriminaliseras innehav av hjälpmedel vid nätbrott.

Försök till vissa brott föreslås bli straffbart. Dessa brott är skadegörelse (SL 35:1), störande av post- och teletrafik (SL 38:5), grovt störande av post- och teletrafik (SL 38:6), lindrigt störande av post- och teletrafik (SL 38:7), systemstörning (SL 38:7 a, ny), grov systemstörning (SL 38:7 b, ny) och grovt dataintrång (SL 38:8 a, ny).

Det föreslås att ansvaret för juridiska personer utvidgas till att omfatta en del nya brott. Dessa är orsakande av fara för informationsbehandling (SL 34:9 a), skadegörelse som riktar sig mot information (SL 35:1, 2), grov skadegörelse som riktar sig mot information (SL 35:2), kränkning av kommunikationshemlighet (SL 38:3), grov kränkning av kommunikationshemlighet (SL 38:4), störande av post- och teletrafik (SL 38:5), grovt störande av post- och teletrafik (SL 38:6), systemstörning (SL 38:7 a, ny), grov systemstörning (SL 38:7 b, ny), dataintrång (SL 38:8), grovt dataintrång (SL 38:8 a, ny) och upphovsrättsbrott (SL 49:1).

I tvångsmedelslagen föreslås nya bestämmelser om föreläggande att säkra data och skyldighet för innehavare av informationssystem att lämna uppgifter. Det föreslås att till tvångsmedelslagens 4 kap. 1 § fogas ett nytt 2 mom., där det för tydlighetens skull sägs att bestämmelserna om beslag även gäller information i form av data. I kapitlet föreslås

en ny 4 a § om skyldighet för innehavare av informationssystem att lämna uppgifter. Enligt paragrafen är innehavaren av ett informationssystem skyldig att på begäran ge förundersökningsmyndigheten lösenord och andra motsvarande uppgifter som personen i fråga innehar och som behövs för att ta i beslag data. Syftet med paragrafen är att underlätta förundersökningsmyndighetens arbete genom att minska tidsåtgången vid beslag av data. I kapitlet föreslås en ny 4 b § om föreläggande att säkra data. Detta är ett nytt tvångsmedel som vid behov kan användas som en förberedande åtgärd före andra tvångsmedel som riktar sig mot data. Syftet med det är att hindra att data som är av betydelse för utredningen av brott går förlorade eller förändras innan de kan tas i besittning genom andra tvångsmedel.

Det föreslås att till förundersökningslagens 27 § fogas ett nytt 2 mom. om skyldighet för ett vittne att vid förundersökningen lägga fram handlingar och annat bevismaterial som vittnet har i sin besittning. Till 15 § i lagen om internationell rättshjälp i straffrättsliga ärenden fogas ett nytt 2 mom., enligt vilket verkställigheten av en begäran om rättshjälp som gäller ett föreläggande att säkra data inte förutsätter dubbel straffbarhet. Det föreslås att 23 § 1 mom. i samma lag ändras så att till förteckningen över tvångsmedel som kan vidtas på grundval av en begäran om rättshjälp fogas det nya tvångsmedlet föreläggande att säkra data, som i denna proposition föreslås bli intaget i 4 kap. 4 b § i tvångsmedelslagen.

I strafflagen föreslås två ändringar som rambeslutet förutsätter. Till strafflagens 38 kap. fogas en bestämmelse om en grov gärningsform av dataintrång. Enligt den föreslagna nya 8 a § skall en gärning betraktas som grov, om den begås som ett led i en i paragrafen avsedd organiserad kriminell sammanslutnings verksamhet eller om den begås särskilt planmässigt. Gärningen skall dessutom vara grov även bedömd som en helhet. Straffskalan för grundrekvisitet för skadegörelse i 35 kap. 1 § i strafflagen ändras så att maximistraffet höjs från ett till två års fängelse.

I propositionen föreslås dessutom en del mindre lagändringar av främst teknisk natur.

4. Propositionens konsekvenser

De nya straffbestämmelserna som fogas till strafflagen förbättrar det straffrättsliga skyddet för data och informationsförmedling i elektronisk form. Dessutom ger propositionen myndigheterna effektivare medel för utredning av databrottslighet. Detta betyder att brottsoffrens rättsliga ställning förbättras.

Det effektivare internationella samarbetet främjar för sin del de finska myndigheternas möjligheter att utreda också sådan gränsöverskridande brottslighet vars följder yppar sig i Finland.

Enligt propositionen skall Finland ordna jour dygnet runt för att sköta de uppgifter som anges närmare i artikel 35. Avsikten är att centralkriminalpolisen skall utses till den kontaktpunkt som förutsätts i konventionen. Till dessa delar har propositionen endast obetydliga konsekvenser för polisens organisation och anställda, och de nuvarande resurserna är tillräckliga i detta avseende.

Det föreslagna nya tvångsmedlet föreläggande att säkra data riktar sig i praktiken alltid mot en utomstående innehavare av data, i allmänhet en teleoperatör. Förelägganden att säkra data kommer sannolikt att utfärdas relativt sällan, och den utfärdande instansen åsamkas således endast obetydliga kostnader för fullgörandet av denna skyldighet. Propositionen har således inte heller till dessa delar några större ekonomiska konsekvenser.

5. Beredningen av propositionen

Propositionen baserar sig på betänkandet av arbetsgruppen för IT-relaterad brottslighet (Justitieministeriet. Arbetsgruppsbetänkande 2003:6) och de utlåtanden som erhållits om det. Utlåtande begärdes av 47 myndigheter, organisationer och sakkunniga. Bland remissinstanserna fanns företrädare för statsförvaltningen, rättsväsendet, polisen och åklagarna, organisationer och företag inom datateknik samt fackförbund inom kommunikationsbranschen. Ett sammandrag har gjorts av utlåtandena (Justitieministeriet. Utlåtanden och utredningar 2004:14).

Enligt arbetsgruppens förslag skulle det beträffande tillverkningen och spridningen av de skadliga program eller program för datain-

trång som avses i bestämmelsen om orsakande av fara för informationsbehandling i 34 kap. 9 a § i strafflagen ha förutsatts att programmet primärt skapats eller anpassats för att äventyra eller skada informationsbehandling eller ett informations- eller kommunikationssystems funktion. Med anledning av utlåtandena har kravet på att ett hjälpmedel vid nätbrott primärt skall ha skapats för ett brottsligt syfte slopats i propositionen.

I tvångsmedelslagen föreslog arbetsgruppen en särskild bestämmelse (en ny 4 a § i 4 kap.) om kopiering och beslag av data. Enligt bestämmelsen kan data kopieras och lagras på en annan lagringsplattform, om det finns skäl att anta att den kan utgöra bevis i brottmål. Enligt bestämmelsen betraktas enbart kopiering av data ännu inte som beslag. Det är fråga om beslag först när data dessutom raderas från lagringsplattformen eller dess användning annars förhindras. Till dessa delar var remissutlåtandena motstridiga.

En del av remissinstanserna, t.ex. skyddspolisen och centralkriminalpolisen, tillstyrkte arbetsgruppens förslag om att kopiering av data inte skall utgöra beslag. På samma sätt som arbetsgruppen motiverade de detta med att bevismaterial i form av data kan bevaras oförändrat endast om en s.k. spegelkopia kan tas av datorns hårddisk med en särskild teknik som gör att kopian inte kan ändras. Spegelkopian motsvarar i varje avseende den kopierade hårddisken vid kopieringstidpunkten, och det är först när den granskas som man får reda på om hårddisken innehåller handlingar som skall tas i beslag. I en del fall kan en sådan spegelkopia vara viktig med hänsyn till brottsutredningen, eftersom en fil på en hårddisk förändras redan när den öppnas och det därför t.ex. inte är möjligt att konstatera om filen har ändrats efter att den har gjorts upp. Genom att granska spegelkopian kan man också söka efter raderad information.

Riksdagens biträdande justitieombudsman anser att den föreslagna bestämmelsen i sig är godtagbar, eftersom förslaget motsvarar den gällande rätten i fråga om kopior av handlingar.

Många av remissinstanserna, bl.a. Finlands Juristförbund, Tingsrättsdomarna rf, Finlands Advokatförbund rf, Finlands Läkarförbund, Finlands Journalistförbund och förbundet Oikeustoimittajat ry motsatte sig förslaget om kopiering och beslag av data och ansåg att bestämmelserna om beslag borde tillämpas på kopiering av data. Remissinstanserna ansåg att samtliga rättsmedel som hänför sig till beslag bör gälla redan kopiering av data, eftersom det väsentliga inte är att lagringsplattformen kvarstår i ägarens besittning utan att utredningsmyndigheten genom kopieringen får tillgång till all den information som finns på lagringsplattformen. Särskilt problematiskt ansåg remissinstanserna det vara att en kopia ofta kan innehålla information som inte hänför sig till det brott som utreds eller dokument som inte får tas i beslag. Detta är fallet t.ex. när beslaget riktar sig mot hårddisken i en advokatbyrås dator. Eftersom den ovan nämnda spegelkopian inte kan ändras, kan dokument som omfattas av förbudet mot beslag inte raderas från kopian.

Frågan om kopiering av handlingar i elektronisk form och om hanteringen av kopiorna är en del av en större problematik som gäller husrannsakan på sådana platser där man vet att det finns också handlingar som inte får tas i beslag, t.ex. på en advokatbyrå, eftersom beslaget så gott som alltid föregås av husrannsakan. Biträdande justitiekanslern har i sitt beslut 22.8.2003, DNr 22/21/00 och 127/1/00, ansett att det i någon mån råder oklarhet om det inbördes förhållandet mellan 4 kap. 2 § 2 mom. i tvångsmedelslagen (förbud mot beslag av handlingar), 17 kap. 23 § 1 mom. 4 punkten i rättegångsbalken (vittnesförbud för rättegångsombud) och 5 c § i lagen om advokater, och att bestämmelserna i tvångsmedelslagen inte är så exakta som den europeiska människorättskonventionen förutsätter när det gäller husrannsakan på advokatbyråer. Biträdande justitiekanslern föreslår att justitieministeriet överväger om det ovan nämnda avgörandet ger anledning att se över lagstiftningen. Också den europeiska domstolen för de mänskliga rättigheterna har i sin dom 27.9.2005, Petri Sallinen m.fl. mot Finland, ansett att rättegångsbalkens 17 kap. 23 § inte innehåller tillräckligt exakta bestämmelser om tystnadsplikten för advokater och det motsvarande förbudet mot beslag i 4 kap. 2 § 2 mom. i tvångsmedelslagen i anslutning till denna. Domstolen ansåg att det

av den förstnämnda bestämmelsen inte framgår om tystnadsplikten för advokater gäller endast uppgifter som har samband med ett visst mål eller förhållandet mellan advokaten och dennes klient i allmänhet ("...only the relationship between a lawyer and his/her clients in a particular case or the relationship generally."). På denna grund ansåg domstolen att det hade brutits mot artikel 8 i människorättskonventionen. Domen hänförde sig till en husrannsakan i en advokatbyrå 1999, då polisen hade kopierat hårddisken i en advokats dator.

Högsta domstolen har genom ett prejudikat, HD 2003:119, som meddelats av den förstärkta avdelningen, klarlagt förhållandet mellan de ovan nämnda lagrummen. Högsta domstolen ansåg i sitt prejudikat att vittnesförbudet för advokater och det förbud mot att ta handlingar i beslag som hänför sig till det är snävare än vittnesförbudet för rättegångsombud och tystnadsplikten för advokater. Vittnesförbudet och förbudet mot att beslagta handlingar gäller endast handlingar som hänför sig till sådana rättegångar och myndighetsförfaranden som antingen är eller kommer att bli anhängiga.

Konventionen förutsätter inte en sådan bestämmelse om kopiering och beslag av data som arbetsgruppen föreslog. Den gällande lagstiftningen uppfyller kraven enligt artikel 19.3 i konventionen när det gäller kopiering av handlingar, även om det i propositionen föreslås att ordalydelsen i lagen klarläggs till dessa delar. Efter att högsta domstolen meddelat sitt prejudikat HD 2002:85 är det inte heller längre nödvändigt att klarlägga den gällande rätten om beslag av handlingar i elektronisk form. Det ovan nämnda problemkomplexet är alltför invecklat för att utredas i samband med det nu aktuella ikraftsättandet av konventionen och genomförandet av rambeslutet. Det finns inte heller någon anledning att fördröja ikraftsättandet av de ovan nämnda internationella åtagandena genom att till propositionen foga lagförslag som varken konventionen eller rambeslutet förutsätter. Därför innehåller propositionen inga bestämmelser om kopiering eller beslag av data.

6. Andra omständigheter som inverkat på propositionens innehåll

Riksdagen behandlar som bäst regeringens proposition 52/2005 rd om genomförande av Europeiska unionens rambeslut om miljöbrott, om godkännande av Europarådets konvention om straffrättsliga sanktioner till skydd för miljön samt med förslag till lagar om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i konventionen och om ändring av strafflagen och vissa andra lagar. I propositionen föreslås att 13 § i strafflagens 34 kap. om allmänfarliga brott ändras så att straffansvaret för juridiska personer utsträcks även till äventyrande av andras hälsa och grovt äventyrande av andras hälsa. Eftersom nämnda 34 kap. 13 § även föreslås bli ändrad också i den föreliggande propositionen, bör förslagen samordnas vid behandlingen i riksdagen.

DETALJMOTIVERING

1. Konventionens innehåll och förhållande till lagstiftningen i Finland

Kapitel I. **Användning av termer**

Artikel 1. *Definitioner.* Artikeln innehåller bestämmelser om de definitioner som används i konventionen.

Enligt punkt a i artikeln avses med datorsystem en apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatiserad behandling av uppgifter. Med termen avses således såväl enskilda apparater som helheter bestående av flera sammankopplade apparater. Definitionen behandlas i punkterna 23 och 24 i den förklarande rapporten. Enligt rapporten består ett datorsystem av apparater och program genom vilka datorbehandlingsbara uppgifter i digital form behandlas automatiskt. En apparat består i allmänhet av en processor och olika periferienheter som utför vissa speciella uppgifter. Med att databehandlingen är automatiserad avses att behandlingen sker självständigt med hjälp av ett program, utan omedelbar medverkan av någon människa. Begreppet datorsystem täcker även informationsnät. Med informationsnät avses datorsystem som hör samman med varandra. Tekniskt kan anslutningen genomföras med hjälp av en elektronisk eller optisk ledning eller radiovågor. Geografiskt kan informationsnätet vara antingen ett litet lokalt nät eller ett globalt nät såsom internet. Det väsentliga i begreppet är att informationsnätet används för att överföra data från en del av ett nätet till ett annat.

Termen datorsystem används i konventionen bl.a. för att avgränsa föremålet för de straffbara gärningarna när det gäller brott som riktar sig mot datorsystem samt, när det gäller brott som begås med användning av datorsystem, gärningssättet. Dessutom används termen i de bestämmelser i konventionen som gäller tvångsmedel för att avgränsa föremålet för tvångsmedel.

Enligt punkt b i artikeln avses med datorbehandlingsbara uppgifter framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett datorsystem, inklusive program som utformats för att få ett datorsystem att utföra en viss funktion. Definitionen behandlas i punkt 25 i den förklarande rapporten. Enligt rapporten grundar sig definitionen på definitionen i en ISO-standard. Det centrala i definitionen är att uppgifterna är i elektronisk eller annan sådan form att de som sådana kan behandlas i ett datorsystem.

Termen i fråga används i konventionen för att avgränsa föremålet för de straffbara gärningarna när det gäller brott som riktar sig mot datorsystem samt i de bestämmelser i konventionen som gäller tvångsmedel för att begränsa föremålet för tvångsmedel.

Enligt punkt c i artikeln avses med tjänsteleverantör en offentlig eller privat enhet som erbjuder användarna av dess tjänster möjlighet att kommunicera med hjälp av ett datorsystem, och varje annan enhet som behandlar eller lagrar datorbehandlingsbara uppgifter för en sådan kommunikationstjänst eller för användarna av en sådan tjänst. Definitionen behandlas i punkterna 26 och 27 i den förklarande rapporten. Enligt rapporten kan den tjänsteleverantör som avses i artikeln vara t.ex. ett företag som tillhandahåller överföring av meddelanden, tillträde till ett nät, underhåll av ett datorsystem eller lagring av datorbehandlingsbara uppgifter. Enbart tillhandahållande av innehåll, t.ex. på internetsidor, är dock inte en sådan kommunikationstjänst som avses i artikeln.

Termen tjänsteleverantör används i de be-

stämmelser i konventionen som gäller tvångsmedel för att avgränsa kretsen av fysiska och juridiska personer som kommer i fråga som föremål för tvångsmedel.

Enligt punkt d i artikeln avses med trafikuppgifter datorbehandlingsbara uppgifter som hänför sig till ett meddelande som förmedlas med hjälp av ett datorsystem, vilka alstrats av ett datorsystem som ingick i kommunikationskedjan och anger meddelandets ursprung, destination, färdväg, tid, datum, storlek, varaktighet eller typ av underliggande tjänst. Definitionen behandlas i punkterna 28–31 i den förklarande rapporten. Enligt rapporten är sådana i artikeln avsedda trafikuppgifter som anger ett meddelandes ursprung eller destination t.ex. ett telefonnummer, en IP-adress eller någon annan med dessa jämförbar teleadress. Med typ av underliggande tjänst avses om kommunikationen t.ex. gäller e-post, filöverföring eller en diskussion som förs i realtid.

Uppgifter om mobiltelefoners läge är däremot inte enligt definitionen sådana trafikuppgifter som avses i artikeln.

Termen trafikuppgifter används i de bestämmelser i konventionen som gäller tvångsmedel för att avgränsa de uppgifter som kommer i fråga som föremål för tvångsmedel.

Kapitel II. Åtgärder som skall vidtas på nationell nivå

Avsnitt 1 Materiell straffrätt

Avdelning 1 Brott mot datorbehandlingsbara uppgifters och datorsystems förtrolighet, integritet och tillgänglighet

Artikel 2. *Olagligt intrång.* Enligt artikeln skall orättmätigt intrång i hela eller en del av ett datorsystem straffbeläggas, när det görs uppsåtligen. En part får uppställa krav på att brottet begås genom intrång i säkerhetsåtgärder med uppsåt att komma över datorbehandlingsbara uppgifter eller med annat brottsligt uppsåt eller mot ett datorsystem som är kopplat till ett annat datorsystem.

Artikeln behandlas i punkterna 44—50 i den förklarande rapporten. Enligt rapporten är syftet med artikeln att trygga informationsbehandlingsfriden. Att säkerställa en tillräcklig datasäkerhet är det primära och effektivaste medlet för att nå detta mål. Utöver detta behövs det också ett straffrättsligt skydd. Det är viktigt att man kan ingripa i en handling på ett så tidigt stadium som möjligt. Detta krav uppfylls bäst genom kriminalisering av rent dataintrång, utan att det i övrigt krävs något särskilt kriminellt syfte med handlingen. En omfattande kriminalisering kan dock enligt medlemsstaternas åsikt vara förknippad med problem. Därför sägs det i konventionen att medlemsstaterna får uppställa ytterligare begränsande krav i fråga om brottet.

En handling kan rikta sig mot antingen hela eller en del av ett datorsystem. Begreppet datorsystem definieras i artikel 1 a. Gärningssättet är intrång. Intrång förutsätter att gärningsmannen på något sätt kommer åt ett datorsystem eller en del av det. Enbart det att någon skickar e-post, en fil, en kaka eller andra data till ett system utgör ännu inte sådant intrång som avses i artikeln. Handlingen skall begås orättmätigt. Därför är det klart att rekvisitet för brott enligt artikeln inte uppfylls om någon med systeminnehavarens tillstånd gör intrång i ett informationssystem i syfte att testa datasäkerheten eller att ladda ner internetsidor som är avsedda att vara offentliga.

I Finland motsvaras olagligt intrång enligt konventionen av bestämmelserna om dataintrång i 38 kap. 8 § i strafflagen. Enligt 1 mom. i det nämnda lagrummet skall den dömas för dataintrång som genom att göra bruk av en användaridentifikation som han inte har rätt till eller genom att annars bryta säkerhetsarrangemang obehörigen tränger in i ett datasystem där data behandlas, lagras eller överförs elektroniskt eller med någon annan sådan teknisk metod eller i en särskilt skyddad del av ett sådant system. Enligt samma paragrafs 2 mom. döms också den för dataintrång som utan att tränga in i datasystemet eller en del av detta med tekniska specialanordningar obehörigen tar reda på information som finns i ett sådant datasystem som avses i 1 mom. Enligt 3 mom. är försök till dataintrång straffbart. Enligt 4 mom. är bestämmelsen sekundär.

Enligt förarbetena till lagen (RP 94/1993

rd) är syftet med bestämmelserna om dataintrång dels att skydda datasystemen mot inkräktare, dels att skydda integriteten vid sådant arbete som utförs med datorer mot sådan yttre observation som inte utgör olovlig avlyssning eller olovlig observation.

Det är för det första straffbart att göra intrång i ett datasystem som man inte har rätt att gå in i. Dessutom är det straffbart att göra intrång i en sådan skyddad del av ett datasystem som man inte har rätt att gå in i, även om man har rätt att använda systemets övriga delar.

I bestämmelsen avses med datasystem ett system där data behandlas elektroniskt eller med någon annan teknisk metod.

Med intrång avses att gärningsmannen skaffar sig tillgång till data som behandlas i ett system. Intrånget kan gälla såväl data som lagras i en dators minne som data som finns på en kommunikationsbuss.

Intrånget skall ske så att systemets säkerhetsarrangemang bryts. Som exempel på ett sådant fall nämns i bestämmelsen att man gör bruk av någon annans användaridentifikation. Gärningsmannen skall vidta uttryckliga åtgärder för att tränga igenom säkerhetsarrangemanget. Om någon med tillstånd av en annan person gör bruk av dennes användaridentifikation är det således inte fråga om dataintrång.

Förutom vad som sagts ovan kriminaliseras i 2 mom. dessutom avlyssning av information med hjälp av en teknisk specialanordning. Det förutsätts då inte något egentligt intrång i systemet, utan dataintrånget görs t.ex. genom att man lagrar och analyserar s.k. elektromagnetiska emissioner från en dator.

Gärningsmannen skall enligt kriterierna för uppsåt vara medveten om att det är fråga om obehörigt intrång. Att någon av misstag får åtkomst till eller kommer in i någon annans datasystem är inte straffbart.

Brottet fullbordas genast när gärningsmannen tar sig igenom systemets skydd. Om säkerhetsarrangemanget består av många faser förutsätts gärningsmannen ha klarat av också den sista fasen. Före det är det fråga om försök till brott.

Den som gör intrånget behöver inte på något sätt röra uppgifterna i systemet för att brottet skall fullbordas. Om brottet framskrider så långt att uppgifterna används eller skadas, tillämpas bestämmelserna om olovligt brukande i strafflagens 28 kap. eller bestämmelserna om skadegörelse i nämnda lags 35 kap.

Försök till dataintrång är straffbart. Redan det att någon försöker få reda på en användaridentifikation eller bryta något annat säkerhetsarrangemang som skyddar ett datasystem utgör brott, om gärningen begås i syfte att obehörigen göra intrång i systemet. I rättspraxis har det ansetts att redan det att någon försöker hitta en säkerhetslucka i ett system genom s.k. portskanning uppfyller rekvisitet för försök till dataintrång (HD 2003:36). Däremot är det inte fråga om försök till dataintrång, om någon i misstag försöker komma in i ett datasystem som han eller hon inte har rätt att gå in i.

Bestämmelserna om dataintrång är sekundära. Bestämmelserna åsidosätts t.ex. vid intrång i ett datasystem i syfte att begå företagsspionerі, skadegörelse som riktar sig mot de uppgifter som lagrats i systemet eller mot själva systemet och kränkning av kommunikationshemlighet. Bestämmelsen om olovligt brukande kan tillämpas om gärningsmannen använder ett system på ett sådant sätt som är specifikt för det, t.ex. skaffar sig uppgifter gratis ur en avgiftsbelagd databank. Om ett sådant syfte kan visas redan när intrånget görs kan det vara fråga om försök till olovligt brukande.

De gällande bestämmelserna motsvarar skyldigheterna enligt artikeln. Enligt förslaget kommer Finland i enlighet med artikel 40 att avge en förklaring om att Finland använder sig av sin rätt att kräva att brottet har begåtts genom att bryta säkerhetsarrangemang.

Artikeln förutsätter inte ändringar i lagstiftningen.

Artikel 3. *Olaglig avlyssning.* Enligt artikeln skall följande gärningar straffbeläggas när de begås uppsåtligen: att med tekniska hjälpmedel orättmätigt avlyssna icke allmänna överföringar av datorbehandlingsbara uppgifter till, från eller inom ett datorsystem, däribland elektromagnetiska emissioner från ett datorsystem med sådana datorbehandlingsbara uppgifter. En part får uppställa krav på att brottet begås med brottsligt uppsåt eller mot ett datorsystem som är kopplat till ett

annat datorsystem.

Artikeln behandlas i punkterna 51—59 i den förklarande rapporten. Enligt rapporten är syftet med artikeln att trygga integritetsskyddet i varje slag av elektronisk kommunikation, oberoende av hur kommunikationen sker tekniskt. Artikelns tillämpningsområde omfattar endast gärningar som begås med tekniska hjälpmedel. Med tekniska hjälpmedel avses förutom apparater och program även användning av lösenord. Med icke allmänna överföringar avses kommunikation som sker i form av målgruppskommunikation. Det avgörande är dock inte arten av det medium som används utan själva meddelandets konfidentiella natur. Därför kan även ett konfidentiellt meddelande som förmedlats i ett medium för masskommunikation höra till artikelns tillämpningsområde. Det kan vara fråga om kommunikation mellan datorer, mellan olika delar i en dator eller mellan en dator och dess användare. Kommunikationen kan också ske genom förmedling av radiovågor. Artikeln omfattar också gärningar som begås genom avlyssning av s.k. elektromagnetiska emissioner. I artikeln förutsätts det att gärningen begås orättmätigt för att den skall utgöra brott. En gärning kan vara berättigad t.ex. på basis av erhållet samtycke av den andra parten eller en myndighets rätt att utreda brott. Artikeln gäller inte heller användningen av s.k. kakor för att spåra användare på internet.

I Finland motsvaras den gärning som avses i konventionen av bestämmelserna om kränkning av kommunikationshemlighet i strafflagens 38 kap. 3 § och, när det gäller den grova gärningsformen, i 38 kap. 4 § samt av bestämmelsen i kapitlets 8 § 2 mom. Enligt den nämnda 3 § 1 mom. skall den dömas för kränkning av kommunikationshemlighet som obehörigen öppnar ett brev eller ett annat tillslutet meddelande som är adresserat till någon annan eller genom att bryta ett säkerhetsarrangemang skaffar uppgifter om ett meddelande som har upptagits elektroniskt eller med någon annan sådan teknisk metod och som är skyddat mot utomstående, eller skaffar uppgifter om innehållet i samtal, telegram, text-, bild- eller dataöverföring eller något annat motsvarande telemeddelande som förmedlas genom telenät eller om avsändande eller mottagande av ett sådant meddelande. För att gärningen skall kunna anses som grov förutsätts det enligt 4 § att gärningsmannen utnyttjar en särskild förtroendeställning, att brottet begås särskilt planmässigt eller att gärningen riktar sig mot synnerligen förtroliga uppgifter. Försök är straffbart i fråga om bägge gärningsformerna.

Bestämmelsens tillämpningsområde är brett. Bestämmelsen omfattar förutom meddelanden i form av data också andra meddelanden, oberoende av deras form. Ett meddelande i form av data skall dock antingen vara skyddat mot utomstående eller förmedlas genom ett telenät. T.ex. ett e-postmeddelande är således skyddat enligt olika ställen i bestämmelsen beroende på var meddelandet finns. Ett e-postmeddelande åtnjuter skydd för meddelanden som förmedlas i ett telenät när det befinner sig i ett telenät men skydd för meddelanden som är skyddade mot utomstående när det är i en parts besittning, t.ex. när det har lagrats i en dator.

I bestämmelsen avses med telenät förutom det allmänna telenätet också t.ex. företagsinterna telenät. Med telemeddelande avses varje slag av meddelande av sådan typ som anges i exempelförteckningen i bestämmelsen. Enligt förarbetena till lagen (RP 94/1993 rd) skall frågan om huruvida det föreligger motsvarighet avgöras speciellt med hänsyn till hur viktigt meddelandet är ur integritetssynpunkt. Bestämmelsen gäller t.ex. inte masskommunikation i telenät. Förutom innehållet i ett meddelande skyddar bestämmelsen också uppgifter om sändning och mottagning av meddelanden. Det är således straffbart att t.ex. skaffa uppgifter om till vilket nummer någon har ringt från en viss telefon.

Bestämmelsen skyddar också meddelanden som utan överföring registreras i en dator för att bli lästa av en eller flera bestämda personer. En förutsättning för straffbarhet är dock att meddelandet genom någon teknisk metod har skyddats mot utomstående och att den som skaffar uppgifter om meddelandet bryter skyddet. Enligt förarbetena till lagen (RP 94/1993 rd) kan detta ske på samma sätt som i fråga om dataintrång. Bestämmelsen täcker således också utnyttjande av s.k. elektromagnetiska emissioner.

Gärningen skall begås obehörigen. En gär-

ning kan vara berättigad t.ex. på basis av erhållet samtycke av den andra parten eller en myndighets rätt att utreda brott.

I strafflagens 38 kap. 8 § 2 mom. finns också en bestämmelse om avlyssning av elektromagnetiska emissioner. Bestämmelsen behandlas i samband med artikel 2.

De gällande bestämmelserna motsvarar till dessa delar skyldigheterna enligt artikeln.

Enligt artikeln får en part uppställa krav på att brottet begås med brottsligt uppsåt eller mot ett datorsystem som är kopplat till ett annat datorsystem. Finland har inte något behov av att uppställa sådana ytterligare krav som avses i artikeln.

Artikeln förutsätter inte ändringar i lagstiftningen.

Artikel 4. *Datastörning.* Enligt punkt 1 i artikeln skall följande gärningar straffbeläggas när de begås uppsåtligen: att orättmätigt skada, radera, försämra, ändra eller undertrycka datorbehandlingsbara uppgifter.

Artikeln behandlas i punkterna 60—64 i den förklarande rapporten. Enligt rapporten är syftet med artikeln att skapa ett motsvarande skydd för datorbehandlingsbara uppgifter som det som gäller reella föremål. Strävan är att förteckningen över gärningssätt skall vara heltäckande. Gärningssätten överlappar därför till viss del varandra. Eftersom t.ex. undertryckande av datorbehandlingsbara uppgifter inte nödvändigtvis innebär att uppgifterna raderas nämns bägge gärningssätten särskilt. På grund av motsvarande små betydelseskillnader nämns även gärningssätten ändra, försämra och skada separat i artikeln. Det gemensamma för gärningssätten är att de datorbehandlingsbara uppgifterna på en lagringsplattform har förändrats till följd av gärningen. Som ett typexempel kan nämnas den skada som ett datavirus som ändrar uppgifterna förorsakar. Gärningen skall vara orättmätig och begås uppsåtligen. I praktiken kan en gärning vara berättigad främst i ett sådant fall när den som innehar uppgifterna ger sitt samtycke till den.

I Finland motsvaras datastörning enligt konventionen av bestämmelserna om skadegörelse i 35 kap. 1 § i strafflagen. Enligt den nämnda paragrafens 2 mom. skall den dömas för skadegörelse som för att skada någon orättmätigt förstör, skadar, döljer eller hemlighåller information som har upptagits på ett datamedium eller någon annan upptagning.

Enligt förarbetena till lagen (RP 66/1988 rd) avses med information som har upptagits på ett datamedium såväl informationens sakinnehåll som de tecken, dvs. data, som förmedlar sakinnehållet. Med datamedium avses t.ex. dokument, grammofonskivor, film, magnetband och disketter. Bestämmelsen täcker således klart de datorbehandlingsbara uppgifter som avses i artikeln. Å andra sidan är tillämpningsområdet för bestämmelsen betydligt mera omfattande än vad artikeln förutsätter.

Trots att förteckningen över gärningssätten i bestämmelsen inte till ordalydelsen motsvarar förteckningen i artikeln omfattas dock samma gärningar av regleringen. Med att information skadas avses i bestämmelsen att informationen ändras antingen till innehållet eller så att den blir helt obegriplig eller obrukbar. Bestämmelsen täcker således varje slag av ingrepp i information som leder till att information som finns på en lagringsplattform antingen ändras eller utplånas. Också kriterierna när det gäller orättmätighet och uppsåtlighet är desamma som i artikeln.

De gällande bestämmelserna motsvarar skyldigheterna enligt artikeln.

Enligt punkt 2 i artikeln får en part förbehålla sig rätten att uppställa krav på att handlande som anges i punkt 1 medför allvarlig skada. Finland har inte något behov av att göra ett sådant förbehåll som avses i punkt 2.

Artikeln förutsätter inte ändringar i lagstiftningen.

Artikel 5. *Systemstörning.* Enligt artikeln skall följande gärningar straffbeläggas när de begås uppsåtligen: att orättmätigt allvarligt hindra ett datorsystems drift genom att mata in, överföra, skada, radera, försämra, ändra eller undertrycka datorbehandlingsbara uppgifter.

Artikeln behandlas i punkterna 65—70 i den förklarande rapporten. Enligt rapporten är syftet med artikeln att säkerställa att datorsystem kan fungera störningsfritt. De gärningssätt som kommer i fråga är för det första gärningssätt som ingriper i de datorbehandlingsbara uppgifterna i ett system, dvs. att skada, radera, försämra, ändra eller undertrycka uppgifter. Till dessa delar motsvarar

förteckningen över gärningssätten den i samband med artikel 4 nämnda förteckningen över gärningssätt som skadar datorbehandlingsbara uppgifter.

Systemstörningen kan även orsakas genom att gärningsmannen matar in eller överför datorbehandlingsbara uppgifter. Med att mata in eller överföra uppgifter avses i artikeln en attack som orsakar en funktionsstörning i föremålet för attacken, dock utan att uppgifterna i systemet skadas på något sätt. Det kan vara fråga om en avsiktlig överbelastning eller t.ex. att uppgifter som är av den typen att de orsakar störningar matas in. Attacken riktar sig således inte mot uppgifterna i systemet utan mot systemets funktion. En dylik s.k. överbelastningsattack som riktar sig mot exempelvis en e-postserver nämns i den förklarande rapporten som exempel på en typisk situation när artikeln blir tillämplig.

Enligt artikeln skall endast allvarligt hindrande av ett datorsystems drift straffbeläggas. Parterna får själva fastställa tröskeln för när en gärning är allvarlig. Parterna kan således besluta om det krävs att systemet lamslås helt och hållet eller endast delvis och om blockeringen skall vara permanent eller tillfällig.

Gärningen skall begås uppsåtligen och vara orättmätig. I praktiken kan en gärning vara berättigad främst i ett sådant fall när den som innehar uppgifterna ger sitt samtycke till den. Avsändandet av stora mängder e-post kan i praktiken leda till att en e-postserver blir långsam vilket medför olägenheter för mottagaren. Dylik s.k. skräppost omfattas dock av tillämpningsområdet för denna artikel endast om gärningsmannen vet om att den orsakar sådana olägenheter som avses i artikeln.

I Finland motsvaras systemstörning enligt konventionen närmast av bestämmelserna om störande av post- och teletrafik i 38 kap. 5 § i strafflagen. Enligt det nämnda lagrummet skall den dömas för störande av post- och teletrafik som genom att ingripa i en för posttrafik eller för tele- eller radiokommunikationer använd anordnings funktion, genom att med en radioanläggning eller över ett telenät av okynne sända störande meddelanden eller på något annat motsvarande sätt obehörigen hindrar eller stör posttrafik eller tele- eller radiokommunikationer.

Enligt förarbetena till lagen (RP 94/1993 rd) gäller bestämmelsen posttrafiken samt tele- och radiokommunikationerna i sin helhet, dvs. både målgruppskommunikation och masskommunikation. Till den sistnämnda kategorin hör t.ex. rundradioverksamhet. Syftet med bestämmelsen är således att utöver posttrafik dessutom täcka även all slags elektronisk kommunikation, oberoende av meddelandenas innehåll och tekniska genomförande. Meddelandena kan överföras antingen via ledning eller trådlöst. Huruvida det telenät som används är ett allmänt nät eller t.ex. ett fristående företagsinternt nät saknar betydelse. Bestämmelsens tillämpningsområde har inte begränsats beträffande gärningssättet annat än genom exempel. Därför är tillämpningsområdet brett och omfattar utöver de gärningar som avses i artikeln också t.ex. att förstöra postlådor och störa analoga TV-sändningar.

När det gäller de gärningar som avses i artikeln, såsom överbelastningsattacker, täcker bestämmelsen klart alla de gärningar som kan anses vara riktade mot kommunikation.

Vanligtvis är det uttryckligen e-post- och internetservrar samt andra motsvarande servrar som sköter överföring, routning och distribution av meddelanden som är föremål för överbelastningsattacker.

Den gällande regleringen av störande av post- och teletrafik täcker således i praktiken artikelns kärnområde.

Den gällande bestämmelsen täcker dock endast störande av tele- och radiokommunikationer. Bestämmelsens tillämpningsområde är i och för sig brett, men det begränsar sig endast till kommunikation, dvs. överföring av meddelanden från ett ställe till ett annat. Bestämmelsen täcker inte systemstörningar som skall straffbeläggas enligt konventionen i ett sådant fall när gärningen inte ens indirekt kan anses störa kommunikation. I en del fall kan sådana systemstörningar som avses i konventionen vara straffbara som skadegörelse enligt strafflagens 35 kap. 1 § 2 mom. Den nämnda bestämmelsen täcker dock inte de gärningar som avses i konventionen i sådana fall när direkta ingrepp inte görs i datorbehandlingsbara uppgifter. Inte heller bestämmelsen om olovligt brukande i strafflagens 28 kap. 7 § täcker de gärningar som av-

ses i konventionen i sådana fall när det inte är fråga om direkt användning av ett informationssystem.

Artikeln förutsätter därför ändringar i den gällande lagstiftningen.

Med hänsyn till bestämmelsernas ursprungliga skyddsobjekt, ett mera allmänt skydd av kommunikation, är det inte ändamålsenligt att ändringen görs så att tillämpningsområdet för bestämmelsen om störande av post- och teletrafik utvidgas till att omfatta alla typer av informationssystem. I regeringens proposition föreslås därför att till strafflagens 38 kap. fogas nya särskilda bestämmelser om systemstörning.

Enligt den nya 7 a § i förslaget skall den dömas för systemstörning som i syfte att orsaka en annan person olägenhet eller ekonomisk skada matar in, överför, skadar, ändrar eller undertrycker data eller på något annat med dessa jämförbart sätt obehörigen hindrar ett informationssystems funktion eller orsakar allvarliga störningar i det. Förslaget innehåller dessutom en bestämmelse om en grov gärningsform. I detaljmotiveringen till lagförslaget i fråga redogörs närmare för förslagets innehåll. Efter att den föreslagna ändringen trätt i kraft uppfyller de gällande bestämmelserna kraven i artikeln.

Artikel 6. *Missbruk av apparatur.* Enligt artikel 6.1 a i skall följande gärningar straffbeläggas: att tillverka, försälja, anskaffa för användning, importera, sprida eller på annat sätt tillgängliggöra apparater och program som är skapade eller anpassade främst för att begå något av de brott som skall straffbeläggas enligt artiklarna 2—5 i konventionen. Detsamma gäller enligt punkt ii även ett datorlösenord *(password)*, en åtkomstkod *(access code)* eller liknande datorbehandlingsbara uppgifter som kan ge åtkomst till ett helt datorsystem eller en del därav. Dessutom förutsätts i konventionen ett uppsåt att begå något av de brott som avses i artiklarna 2—5.

Enligt punkt 1 b i artikeln skall även innehav av ett föremål som avses i punkt a med uppsåt att det skall användas för att begå något av de brott som avses i artiklarna 2—5 straffbeläggas. Till dessa delar får en part i lag uppställa krav på att flera sådana föremål skall innehas för att straffansvar skall gälla.

I punkt 2 i artikeln sägs för tydlighetens skull att artikeln inte skall tolkas som att den ålägger straffansvar i de fall där tillverkning, försäljning, anskaffning för användning, import, spridning eller annat tillgängliggörande eller innehav som avses i punkt 1 i artikeln inte har till syfte att något av de brott som straffbeläggs i enlighet med artiklarna 2—5 i konventionen skall begås, såsom exempelvis för att i behörig ordning testa eller skydda ett datorsystem.

Artikeln behandlas i punkterna 71—78 i den förklarande rapporten. Enligt rapporten är syftet med artikeln att indirekt förebygga egentliga nätbrott genom att införa en särskild straffbestämmelse som gör det möjligt att ingripa redan vid spridning och innehav av hjälpmedel som används för att begå dessa brott.

När apparatur används för att begå brott kan det vara fråga om att apparaturen används för att orsaka skada eller att den används för obehörigt dataintrång. Artikeln omfattar således utöver virus och andra motsvarande skadliga program också program som används vid dataintrång. Artikeln täcker förutom datorprogram även apparater. Dessutom tillämpas artikeln också på lösenord och andra data som används vid autentisering.

Vid beredningen av artikeln har man fäst särskild uppmärksamhet vid de problem som uppstår på grund av att apparater kan ha dubbel användning. Om artikelns tillämpningsområde skulle omfatta enbart sådan apparatur som uteslutande används i syfte att begå nätbrott, skulle det straffrättsliga skyddet i praktiken vara så gott som obefintligt på grund av bevissvårigheter. Därför gäller artikeln apparatur som primärt är tänkt att användas för att begå brott. Enligt den förklarande rapporten avses härmed det objektiva användningsändamålet. Visserligen innebär även denna formulering att apparater med dubbel användning i praktiken huvudsakligen hamnar utanför artikelns tillämpningsområde.

Gärningen skall begås uppsåtligen och orättmätigt. Spridning och innehav som avses ovan är t.ex. berättigat när syftet är att utveckla eller testa ett system. Detta sägs även i punkt 2 i artikeln.

I Finland motsvaras missbruk av apparatur enligt artikeln närmast av bestämmelserna om orsakande av fara för informationsbe-

handling i 34 kap. 9 a § i strafflagen. Enligt den nämnda paragrafens 1 punkt skall den dömas för orsakande av fara för informationsbehandling som för att orsaka olägenhet för informationsbehandling eller ett data- eller telesystems funktion tillverkar eller ställer till förfogande ett sådant datorprogram eller sådana programinstruktioner som har planerats för att äventyra informationsbehandling eller ett data- eller telesystems funktion eller för att skada data eller programvara som ingår i ett sådant system, eller sprider ett sådant datorprogram eller sådana programinstruktioner. Enligt paragrafens 2 punkt skall även den dömas som ställer till förfogande anvisningar för tillverkning av ett sådant datorprogram eller sådana programinstruktioner som avses i 1 punkten eller sprider sådana anvisningar.

Av de gärningar som avses i konventionen täcker den gällande bestämmelsen endast tillverkning och spridning av datavirus och motsvarande skadliga program. Innehav av skadliga program omfattas däremot inte av den nuvarande regleringen. Det finns inte heller några bestämmelser om den apparatur och de lösenord som avses i konventionen. Detsamma gäller program som används för att begå brott men som inte är skadliga program i egentlig mening, t.ex. program för dataintrång.

Enligt 6 § i lagen om dataskydd vid elektronisk kommunikation (516/2004) är innehav, import, tillverkning och distribution av system för avkodning av det tekniska skyddet vid elektronisk kommunikation eller av en del av ett sådant system förbjudet, om det primära ändamålet med systemet eller dess del är obehörig avkodning av det tekniska skyddet. Kommunikationsverket kan av godtagbara skäl bevilja tillstånd att avvika från detta förbud. I lagens 42 § finns en sekundär bestämmelse om uppsåtligt brott mot förbudet.

Artikel 6 i konventionen förutsätter ändringar i den gällande lagstiftningen.

I regeringens proposition föreslås att strafflagens 34 kap. 9 a § ändras så att bestämmelsen täcker de program och apparater som avses i artikel 6 i konventionen samt alla de gärningsformer som avses i artikeln.

Enligt den föreslagna 9 a § kan gärningen rikta sig mot apparater, datorprogram eller programinstruktioner som har skapats eller anpassats för att äventyra eller skada informationsbehandling eller ett informations- eller kommunikationssystems funktion eller för att bryta eller avkoda det tekniska skyddet vid elektronisk kommunikation eller skyddet för ett informationssystem.

Den föreslagna bestämmelsens tillämpningsområde är till dessa delar brett, och avsikten är att bestämmelsen skall täcka dels hjälpmedel som är avsedda för att begå dataintrång och skadegörelse i form av rent ofog, dels fysiska apparater, datorprogram och fragment av programkoder. Det i princip breda tillämpningsområdet begränsas dock avsevärt av kravet på att gärningen begås i syfte att orsaka skada eller olägenhet samt att användningsändamålet för den apparatur som är föremål för innehav, spridning eller en annan åtgärd enligt en objektiv bedömning skall vara klandervärt. Bägge villkoren skall vara uppfyllda samtidigt för att gärningen skall vara straffbar enligt bestämmelsen.

När det gäller apparatur täcker den föreslagna 9 a § ett något bredare område än den bestämmelse i artikel 6.1 a i i konventionen enligt vilken artikelns tillämpningsområde bestäms utifrån en apparats primära användningsändamål. Enligt punkt 73 i den förklarande rapporten avses med det primära användningsändamålet i detta sammanhang uttryckligen en apparats objektiva användningsändamål, dvs. det ändamål för vilket en apparat skapats och även kan användas för. Apparater med många olika användningssätt kan ha flera sådana användningsändamål. I den förklarande rapporten är utgångspunkten den att apparater med många olika användningssätt i regel inte omfattas av artikelns tillämpningsområde.

Om kriminaliseringen i enlighet med artikel 6 i konventionen begränsades till att endast gälla sådana apparater och program vilkas främsta syfte är att skada datorsystem eller användas i ett brottsligt förfarande, skulle detta betyda att ett stort antal apparater som kan användas även i brottslig verksamhet skulle hamna utanför kriminaliseringen. Det skulle inte vara straffbart att inneha och sprida dessa apparater, trots att det inte råder något tvivel om att de är avsedda att användas i

brottsligt syfte. Det finns ingen anledning att inte straffbelägga spridning av sådana apparater med dubbel användning vars främsta användningsändamål helt klart är godtagbart enbart på den grunden att konventionen inte nödvändigtvis förutsätter en kriminalisering, om syftet med användningen är att orsaka olägenhet eller skada för informationsbehandling.

Den föreslagna paragrafens tillämpningsområde begränsas i vilket fall som helst i tillräcklig utsträckning av kravet på att syftet med spridningen och de övriga gärningssätten som anges i bestämmelsen skall vara att orsaka olägenhet eller skada för ett informations- eller kommunikationssystem. Detta krav begränsar i praktiken väsentligt bestämmelsens tillämpningsområde i sådana situationer när det är fråga om apparater med dubbel användning. Om det har klarlagts att syftet med tillverkningen eller spridningen har varit att åstadkomma skada är det onödigt att dessutom uppställa ytterligare krav som gäller det primära användningsändamålet.

Förslagets innehåll behandlas närmare i detaljmotiveringen till lagförslaget i fråga.

Efter att den föreslagna ändringen trätt i kraft uppfyller de gällande bestämmelserna kraven i artikeln.

Enligt punkt 3 i artikeln får varje part förbehålla sig rätten att inte tillämpa punkt 1 i artikeln, om förbehållet inte avser försäljning, spridning eller annat tillgängliggörande av lösenord och åtkomstkoder som avses i punkt 1 a ii i artikeln.

Finland har inte något behov av att göra ett sådant förbehåll som avses i punkt 3.

Avdelning 2 Datorrelaterade brott

Artikel 7. *Datorrelaterad förfalskning.* Enligt artikeln skall följande gärningar straffbeläggas när de begås uppsåtligen och orättmätigt: att mata in, ändra, radera eller undertrycka datorbehandlingsbara uppgifter så att icke autentiska uppgifter uppstår med uppsåt att dessa skall beaktas eller ligga till grund för handlande i rättsliga hänseenden som om de vore autentiska, oavsett om uppgifterna är direkt läsbara och begripliga. En part får uppställa krav på bedrägligt uppsåt eller liknande brottsligt uppsåt för att straffansvar skall gälla.

Artikeln behandlas i punkterna 81—85 i den förklarande rapporten. Enligt rapporten är syftet med artikeln att datorrelaterad förfalskning skall omfattas av en likadan straffrättslig reglering som sedvanlig förfalskning. Artikelns skyddsobjekt är således integriteten och tillförlitligheten hos rättsligt relevanta data.

Förteckningen över gärningssätt motsvarar huvudsakligen förteckningen över gärningssätt som gäller systemstörning i artikel 5. Det väsentliga när det gäller artikel 7 är att det som en följd av gärningen uppstår icke autentiska uppgifter som kan användas som vilseledande bevis i rättsliga sammanhang. Det saknar betydelse för regleringen om de handlingar eller andra dokument i form av data som gärningen riktar sig mot är privata eller offentliga.

I Finland motsvaras datorrelaterad förfalskning närmast av bestämmelserna om förfalskning i 33 kap. 1 § och den kompletterande bestämmelsen med definitioner i 33 kap. 6 § i strafflagen. Enligt den nämnda straffbestämmelsen skall den dömas för förfalskning som framställer en falsk handling eller annat bevismedel eller som förfalskar ett dylikt bevismedel för att användas som vilseledande bevis, eller såsom sådant bevis använder ett falskt eller förfalskat bevismedel. Enligt definitionsbestämmelsen anses som bevismedel även upptagningar som lämpar sig för automatisk databehandling, om de används eller kan användas såsom rättsligt betydelsefulla bevis om rättigheter, förpliktelser eller fakta.

Gärningssätten är enligt bestämmelsen framställning eller förfalskning av bevismedel. Med framställning avses att ett nytt bevismedel skapas och med förfalskning att ett redan befintligt bevismedels innehåll ändras. Redan en obetydlig ändring kan innebära förfalskning. De två gärningssätten som nämns i bestämmelsen täcker tillsammans klart förteckningen över gärningssätt i artikeln.

Också en upptagning som lämpar sig för automatisk databehandling kan vara föremål för förfalskning. Som en sådan upptagning betraktas enligt förarbetena till lagen (RP 66/1988 rd) också t.ex. uppgifter som är lagrade i ett datorminne på maskinspråk och

som ännu inte matats ut på papper eller en bildskärm i synlig och begriplig form. Den upptagning som avses i bestämmelsen motsvarar således klart de datorbehandlingsbara uppgifter som anges i artikeln när det gäller föremålet för förfalskningen.

De gällande bestämmelserna motsvarar till dessa delar skyldigheterna enligt artikeln.

Artikeln förutsätter inte ändringar i lagstiftningen.

Enligt den sista meningen i artikeln får en part uppställa krav på bedrägligt uppsåt eller liknande brottsligt uppsåt för att straffansvar skall gälla.

Finland har inte något behov av att göra ett sådant förbehåll.

Artikel 8. *Datorrelaterat bedrägeri.* Enligt artikeln skall följande gärningar straffbeläggas när de begås uppsåtligen och orättmätigt: att förorsaka en annan person förlust av egendom genom att mata in, ändra, radera eller undertrycka datorbehandlingsbara uppgifter eller störa ett datorsystems drift, med bedrägligt eller annat brottsligt uppsåt och orättmätigt skaffa sig själv eller en annan person en ekonomisk förmån.

Artikeln behandlas i punkterna 86—90 i den förklarande rapporten. Enligt rapporten är syftet med artikeln att straffbelägga sådana egendomsbrott som begås genom att man ingriper i datorbehandlingsbara uppgifter eller ett datorsystems drift. Förteckningen över gärningssätt motsvarar huvudsakligen förteckningen i artikel 5, som gäller systemstörning. För att säkerställa att artikeln är heltäckande nämns i den dessutom också störande av ett datorsystems drift. Det väsentliga i fråga om artikel 8 är att en annan person förorsakas förlust av egendom till följd av gärningen och att gärningen begås med uppsåt att skaffa sig själv eller en annan person en ekonomisk förmån. För tydlighetens skull konstateras i artikeln dessutom att gärningen skall begås uppsåtligen och orättmätigt. När det gäller uppsåtet bör det noteras att uppsåtet skall innefatta samtliga element i rekvisitet.

I Finland motsvaras datorrelaterat bedrägeri enligt konventionen närmast av bestämmelserna om bedrägeri i strafflagens 36 kap. 1 § och särskilt dess 2 mom. Enligt grundrekvisitet i 1 mom. skall den dömas för bedrägeri som för att bereda sig eller någon annan orättmätig ekonomisk vinning eller för att skada någon annan, genom att vilseleda eller utnyttja misstag, förmår någon att göra eller underlåta något och därigenom orsakar ekonomisk skada för den som misstagit sig eller den vars intressen han kunnat förfoga över.

I 2 mom. föreskrivs om ett datorrelaterat gärningssätt. Enligt momentet döms också den för bedrägeri som i sådant syfte som nämns i 1 mom. matar in, ändrar, förstör eller undertrycker data eller på något annat sätt ingriper i ett informationssystems funktion så att resultatet av databehandlingen förvanskas och därigenom orsakar ekonomisk skada för någon annan. Bestämmelsen motsvarar artikel 8 i konventionen.

Enligt strafflagens 37 kap. 8 § skall dessutom den dömas för betalningsmedelsbedrägeri som olovligen använder eller överlåter ett betalningsmedel som lämpar sig för användning i ett datanät, eller som överskrider täckningen på ett konto eller en avtalad högsta kreditgräns.

De gällande bestämmelserna uppfyller nästan ordagrant kraven i artikeln. Artikeln förutsätter inte ändringar i lagstiftningen.

Avdelning 3 Innehållsrelaterade brott

Artikel 9. *Brott som hänför sig till barnpornografi.* Enligt punkt 1 i artikeln skall följande gärningar straffbeläggas:

a) Att framställa barnpornografi i syfte att sprida den med hjälp av datorsystem.

b) Att bjuda ut eller tillgängliggöra barnpornografi med hjälp av datorsystem.

c) Att sprida eller överföra barnpornografi med hjälp av datorsystem.

d) Att anskaffa barnpornografi åt sig själv eller någon annan med hjälp av datorsystem.

e) Att inneha barnpornografi i ett datorsystem eller i ett medium för lagring av datorbehandlingsbara uppgifter.

För de syften som avses i punkt 1 i artikeln skall enligt punkt 2 termen barnpornografi innefatta pornografiskt material som visuellt avbildar

a) en minderårig som ägnar sig åt handlande med uttrycklig sexuell innebörd,

b) en person som ser ut att vara minderårig som ägnar sig åt handlande med uttrycklig sexuell innebörd, och

c) realistiska bilder som föreställer en minderårig som ägnar sig åt handlande med uttrycklig sexuell innebörd.

För de syften som avses i punkt 2 i artikeln skall enligt punkt 3 termen minderårig innefatta alla personer under 18 års ålder. En part får dock kräva en lägre åldersgräns, som inte skall vara lägre än 16 år.

I Finland motsvaras de i artikeln avsedda brotten som hänför sig till barnpornografi av bestämmelserna om spridning av pornografisk bild i 18 §, grov spridning av barnpornografisk bild i 18 a § och innehav av barnpornografisk bild i 19 § i strafflagens 17 kap. Enligt den nämnda 18 § skall den dömas för spridning av pornografisk bild som tillverkar, saluför eller till uthyrning bjuder ut, för in i eller ut ur Finland eller genom Finland till ett annat land eller på annat sätt sprider bilder eller bildupptagningar som på ett sedlighetssårande sätt visar barn, våld, eller könsumgänge med djur. Enligt den nämnda 19 § skall den dömas för innehav av barnpornografisk bild som obehörigen innehar ett fotografi, ett videoband, en film eller någon annan verklighetstrogen bildupptagning som visar ett i 18 § 4 mom. avsett barn som deltar i samlag eller i något därmed jämförbart sexuellt umgänge, eller som visar barn på något annat uppenbart sedlighetssårande sätt.

Som barn betraktas enligt nämnda 18 § 4 mom. den som är yngre än aderton år och den vars ålder inte kan utredas, om det finns grundad anledning att anta att personen är yngre än aderton år.

De gällande bestämmelserna täcker också spridning och innehav av barnpornografi med hjälp av informationssystem. De gällande bestämmelserna uppfyller kraven i artikeln.

Avdelning 4 Brott som hänför sig till intrång i upphovsrätt och närstående rättigheter

Artikel 10. *Brott som hänför sig till intrång i upphovsrätt och närstående rättigheter.* Enligt artikeln skall vissa fall av intrång i upphovsrätt och närstående rättigheter straffbeläggas, när gärningarna begås uppsåtligen och med hjälp av ett datorsystem. Artikelns tillämpningsområde har begränsats till att gälla endast gärningar som begås i kommersiell skala. Artikeln gäller inte upphovsrättens ideella utan endast dess ekonomiska dimensioner. De upphovsrätter som avses i artikeln specificeras på ett uttömmande sätt genom en hänvisning till de internationella konventionerna om upphovsrätt. Artikeln ålägger således endast parterna en skyldighet att se till att även de gärningssätt som hänför sig till utnyttjande av informationssystem beaktas i de kriminaliseringar som grundar sig på de nämnda konventionerna.

Artikeln behandlas i punkterna 107—117 i den förklarande rapporten. Enligt rapporten är uttryckligen brott som hänför sig till intrång i upphovsrätt den överlägset vanligaste brottstypen i internetmiljön, vilket beror på den tilltagande digitaliseringen som leder till att olika verk blir lätta att kopiera. Därför har det varit nödvändigt att i konventionen ta in bestämmelser också om intrång i upphovsrätt. Artikeln gäller däremot inte patenträtt eller varumärkesrätt.

Artikeln är för respektive medlemsstats del förpliktande endast inom de ramar som de internationella överenskommelser till vilka det hänvisas i artikeln anger. Om en stat inte är part i en internationell överenskommelse om upphovsrätt, är artikeln över huvud taget inte förpliktande till dessa delar. Om en stat har gjort ett förbehåll till en överenskommelse är artikeln förpliktande endast i den omfattning som förbehållet anger. Om en stat står i beråd att tillträda en internationell överenskommelse om upphovsrätt, är artikeln förpliktande först fr.o.m. tillträdandet. Trots att skyldigheterna enligt artikeln har begränsats så att de endast omfattar gärningar som begås i kommersiell skala hindrar detta inte de fördragsslutande staterna från att bestämma om mera långtgående skyldigheter.

I artikeln hänvisas till följande internationella överenskommelser:

1. Bernkonventionen från 1886 för skydd av litterära och konstnärliga verk (nedan Bernkonventionen)

2. Romkonventionen från 1961 om skydd för utövande konstnärer, framställande av fonogram och radioföretag (nedan Romkonventionen)

3. Avtalet från 1995 om handelsrelaterade aspekter av immaterialrätter (nedan TRIPS-avtalet)
4. WIPO-fördraget från 1996 om upphovsrätt och
5. WIPO-fördraget från 1996 om framföranden och fonogram.

Bernkonventionen (FördrS 79/1986) är den viktigaste överenskommelsen om internationellt upphovsrättsligt skydd. Konventionen upprättades 1886, och den har reviderats i genomsnitt vart tjugonde år. Senast reviderades konventionen i Paris 1971. Bernkonventionens huvudprinciper är nationell behandling och minimiskydd. Verk med ursprung i en annan fördragsslutande stat skall tillerkännas samma skydd som verk av den egna statens medborgare. Till de viktigaste skyldigheterna med avseende på skyddsnivån hör bl.a. skyddstiden på 50 år som räknas från det år då upphovsmannen avlidit, rätten att framställa exemplar av ett verk samt rätten till framförande och till rundradiering. Bernkonventionen administreras av Världsorganisationen för den intellektuella äganderätten WIPO (World Intellectual Property Organization). Bernkonventionen har tillträtts av 149 stater. Finland anslöt sig till konventionen 1928.

Romkonventionen (FördrS 56/1983) är den viktigaste överenskommelsen om internationellt skydd för närstående rättigheter. Konventionen är avsedd att utgöra ett grundfördrag om de rättigheter som tillkommer utövande konstnärer, fonogramproducenter samt radio- och televisionsföretag. I konventionen tillerkänns varje rättsinnehavargrupp vissa minimirättigheter. Konventionen förpliktar även de fördragsslutande staterna att bevilja nationell behandling med avseende på det särskilda skydd som tillförsäkras genom konventionen. Romkonventionen administreras av ett trepartssekretariat upprättat av WIPO, Unesco och Internationella arbetsorganisationen. Romkonventionen har tillträtts av 68 stater. Finland anslöt sig till konventionen 1983.

TRIPS-avtalet utgör ett handelspolitiskt instrument som ingår som bilaga till grundfördraget om upprättandet av Världshandelsorganisationen (WTO). Syftet med avtalet är att fastställa ett globalt skydd för industriella rättigheter och upphovsrättigheter. Avtalets upphovsrättsliga substans består av bestämmelser om bl.a. skydd av utövande konstnärer, fonogramproducenter och rundradioorganisationer samt fastställandet att Bernkonventionen skall iakttas av varje medlemsstat i WTO. Avtalet innehåller således bestämmelser om såväl upphovsrättigheter som närstående rättigheter. I avtalet ingår även bestämmelser om verkställighet av rättigheter, bestämmelser om avgörande av meningsskiljaktigheter och kriminaliseringsskyldigheter av tvingande natur som gäller t.ex. kommersiell piratism. Eftersom Finland är medlem av WTO är avtalet bindande för Finland.

WIPO-fördraget om upphovsrätt är en särskild överenskommelse som kompletterar Bernkonventionen. Fördraget innebär inte någon ändring av Bernkonventionen. Även sådana stater som är medlemmar av WIPO men inte har tillträtt Bernkonventionen kan tillträda fördraget. WIPO-fördraget om upphovsrätt kompletterar Bernkonventionen genom att på global nivå garantera upphovsmän till litterära och konstnärliga verk nya rättigheter och effektivare utövning av deras existerande rättigheter.

WIPO-fördraget om framföranden och fonogram är ett nytt fördrag om utövande konstnärers och fonogramproducenters rättigheter, som på motsvarande sätt inte inverkar på tillämpningen av Romkonventionen. Även sådana stater som är medlemmar av WIPO men inte har tillträtt Romkonventionen kan tillträda WIPO-fördraget. WIPO-fördraget om framföranden och fonogram förbättrar det globala skyddet för utövande konstnärers och fonogramproducenters rättigheter bl.a. genom att garantera dem nya rättigheter och effektivare utövning av deras existerande rättigheter.

Genom WIPO-fördragen anpassas det internationella fördragssystemet inom upphovsrättsområdet till de speciella frågor som gäller digitalteknik och datanät. I fördragen har särskilt beaktats den inverkan som utvecklingen av och samverkan mellan informations- och kommunikationsteknologierna har på skapandet och användningen av litterära och konstnärliga verk samt framställningen och användningen av framföranden

och fonogram. Fördragen innehåller också bestämmelser om rättsligt skydd av tekniska åtgärder samt av information om rättighetsförvaltning.

Lagarna om sättande i kraft av de bestämmelser i WIPO-fördraget om upphovsrätt och WIPO-fördraget om framföranden och fonogram som hör till området för lagstiftningen stadfästes den 14 oktober 2005 (823—824/2005). Om ikraftträdandet av lagarna bestäms senare genom förordning.

De straffrättsliga bestämmelser som de överenskommelser som har satts i kraft nationellt förutsätter finns i upphovsrättslagen och i strafflagen.

De gällande bestämmelserna om de brott som motsvarar de gärningar som avses i konventionen finns huvudsakligen i strafflagens 49 kap. 1 §, som gäller upphovsrättsbrott. Enligt paragrafens 1 mom. skall den dömas för upphovsrättsbrott som i förvärvssyfte i strid med upphovsrättslagen och så att gärningen är ägnad att åsamka innehavaren av den kränkta rätten betydande men eller skada, gör intrång i någon annans rätt till en sådan upphovsrätt eller närstående rättighet som anges närmare i bestämmelsen. Enligt 2 mom. är det också straffbart att föra in olagliga kopior i landet i syfte att sprida dessa. I upphovsrättslagens 56 a § finns dessutom en bestämmelse om förseelser där det varken förutsätts något förvärvssyfte eller att betydande skada har förorsakats.

Lagen om ändring av 49 kap. i strafflagen (822/2005) trädde i kraft den 1 januari 2006. Genom lagen fogades ett nytt 3 mom. till bestämmelsen om upphovsrättsbrott i 49 kap. 1 § i strafflagen. För upphovsrättsbrott döms enligt momentet också den som med hjälp av datanät eller datasystem gör intrång i någon annans rättigheter när det gäller skyddade objekt som nämns i paragrafens 1 mom. på ett sådant sätt att gärningen är ägnad att åsamka innehavaren av den kränkta rätten betydande skada eller olägenhet. Efter lagändringen förutsätts det inte längre något förvärvssyfte när ett upphovsrättsbrott begås i ett datasystem eller med hjälp av ett datanät. I och med detta blir det lättare än förut att bedöma en gärning som upphovsrättsbrott i stället för upphovsrättsförseelse, vilket för sin del enligt motiveringen till regeringens proposition (RP 28/2004 rd) effektiverar utredningen av dessa brott bl.a. genom att husrannsakan blir möjlig.

Artikel 8 i konventionen innefattar endast kränkningar som gjorts i kommersiellt syfte. Efter att den ovan nämnda ändringen av 49 kap. 1 § i strafflagen trätt i kraft går lagstiftningen utöver vad som krävs i artikeln när det gäller upphovsrättsbrott som begås i ett datasystem eller med hjälp av ett datanät, eftersom det inte längre förutsätts något förvärvssyfte. Artikeln förutsätter inte ändringar i lagstiftningen.

I punkt 3 i artikeln sägs att en part får förbehålla sig rätten att inte införa straffansvar enligt punkterna 1 och 2 i denna artikel i begränsad omfattning, under förutsättning att andra effektiva rättsliga åtgärder kan komma i fråga och att förbehållet inte innebär ett avsteg från partens internationella skyldigheter enligt de internationella instrument som nämns i punkterna 1 och 2 i denna artikel.

Finland har inte något behov av att göra sådana förbehåll som avses i punkten.

Avdelning 5 Andra former av ansvar och påföljder

Artikel 11. *Försök och medhjälp.* Enligt punkt 1 i artikeln skall uppsåtlig medhjälp till något av de brott som straffbeläggs i enlighet med artiklarna 2—10 i konventionen med uppsåt att begå sådant brott straffbeläggas.

Punkt 1 i artikeln behandlas i punkterna 118 och 119 i den förklarande rapporten. Enligt rapporten kan t.ex. en operatör som deltar i förmedlingen av ett meddelande som innehåller brottsligt material på grund av kravet på uppsåt inte bli straffrättsligt ansvarig enbart på denna grund. Artikeln medför inte heller någon skyldighet för operatören att självmant övervaka innehållet i de meddelanden som förmedlas.

I Finland kriminaliseras anstiftan och medhjälp i 5 och 6 § i strafflagens 5 kap. En anstiftare jämställs med en gärningsman med avseende på straffbarheten. En medhjälpare döms enligt en lindrigare skala.

De gällande bestämmelserna motsvarar till dessa delar skyldigheterna enligt artikeln. Artikeln förutsätter inte ändringar i lagstiftningen.

Enligt punkt 2 i artikeln skall uppsåtligt försök till något av de brott som straffbeläggs i enlighet med artiklarna 3—5, 7, 8 samt 9.1 a och 9.1 c i konventionen straffbeläggas. Enligt punkt 3 i artikeln får varje part förbehålla sig rätten att, helt eller delvis, inte tillämpa punkt 2, som gäller kriminalisering av försök.

Punkt 2 i artikeln behandlas i punkterna 120—122 i den förklarande rapporten. Enligt rapporten har de lagstiftningstekniska och eventuella andra problem som inom de olika rättssystemen hänför sig till kriminalisering av försök beaktats i punkt 2 i artikeln. Tillämpningsområdet för punkt 2 har i enlighet med detta begränsats till endast vissa sådana brott i fråga om vilka en kriminalisering av försök inte torde vara förenat med några särskilda problem. Utöver detta kan en part göra ett förbehåll beträffande vilket som helst brott eller vid behov beträffande hela punkten.

Enligt artikeln skall således varje part antingen göra ett förbehåll eller straffbelägga försök, om detta inte redan har gjorts, när det gäller följande brott enligt konventionen:

1) olaglig avlyssning (artikel 3),
2) datastörning (artikel 4),
3) systemstörning (artikel 5),
4) datorrelaterad förfalskning (artikel 7),
5) datorrelaterat bedrägeri (artikel 8),
6) att framställa barnpornografi (artikel 9.1 a) och
7) att sprida eller överföra barnpornografi (artikel 9.1 c).

I Finland är försök straffbart i fråga om följande brott som motsvarar de brott som anges ovan:

1) kränkning av kommunikationshemlighet (SL 38:3 §),
2) grov kränkning av kommunikationshemlighet (SL 38:4 §),
3) grov skadegörelse (SL 35:2 §),
4) förfalskning (SL 33:1 §),
5) grov förfalskning (SL 33:2 §),
6) bedrägeri (SL 36:1 §),
7) grovt bedrägeri (SL 36:2 §) och
8) spridning av pornografisk bild (SL 17:18 §).

Artikeln förutsätter således att ett förbehåll görs eller att försök kriminaliseras i fråga om följande brott i strafflagen:

1) skadegörelse (SL 35:1 §),
2) lindrig skadegörelse (SL 35:3 §),
3) störande av post- och teletrafik (SL 38:5 §),
4) grovt störande av post- och teletrafik (SL 38:6 §),
5) lindrigt störande av post- och teletrafik (SL 38:7 §) och
6) lindrig förfalskning (SL 33:3 §).

Dessutom bör ett förbehåll göras eller försök kriminaliseras i fråga om systemstörning och den grova gärningsformen av brottet. Bestämmelser om dessa brott föreslås i denna proposition bli intagna som nya 7 a och 7 b § i strafflagens 38 kap.

I regeringens proposition föreslås att försök till följande brott kriminaliseras:

1) skadegörelse (SL 35:1 §),
2) störande av post- och teletrafik (SL 38:5 §),
3) grovt störande av post- och teletrafik (SL 38:6 §),
4) lindrigt störande av post- och teletrafik (SL 38:7 §),
5) systemstörning (SL 38:7 a §, ny) och
6) grov systemstörning (SL 38:7 b §, ny).

Efter att den föreslagna ändringen trätt i kraft uppfyller de gällande bestämmelserna till dessa delar kraven enligt artikeln.

Beträffande de övriga brott som avses i artikeln kommer Finland enligt förslaget att göra ett förbehåll. Förbehållet gäller således lindrig skadegörelse (SL 35:3 §) och lindrig förfalskning (SL 33:3 §).

När det gäller lindrig skadegörelse och förfalskning är det inte ändamålsenligt att kriminalisera försök, eftersom detta skulle medföra ett alltför omfattande straffrättsligt ansvar med hänsyn till gärningarnas ringa natur. I fråga om lindrig förfalskning bör det dessutom noteras att innehav av förfalskningsredskap eller -tillbehör med stöd av strafflagens 33 kap. 4 § är straffbart som innehav av förfalskningsmaterial.

Artikel 12. *Juridiska personers ansvar.* Enligt punkt 1 i artikeln skall juridiska personer kunna ställas till ansvar för gärningar som straffbeläggs i enlighet med konventionen, om de har begåtts till deras förmån av en fysisk person som handlat individuellt eller som en del av ett organ tillhörande den juridiska personen och som har en ledande ställ-

ning inom denna grundad på en fullmakt att företräda den juridiska personen, ett bemyndigande att fatta beslut på den juridiska personens vägnar eller ett bemyndigande att utöva kontroll inom den juridiska personen. Enligt punkt 2 skall en juridisk person kunna ställas till ansvar för gärningar som straffbeläggs i konventionen också när bristande övervakning eller kontroll som skall utföras av en sådan fysisk person som avses i punkt 1 i artikeln har gjort det möjligt för en fysisk person, som handlar på den juridiska personens vägnar, att begå brott som straffbeläggs i enlighet med konventionen till förmån för den juridiska personen. I punkt 4 konstateras för tydlighetens skull att sådant ansvar inte skall inverka på straffansvaret för de fysiska personer som har gjort sig skyldiga till brottet.

Artikeln behandlas i punkterna 123—127 i den förklarande rapporten. Enligt rapporten står bestämmelserna i samklang med den rådande allmänna trenden som betonar straffrättsligt ansvar för juridiska personer. Artikeln omfattar utöver aktiva gärningar också försummelse av övervakningsskyldighet.

Följande fyra villkor skall vara uppfyllda för att ansvar enligt punkt 1 skall gälla: ett brott som avses i konventionen har begåtts, brottet har begåtts till förmån för en juridisk person, gärningsmannen har en ledande ställning inom den juridiska personen och gärningsmannen har begått gärningen genom att utnyttja fullmakter eller bemyndiganden som han eller hon har i kraft av sin ledande ställning. Punkt 2 i artikeln omfattar också situationer när gärningen har begåtts för en juridisk persons räkning av en person som inte har en ledande ställning inom den juridiska personen, om en person i ledande ställning kan anses ha försummat sin övervakningsskyldighet. I dessa fall är det vanligtvis fråga om t.ex. en arbetstagare inom ett företag. Övervakningsskyldigheten för en person i ledande ställning skall tolkas så att den begränsar sig endast till sedvanliga övervakningsåtgärder av normal omfattning. Vad detta innebär i praktiken skall avgöras från fall till fall med beaktande av t.ex. affärsverksamhetens art och omfattning.

I Finland finns de allmänna bestämmelserna om straffansvar för juridiska personer i strafflagens 9 kap. När det gäller de enskilda straffbestämmelserna förutsätts det för att straffansvar för juridiska personer skall bli tillämpligt att det finns en hänvisningsbestämmelse om saken i strafflagen.

Enligt 9 kap. 2 § 1 mom. i strafflagen döms en juridisk person till samfundsbot, om någon som hör till ett av dess lagstadgade organ eller annars hör till dess ledning eller utövar faktisk beslutanderätt inom den juridiska personen har varit delaktig i brottet eller tillåtit att brottet har begåtts eller om i den juridiska personens verksamhet inte har iakttagits den omsorg och försiktighet som krävs för att förebygga brottet. Begreppet delaktig i brott används i paragrafen i vid bemärkelse så att det även innefattar egentligt gärningsmannaansvar. Enligt samma paragrafs 2 mom. döms samfundsbot ut även om det inte kan utredas vem gärningsmannen är eller om gärningsmannen av någon annan anledning inte döms till straff. Enligt kapitlets 3 § anses ett brott begånget i en juridisk persons verksamhet, om gärningsmannen har handlat på den juridiska personens vägnar eller till dess förmån och han hör till den juridiska personens ledning eller står i tjänste- eller arbetsförhållande till denna eller han har handlat på uppdrag av en representant för den juridiska personen.

Den ovan nämnda regleringen motsvarar inte till alla delar ordalydelse i artikeln.

Punkt 1 i artikeln gäller en juridisk persons ansvar när gärningsmannen hör till den juridiska personens ledning. I artikeln definieras också vad som avses med ledande ställning. En persons ledande ställning inom en juridisk person kan grunda sig på en fullmakt att företräda den juridiska personen, ett bemyndigande att fatta beslut på den juridiska personens vägnar eller ett bemyndigande att utöva kontroll inom den juridiska personen.

I strafflagens 9 kap. finns inte någon uttömmande definition av begreppet ledning. I kapitlets 2 § 1 mom. sägs att den som hör till ett lagstadgat organ inom en juridisk person hör till den juridiska personens ledning. Med lagstadgat organ avses t.ex. en förenings, en stiftelses eller ett aktiebolags styrelse, ett aktiebolags förvaltningsråd och verkställande direktör samt en ansvarig bolagsman i kommanditbolag. Dessutom konstateras i mo-

mentet att även verksamhet som bedrivs av personer som annars hör till en juridisk persons ledning kan utgöra grund för ansvar för den juridiska personen.

Enligt punkt 1 a i artikeln skall ansvaret utsträckas till personer som har en ledande ställning inom en juridisk person grundad på en fullmakt att företräda den juridiska personen. Enligt finsk rätt anses den som har fullmakt att företräda en juridisk person inte nödvändigtvis höra till den juridiska personens ledning. Om en sådan person har handlat på uppdrag av en representant för den juridiska personen så som anges i 9 kap. 3 § 1 mom. i strafflagen kan straffrättsligt ansvar dock uppkomma för den juridiska personen. Till dessa delar uppfyller lagstiftningen således kraven i konventionen.

Enligt punkt 1 b i artikeln skall ansvaret utsträckas till personer som har en ledande ställning inom en juridisk person grundad på ett bemyndigande att fatta beslut på den juridiska personens vägnar. För att ansvar skall kunna uppkomma på grundval av beslutanderätt så som avses i 9 kap. 2 § i strafflagen måste personen i fråga ha vida befogenheter att fatta självständiga beslut. Den som hör till mellanledningen har i allmänhet inte i denna bemärkelse ansetts höra till ledningen så som avses i 2 § (RP 95/1993 rd). Eftersom utövandet av faktisk beslutanderätt nämns särskilt som en omständighet som utgör grund för ansvar, uppfyller lagstiftningen även till dessa delar kraven i konventionen.

Enligt punkt 1 c i artikeln skall ansvaret utsträckas till personer som har en ledande ställning inom en juridisk person grundad på ett bemyndigande att utöva kontroll inom den juridiska personen. I Finland anses sådana personer i allmänhet inte höra till en juridisk persons ledning. Om en sådan person har begått ett brott kan straffrättsligt ansvar dock uppkomma för den juridiska personen på basis av personens ställning som arbetstagare, trots att han eller hon inte hör till den juridiska personens ledning.

Den bristande övervakning eller kontroll som avses i punkt 2 i artikeln motsvaras av bestämmelsen om underlåtelse att iaktta omsorg och försiktighet i 9 kap. 2 § 1 mom. i strafflagen. I konventionen har försummelsen dock, till skillnad från vad som är fallet i Finland, kopplats till en sådan ledande ställning inom en juridisk person som avses i punkt 1 i artikeln. Så som konstaterats ovan hör hela den krets av personer som avses i punkt 1 i artikeln inte enligt strafflagens 9 kap. till en juridisk persons ledning. För att en juridisk person skall kunna ställas till straffrättsligt ansvar för en försummelse enligt 9 kap. 2 § 1 mom. i strafflagen förutsätts det inte att den som gjort sig skyldig till den omedelbara försummelse som har möjliggjort brottet hör till den juridiska personens ledning. Det räcker att det har varit fråga om någon form av försumlighet även från ledningens sida. För att bestämmelsen skall kunna tillämpas bör försummelsen dessutom åtminstone ha väsentligt ökat möjligheten att begå ett brott i den juridiska personens verksamhet.

Enligt 9 kap. 2 § 2 mom. i strafflagen döms samfundsbot ut även om det inte kan utredas vem gärningsmannen är eller om gärningsmannen av någon annan anledning inte döms till straff. I finsk rätt går huvudprinciperna för straffansvar för juridiska personer således något utöver vad som bestäms i konventionen, eftersom konventionen inte förutsätter att en dylik anonym skuld utsträcks till de brott som nämns i den.

Den allmänna regleringen som behandlats ovan uppfyller således till sitt innehåll kraven i konventionen. Enligt de gällande bestämmelserna är ansvar för juridiska personer dock inte tillämpligt på alla de brott som avses i artikeln. Artikeln verkar därför förutsätta ändringar i den gällande lagstiftningen, åtminstone till den del brotten har begåtts med hjälp av ett informationssystem.

Enligt punkt 3 i artikeln får den juridiska personens ansvar dock vara av straffrättslig, civilrättslig eller administrativ natur, beroende på principerna i partens rättsordning. Enligt artikeln behöver ansvaret således inte nödvändigtvis vara av straffrättslig natur, utan t.ex. ett civilrättsligt skadeståndsansvar är tillräckligt för att kraven i artikeln skall uppfyllas. I Finland kan en juridisk person i de fall som avses i artikeln alltid bli skadeståndsansvarig för en skada som orsakats genom brott. Även vinningen av brott konfiskeras. Finland behöver därför inte göra något förbehåll i saken eller avge någon förklaring, även om lagen inte ändras på grund av arti-

keln.

I Finland gäller dock straffrättsligt ansvar för juridiska personer, och det är naturligt att utsträcka detta ansvar till att omfatta även de brott som avses i konventionen. Dessutom förutsätter artikel 9 i rambeslutet såsom anges nedan att juridiska personer kan bli föremål för böter eller administrativa avgifter. Uppkomsten av skadeståndsansvar är inte tillräckligt för att uppfylla skyldigheterna enligt rambeslutet.

Av dessa orsaker föreslås det i regeringens proposition att straffansvaret för juridiska personer utsträcks till att gälla följande brott:

1) orsakande av fara för informationsbehandling (SL 34:9 a §)
2) skadegörelse (SL 35:1 §),
3) grov skadegörelse (SL 35:2 §),
4) kränkning av kommunikationshemlighet (SL 38:3 §),
5) grov kränkning av kommunikationshemlighet (SL 38:4 §),
6) störande av post- och teletrafik (SL 38:5 §),
7) grovt störande av post- och teletrafik (SL 38:6 §),
8) systemstörning (SL 38:7 a §, ny),
9) grov systemstörning (SL 38:7 b §, ny),
10) dataintrång (SL 38:8 §),
11) grovt dataintrång (SL 38:8 a §, ny) och
12) upphovsrättsbrott (SL 49:1 §).

För att det straffrättsliga systemet skall vara klart och konsekvent bör straffansvaret för juridiska personer inte utan tvingande skäl begränsas så att det gäller en särskilt specificerad kategori gärningar som uppfyller ett visst rekvisit. Därför föreslås det också att straffansvaret för juridiska personer utsträcks till att gälla t.ex. upphovsrättsbrott i dess helhet. När det gäller upphovsrättsbrott faller detta sig också annars naturligt, eftersom den verksamhet som kriminaliseras i bestämmelsen om detta brott ofta bedrivs av en juridisk person.

Däremot är det inte ändamålsenligt att utsträcka straffansvaret för juridiska personer till de lindriga gärningsformerna av skadegörelse och störande av post- och teletrafik eller till innehav av hjälpmedel vid nätbrott med tanke på dessa gärningars art och ringa betydelse. Därför föreslås inga ändringar i den gällande lagen för deras del.

Efter att de ändringar som föreslås här har trätt i kraft motsvarar de gällande bestämmelserna skyldigheterna i konventionen, med undantag av lindrig skadegörelse, lindrigt störande av post- och teletrafik, lindrig systemstörning och innehav av hjälpmedel vid nätbrott.

Artikel 13. *Påföljder och åtgärder.* Enligt punkt 1 i artikeln skall varje part tillse att de brott som straffbeläggs i enlighet med artiklarna 2—11 är straffbara med effektiva, proportionella och avskräckande påföljder, innefattande frihetsberövande.

I punkt 2 i artikeln sägs att varje part skall tillse att juridiska personer som fälls till ansvar i enlighet med artikel 12 underkastas effektiva, proportionella och avskräckande straffrättsliga eller icke straffrättsliga påföljder eller åtgärder, innefattande ekonomiska påföljder.

I artikeln överlåts det på parterna att bestämma påföljd och skalor. Artiklarna förutsätter inte ändringar i lagstiftningen.

Avsnitt 2 Processrätt

Avdelning 1 Gemensamma bestämmelser

Artikel 14. *De processrättsliga bestämmelsernas räckvidd.* Artikeln innehåller bestämmelser om tillämpningsområdet för avsnitt 2, som gäller processrätt, samt om de förbehåll som får göras beträffande avsnittet. Artikeln gäller enligt 1 punkten alla de tvångsmedel som regleras i avsnitt 2, dvs. skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter (artikel 16), skyndsamt säkrande och partiellt röjande av trafikuppgifter (artikel 17), skyldighet att lämna uppgifter (artikel 18), husrannsakan och beslag av lagrade datorbehandlingsbara uppgifter (artikel 19), insamling i realtid av trafikuppgifter (artikel 20) och avlyssning av innehållsuppgifter (artikel 21).

Enligt punkt 2 i artikeln skall tvångsmedlen i regel i samtliga fall tillämpas på de brott som straffbeläggs i enlighet med konventionen, andra brott som begåtts med hjälp av ett datorsystem och insamling av bevis i elektronisk form om ett brott. Rätten att begränsa de tvångsmedel som avses i artikel 21, som gäller innehållsuppgifter, till enbart vissa

grova brott utgör dock ett undantag från denna huvudregel.

I punkt 3 a i artikeln sägs att varje part får förbehålla sig rätten att endast tillämpa de åtgärder som avses i artikel 20, som gäller trafikuppgifter, på brott eller brottstyper som anges i förbehållet, under förutsättning att omfattningen av dessa brott eller brottstyper inte är mer begränsad än det urval av brott på vilka parten med stöd av artikel 21 tillämpar de åtgärder som avses i den artikeln.

Enligt punkt 3 b i artikeln får varje part förbehålla sig rätten att inte tillämpa de åtgärder som avses i artiklarna 20 och 21 på meddelanden som överförs inom ett datorsystem som drivs för en sluten användargrupp och inte använder allmänna kommunikationsnät och inte är anslutet till ett annat datorsystem, oavsett om detta är offentligt eller enskilt.

Artikeln behandlas i punkterna 140—144 i den förklarande rapporten. Enligt rapporten är tvångsmedlens tillämpningsområde brett, eftersom avsikten med konventionen är att elektroniskt bevismaterial i digital form och insamling av dylikt bevismaterial skall ha samma ställning som konventionellt bevismaterial i fråga om samtliga brott.

Avlyssning av innehållsuppgifter och insamling av trafikuppgifter utgör dock ett undantag. I dessa fall har parterna möjlighet att begränsa användningen av tvångsmedel. Detta beror på att dessa tvångsmedel är av sådan karaktär att de utgör ett intrång i hemligheten i fråga om förtroliga meddelanden och en integritetskränkning. Avlyssning av innehållsuppgifter ingriper i högre grad i en persons rättsliga ställning än enbart insamling av trafikuppgifter. Enligt artikeln har parterna därför inte rätt att begränsa användningen av tvångsmedel mera i fråga om trafikuppgifter än i fråga om ett meddelandes innehållsuppgifter.

Syftet med artikelns punkt 3 b, som gäller fristående slutna nät, är att garantera parter som till följd av begränsningar i sin nationella lagstiftning inte kan tillåta användning av tvångsmedel enligt artiklarna 20 och 21 i sådana helt privata nät en möjlighet att göra ett förbehåll.

När det gäller denna artikel bör det ytterligare noteras att tillämpningsområdet sådant det fastställs i artikeln inte innefattar polisens kriminalunderrättelseverksamhet.

Artikelns konsekvenser för behovet av att ändra lagstiftningen påverkas också av de artiklar som gäller tvångsmedlens innehåll. Behovet av att göra eventuella förbehåll bedöms i motiveringen till artiklarna 20 och 21.

Artikel 15. *Villkor och garantier.* Artikeln innehåller allmänna bestämmelser om principerna för de villkor som iakttas vid användningen av tvångsmedel och om rättsskyddsgarantier.

Enligt punkt 1 i artikeln skall vid användningen av tvångsmedel iakttas proportionalitetsprincipen och även i övrigt tillses att användningen av dessa inte står i strid med skyddet för mänskliga rättigheter och friheter enligt internationella fördrag.

I punkt 2 i artikeln sägs att ändamålsenliga rättsskyddsgarantier såsom rättslig tillsyn och tillräcklig begränsning av omfattningen och varaktigheten av tvångsmedlet skall säkerställas.

Enligt punkt 3 i artikeln skall även tredje mans rättmätiga intressen beaktas vid användningen av tvångsmedel.

Artikeln behandlas i punkterna 145—148 i den förklarande rapporten. Enligt rapporten har det avsiktligt överlåtits åt parterna att bestämma hur principerna för villkor och rättsskyddsgarantierna genomförs i den nationella lagstiftningen. Parternas rättssystem skiljer sig från varandra, och det är därför inte möjligt att utfärda detaljerade bestämmelser om saken. De människorättskonventioner som nämns i exempelförteckningen i punkt 1 i artikeln anger minimikraven för regleringen. I enlighet med proportionalitetsprincipen skall det tvångsmedel som används och de olägenheter som det medför stå i rimlig proportion till hur skadligt brottet är och andra motsvarande omständigheter. Också rätten att begränsa de tvångsmedel som avses i artikel 21 till endast vissa grova brott följer av proportionalitetsprincipen. De rättsskyddsgarantier och villkor som avses i punkt 2 i artikeln skall dimensioneras så att de står i rimlig proportion till de olägenheter som tvångsmedlet medför. T.ex. avlyssning av innehållsuppgifter ingriper i högre grad i en persons rättsliga ställning än enbart ett föreläggande att säkra ett meddelande. Därför kan

även rättsskyddsgarantierna och villkoren skilja sig från varandra i fråga om dessa tvångsmedel. En sådan tredje man som avses i punkt 3 i artikeln kan vara t.ex. en teleoperatör. Parterna skall beakta tvångsmedlens konsekvenser också med hänsyn till allmänintresset och tredje man och i mån av möjlighet försöka minska de olägenheter som uppstår.

De internationella fördrag som det hänvisas till i punkt 1 i artikeln är i Finland i kraft såsom lag.

Frågan om hur artikeln förhåller sig till den gällande lagstiftningen och de föreslagna ändringarna behandlas i samband med artiklarna om tvångsmedlen och dessutom också i detaljmotiveringen till de lagändringar som dessa föranleder.

Avdelning 2 Skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter

Artikel 16. *Skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter.* Artikeln innehåller bestämmelser om skyldighet att säkra datorbehandlingsbara uppgifter. Enligt punkt 1 i artikeln skall myndigheterna kunna hindra att datorbehandlingsbara uppgifter som är av betydelse vid utredningen av brott går förlorade eller förändras innan de kan tas i besittning med stöd av något annat tvångsmedel. Att uppgifterna inte förändras kan säkerställas genom att den som har uppgifterna i sin vård ges ett särskilt föreläggande att säkra uppgifterna eller på något annat sätt som parterna finner lämpligt. Artikeln gäller också säkrande av trafikuppgifter. Begreppet trafikuppgifter behandlas närmare i motiveringen till artikel 17 nedan.

Punkt 2 i artikeln gäller förelägganden om att säkra uppgifter. Enligt punkten kan föreläggandet ges till den som har uppgifterna i sin besittning eller under sin kontroll. Föreläggandet skall gälla tillräckligt länge med hänsyn till dess syfte, dock högst 90 dagar. Föreläggandet får dock förnyas.

Enligt punkt 3 i artikeln är den som har de datorbehandlingsbara uppgifterna i sin vård skyldig att hemlighålla ett ovan nämnt föreläggande.

I punkt 4 i artikeln sägs att bestämmelserna om räckvidd samt begränsningsgrunder och rättsskyddsgarantier i artiklarna 14 och 15 skall gälla för de tvångsmedel som avses i artikeln.

Artikeln behandlas i punkterna 149—164 i den förklarande rapporten. Enligt rapporten är syftet med bestämmelserna att ge ett alternativ till t.ex. beslag som gör det möjligt att snabbt och enkelt säkra och bevara datorbehandlingsbara uppgifter orubbade utan att man inkräktar mer än vad som är nödvändigt på rättigheterna för den som har uppgifterna i sin vård. När det gäller IT-relaterad brottslighet finns det viktigaste bevismaterialet ofta i form av datorbehandlingsbara uppgifter. Informationssystemen innehåller stora mängder uppgifter, som tekniskt sett är lätta att utplåna eller ändra. Därför är det viktigt med särskild reglering uttryckligen för att säkra datorbehandlingsbara uppgifter. Särskilt viktigt är detta i gränsöverskridande fall där det traditionella internationella samarbetet ofta går långsamt på grund av tidskrävande förfaringsregler. Om prövningen av en framställning om rättslig hjälp räcker länge kan det hända att datorbehandlingsbara uppgifter som utgör bevismaterial går förlorade under förfarandet. I detta sammanhang bör noteras att det i bestämmelsen om internationellt samarbete i artikel 29.3 för att påskynda förfarandet bl.a. sägs att dubbel straffbarhet inte får uppställas som ett villkor i fråga om besvarande av en framställning om föreläggande att säkra datorbehandlingsbara uppgifter.

Artikeln gäller endast befintliga uppgifter, och dess konsekvenser begränsar sig endast till sådana. Artikeln inverkar således inte på eventuella rättigheter eller skyldigheter att samla in och lagra trafikuppgifter eller andra datorbehandlingsbara uppgifter som den som har uppgifterna i sin vård, t.ex. en teleoperatör, har på basis av andra bestämmelser. Artikeln gäller endast förhindrande av att befintliga uppgifter går förlorade. I punkt 1 i artikeln nämns föreläggandet att säkra uppgifter endast som ett exempel på reglering i syfte att säkra att uppgifter inte förändras. Tekniskt kan en part också genomföra regleringen på något annat sätt, t.ex. i anslutning till bestämmelserna om beslag av eller skyldighet att lämna ut datorbehandlingsbara uppgifter.

I artikeln avses med att säkra uppgifter endast att uppgifterna skyddas på ett effektivt sätt. Användningen av uppgifterna behöver inte nödvändigtvis förhindras helt och hållet. I artikeln överlåts det på parterna att överväga hur ett tillräckligt effektivt skydd för uppgifterna tekniskt kan genomföras. Enligt artikeln skall myndigheterna kunna säkra datorbehandlingsbara uppgifter särskilt i de fall där det finns anledning att förmoda att uppgifterna löper särskild risk att gå förlorade eller förändras. En dylik misstanke kan grunda sig på t.ex. på information om hur länge den som innehar uppgifterna i sin vård bevarar dem eller om att den metod som används för att bevara uppgifterna är otillförlitlig. De uppgifter som avses i föreläggandet kan finnas antingen i den persons eller det företags besittning som föreläggandet riktar sig mot eller någon annanstans, förutsatt att denna instans har rätt att förfoga över uppgifterna. Parterna är skyldiga att i sin nationella lagstiftning föreskriva om en maximitid för föreläggandet. Denna tid får inte vara längre än den tid på 90 dagar som anges i artikeln. Syftet med bestämmelsen om hemlighållande är att säkerställa att brottsutredningen kan ske störningsfritt men också att skydda den misstänktes integritet.

I den gällande lagstiftningen i Finland finns inte några sådana bestämmelser som skulle motsvara föreläggandet att säkra uppgifter enligt artikeln. Artikeln förutsätter därför ändringar i den gällande lagstiftningen.

I regeringens proposition föreslås att till tvångsmedelslagen fogas sådana bestämmelser om förelägganden att säkra uppgifter som denna artikel och artikel 17, som behandlas nedan, förutsätter. De föreslagna bestämmelserna behandlas närmare i detaljmotiveringen till bestämmelserna om föreläggande att säkra uppgifter i 4 kap. 4 b § i tvångsmedelslagen och bestämmelserna om varaktigheten av ett föreläggande att säkra uppgifter och tystnadsplikt i nämnda kapitels 4 c §.

Efter att den föreslagna ändringen har trätt i kraft uppfyller de gällande bestämmelserna kraven enligt såväl denna artikel som artikel 17.

Artikel 17. *Skyndsamt säkrande och partiellt röjande av trafikuppgifter.* I artikeln finns bestämmelser om säkrande av trafikuppgifter och om röjande av vissa uppgifter om färdväg. Såsom redan konstaterats i samband med artikel 16 gäller den skyldighet att säkra uppgifter som avses där även trafikuppgifter. Begreppet trafikuppgifter definieras i artikel 1 d. Enligt definitionen avses med trafikuppgifter datorbehandlingsbara uppgifter som hänför sig till ett meddelande som förmedlas med hjälp av ett datorsystem, vilka alstrats av ett datorsystem som ingick i kommunikationskedjan och anger meddelandets ursprung, destination, färdväg, tid, datum, storlek, varaktighet eller typ av underliggande tjänst. Sådana i artikeln nämnda trafikuppgifter som anger ett meddelandes ursprung eller destination är t.ex. ett telefonnummer, en IP-adress eller någon annan med dessa jämförbar teleadress. Till dessa delar är det fråga om uppgifter som motsvarar de uppgifter som i tvångsmedelslagens 5 a kap. benämns identifieringsuppgifter. Med uppgifter som anger typ av underliggande tjänst avses om det vid kommunikationen är fråga om t.ex. e-post, filöverföring eller diskussion i realtid.

Enligt punkt 1 a i artikeln skall trafikuppgifter skyndsamt kunna säkras, oavsett om en eller flera tjänsteleverantörer har deltagit i överföringen av meddelandet. Enligt punkt 1 b i artikeln skall myndigheterna dessutom ha rätt att få trafikuppgifter som behövs för att identifiera tjänsteleverantörer, om flera tjänsteleverantörer har deltagit i överföringen av meddelandet. Begreppet tjänsteleverantör definieras i artikel 1 c. Enligt definitionen avses med tjänsteleverantör en offentlig eller privat enhet som erbjuder användarna av dess tjänster möjlighet att kommunicera med hjälp av ett datorsystem, och varje annan enhet som behandlar eller lagrar datorbehandlingsbara uppgifter för en sådan kommunikationstjänst eller för användarna av en sådan tjänst. Den tjänsteleverantör som avses i artikeln kan vara t.ex ett företag som tillhandahåller överföringstjänster, åtkomst till nät, underhåll av datorsystem eller lagring av uppgifter.

Enligt punkt 2 i artikeln skall bestämmelserna om räckvidd, begränsningsgrunder och rättsskyddsgarantier i artiklarna 14 och 15 gälla för de tvångsmedel som avses i artikeln.

Artikeln behandlas i punkterna 165—169 i den förklarande rapporten. Enligt rapporten

kan trafikuppgifterna vara det enda och avgörande bevismaterialet om vem som har begått ett nätbrott. De tider som trafikuppgifterna bevaras kan dock vara mycket korta t.ex. på grund av andra bestämmelser som betonar integritetsskyddet. Därför är det viktigt att trafikuppgifter vid behov snabbt och effektivt kan säkras.

Artikeln innehåller särskilda bestämmelser om det föreläggande att säkra trafikuppgifter som avses i artikel 16. Den viktigaste av dem är bestämmelsen om att myndigheterna skall ha rätt att få sådana trafikuppgifter som behövs för att identifiera tjänsteleverantörer, om flera tjänsteleverantörer har deltagit i överföringen av ett meddelande. Till dessa delar är det således inte enbart fråga om att säkra uppgifter utan om begränsad rätt för myndigheterna att få uppgifter.

Ett meddelande som förmedlas i ett datorsystem kan passera genom flera teleoperatörers nät. I sådana fall är det inte alltid tillräckligt att en av operatörerna i överföringskedjan ges ett föreläggande att säkra uppgifterna för att förhindra att meddelandet eller trafikuppgifterna går förlorade. För att föreläggandet skall kunna riktas till alla dem som deltagit i överföringskedjan behövs det information om samtliga operatörer som har deltagit i överföringen. Varje operatör har uppgifter om den operatör från vilken ett meddelande har kommit och till vem det har sänts. Dessa trafikuppgifter är sådana i artikeln avsedda uppgifter som behövs för att identifiera tjänsteleverantörer, och rätten för myndigheterna att få del av innehållet i trafikuppgifter enligt artikeln gäller endast dem.

Om det skulle krävas att ett särskilt föreläggande riktas uttryckligen till varje operatör i överföringskedjan skulle förfarandet bli långsamt och ineffektivt. Det är mera effektivt att föreläggandet ges t.ex. så att förundersökningsmyndigheternas rätt att få information och föreläggandet att säkra uppgifter genom ett öppet föreläggande riktas till alla operatörerna i kedjan, trots att dessa ännu inte kan identifieras när föreläggandet ges. Också tjänsteleverantörer kan åläggas att medverka vid klarläggandet av överföringskedjan. I artikeln överlåts det dock på parterna att bestämma på vilket sätt och hur effektivt bestämmelserna om klarläggande av kommunikationskedjan tekniskt genomförs.

Den gällande lagstiftningen i Finland innehåller inte några bestämmelser som skulle motsvara vad som i artikeln sägs om säkrande av trafikuppgifter och röjande av uppgifter om ett meddelandes färdväg.

Artikeln förutsätter därför ändringar i den gällande lagstiftningen.

I regeringens proposition föreslås att till tvångsmedelslagen fogas de bestämmelser om föreläggande att säkra uppgifter och röjande av uppgifter om ett meddelandes färdväg som denna artikel och artikel 16 förutsätter. De föreslagna bestämmelserna behandlas närmare i detaljmotiveringen till bestämmelserna om föreläggande att säkra uppgifter i 4 kap. 4 b § i tvångsmedelslagen och till bestämmelserna om varaktigheten av ett föreläggande att säkra uppgifter och tystnadsplikt i nämnda kapitels 4 c §.

Efter att den föreslagna ändringen har trätt i kraft uppfyller de gällande bestämmelserna kraven enligt såväl denna artikel som artikel 16.

Avdelning 3 Skyldighet att lämna uppgifter

Artikel 18. *Skyldighet att lämna uppgifter.* Artikeln innehåller bestämmelser om en allmän skyldighet att lämna ut uppgifter och en särskild skyldighet för tjänsteleverantörer att lämna ut abonnentuppgifter vilken innefattar också annat bevismaterial än datorbehandlingsbara uppgifter.

Enligt punkt 1 a i artikeln är en person skyldig att på föreläggande av en myndighet lämna ut datorbehandlingsbara uppgifter som personen i fråga har i sin besittning eller under sin kontroll.

Enligt punkt 1 b i artikeln är en tjänsteleverantör skyldig att lämna ut abonnentuppgifter, dvs. varje information i form av datorbehandlingsbara uppgifter eller uppgifter i annan form som innehas av tjänsteleverantören och som hänför sig till andra uppgifter om dennes abonnenter än trafikuppgifter eller innehållsuppgifter.

Begreppet tjänsteleverantör definieras i artikel 1 c. Enligt definitionen avses med tjänsteleverantör en offentlig eller privat enhet som erbjuder användarna av dess tjänster

möjlighet att kommunicera med hjälp av ett datorsystem, och varje annan enhet som behandlar eller lagrar datorbehandlingsbara uppgifter för en sådan kommunikationstjänst eller för användarna av en sådan tjänst. Den tjänsteleverantör som avses i artikeln kan vara t.ex. ett företag som tillhandahåller överföringstjänster, åtkomst till nät, underhåll av datorsystem eller lagring av uppgifter. Med abonnentuppgifter avses enligt artikeln information om den typ av kommunikationstjänst som använts, abonnentens person- och kontaktuppgifter samt uppgifter om var kommunikationsutrustningen är belägen.

Enligt punkt 2 i artikeln skall även bestämmelserna om räckvidd, begränsningsgrunder och rättsskyddsgarantier i artiklarna 14 och 15 gälla för den skyldighet som avses i artikeln.

Artikeln behandlas i punkterna 170—183 i den förklarande rapporten. Enligt rapporten är syftet med bestämmelserna att ge ett alternativ till t.ex. beslag som gör det möjligt att skaffa bevismaterial som har formen av datorbehandlingsbara uppgifter utan att man inkräktar mer än vad som är nödvändigt på rättigheterna för den som har uppgifterna i sin vård.

Artikeln gäller endast redan befintliga uppgifter eller uppgifter i befintlig form. Med stöd av artikeln kan en teleoperatör eller någon annan t.ex. inte åläggas att samla in eller lagra uppgifter eller försäkra sig om att uppgifter är korrekta. De uppgifter som avses i föreläggandet kan finnas antingen i den persons eller det företags besittning som föreläggandet riktar sig mot eller någon annanstans, förutsatt att personen eller företaget har rätt att förfoga över uppgifterna. Föreläggandet kan innehålla närmare bestämmelser om i vilken form de datorbehandlingsbara uppgifterna eller annan information skall lämnas. Begreppet abonnentuppgifter skall tolkas i vid bemärkelse så att de t.ex. förutom avgiftsbelagda tjänster avser också uppgifter om sådana abonnenter som använder tjänsterna gratis. I praktiken är det fråga om antingen uppgifter om vilka tjänster en viss person använder och närmare information om dem eller uppgifter om någon viss tjänst och om vem som använder tjänsten och dennes närmare person- och kontaktuppgifter. En viktig begränsningsgrund är att det aldrig kan vara fråga om trafikuppgifter eller uppgifter om ett meddelandes innehåll. Av artikeln följer inte heller någon rätt att slumpmässigt samla in uppgifter, utan behovet av information måste kunna specificeras tillräckligt ingående redan när föreläggandet ges. De begränsningsgrunder och rättsskyddsgarantier till vilka det hänvisas i punkt 2 i artikeln kan dimensioneras olika i olika situationer, med hänsyn till t.ex. arten av de uppgifter som skall lämnas ut och vilken ställning den som skall lämna ut uppgifterna har.

I Finland motsvaras bestämmelserna i artikeln närmast av förundersökningslagens 27 §, där det sägs att ett vittne sanningsenligt och utan att förtiga något skall uppge vad han vet om den sak som undersöks. Såsom bestämmelsen är formulerad innebär den dock endast en skyldighet för vittnet att muntligt berätta vad han vet. I praktiken kan ett vittne givetvis självmant lägga fram sådant material som han har i sin besittning. Dessutom kan en handling eller något annat material, t.ex. ett dokument som har formen av datorbehandlingsbara uppgifter, med stöd av den gällande lagen tas i beslag. Om det inte är känt var materialet finns, är innehavaren skyldig att som vittne tala om det. Först vid en rättegång kan ett vittne med stöd av 17 kap. 12 § i rättegångsbalken åläggas att förete sådant material som vittnet har i sin besittning. I förundersökningslagen finns inte någon motsvarande bestämmelse.

Även om den gällande lagstiftningen särskilt med hänsyn till de praktiska behoven i hög grad uppfyller kraven enligt artikeln, skiljer sig artikeln till ordalydelsen från den gällande lagstiftningen.

Artikeln förutsätter därför ändringar i den gällande lagstiftningen.

I regeringens proposition föreslås att till förundersökningslagen fogas sådana bestämmelser om skyldighet att förete bevismaterial som artikeln förutsätter. Den föreslagna regleringen behandlas närmare i motiveringen till förslaget om ändring av 27 och 28 § i förundersökningslagen.

Efter att den föreslagna ändringen har trätt i kraft uppfyller de gällande bestämmelserna kraven enligt artikeln.

Avdelning 4 Husrannsakan och beslag av lagrade datorbehandlingsbara uppgifter

Artikel 19. *Husrannsakan och beslag av lagrade datorbehandlingsbara uppgifter.* Artikeln innehåller bestämmelser om husrannsakan och beslag av datorbehandlingsbara uppgifter.

Enligt punkt 1 i artikeln skall myndigheterna ha rätt att antingen genom husrannsakan eller på något liknande sätt bereda sig åtkomst till ett datorsystem eller en del därav, någon motsvarande lagringsplattform samt uppgifterna däri.

Enligt punkt 2 i artikeln skall husrannsakan eller någon annan åtgärd skyndsamt kunna utvidgas från det ursprungliga objektet till ett annat objekt, om det visar sig att de eftersökta uppgifterna är lagligen åtkomliga eller tillgängliga där för det första objektet.

Enligt punkt 3 i artikeln skall myndigheterna ha rätt att beslagta eller på liknande sätt säkra ett datorsystem eller en del av det, någon annan lagringsplattform samt uppgifterna däri. De datorbehandlingsbara uppgifterna skall dessutom kunna kopieras och avlägsnas från datorsystemet eller göras oåtkomliga.

I punkt 4 i artikeln sägs att en person som har kunskap om ett datorsystems funktion eller om skyddandet av de datorbehandlingsbara uppgifter som finns däri är skyldig att lämna den information som är nödvändig för att möjliggöra husrannsakan enligt punkterna 1 och 2.

I punkt 5 i artikeln sägs att bestämmelserna om räckvidd, begränsningsgrunder och rättsskyddsgarantier i artiklarna 14 och 15 skall gälla även för de åtgärder som avses i artikeln.

Artikeln behandlas i punkterna 184—204 i den förklarande rapporten. Enligt rapporten är syftet med artikeln att harmonisera bestämmelserna om husrannsakan och beslag av datorbehandlingsbara uppgifter så att likadana bestämmelser i parternas nationella lagstiftning skall gälla för dem som för t.ex. husrannsakan och beslag av föremål. På grund av de datorbehandlingsbara uppgifternas immateriella karaktär är det nödvändigt med särskilda bestämmelser som gäller dem. Husrannsakan enligt punkt 1 i artikeln kan förutom mot ett datorsystem även rikta sig mot en del av det, t.ex. en särskild lagringsenhet eller någon annan lagringsplattform, exempelvis en CD-romskiva. Om innehållet i de eftersökta uppgifterna är t.ex. ett e-postmeddelande skall parterna överväga om bestämmelserna om husrannsakan eller bestämmelserna om avlyssning av innehållsuppgifter i ett konfidentiellt meddelande skall tillämpas.

Husrannsakan kan utvidgas så som avses i punkt 2 i artikeln endast till ett datorsystem eller en del av ett datorsystem inom den ifrågavarande partens territorium. Artikeln medför således inte rätt till gränsöverskridande husrannsakan. I artikeln överlåts det på parterna att bestämma hur utvidgningen genomförs tekniskt. Det väsentliga är att utvidgningen skall kunna genomföras snabbt. De åtgärder som avses i punkt 3 i artikeln har två skilda syften. Syftet med att säkra och kopiera uppgifter är att samla bevis. Om det inte är möjligt att kopiera uppgifterna bör hela lagringsplattformen kunna tas i beslag. I extremfall kan beslaget även innefatta servrar med ett stort antal användare.

Syftet med att avlägsna datorbehandlingsbara uppgifter eller göra dem oåtkomliga är främst att förhindra att uppgifterna används för att orsaka skada. Att uppgifterna avlägsnas betyder inte att de utplånas helt och hållet utan endast att de överförs från en lagringsplattform till en annan. Användningen av uppgifter kan förhindras t.ex. genom kryptering eller på något annat lämpligt sätt. Skyldigheten enligt punkt 4 i artikeln för innehavaren av ett datorsystem eller någon annan person att lämna information syftar till att underlätta och påskynda myndigheternas arbete. Detta kan indirekt gynna även den misstänkte och dennes arbetsgivare. Skyldigheten att lämna information begränsas dock av kravet på skälighet. Vad som i olika situationer skall betraktas som skäligt skall avgöras från fall till fall. En sådan begränsningsgrund som avses i punkt 5 i artikeln kan vara t.ex. en skälig ersättning som betalas till den som skall lämna informationen. I artikeln överlåts det på parterna att besluta om den misstänkte skall informeras om de tvångsmedel som avses i artikeln och när detta i så fall sker.

I Finland finns det inte några särskilda be-

stämmelser som skulle motsvara husrannsakan av datorbehandlingsbara uppgifter enligt punkt 1 eller utvidgning av husrannsakan enligt punkt 2 i artikeln. I fråga om husrannsakan gäller i dessa fall indirekt samma allmänna bestämmelser i tvångsmedelslagens 5 kap som de som gäller fysiska föremål. I lagstiftningen föreskrivs om särskilda villkor för husrannsakan om åtgärden riktar sig mot hemfriden, skyddet för privatlivet eller en persons fysiska integritet.

De datorbehandlingsbara uppgifterna finns alltid lagrade på en fysisk plattform, t.ex. en dators hårddisk. Var lagringsplattformen finns avgör således den åtgärd som vidtas för att undersöka plattformen och de uppgifter den innehåller. Om plattformen t.ex. finns inom ett hemfridsskyddat område förutsätts det först att villkoren för husrannsakan är uppfyllda för att man skall kunna söka efter uppgifterna på den. Om plattformen finns i en persons portfölj skall på motsvarande sätt villkoren för kroppsvisitation vara uppfyllda. Båda de ovan nämnda tvångsmedlen förutsätter att ett brott har begåtts vars straffmaximum är fängelse i minst sex månader. Efter att man har kommit åt lagringsplattformen med hjälp av de ovan nämnda åtgärderna kan dess innehåll undersökas. Lagringsplattformen och de uppgifter den innehåller kan samtidigt också tas i beslag.

Om den persons dator som skall undersökas har kopplats till en annan dator t.ex. via ett lokalt nät och uppgifter som tillhör personen i fråga har lagrats på den, kan även dessa uppgifter undersökas utan att det behövs ett nytt förordnande om husrannsakan. Ett nytt förordnande behövs endast om utvidgningen av åtgärden förutsätter fysiskt tillträde till en sådan hemfridsskyddad plats som det ursprungliga förordnandet inte gäller. Också i sådana fall när ett nytt förordnande behövs kan husrannsakan utvidgas snabbt, eftersom en anhållningsberättigad tjänsteman beslutar om åtgärden. I brådskande fall kan beslutet också fattas av en polisman.

Bestämmelserna om husrannsakan i punkt 1 och om utvidgning av åtgärden i punkt 2 i artikeln förutsätter således inte att de ifrågavarande bestämmelserna i tvångsmedelslagen ändras.

Bestämmelserna om beslag i punkt 3 i artikeln motsvaras i Finland närmast av bestämmelserna om beslag av föremål och handlingar i tvångsmedelslagen. I den finska lagstiftningen finns dock inte några särskilda bestämmelser om beslag av datorsystem och uppgifter i sådana.

Datorsystem, delar av datorsystem och andra lagringsplattformer samt uppgifter som dessa innehåller kan säkras så som artikeln förutsätter med stöd av bestämmelserna om tagande i beslag av föremål. Enligt 4 kap. 1 § i tvångsmedelslagen får ett föremål tas i beslag, om det finns skäl att anta att det kan ha betydelse som bevis i brottmål eller att det har avhänts någon genom brott eller att en domstol förklarar det förbrutet. I samma kapitels 2 § finns dessutom bestämmelser om sådana handlingar som på grund av sitt innehåll inte får tas i beslag när de innehas antingen av den som misstänks för brott eller av någon annan person som anges i paragrafen. Bestämmelserna gäller även handlingar i form av datorbehandlingsbara uppgifter. Enligt kapitlets 10 § kan beslaget också genomföras så att föremålet kvarlämnas i ägarens besittning, t.ex. försett med sigill, och ägaren förbjuds att använda det. Att hela föremålet kan tas i beslag innebär att också datorbehandlingsbara uppgifter som det innehåller kan tas i beslag.

Tvångsmedelslagens 4 kap. 1 § gäller enligt ordalydelsen i paragrafen beslag av föremål. Enligt kapitlets 18 § jämställs ämnen med föremål. Med föremål avses även handlingar. I dag anses det klart att även handlingar i digital form, t.ex. på en dators hårddisk, kan tas i beslag (Helminen, Lehtola, Virolainen: Esitutkinta ja pakkokeinot, Helsingfors 2005, s. 621). Det föreslås dock att kapitlets 1 § förtydligas så att i paragrafen utöver handlingar uttryckligen nämns också handlingar i form av data. Dessutom föreslås det att bestämmelsens tillämpningsområde utvidgas så att beslaget även kan rikta sig mot information som har formen av data, eftersom dylik information inte nödvändigtvis alltid uppfyller definitionen av handling.

Det föreslås att även förundersökningslagens 27 § ändras så att den obestridligen uppfyller kraven i artikel 19.4 i konventionen.

De bestämmelser som närmast motsvarar skyldigheten enligt punkt 4 i artikeln för den

som innehar ett datorsystem och andra personer att lämna information finns i Finland i förundersökningslagens 27 §, där det sägs att ett vittne sanningsenligt och utan att förtiga något skall uppge vad han vet om den sak som undersöks. Enligt ordalydelsen i bestämmelsen gäller skyldigheten främst det brott som undersöks och inte ett datorsystems egenskaper så som avses i artikeln. I detta avseende lämnar paragrafen rum för tolkning, och det finns inte någon rättspraxis om saken.

Avdelning 5 Insamling i realtid av datorbehandlingsbara uppgifter

Artikel 20. *Insamling i realtid av trafikuppgifter.* Artikeln innehåller bestämmelser om insamling i realtid av trafikuppgifter.

Enligt punkt 1 a i artikeln skall myndigheterna ha rätt att med tekniska hjälpmedel insamla eller ta upp trafikuppgifter som hör till särskilt angivna meddelanden som överförs med hjälp av ett datorsystem. Också en tjänsteleverantör skall enligt punkt 1 b kunna åläggas att antingen själv insamla eller biträda myndigheterna med insamling av trafikuppgifter.

I punkt 2 i artikeln sägs att en part inte behöver iaktta punkt 1 a, om det inte är möjligt beroende på gällande principer i partens nationella rättsordning.

Enligt punkt 3 i artikeln är en tjänsteleverantör skyldig att hemlighålla en åtgärd.

I punkt 4 i artikeln sägs att även bestämmelserna om räckvidd, begränsningsgrunder och rättsskyddsgarantier i artiklarna 14 och 15 skall gälla för de tvångsmedel som avses i artikeln.

Begreppet trafikuppgifter definieras i artikel 1 d. Enligt definitionen avses med trafikuppgifter datorbehandlingsbara uppgifter som hänför sig till ett meddelande som förmedlas med hjälp av ett datorsystem, vilka alstrats av ett datorsystem som ingick i kommunikationskedjan och anger meddelandets ursprung, destination, färdväg, tid, datum, storlek, varaktighet eller typ av underliggande tjänst.

Begreppet tjänsteleverantör definieras i artikel 1 c. Enligt definitionen avses med tjänsteleverantör en offentlig eller privat enhet som erbjuder användarna av dess tjänster möjlighet att kommunicera med hjälp av ett datorsystem, och varje annan enhet som behandlar eller lagrar datorbehandlingsbara uppgifter för en sådan kommunikationstjänst eller för användarna av en sådan tjänst.

Artikeln behandlas i punkterna 205—227 i den förklarande rapporten. Enligt rapporten kan trafikuppgifterna vara det enda eller avgörande bevismaterialet vid utredningen av vem som har begått ett nätbrott. I vissa fall bevaras trafikuppgifterna dock bara en mycket kort tid. Därför är det viktigt att uppgifterna kan insamlas i realtid. Begreppet datorsystem i punkt 1 i artikeln skall förstås i vid bemärkelse. Begreppet behandlas mera ingående i motiveringen till artikel 1 a. Det innefattar alla slag av datornät oberoende av hur de genomförts tekniskt. Det saknar också betydelse om nätet är i privat eller offentlig ägo. Med realtid avses att uppgifterna insamlas under kommunikationen. Med tanke på myndigheternas befogenheter betyder detta rätt att få tillgång till framtida trafikuppgifter. För att bestämmelsen skall vara tydlig och heltäckande nämns insamling och upptagning separat i artikeln. Det brott som tvångsmedlet grundar sig på och den kommunikation som hänför sig till det skall kunna specificeras tillräckligt ingående. Artikeln medför således inte rätt att insamla stora mängder trafikuppgifter enbart i syfte att få kännedom om eventuella brott. Av punkt 1 a i artikeln följer att myndigheterna skall ha tillräcklig teknisk beredskap att insamla trafikuppgifter. Skyldigheten för en operatör att biträda myndigheterna enligt punkt 1 b i artikeln begränsar sig däremot endast till den tekniska beredskap som operatören besitter. Den ovan nämnda a och b punkten utesluter inte varandra, utan meningen är att punkterna skall komplettera varandra och tillämpas parallellt. I punkt 2 i artikeln sägs det dock att en part inte behöver iaktta skyldigheten enligt punkt 1 a. Parten skall då ålägga operatörerna att se till att de även har teknisk beredskap att insamla trafikuppgifter. Artikeln gäller endast kommunikation som sker inom en parts territorium. Detta villkor uppfylls dock redan om kommunikationen sker över partens territorium. Syftet med den tystnadsplikt som avses i punkt 3 i artikeln är att säkerställa att åtgär-

derna är effektiva. Hur tystnadsplikten lagtekniskt genomförs överlåts i artikeln på parterna. En skälig tidsbegränsning kan uppställas för tystnadsplikten.

De begränsningsgrunder och rättsskyddsgarantier till vilka det hänvisas i punkt 4 i artikeln kan dimensioneras t.ex. enligt i hur hög grad en åtgärd kränker den persons integritet som den riktar sig mot.

Definitionen av trafikuppgifter behandlas i punkterna 28–31 i den förklarande rapporten. Enligt rapporten är sådana trafikuppgifter som utvisar meddelandets ursprung och destination t.ex. ett telefonnummer, en IP-adress eller någon annan med dessa jämförbar teleadress. Med uppgifter om typ av underliggande tjänst avses om det vid kommunikationen är fråga om t.ex. e-post, filöverföring eller en diskussion som förs i realtid.

Definitionen av tjänsteleverantör behandlas i punkterna 26 och 27 i den förklarande rapporten. Enligt rapporten kan den tjänsteleverantör som avses i artikeln vara t.ex. ett teleföretag eller något annat företag som tillhandahåller överföringstjänster, åtkomst till nät, underhåll av datorsystem eller lagring av uppgifter.

I Finland motsvaras artikeln av bestämmelserna om tvångsmedlet teleövervakning i tvångsmedelslagens 5 a kap. Med teleövervakning avses i tvångsmedelslagen detsamma som med insamling av trafikuppgifter i artikeln.

Enligt 5 a kap. 3 § i tvångsmedelslagen har förundersökningsmyndigheten rätt att vid utredning av vissa brott med domstolens tillstånd skaffa sekretessbelagda identifieringsuppgifter som gäller telemeddelanden.

Med identifieringsuppgifter avses telefonnummer eller motsvarande adressuppgifter om sändaren eller mottagaren av ett meddelande eller om en teleterminalutrustning, hur länge förbindelsen varat och tidpunkten för den samt annan motsvarande information. Också uppgifter för identifiering av en mobilteleapparat samt uppgifter om apparatens läge är identifieringsuppgifter.

Det brott som undersöks kan vara ett brott som riktar sig mot ett automatiskt databehandlingssystem och som har begåtts med hjälp av en teleterminalutrustning, koppleri, övergrepp i rättssak, olaga hot, narkotikabrott eller försök till dessa brott samt förberedelse till brott som begås i terroristiskt syfte. Dessutom kan tvångsmedel användas om det föreskrivna strängaste straffet för brottet är fängelse i minst 4 år. Ett ytterligare villkor är att de uppgifter som fås kan antas vara av synnerlig vikt för utredning av brottet. Det sistnämnda gäller dock inte om tvångsmedlet med målsägandens samtycke riktar sig mot en teleanslutning som denne själv använder.

Identifieringsuppgifter kan endast inhämtas om sådana telemeddelanden som har förmedlats genom ett allmänt kommunikationsnät eller ett därtill anslutet kommunikationsnät (TVL 5a:1 §). Med allmänt kommunikationsnät avses ett nät som tillhandahålls en grupp av användare som inte har avgränsats på förhand. Tillämpningsområdet innefattar således inte kommunikation inom ett separat nät, om inte detta har kopplats till ett allmänt kommunikationsnät. Bestämmelserna omfattar traditionell telefon- och datakommunikation.

I domstolens tillstånd skall de identifieringsuppgifter som tvångsmedlet riktar sig mot individualiseras. Individualiseringsgrunden kan vara en teleanslutning, en e-postadress eller någon annan sådan teleadress eller teleterminalutrustning som den misstänkte innehar eller annars kan antas använda. Individualiseringsgrunden har således lämnats öppen när det gäller teleadresser.

Tillstånd kan beviljas för en månad åt gången (TVL 5a:7 §). Tillstånd kan beviljas också för tiden före tillståndsbeslutet och kan då utan tidsbegränsning beviljas också för en längre tid. I brådskande fall kan också en anhållningsberättigad tjänsteman bevilja temporärt tillstånd (TVL 5a:5 §).

Den misstänkte skall underrättas om användningen av tvångsmedel först efter att förundersökningen har avslutats (TVL 5a:11 §). Därför är det klart att också en teleoperatör är skyldig att hemlighålla saken, trots att det inte finns någon uttrycklig bestämmelse om detta.

Enligt 95 § i kommunikationsmarknadslagen (393/2003) är en teleoperatör skyldig att utrusta sitt nät så att identifieringsuppgifter kan inhämtas, och en teleoperatör är även annars enligt 5 a kap. 9 § i tvångsmedelslagen skyldig att biträda förundersöknings-

myndigheterna.

De begränsningsgrunder och rättsskyddsgarantier som avses i tvångsmedelslagen står i samklang med bestämmelserna i artiklarna 14 och 15, till vilka det hänvisas i punkt 4 i artikeln. Bestämmelserna i lagen uppfyller även i övrigt kraven enligt artikeln. De gällande bestämmelserna uppfyller således förpliktelserna enligt artikeln.

Artikeln förutsätter inte ändringar i lagstiftningen.

Enligt artikel 14.3 a i konventionen får en part förbehålla sig rätten att endast tillämpa de åtgärder som avses i denna artikel på brott eller brottstyper som anges i förbehållet, under förutsättning att omfattningen av dessa inte är mer begränsad än det urval av brott på vilka parten tillämpar de åtgärder som avses i artikel 21.

Enligt förslaget kommer Finland att så som anges i artikel 14.3 a förbehålla sig rätten att tillämpa åtgärderna endast på brott som riktar sig mot ett automatiskt databehandlingssystem och som har begåtts med hjälp av en teleterminalutrustning samt på koppleri, övergrepp i rättssak, olaga hot, narkotikabrott och försök till dessa brott samt på förberedelse till brott som begås i terroristiskt syfte och på brott för vilka det föreskrivna strängaste straffet är fängelse i minst fyra år.

Enligt artikel 14.3 b i konventionen får en part förbehålla sig rätten att inte tillämpa de tvångsmedel som avses i denna artikel eller i artikel 21 på meddelanden som överförs inom ett datorsystem som drivs för en sluten användargrupp och inte använder allmänna kommunikationsnät och inte är anslutet till ett annat datorsystem, oavsett om detta är offentligt eller enskilt.

Enligt förslaget kommer Finland att beträffande denna artikel göra ett sådant förbehåll som avses i artikel 14.3 b.

Artikel 21. *Avlyssning av innehållsuppgifter.* Artikeln innehåller bestämmelser om avlyssning i realtid av innehållsuppgifter i meddelanden.

I punkt 1 a i artikeln sägs att myndigheterna skall ha rätt att med tekniska hjälpmedel insamla eller ta upp innehållsuppgifter i särskilt angivna meddelanden som överförs med hjälp av ett datorsystem. Artikeln tillämpas endast på vissa allvarliga brott som bestäms i den nationella lagstiftningen. Också en tjänsteleverantör skall enligt punkt 1 b kunna åläggas att antingen själv insamla uppgifter eller att biträda myndigheterna vid insamlingen.

I punkt 2 i artikeln sägs att en part inte behöver iaktta punkt 1 a, om detta inte är möjligt beroende på gällande principer i dess nationella rättsordning.

Enligt punkt 3 i artikeln är en tjänsteleverantör skyldig att hemlighålla en åtgärd.

I punkt 4 i artikeln sägs att även bestämmelserna om räckvidd, begränsningsgrunder och rättsskyddsgarantier i artiklarna 14 och 15 skall gälla för de tvångsmedel som avses i artikeln.

Artikeln behandlas i punkterna 205—215 och 228—231 i den förklarande rapporten. Enligt rapporten är de tvångsmedel som avses i artikeln nödvändiga av samma orsaker som traditionell telefonavlyssning. Om uppgifter inte kan insamlas i realtid t.ex. för att de brott som undersöks håller på att begås är det svårt eller t.o.m. omöjligt att ingripa i brotten innan skador hinner uppstå. Artikeln är uppbyggd på nästan samma sätt som artikel 20 ovan och gäller i stort sett samma saker. Vad som i den förklarande rapporten sägs om insamling av trafikuppgifter så som anges ovan gäller således även denna artikel.

I Finland motsvaras artikeln av bestämmelserna om tvångsmedlet teleavlyssning i tvångsmedelslagens 5 a kap.

Enligt 5 a kap. 2 § i tvångsmedelslagen har förundersökningsmyndigheten rätt att vid utredning av vissa grova brott med domstolens tillstånd avlyssna och uppta telemeddelanden för att utreda deras innehåll. I paragrafen finns en uttömmande förteckning över de brott, angivna med brottsbeteckning, som tvångsmedlet kan tillämpas på. Dylika brott är t.ex. landsförräderi och högförräderi, brott mot liv, grova brott som riktar sig mot friheten, vissa grova faredelikt, vissa grova förmögenhetsbrott, grovt narkotikabrott och vissa grova ekonomiska brott som begås professionellt samt försök till dessa brott. Ett ytterligare villkor är att de uppgifter som fås kan antas vara av synnerlig vikt för utredning av brottet.

Med teleavlyssning avses enligt 5 a kap. 1 § i tvångsmedelslagen att ett meddelande

som förmedlas till eller från en viss teleanslutning, e-postadress eller någon annan sådan teleadress eller till eller från teleterminalutrustning genom ett sådant allmänt kommunikationsnät eller ett sådant därtill anslutet kommunikationsnät som avses i kommunikationsmarknadslagen i hemlighet avlyssnas eller upptas för utredning av innehållet i meddelandet. Uppgifter kan således endast inhämtas om innehållet i sådana telemeddelanden som har förmedlats genom ett allmänt kommunikationsnät eller ett därtill anslutet kommunikationsnät. Med allmänt kommunikationsnät avses ett nät som tillhandahålls en användargrupp som inte har avgränsats på förhand. Tillämpningsområdet innefattar således inte kommunikation inom ett separat nät, om inte detta är anslutet till ett allmänt kommunikationsnät. Bestämmelserna omfattar traditionell telefon- och datakommunikation.

I domstolens tillstånd skall den kommunikation som tvångsmedlet riktar sig mot individualiseras. Individualiseringsgrunden kan vara en teleanslutning, en e-postadress eller någon annan sådan teleadress eller teleterminalutrustning som den misstänkte innehar eller annars kan antas använda. Individualiseringsgrunden har således lämnats öppen när det gäller teleadresser.

Tillstånd kan beviljas för en månad åt gången (TVL 5a:7 §). Domstolen kan även förena tillståndet med andra villkor och begränsningar.

Den misstänkte skall underrättas om användningen av tvångsmedel först efter att förundersökningen har avslutats (TVL 5a:11 §). Därför är det klart att också en teloperatör är skyldig att hemlighålla saken, trots att det inte finns någon uttrycklig bestämmelse om detta.

Enligt 95 § i kommunikationsmarknadslagen är en teleoperatör skyldig att utrusta sitt nät så att uppgifter om ett meddelandes innehåll kan inhämtas, och en teleoperatör är även annars enligt 5 a kap. 9 § i tvångsmedelslagen skyldig att biträda förundersökningsmyndigheterna.

De begränsningsgrunder och rättsskyddsgarantier som avses i tvångsmedelslagen står i samklang med bestämmelserna i artiklarna 14 och 15, till vilka det hänvisas i punkt 4 i artikeln. Bestämmelserna i lagen uppfyller även i övrigt kraven enligt artikeln. De gällande bestämmelserna uppfyller således förpliktelserna enligt artikeln.

Artikeln förutsätter inte ändringar i lagstiftningen.

Enligt artikel 14.3 b i konventionen får en part förbehålla sig rätten att inte tillämpa de tvångsmedel som avses i denna artikel eller i artikel 20 på meddelanden som överförs inom ett datorsystem som drivs för en sluten användargrupp och inte använder allmänna kommunikationsnät och inte är anslutet till ett annat datorsystem, oavsett om detta är offentligt eller enskilt.

Enligt förslaget kommer Finland att beträffande denna artikel göra ett sådant förbehåll som avses i artikel 14.3 b.

Avdelning 3 Domsrätt

Artikel 22. *Domsrätt.* Artikeln innehåller bestämmelser om den territoriella räckvidden av de straffbestämmelser som grundar sig på konventionen.

Enligt punkt 1 a—c i artikeln skall varje part kunna utöva domsrätt över ett brott som har begåtts inom dess territorium (a), ombord på ett fartyg som för dess flagg (b) eller ombord på ett luftfartyg som är registrerat enligt dess lagar (c).

Enligt punkt 1 d i artikeln skall varje part kunna utöva domsrätt över ett brott som har begåtts av en av dess medborgare, om brottet är straffbart enligt strafflagstiftningen där det begicks eller om brottet inte faller under någon stats territoriella behörighet.

I punkt 2 i artikeln sägs att varje part får förbehålla sig rätten att inte alls tillämpa eller att bara i vissa fall och under särskilda förhållanden tillämpa de regler om domsrätt som anges i punkt 1 b—d i artikeln eller en del av dessa regler.

Enligt punkt 3 i artikeln skall varje part kunna utöva domsrätt i de fall då en påstådd gärningsman befinner sig inom dess territorium och parten inte på begäran utlämnar honom eller henne till en annan part endast på grund av hans eller hennes nationalitet.

I punkt 4 i artikeln sägs för tydlighetens skull att artikeln inte utesluter straffrättslig domsrätt som utövas av en part i enlighet

med dess nationella lagstiftning och att förteckningen i artikeln således inte är uttömmande.

I punkt 5 i artikeln finns en bestämmelse om att parterna skall samråda i de fall där mer än en part gör gällande domsrätt över samma brott.

Artikeln behandlas i punkterna 232—239 i den förklarande rapporten. Enligt rapporten grundar sig bestämmelserna om tillämpningsområdet i fråga om punkt 1 a—c på territorialitetsprincipen och vad som kan härledas ur den och i fråga om punkt 1 d på personalitetsprincipen. Bestämmelsen i punkt 3 i artikeln grundar sig för sin del på principen om att utlämna eller döma, som tillämpas vid utlämning. Rätten att göra förbehåll enligt punkt 2 gäller endast punkt 1 b—d så som nämns i punkten. Förbehåll kan inte göras i fråga om punkt 1 a eller punkt 3 i artikeln. Den skyldighet att samråda som avses i punkt 5 är inte ovillkorlig, utan parterna skall samråda om de finner det lämpligt.

I Finland finns de gällande bestämmelserna om strafflagens tillämpningsområde i strafflagens 1 kap.

Punkt 1 a i artikeln motsvaras av kapitlets 1 §, enligt vilken finsk lag tillämpas på brott som har begåtts i Finland. Enligt kapitlets 10 § anses ett brott vara begånget såväl där den brottsliga handlingen företogs som där den rekvisitsenliga följden av brottet framträdde.

Punkt 1 b och c i artikeln motsvaras av kapitlets 2 §, enligt vilken finsk lag tillämpas på brott som har begåtts ombord på ett finskt fartyg eller luftfartyg. I regel tillämpas finsk lag även när fartyget befinner sig inom eller ovanför en främmande stats område.

Punkt 1 d i artikeln motsvaras av kapitlets 6 §, enligt vilken finsk lag tillämpas på brott som en finsk medborgare har begått utanför Finland. Ett ytterligare villkor är enligt 11 § att gärningen är straffbar också enligt lagen på gärningsorten och att även en domstol i den främmande staten kunde ha dömt ut straff för gärningen. För brottet får härvid inte i Finland dömas ut en påföljd som är strängare än den som föreskrivs för brottet enligt lagen på gärningsorten. Om ett brott har förövats inom ett område som inte tillhör någon stat, är enligt 6 § en förutsättning för straffbarheten att på brottet enligt finsk lag kan följa fängelse i över sex månader. Maximistraffet för samtliga de brott som avses i konventionen är minst ett års fängelse.

Punkt 3 i artikeln motsvaras av kapitlets 8 §, enligt vilken på brott som har begåtts utanför Finland och på vilket enligt finsk lag kan följa fängelse i över sex månader tillämpas finsk lag, om den stat inom vars område brottet har förövats har begärt att åtal för brottet skall väckas vid finsk domstol eller med anledning av brottet har framställt begäran om att gärningsmannen skall utlämnas men begäran har avslagits.

Punkterna 4 och 5 i artikeln har inte omedelbara konsekvenser för lagstiftningen.

De gällande bestämmelserna uppfyller således förpliktelserna enligt artikeln.

Artikeln förutsätter inte ändringar i lagstiftningen.

Finland har inte behov av att göra ett sådant förbehåll som avses i punkt 2 i artikeln.

Kapitel III. **Internationellt samarbete**

Avsnitt 1 Allmänna principer

Avdelning 1 Allmänna principer för internationellt samarbete

Artikel 23. *Allmänna principer för internationellt samarbete.* Artikeln innehåller bestämmelser om de allmänna principerna för hela det internationella samarbete som regleras i kapitel III. Bestämmelserna i artikeln gäller således såväl utlämning som ömsesidig rättslig hjälp. I artikeln sägs att parterna i största möjliga utsträckning skall samarbeta med varandra i enlighet med bestämmelserna i kapitlet och genom tillämpning av relevanta överenskommelser och nationella lagar för att utreda eller lagföra brott som är relaterade till datorsystem eller för insamling av bevis i elektronisk form om brott.

Artikeln behandlas i punkterna 241—244 i den förklarande rapporten. Enligt rapporten framgår tre generella principer av artikeln. För det första skall parterna genom internationellt samarbete sträva efter att tillämpa olika rättskällor i så stor utsträckning som möjligt. För det andra omfattar det internationella samarbetet enligt konventionen förutom nätbrott också insamling av bevismate-

rial i elektronisk form som hänför sig till andra brott. För det tredje åsidosätter bestämmelserna i kapitel III i konventionen inte bestämmelser om samma sak i andra konventioner eller i bilaterala överenskommelser.

Bestämmelserna i kapitel III i konventionen gäller enbart utredning och lagföring av brott. De omfattar således inte t.ex. kriminalunderrättelseverksamhet.

Avdelning 2 Principer för utlämning

Artikel 24. *Utlämning.* Artikeln innehåller bestämmelser om utlämning.

I punkt 1 a i artikeln sägs att artikeln tillämpas endast på utlämning för brott som straffbeläggs i enlighet med artiklarna 2—11 i konventionen. En ytterligare förutsättning är att brotten enligt lagstiftningen i både den anmodade parten och den begärande parten kan bestraffas med frihetsberövande och maximistraffet uppgår till lägst ett år. Enligt punkt 1 b åsidosätts dock det villkor i artikeln som gäller maximistraffet i de fall där en annan bestämmelse som avviker från bestämmelsen i artikeln skall tillämpas enligt en överenskommelse som är bindande för en part.

Enligt punkt 2 i artikeln skall de brott som avses i punkt 1 i artikeln anses tillhöra de utlämningsbara brotten i ett utlämningsavtal som gäller mellan två eller flera parter. Parterna förbinder sig också att ta med sådana brott i utlämningsavtal som kommer att slutas mellan två eller flera av dem.

Om en part ställer som villkor för utlämning att det finns ett bilateralt utlämningsavtal, får parten enligt punkt 3 i artikeln betrakta denna konvention som rättslig grund för utlämning. Parter som för utlämning inte ställer som villkor att ett ovan nämnt särskilt utlämningsavtal skall föreligga skall enligt punkt 4 erkänna de brott som avses i punkt 1 i artikeln som utlämningsbara brott.

I punkt 5 i artikeln sägs att för utlämning skall gälla de villkor som anges i den anmodade partens lagstiftning eller i ett utlämningsavtal som är bindande för parten. Detta gäller även de skäl på grund av vilka den anmodade parten får vägra att bevilja utlämning.

Punkt 6 i artikeln gäller sådana fall där en part vägrar att bevilja utlämning endast på grund av den sökta personens nationalitet eller därför att den anser sig ha domsrätt över brottet. Den anmodade parten skall då efter framställning från den begärande parten hänskjuta ärendet till sina behöriga myndigheter för lagföring och rapportera slutresultatet till den begärande parten.

Punkt 7 i artikeln innehåller bestämmelser om att varje part skall utse en ansvarig myndighet och om den förteckning som skall föras över de myndigheter som parterna utsett.

Artikeln behandlas i punkterna 245—252 i den förklarande rapporten. Enligt rapporten är den strafftröskel som enligt 1 punkten utgör en förutsättning för utlämning nödvändig, eftersom en del av de brott som kommer i fråga kan vara relativt lindriga. Det väsentliga är då inte det straff som i praktiken kunde dömas ut för gärningen utan den skala som skall tillämpas. Punkt 2 i artikeln förutsätter inte att utlämning alltid skall ske för samtliga de brott som nämns utan endast att utlämning skall vara möjlig. Punkt 3 i artikeln är inte bindande för de parter som den tillämpas på utan medför endast sådan rätt som anges där. Punkt 4 i artikeln är däremot bindande. Punkt 5 gäller också skäl för att vägra utlämning på grund av ett utlämningsavtal som är bindande för en part. Punkt 6 grundar sig på principen om att utlämna eller döma. Syftet med punkt 7 är att underlätta och säkerställa informationen till parterna.

I Finland finns de gällande bestämmelserna om utlämning i lagen om utlämning för brott, som är den allmänna lagen om utlämning, samt i vissa speciallagar och i de konventioner och bilaterala avtal som har satts i kraft i Finland. För den gällande rätten redogörs till dessa delar också i allmänna motiveringen.

Artikeln innehåller bestämmelser om utlämning för de brott som avses i konventionen i enlighet med de utlämningsavtal som gäller mellan parterna eller, i de fall då det inte finns något avtal, i enlighet med denna konvention.

De brott som avses i punkt 1 i artikeln är sådana brott för vilka utlämning i regel kan ske enligt finsk lagstiftning. Eftersom utlämningen enligt punkt 5 dessutom kan förenas med villkor som anges i den anmodade statens lagstiftning eller gällande utlämningsav-

tal, står artikeln även i övrigt i samklang med gällande rätt i Finland.

När det gäller punkt 6 i artikeln bör det noteras att finska medborgare enligt 9 § i Finlands grundlag inte mot sin vilja får utlämnas eller föras till ett annat land. Enligt 2 § i utlämningslagen får finska medborgare inte utlämnas. Till Europeiska unionens medlemsstater samt Island och Norge får finska medborgare utlämnas under vissa förutsättningar. Enligt 1 kap. 6 § i strafflagen kan en finsk medborgare dömas till straff i Finland för ett brott som har begåtts utanför Finland, om gärningen är straffbar också enligt lagen på gärningsorten. Dessutom bör det noteras att finsk lag enligt 1 kap. 8 § skall tillämpas, om den stat inom vars område brottet har förövats har begärt att åtal för brottet skall väckas vid finsk domstol eller med anledning av brottet har framställt begäran om att gärningsmannen skall utlämnas men begäran har avslagits. I bestämmelsen förutsätts dubbel straffbarhet samt att fängelse i över sex månader enligt finsk lag kan följa på gärningen. Inom Europeiska unionens medlemsstater förutsätts inte dubbel straffbarhet i fråga om vissa brott som anges särskilt, och inte heller i fråga om de övriga brotten finns det något krav gällande maximistraffet.

Justitieministeriet är i Finland den myndighet som avses i punkt 7 i artikeln.

Bestämmelserna i konventionen står inte i strid med gällande rätt i Finland.

Avdelning 3 Allmänna principer för ömsesidig rättslig hjälp

Artikel 25. *Allmänna principer för ömsesidig rättslig hjälp.* Artikeln innehåller bestämmelser om allmänna principer för ömsesidig rättslig hjälp.

Enligt punkt 1 i artikeln skall parterna i största möjliga utsträckning lämna varandra ömsesidig rättslig hjälp för att utreda och lagföra brott som är relaterade till datorsystem eller för insamling av bevis i elektronisk form om brott, och enligt punkt 2 skall varje part vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att säkerställa att konventionen följs.

I punkt 3 i artikeln sägs att en part i brådskande fall får göra framställningar om rättslig hjälp genom elektronisk post eller genom något annat snabbt kommunikationsmedel. Framställningen skall då också besvaras genom ett snabbt kommunikationsmedel.

För rättslig hjälp skall enligt punkt 4 gälla de villkor som föreskrivs i den anmodade partens lagstiftning eller i de avtal om ömsesidig rättslig hjälp som är bindande för parten, innefattande de skäl på grund av vilka en part får vägra rättslig hjälp. Rättslig hjälp får inte vägras i fråga om brott som avses i artiklarna 2—11 endast av det skälet att parten anser brottet vara ett fiskalt brott.

Enligt punkt 5 skall kravet på dubbel straffbarhet anses vara uppfyllt, oberoende av om brottet rubriceras med samma termer eller placeras inom samma kategori av brott, om det handlande som ligger bakom brottet är detsamma.

Artikeln behandlas i punkterna 253—259 i den förklarande rapporten. Enligt rapporten är tillämpningsområdet enligt punkt 1 i artikeln detsamma som i artikel 23, och det täcker således de situationer som avses i artikel 14. Punkt 2 i artikeln ålägger parterna att se till att det finns en tillräcklig rättslig grund för åtgärderna i den nationella lagstiftningen. Bestämmelsen om snabba kommunikationsmedel i punkt 3 är nödvändig, eftersom uppgifter som är av betydelse för utredning av brott annars kan gå förlorade under förfarandet när rättslig hjälp lämnas. I den förklarande rapporten tas det inte ställning till om en framställning om rättslig hjälp kan göras per telefon. Punkt 4 i artikeln medför inte rätt att föreskriva om villkor som står i strid med uttryckliga bestämmelser i konventionen. Syftet med artikel 5 är att hindra parterna från att tolka kravet på dubbel straffbarhet alltför strikt.

I Finland finns de gällande bestämmelserna om ömsesidig rättslig hjälp i lagen om internationell rättshjälp i straffrättsliga ärenden, dvs. lagen om straffrättslig rättshjälp, som är den allmänna lagen om inbördes rättslig hjälp, samt i vissa speciallagar och i de konventioner och bilaterala avtal som har satts i kraft i Finland. För den gällande rätten redogörs till dessa delar också i allmänna motiveringen.

Artikeln innehåller allmänna bestämmelser om inbördes rättslig hjälp när det gäller nät-

brott och bevismaterial i elektronisk form i enlighet med gällande avtal om rättslig hjälp eller, om något sådant inte finns, i enlighet med denna konvention.

I regel kan rättslig hjälp lämnas enligt lagen om straffrättslig rättshjälp i de fall som avses i punkt 1 i artikeln.

Bestämmelser som motsvarar punkt 3 i artikeln finns i 7 § i lagen om straffrättslig rättshjälp. När en utländsk myndighet begär rättshjälp av en finsk myndighet kan enligt paragrafen begäran framställas skriftligen, som en teknisk upptagning eller muntligen och den kan också sändas som ett elektroniskt meddelande. Om det uppstår tvivel om begärans eller den bifogade handlingens äkthet eller innehåll, kan justitieministeriet eller den behöriga myndigheten be att begäran till behövliga delar bekräftas skriftligen. Legalisering behövs inte för begäran om rättshjälp och därtill hörande handlingar. Enligt lagen om straffrättslig rättshjälp är det således möjligt att använda sådana snabba kommunikationsmedel som avses i artikeln.

Bestämmelserna om fiskala brott i punkt 4 och om dubbel straffbarhet i punkt 5 saknar relevans för Finland. Enligt lagen om straffrättslig rättshjälp lämnas rättslig hjälp även när en framställning gäller fiskala brott. Vid bedömningen av frågan om dubbel straffbarhet är det avgörande enligt 15 § 1 mom. i lagen om straffrättslig rättshjälp inte hur gärningen har rubricerats i framställningen.

Artikel 26. *Upplysningar som lämnas på eget initiativ.* Artikeln innehåller bestämmelser om parternas rätt att lämna upplysningar på eget initiativ. Enligt punkt 1 i artikeln får en part också utan en föregående framställning till en annan part överlämna information för att hjälpa den mottagande parten vid utredningar om brott. Enligt punkt 2 får den part som lämnar informationen ställa villkor för användningen av uppgifterna som den mottagande parten är skyldig att följa.

Artikeln behandlas i punkterna 260 och 261 i den förklarande rapporten. Enligt rapporten berättigar artikeln parterna att lämna uppgifter men förpliktar dem inte till detta. Artikeln är nödvändig eftersom rätten att lämna uppgifter på eget initiativ för vissa staters del förutsätter en särskild avtalsbestämmelse. Enligt artikeln får information överlämnas inom gränserna för en parts nationella lagstiftning.

I sådana fall när Finland är den part som lämnar uppgifter sker överlämnandet inom ramen för Finlands lagstiftning. Den finska lagstiftningen ställer inga allmänna hinder för det utbyte av information som avses i artikeln. Enligt 30 § i lagen om offentlighet i myndigheternas verksamhet (621/1999) kan även sekretessbelagda uppgifter lämnas ut till utländska myndigheter i sådana fall när saken regleras i en för Finland bindande överenskommelse.

I sådana fall när Finland är den part som mottar uppgifter har en myndighet med stöd av 27 § i lagen om straffrättslig rättshjälp rätt och skyldighet att iaktta gällande sekretess- och övriga villkor. Enligt paragrafens 2 mom. skall myndigheten dessutom iaktta villkoren för den främmande statens rättshjälp.

Av denna anledning och eftersom artikeln inte är förpliktande är godkännandet av den inte förenat med några problem för Finlands del.

Avdelning 4 Förfaranden vid framställningar om ömsesidig rättslig hjälp i avsaknad av tillämpliga internationella avtal

Artikel 27. *Förfaranden vid framställningar om ömsesidig rättslig hjälp i avsaknad av tillämpliga internationella avtal.* Enligt punkt 1 tillämpas artikeln endast om det saknas gällande avtal eller överenskommelser om saken mellan de berörda parterna.

Enligt punkt 2 skall varje part utse en centralmyndighet som skall ansvara för frågor som gäller rättslig hjälp, och en förteckning skall föras över dessa myndigheter. Enligt artikeln skall centralmyndigheterna kommunicera direkt med varandra.

Enligt punkt 3 skall framställningar om rättslig hjälp göras i enlighet med det förfarande som anges av den begärande parten, utom när det är oförenligt med den anmodade partens lagstiftning.

Enligt punkt 4 får en framställning om hjälp, utöver de skäl för avslag som anges i artikel 25.4, avslås endast om den anmodade parten betraktar brottet som ett politiskt brott eller om verkställandet av framställningen

kan inkräkta på dess viktiga intressen. I artikeln hänvisas till artikel 25.4, där det sägs att för rättslig hjälp skall gälla de villkor som föreskrivs i den anmodade partens lagstiftning eller i de avtal om ömsesidig rättslig hjälp som är bindande för parten. Detta gäller även skälen för avslag.

Enligt punkt 5 i artikeln får en part skjuta upp verkställandet av en framställning av skäl som hänför sig till brottsutredningar som utförs av den.

Enligt punkt 6 skall den anmodade parten innan den avslår en framställning eller uppskjuter hjälp samråda med den begärande parten om begränsning av framställningen.

I punkt 7 sägs att den anmodade parten ofördröjligen skall underrätta den begärande parten om utfallet av hjälpen. Skälen för avslag eller uppskjutande av framställningen skall anges. Den begärande parten skall också underrättas om det är omöjligt att verkställa framställningen eller om verkställandet försenas avsevärt.

En part får enligt artikel 8 anhålla om att en framställning hemlighålls. Om den anmodade parten inte kan tillmötesgå anhållan om hemlighållande, skall den ofördröjligen meddela den begärande parten, som då skall avgöra om framställningen ändå skall verkställas.

I punkt 9 finns bestämmelser om översändande av framställningar om rättslig hjälp. Enligt punkt 9 a får framställningar i brådskande fall och i vissa andra fall sändas direkt till den behöriga myndigheten i stället för eller vid sidan av att de sänds till centralmyndigheten. I punkt 9 c finns bestämmelser om remittering av framställningar till behörig myndighet i dessa fall. Enligt punkt 9 e får en part meddela att framställningar enligt punkten av effektivitetsskäl skall ställas direkt till dess centralmyndighet.

Artikeln behandlas i punkterna 262—274 i den förklarande rapporten. Att artikelns tillämpningsområde har begränsats till att gälla endast sådana fall när det inte finns någon annan överenskommelse grundar sig enligt rapporten på ändamålsenlighetsskäl. Det är enklare för en part att tillämpa redan befintliga överenskommelser, och samtidigt undviker man eventuella konflikter till följd av överlappande avtal. Artikeln tillämpas således inte t.ex. av parterna i den europeiska konventionen om inbördes rättshjälp i brottmål och dess tilläggsprotokoll. Också eventuella avtal som ingås senare kan utesluta tillämpningen av artikeln. Artikeln innehåller endast allmänna bestämmelser om de principer som iakttas vid lämnandet av rättslig hjälp. Sådan rättslig hjälp genom centralmyndigheterna som avses i punkt 2 i artikeln är ett avsevärt effektivare tillvägagångssätt än den diplomatiska vägen. Syftet med punkt 3 i artikeln är att säkerställa att bevismaterial som har inhämtats genom rättslig hjälp är formellt giltigt också i t.ex. mottagarens domstol. De skäl för avslag som anges i punkt 4 får inte tolkas så brett att de i praktiken förhindrar rättslig hjälp. Det uppskov som avses i punkt 5 och de begränsningar som avses i punkt 6 i artikeln är tänkta att utgöra ändamålsenliga alternativ till att avslå en framställning om rättslig hjälp. Syftet med skyldigheten enligt punkt 7 att ange skälen till ett avslag eller uppskov är att främja informationen till parterna och därmed möjligheterna att utveckla samarbetet. Sekretessen enligt punkt 8 gäller endast framställningar och deras innehåll. Skyldigheten att hemlighålla en framställning får inte vara så omfattande att den försvårar eller gör det omöjligt att vidta en åtgärd.

Av punkt 1 i artikeln följer att artikeln inte till någon del tillämpas mellan Finland och t.ex. de stater som är parter i den europeiska konventionen om inbördes rättshjälp i brottmål.

I Finland är justitieministeriet enligt 3 § i lagen om straffrättslig rättshjälp den centralmyndighet som avses i punkt 2 i artikeln.

En bestämmelse som motsvarar punkt 3 i artikeln finns i 11 § i lagen om straffrättslig rättshjälp. Enligt paragrafens 1 mom. kan en framställning om en särskild form eller ett särskilt förfarande i en begäran om rättshjälp iakttas, om inte detta strider mot finsk lagstiftning.

En bestämmelse som motsvarar punkt 4 i artikeln finns för det första i 12 § i lagen om straffrättslig rättshjälp. I paragrafen föreskrivs om de ovillkorliga grunderna för att vägra rättslig hjälp. I 1 mom. sägs att rättshjälp inte lämnas om lämnandet av hjälpen kunde kränka Finlands suveränitet eller även-

tyra Finlands säkerhet eller andra väsentliga intressen. Enligt 2 mom. lämnas rättshjälp inte heller om lämnandet av hjälpen strider mot principerna om de mänskliga rättigheterna och grundläggande friheterna eller om lämnandet av hjälpen annars strider mot grundprinciperna för Finlands rättsordning. I lagens 13 § finns dessutom bestämmelser om de av prövning beroende grunderna för att vägra rättslig hjälp. Enligt paragrafen kan rättshjälp förvägras bl.a. om begäran hänför sig till en gärning som skall betraktas som ett politiskt brott. Paragrafen innehåller dessutom en del andra grunder för förvägrande, vilka hänför sig till preskription av åtalsrätten, pågående rättegång och motsvarande omständigheter.

En bestämmelse som motsvarar punkt 5 i artikeln finns i 13 § 2 mom. i lagen om straffrättslig rättshjälp. Verkställandet av en begäran om rättshjälp kan enligt bestämmelsen uppskjutas, om verkställandet kunde störa eller fördröja en brottsutredning, en förundersökning eller en rättegång i Finland.

I lagen om straffrättslig rättshjälp finns inte någon uttrycklig bestämmelse som skulle motsvara den samrådsskyldighet som avses i punkt 6 i artikeln. Det är dock möjligt att i samband med de meddelanden som avses nedan i 9 § också samråda med en part och be parten att ändra sin framställning. De finska myndigheterna skall också till dessa delar direkt följa bestämmelserna i konventionen. Det är varken nödvändigt eller ändamålsenligt att ändra lagen om straffrättslig rättshjälp på grund av en dylik obetydlig motstridighet.

En bestämmelse som motsvarar punkt 7 i artikeln finns i 9 § i lagen om straffrättslig rättshjälp. Om en begäran om rättshjälp inte kan uppfyllas eller om verkställigheten fördröjs, skall detta enligt paragrafens 3 mom. utan dröjsmål meddelas den utländska myndighet som framställt begäran. Samtidigt skall grunden för att begäran inte uppfylls eller orsaken till dröjsmålet nämnas. Om begäran om rättshjälp eller de bifogade handlingarna är så bristfälliga att begäran inte kan uppfyllas, skall enligt samma paragrafs 2 mom. den utländska myndighet som framställt begäran utan dröjsmål uppmanas att komplettera begäran eller att ge ytterligare upplysningar i saken.

I fråga om punkt 8 i artikeln bör det noteras att bestämmelsen inte ålägger parterna att hemlighålla en framställning utan endast att meddela om de inte kan tillmötesgå en anhållan om hemlighållande. Bestämmelsen är också annars problemfri för Finland, eftersom en internationell framställning om rättslig hjälp i Finland är sekretessbelagd på grund av att den hänför sig till förundersökningen.

Punkt 9 i artikeln motsvaras av 4 § i lagen om straffrättslig rättshjälp. Enligt paragrafen skall en utländsk myndighet sända begäran om rättshjälp till justitieministeriet eller direkt till den myndighet som är behörig att uppfylla begäran. Har begäran om rättshjälp sänts till justitieministeriet, skall ministeriet utan dröjsmål vidarebefordra begäran till den myndighet som är behörig att verkställa den, om justitieministeriet inte är behörigt att uppfylla den. Finland har inget behov av att göra ett sådant meddelande som avses i punkt 9 e.

Artikel 28. *Sekretess och begränsningar i fråga om användning.* Enligt punkt 1 skall artikeln tillämpas endast om det saknas gällande avtal eller överenskommelse om rättslig hjälp mellan de berörda parterna.

I punkt 2 sägs att den anmodade parten får göra lämnande av upplysningar eller material beroende av att de hemlighålls i de fall framställningen inte kan verkställas om så inte är fallet eller inte används för andra utredningar eller annan lagföring än som anges i framställningen.

Enligt punkt 3 skall den begärande parten meddela den andra parten om den inte kan uppfylla ett villkor. Om den begärande parten godtar villkoret, är den bunden av det.

I punkt 4 sägs att en part som lämnar upplysningar eller material med ett förbehåll har rätt att på begäran få en förklaring om hur upplysningarna eller materialet har använts.

Artikeln behandlas i punkterna 275—280 i den förklarande rapporten. Enligt rapporten är ett av syftena med artikeln att skydda känsliga uppgifter t.ex. i situationer som hänför sig till integritetsskyddet. Artikelns tillämpningsområde har begränsats av samma orsaker som när det gäller artikel 27. Som exempel på upplysningar som det är nödvändigt att hemlighålla enligt punkt 2 nämns

skyddande av en konfidentiell informationskällas identitet. När det gäller begränsning av användningen av information kan det i praktiken vara omöjligt att säkerställa att material inte t.ex. till följd av en offentlig rättegång används också i andra syften än det som avses i en framställning. Syftet med punkt 4 i artikeln är att den som gör ett förbehåll skall kunna kontrollera att detta följs.

Av punkt 1 i artikeln följer att artikeln inte till någon del tillämpas mellan Finland och t.ex. de stater som är parter i den europeiska konventionen om inbördes rättshjälp i brottmål och dess tilläggsprotokoll.

En bestämmelse som motsvarar punkterna 2—4 i artikeln när Finland är den begärande parten finns i 27 § i lagen om straffrättslig rättshjälp. Enligt paragrafens 2 mom. skall vid lämnande av rättshjälp i fråga om hemlighållande, tystnadsplikt, begränsningar i användningen av uppgifterna eller återsändande eller förstörande av överlåtet material iakttas bestämmelserna i gällande avtal mellan Finland och den främmande staten eller villkoren för den främmande statens rättshjälp. Finland kan således på ett bindande sätt godta ett villkor så som avses i 3 punkten. I 25 a § i lagen om straffrättslig rättshjälp finns bestämmelser om utlämnande av uppgifter från Finland till en annan stat. Enligt paragrafen får även handlingar som innehåller sekretessbelagda uppgifter lämnas ut till en främmande stat som begär rättshjälp för att användas som bevis i ett straffrättsligt ärende, om inte utlämnande av upplysningen eller handlingen till utlandet eller användning av upplysningen som bevis förbjudits eller begränsats i lag.

Avsnitt 2 Särskilda bestämmelser

Avdelning 1 Ömsesidig rättslig hjälp med provisoriska åtgärder

Artikel 29. *Skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter.* Artikeln innehåller bestämmelser om rättslig hjälp med förelägganden att säkra datorbehandlingsbara uppgifter. Föreläggandet att säkra data är i propositionen ett nytt tvångsmedel som vid behov kan användas före de övriga tvångsmedlen som riktar sig mot datorbehandlingsbara uppgifter. Syftet med föreläggandet är att förhindra att uppgifter som är av betydelse vid utredning av brott går förlorade eller förändras innan de kan tas i besittning med stöd av andra tvångsmedel. För föreläggandet att säkra data redogörs närmare i motiveringen till artikel 16 och 4 kap. 4 b § i tvångsmedelslagen.

Enligt punkt 1 i artikeln får en part anmoda en annan part att ge ett föreläggande om att säkra datorbehandlingsbara uppgifter. En förutsättning för detta är att parten har för avsikt att överlämna en framställning om rättslig hjälp för att få uppgifterna i sin besittning.

I punkt 2 finns detaljerade bestämmelser om vad en framställning om säkrande av uppgifter skall innehålla.

Enligt punkt 3 skall den anmodade parten skyndsamt besvara framställningen. Dubbel straffbarhet får inte uppställas som villkor för säkrandet.

En part som ställer dubbel straffbarhet som villkor för användning av tvångsmedel genom vilka datorbehandlingsbara uppgifter tas i besittning får enligt punkt 4 förbehålla sig rätten att förutsätta dubbel straffbarhet också i fråga om ett föreläggande att säkra uppgifter. Förbehållet får dock inte gälla de brott som avses i artiklarna 2—11 i konventionen.

Enligt punkt 5 får rättslig hjälp i form av ett föreläggande om att säkra uppgifter förvägras endast om framställningen gäller ett brott som den anmodade parten betraktar som ett politiskt brott eller om hjälpen skulle inkräkta på dess viktiga intressen.

I punkt 6 sägs att en part är skyldig att meddela den andra parten om den anser att ett föreläggande om att säkra uppgifter inte kommer att vara effektivt eller att det kommer att hota sekretessen för eller på annat sätt störa brottsutredningen.

Ett säkrande skall enligt punkt 7 gälla under en period om minst 60 dagar. Om en framställning om att ta uppgifter i besittning görs under denna tid, skall föreläggandet gälla till dess att beslut om framställningen har fattats.

Artikeln behandlas i punkterna 282—289 i den förklarande rapporten. Enligt rapporten är syftet med artikeln att skapa ett medel för att förhindra att bevismaterial i elektronisk

form går förlorat som dels är snabbt, dels inkräktar så litet som möjligt på rättigheterna för den som är föremål för åtgärderna. Artikeln är nödvändig eftersom det går mycket lätt att förstöra bevismaterial och det traditionella samarbetet vid rättslig hjälp kan vara långsamt. Av samma orsaker behöver enligt punkt 2 i artikeln endast sådana grundläggande uppgifter lämnas som är nödvändiga för att en framställning om rättslig hjälp skall kunna avgöras. Dubbel straffbarhet får enligt punkt 3 inte utgöra ett villkor för en åtgärd, eftersom det normalt dröjer länge att utreda denna omständighet. Ett förbehåll enligt punkt 4 får inte göras när det gäller de brott som avses i artiklarna 2—11, eftersom villkoret i praktiken ändå uppfylls i fråga om dem. En framställning får inte avslås på andra grunder än de som anges i punkt 5 i artikeln. Punkt 6 är nödvändig eftersom det kan hända att det först vid verkställigheten av ett föreläggande om att säkra uppgifter visar sig att föreläggandet är oändamålsenligt.

I 23 § i lagen om straffrättslig rättshjälp finns en bestämmelse om tvångsmedel. Eftersom föreläggandet att säkra uppgifter är ett nytt tvångsmedel nämns det inte särskilt i paragrafen. Punkt 1 i artikeln förutsätter således att paragrafen ändras. Denna regeringsproposition innehåller ett förslag enligt vilket paragrafens 1 mom. ändras så att till förteckningen över tvångsmedel som kan vidtas på grundval av en begäran om rättslig hjälp fogas det nya tvångsmedlet föreläggande att säkra data, som förelås i 4 kap. 4 d § i tvångsmedelslagen i propositionen. Efter att förslaget har trätt i kraft motsvarar de gällande bestämmelserna punkt 1 i artikeln.

Enligt punkt 3 i artikeln får dubbel straffbarhet inte uppställas som ett villkor för en åtgärd. I 15 § 1 mom. i lagen om straffrättslig rättshjälp sägs att om en begäran om rättshjälp avser eller dess uppfyllande förutsätter att tvångsmedel enligt tvångsmedelslagen används, får tvångsmedel inte användas, om detta inte skulle vara tillåtet enligt finsk lag i ett sådant fall där den gärning till vilken begäran hänför sig har begåtts i Finland under motsvarande omständigheter. Den gällande rätten står till dessa delar inte i samklang med kraven enligt artikeln.

I regeringens proposition ingår ett förslag enligt vilket till 15 § i lagen om straffrättslig rättshjälp fogas ett nytt 2 mom., där det sägs att vad som föreskrivs i 1 mom. inte gäller förelägganden att säkra data. Till dessa delar bör det noteras att den föreslagna bestämmelsen på grund av det breda tillämpningsområdet för lagen om straffrättslig rättshjälp även gäller stater som inte har tillträtt konventionen. Efter att förslaget har trätt i kraft motsvarar de gällande bestämmelserna punkt 3 i artikeln.

Punkt 5 i artikeln motsvaras för det första av den bestämmelse om ovillkorliga grunder för förvägrande som finns i 12 § i lagen om straffrättslig rättshjälp. Enligt paragrafens 1 mom. lämnas rättshjälp inte om lämnandet av hjälpen kunde kränka Finlands suveränitet eller äventyra Finlands säkerhet eller andra väsentliga intressen. Enligt 2 mom. lämnas rättshjälp inte heller om lämnandet av hjälpen strider mot principerna om de mänskliga rättigheterna och grundläggande friheterna eller om lämnandet av hjälpen annars strider mot grundprinciperna för Finlands rättsordning. I 13 § i lagen om straffrättslig rättshjälp finns dessutom bestämmelser om av prövning beroende grunder för förvägrande. Enligt paragrafen kan rättshjälp förvägras bl.a. om begäran hänför sig till en gärning som skall betraktas som ett politiskt brott. I paragrafen föreskrivs dessutom om andra grunder för förvägrande, vilka hänför sig till preskription av åtalsrätten, en anhängig rättegång och andra motsvarande omständigheter.

Punkterna 2, 6 och 7 i artikeln kan tillämpas som sådana, och de finska myndigheterna kan till dessa delar direkt följa bestämmelserna i konventionen.

Det är således inte nödvändigt att i övrigt ändra lagen om straffrättslig rättshjälp på grund av artikeln.

Enligt förslaget kommer Finland inte att göra något sådant förbehåll som avses i punkt 4 i artikeln, eftersom det inte finns några rationella grunder för att ha olika bestämmelser för olika brottstyper i dessa fall. Denna lösning står också i samklang med den princip som framgår av lagen om straffrättslig rättshjälp, dvs. att Finland strävar efter att lämna rättslig hjälp i så stor utsträckning som möjligt. Det undantag som gäller dubbel straffbarhet går i Finland i och med

detta utöver det absoluta kravet i konventionen.

Artikel 30. *Skyndsamt röjande av säkrade trafikuppgifter.* Artikeln innehåller bestämmelser om rättslig hjälp för att snabbt röja uppgifter om ett meddelandes rutt. Denna nya åtgärd ingår i regeringens proposition och hör nära samman med det föreläggande att säkra uppgifter som avses i artikel 29, och dess syfte är att säkerställa att ett föreläggande om att säkra uppgifter snabbt kan riktas mot rätt objekt i ett sådant fall när flera tjänsteleverantörer i olika länder har deltagit i överföringen av ett meddelande. Artikeln gäller endast sådana trafikuppgifter som har samband med ett meddelande och även då endast sådana uppgifter som är nödvändiga för att klarlägga meddelandets rutt. I praktiken betyder detta endast uppgifter om vilka operatörer som har deltagit i förmedlingen av meddelandet. Skyldigheten att lämna ut uppgifter om ett meddelandes rutt behandlas närmare i motiveringen till artikel 17 och till 4 kap. 4 b § i tvångsmedelslagen.

Om en part upptäcker att en tjänsteleverantör i en annan stat har medverkat i överföringen av ett meddelande, skall parten enligt punkt 1 i artikeln på eget initiativ för den begärande parten röja de trafikuppgifter som är nödvändiga för att identifiera tjänsteleverantören och meddelandets rutt.

Enligt punkt 2 får rättslig hjälp i form av röjande av trafikuppgifter förvägras endast om framställningen gäller ett brott som den anmodade parten betraktar som ett politiskt brott eller om hjälpen skulle inkräkta på dess viktiga intressen.

Artikeln behandlas i punkterna 290—291 i den förklarande rapporten. Enligt rapporten är syftet med artikeln att säkerställa att föreläggandet att säkra trafikuppgifter kan användas också vid gränsöverskridande kommunikation. Med hjälp av de uppgifter som röjs kan den begärande parten snabbt också hos en annan stat genom vilken meddelandet har passerat göra en ny framställning om rättslig hjälp i form av ett föreläggande att säkra uppgifter.

I motiveringen till artikel 29 behandlas den ändring som punkt 1 i artikeln förutsätter i 23 § i lagen om straffrättslig rättshjälp. Genom ändringen uppfylls även kraven enligt denna artikel.

I 12 och 13 § i lagen om straffrättslig rättshjälp finns en bestämmelse som motsvarar punkt 2 i artikeln. Även innehållet i dessa paragrafer behandlas i motiveringen till artikel 29.

I övrigt kan artikeln tillämpas som sådan, och de finska myndigheterna kan till dessa delar direkt följa bestämmelserna i konventionen. Det är inte nödvändigt att ändra lagen om straffrättslig rättshjälp utöver vad som sägs ovan i samband med artikel 29.

Avdelning 2 Ömsesidig rättslig hjälp med utredningsbefogenheter

Artikel 31. *Ömsesidig rättslig hjälp med åtkomst till lagrade datorbehandlingsbara uppgifter.* Artikeln innehåller bestämmelser om rättslig hjälp med husrannsakan och beslag av datorbehandlingsbara uppgifter.

Enligt punkt 1 i artikeln får en part anmoda en annan part att företa husrannsakan, beslag eller motsvarande tvångsmedel i fråga om uppgifter som lagrats inom den anmodade partens territorium. Bestämmelsen gäller även uppgifter som omfattas av ett föreläggande att säkra uppgifter.

Den anmodade parten skall enligt punkt 2 besvara framställningen under tillämpning av de internationella instrument, överenskommelser och lagar som avses i artikel 23 och i enlighet med andra tillämpliga bestämmelser i kapitlet.

Enligt punkt 3 skall framställningen besvaras skyndsamt när uppgifterna i fråga löper särskild risk att gå förlorade eller förändras. Utöver detta skall också bestämmelser i andra överenskommelser som är bindande för parten iakttas.

Artikeln behandlas i punkt 292 i den förklarande rapporten. Enligt rapporten gäller en myndighets i artikel 19 avsedda rätt till husrannsakan och beslag av datorbehandlingsbara uppgifter endast på den ifrågavarande statens territorium. Syftet med den föreliggande artikeln är att samma åtgärder även skall kunna vidtas inom ramen för den internationella rättsliga hjälpen.

De tvångsmedel som avses i punkt 1 i artikeln är av det slaget att rättslig hjälp enligt

23 § i lagen om straffrättslig rättshjälp i regel kan lämnas i Finland. När det gäller beslag av datorbehandlingsbara uppgifter ingår i regeringens proposition ett förslag om att ändra bestämmelsen om rättslig hjälp i form av beslag i 4 kap. 15 a § i lagen om straffrättslig rättshjälp så att till förteckningen över objekt som kan tas i beslag för tydlighetens skull fogas även data.

Punkterna 2 och 3 kan tillämpas som sådana, och de finska myndigheterna kan till dessa delar utöver bestämmelserna i lagen också följa konventionen direkt.

Det är inte nödvändigt att ändra lagen om straffrättslig rättshjälp på grund av artikeln.

Artikel 32. *Gränsöverskridande åtkomst till lagrade datorbehandlingsbara uppgifter med samtycke eller i de fall de är allmänt tillgängliga.* Enligt punkt a i artikeln får en part utan tillstånd av en annan part bereda sig åtkomst till datorbehandlingsbara uppgifter i sådana fall när dessa är allmänt tillgängliga.

I punkt b sägs att en part får bereda sig åtkomst till datorbehandlingsbara uppgifter som inte finns på dess territorium, om den erhåller samtycke av den person som har rätt att röja uppgifterna.

Artikeln behandlas i punkterna 293 och 294 i den förklarande rapporten. Enligt rapporten var avsikten vid beredningen av konventionen att föreskriva om betydligt större rättigheter att skaffa datorbehandlingsbara uppgifter inom en annan stats territorium. Detta visade sig dock vara omöjligt, och den föreliggande artikeln innehåller bestämmelser som samtliga parter utan svårigheter kunde acceptera.

De rättigheter som avses i artikeln är självklara från finsk synpunkt och kan således tillämpas utan problem.

Artikel 33. *Ömsesidig rättslig hjälp med insamling i realtid av trafikuppgifter.* Artikeln innehåller bestämmelser om rättslig hjälp med ett tvångsmedel som motsvarar teleövervakning. I motiveringen till artikel 20 redogörs närmare för detta tvångsmedel.

Enligt artikeln skall parterna lämna varandra rättslig hjälp med teleövervakning åtminstone med avseende på brott för vilka teleövervakning skulle vara möjlig i ett nationellt fall. I övrigt skall de villkor och förfaranden som anges i den nationella lagstiftningen gälla.

Artikeln behandlas i punkterna 295 och 296 i den förklarande rapporten. På grund av att trafikuppgifter ofta bevaras endast en kort tid är det enligt rapporten viktigt att dessa uppgifter kan insamlas i realtid också när kommunikationen är gränsöverskridande. Punkt 2 i artikeln skall tolkas som en rekommendation till parterna att godkänna en så omfattande rättslig hjälp som möjligt med avseende på denna artikel.

Det tvångsmedel som avses i artikeln är sådant att Finland med stöd av 23 § i lagen om straffrättslig rättshjälp i regel kan lämna rättslig hjälp med det på samma villkor som tvångsmedlet kan användas nationellt. I motiveringen till artikel 20 redogörs för den gällande rätten till dessa delar. Enligt förslaget kommer Finland att göra ett förbehåll om att Finland nationellt tillämpar det ovan nämnda tvångsmedlet endast på vissa särskilt angivna brott. Även förbehållet behandlas närmare i motiveringen till artikel 20.

Artikel 34. *Ömsesidig rättslig hjälp med avlyssning av innehållsuppgifter.* Artikeln innehåller bestämmelser om rättslig hjälp med ett tvångsmedel som motsvarar teleavlyssning. I motiveringen till artikel 21 redogörs närmare för detta tvångsmedel.

Enligt artikeln skall parterna, i den utsträckning det är tillåtet enligt gällande avtal och nationell lagstiftning, lämna varandra rättslig hjälp i fråga om insamling eller upptagning i realtid av innehållsuppgifter i särskilt angivna meddelanden som överförs med hjälp av ett datorsystem.

Artikeln behandlas i punkt 297 i den förklarande rapporten. Enligt rapporten skall lämnandet av rättslig hjälp med detta tvångsmedel på grund av åtgärdens natur avgöras i parternas nationella lagstiftning.

Beträffande denna artikel och artikel 33, som behandlas ovan, bör det noteras att den europeiska konventionen om inbördes rättshjälp i brottmål inte innehåller några bestämmelser om teleövervakning eller teleavlyssning. Dylika bestämmelser ingår däremot i EU:s konvention om rättslig hjälp. Såsom sagts i allmänna motiveringen har EU:s konvention om rättslig hjälp satts i kraft i Finland, och konventionen trädde också i kraft internationellt den 11 augusti 2005.

Det tvångsmedel som avses i artikeln är dock sådant att Finland i regel kan lämna rättslig hjälp med det direkt med stöd av 23 § i lagen om straffrättslig rättshjälp på samma villkor som tvångsmedlet kan användas nationellt.

Avdelning 3 Nätverk 24/7

Artikel 35. *Nätverk 24/7.* Artikeln innehåller bestämmelser om de särskilda kontaktpunkter som skall utses och deras uppgifter.

Enligt punkt 1 i artikeln skall varje part utse en kontaktpunkt som skall ge hjälp och i mån av möjlighet vidta åtgärder i ärenden som grundar sig på konventionen. Kontaktpunkten skall vara tillgänglig 24 timmar om dygnet sju dagar i veckan. Till kontaktpunktens uppgifter hör att tillhandahålla teknisk rådgivning, säkra uppgifter, insamla bevis, tillhandahålla rättslig information och lokalisera misstänkta.

I punkt 2 sägs att en parts kontaktpunkt skall kunna skyndsamt kommunicera med en annan parts kontaktpunkt och, vid behov, med sina nationella myndigheter som ansvarar för rättslig hjälp.

Enligt punkt 3 skall varje part tillse att den har tillgång till utbildad och välutrustad personal.

Artikeln behandlas i punkterna 298—302 i den förklarande rapporten. Enligt rapporten måste det internationella samarbetet vid utredningen av nätbrott ibland kunna ske mycket snabbt. Kontaktpunkterna enligt artikeln är således av avgörande betydelse för att de mål som uppställs i konventionen skall kunna nås. En kontaktpunkt skall antingen säkerställa eller själv utföra de uppgifter som avses i artikeln. Det är upp till parterna att bestämma inom vilken organisation kontaktpunkten skall finnas. Det bör dock beaktas att kontaktpunkterna sköter uppgifter av mycket varierande karaktär. Med bestämmelsen i punkt 3 avses i praktiken åtminstone effektiva kommunikationsmedier och en tillräckligt språkkunnig personal.

Finland kommer att utse centralkriminalpolisen till sådan kontaktpunkt som avses i artikeln.

Kapitel IV. **Slutbestämmelser (artiklarna 36—48)**

I kapitel IV i konventionen finns bestämmelser om konventionens undertecknande och ikraftträdande (artikel 36), anslutning till konventionen (artikel 37), territoriell tillämpning (artikel 38), konventionens verkan (artikel 39), förklaringar (artikel 40), möjlighet för federala stater att göra förbehåll (artikel 41), övriga förbehåll (artikel 42), förbehållens status och återtagande (artikel 43), ändringar i konventionen (artikel 44), tvistlösning (artikel 45), samråd mellan parterna (artikel 46), uppsägning av konventionen (artikel 47) och meddelanden (artikel 48). Artiklarna behandlas i punkterna 303—330 i den förklarande rapporten. Slutbestämmelserna är i huvudsak sådana sedvanliga bestämmelser som ingår i Europarådets konventioner.

Enligt artikel 36 träder konventionen i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då fem stater, varav minst tre medlemsstater i Europarådet, har uttryckt sitt samtycke till att vara bundna av konventionen i enlighet med bestämmelserna i punkterna 1 och 2 i artikeln. För en signatärstat som senare uttrycker sitt samtycke till att vara bunden av konventionen träder denna i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då den har uttryckt sitt samtycke till att vara bunden av konventionen.

Artikel 40 innehåller bestämmelser om förklaringar. Enligt artikeln får en stat meddela att den begagnar sig av möjligheten att kräva ytterligare rekvisit enligt vad som anges i artiklarna 2, 3, 6.1 b, 7, 9.3 och 27.9 e. Enligt förslaget kommer Finland att avge en förklaring enligt artikel 2. Innehållet i den förklaring som Finland kommer att avge och i eventuella övriga förklaringar behandlas närmare i motiveringen till artiklarna i fråga.

Artikel 42 i konventionen innehåller en uttömmande förteckning över de tillåtna förbehållen. Tillåtna förbehåll är de som anges i artiklarna 4.2, 6.3, 9.4, 10.3, 11.3, 14.3, 22.2, 29.4 och 41.1.

Enligt förslaget kommer Finland att göra förbehåll enligt artiklarna 11.3 och 14.3 a

och b. Innehållet i de förbehåll som Finland kommer att göra och i eventuella övriga förbehåll behandlas närmare i motiveringen till artiklarna i fråga.

I artikel 45 i konventionen finns bestämmelser om lösandet av eventuella tvister till följd av konventionen. Om en tvist skulle uppstå, skall parterna enligt artikeln söka lösa den genom förhandling eller andra fredliga medel efter deras eget val. Bestämmelsen i artikeln är en rekommendation och förpliktar inte Finland att underordna sig något särskilt förfarande för tvistlösning.

2. Rambeslutet och den gällande lagstiftningen

I rambeslutet finns bestämmelser om intrång i informationssystem (artikel 2), systemstörning (artikel 3), datastörning (artikel 4) samt bestämmelser om anstiftan, medhjälp och försök samt juridiska personers ansvar i samband med dessa brott (artiklarna 5 och 8). Dessutom finns i rambeslutet bestämmelser om behörighet (artikel 10) och utbyte av uppgifter (artikel 11). Samtliga de ovan nämnda frågorna regleras även i konventionen genom bestämmelser med i huvudsak likadant innehåll.

En väsentlig skillnad som även inverkar på den finska lagstiftningen är emellertid att rambeslutet dessutom innehåller minimikrav när det gäller straffskalan för fängelsestraff (artiklarna 6 och 7). Bestämmelserna om dataintrång och skadegörelse i den finska lagstiftningen uppfyller inte rambeslutets krav när det gäller straffskalan, såsom anges närmare nedan. Efter att de ändringar som konventionen förutsätter har gjorts uppfyller den finska lagstiftningen till alla övriga delar även kraven i rambeslutet.

Eftersom förhållandet mellan konventionen och den finska lagstiftningen redan har behandlats ovan, görs det för att undvika onödiga upprepningar inte mera någon likadan ingående jämförelse mellan rambeslutet och den finska lagstiftningen. Till den del kraven enligt rambeslutet motsvarar kraven enligt konventionen hänvisas det i propositionen endast till de slutsatser som dragits i motiveringen till de enskilda artiklarna i konventionen.

Artikel 1. *Definitioner.* Artikeln innehåller bestämmelser om de definitioner som används i rambeslutet.

Enligt punkt a i artikeln avses med informationssystem en apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av datorbehandlingsbara uppgifter. Dessutom omfattar definitionen datorbehandlingsbara uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av dessa för att de skall kunna drivas, användas, skyddas och underhållas. Datorbehandlingsbara uppgifter definieras i punkt b. Begreppet används i artiklarna 2, 3 och 4 för att avgränsa föremålet för de straffbara handlingarna.

Definitionen avviker till sin ordalydelse från motsvarande definition i konventionen genom att det i konventionen inte särskilt nämns att begreppet datorsystem innefattar även datorbehandlingsbara uppgifter. Preciseringen i rambeslutet är dock onödig, och denna skillnad saknar därför praktisk betydelse.

Enligt punkt b avses med datorbehandlingsbara uppgifter framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett informationssystem, inklusive program som lämpar sig för att få ett informationssystem att utföra en viss uppgift. Begreppet används i definitionen av informationssystem i punkt a ovan, i artikel 3 för att avgränsa gärningssättet för de straffbara handlingarna och i artikel 4 för att avgränsa föremålet för de straffbara handlingarna. Definitionen motsvarar ordagrant motsvarande definition i konventionen.

Enligt punkt c i artikeln avses med juridisk person en enhet som har sådan status enligt tillämplig lagstiftning, med undantag av stater eller andra offentliga organ vid utövandet av de befogenheter som de har i egenskap av statsmakter samt internationella offentliga organisationer. Av definitionen följer att begreppet juridisk person bestäms enligt den nationella lagstiftningen. Definitionens enda innehåll består i att den ur begreppet utesluter stater och andra motsvarande offentliga organ. Begreppet används i artiklarna 8 och 9 för att avgränsa tillämpningsområdet för be-

stämmelserna om juridiska personers ansvar samt i artikel 10.1 c, som innehåller en särskild bestämmelse om behörighet. I konventionen finns inte någon motsvarande definition.

Enligt punkt d i artikeln avses med orättmätigt ett intrång eller en störning som sker utan tillstånd från ägaren eller annan rättighetshavare till systemet eller del av detta eller som inte medges i den nationella lagstiftningen. Definitionen används i artiklarna 2, 3 och 4 för att handlingar som begås med ägarens tillstånd eller på något annat behörigt sätt inte skall omfattas av artiklarnas tillämpningsområde. I konventionen finns inte någon motsvarande definition.

Artikel 2. *Olagligt intrång i informationssystem.* Enligt punkt 1 i artikeln skall uppsåtligt orättmätigt intrång i ett informationssystem som en helhet eller en del av ett sådant system straffbeläggas. Bestämmelsen gäller dock inte sådana fall som är ringa.

I punkt 2 sägs att varje medlemsstat får besluta att det handlande som avses i punkt 1 endast skall kriminaliseras när brottet begås genom intrång i en säkerhetsåtgärd.

Artikeln skiljer sig från artikel 2 i konventionen, som gäller samma sak, genom att en part enligt konventionen förutom att uppställa krav på att brottet begås genom intrång i säkerhetsåtgärder dessutom får bestämma om en del andra villkor för straffbarheten. I konventionen finns inte heller någon uttrycklig undantagsbestämmelse som gäller ringa fall. Till övriga delar är kraven i artiklarna i sak identiska.

Skillnaderna saknar praktisk betydelse för Finland. Av de skäl som anges i motiveringen till artikel 2 i konventionen förutsätter den nämnda artikeln inte några ändringar i lagstiftningen. Av samma skäl förutsätter inte heller den föreliggande artikeln i rambeslutet några ändringar i lagstiftningen.

Enligt förslaget kommer Finland att använda sig av rätten att i enlighet med punkt 2 i artikeln endast kriminalisera det handlande som avses i punkt 1 när brottet begås genom intrång i en säkerhetsåtgärd.

Artikel 3. *Olaglig systemstörning.* Enligt artikeln skall det vara straffbart att uppsåtligen allvarligt hindra eller avbryta driften av ett informationssystem genom att mata in, överföra, skada, radera, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter, när gärningen utförs orättmätigt. Bestämmelsen gäller dock inte sådana fall som är ringa.

Artikeln skiljer sig från artikel 5 i konventionen, som gäller samma sak, endast genom att konventionen inte innehåller någon uttrycklig undantagsbestämmelse som gäller ringa fall. Till övriga delar är kraven i artiklarna i sak identiska.

Skillnaden saknar praktisk betydelse för Finland. I motiveringen till artikel 5 i konventionen redogörs för de ändringar som den nämnda artikeln förutsätter i den finska lagstiftningen. Efter att den föreslagna ändringen har trätt i kraft uppfyller de gällande bestämmelserna också kraven enligt den föreliggande artikeln i rambeslutet.

Artikel 4. *Olaglig datastörning.* Enligt artikeln skall det vara straffbart att uppsåtligen radera, skada, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem, när gärningen utförs orättmätigt. Bestämmelsen gäller dock inte sådana fall som är ringa.

Artikeln skiljer sig från artikel 4 i konventionen, som gäller samma sak, endast genom att konventionen inte innehåller någon uttrycklig undantagsbestämmelse som gäller ringa fall. Till övriga delar är kraven i artiklarna i sak identiska.

Skillnaden saknar praktisk betydelse för Finland. Av de skäl som anges i motiveringen till artikel 4 i konventionen förutsätter den nämnda artikeln inte några ändringar i lagstiftningen. Av samma skäl förutsätter inte heller den föreliggande artikeln i rambeslutet några ändringar i lagstiftningen.

Artikel 5. *Anstiftan, medhjälp och försök.* Enligt punkt 1 i artikeln skall anstiftan av och medhjälp till olagligt intrång i informationssystem enligt artikel 2, olaglig systemstörning enligt artikel 3 och olaglig datastörning enligt artikel 4 straffbeläggas.

I konventionen finns en likadan bestämmelse som gäller motsvarande brott. Av de skäl som anges i motiveringen till artikel 11.1 i konventionen förutsätter den nämnda artikeln inte några ändringar i lagstiftningen. Av samma skäl förutsätter inte heller punkt 1

i den föreliggande artikeln i rambeslutet några ändringar i lagstiftningen.

Enligt punkt 2 i artikeln skall försök till de brott som avses i punkt 1 straffbeläggas. I punkt 3 sägs dock att en medlemsstat får besluta att inte tillämpa punkt 2 för olagligt intrång enligt artikel 2.

I konventionen finns motsvarande bestämmelser i artikel 11.2 och 11.3. Enligt det lagförslag som ingår i propositionen kommer Finland att kriminalisera försök till vissa brott så som anges i motiveringen till artikel 11. Bestämmelserna i konventionen skiljer sig dock från bestämmelserna i rambeslutet genom att konventionen medger förbehåll i fråga om samtliga kriminaliseringsskyldigheter som gäller försök.

Skillnaden är av betydelse eftersom Finland enligt förslaget kommer att göra ett förbehåll till konventionen enligt vilket Finland inte när det gäller lindrig skadegörelse tillämpar den bestämmelse som förpliktar till kriminalisering av försök.

Enligt artikel 4 i rambeslutet kan tillämpningsområdet för bestämmelsen om datastörning dock begränsas så att det inte omfattar ringa fall. Bestämmelsen skall tolkas så att detsamma gäller också försök till en ringa gärning enligt artikel 4 i ett sådant fall när gärningen är straffbar om den fullbordas. En annorlunda tolkning skulle leda till ett slutresultat som strider mot rambeslutets syften.

I strafflagens 35 kap. 3 §, som gäller lindrig skadegörelse, är det fråga om just en sådan ringa gärning som avses i artikel 4 i rambeslutet. Därför förutsätter punkt 2 i artikeln inte några ändringar i lagstiftningen.

Till övriga delar motsvarar kraven i rambeslutet och konventionen varandra. I motiveringen till artikel 11.2 i konventionen redogörs för de ändringar som den nämnda punkten förutsätter i den finska lagstiftningen. Efter att de föreslagna ändringarna har trätt i kraft uppfyller de gällande bestämmelserna även kraven i artikel 5.2 i rambeslutet.

Artikel 6. *Påföljder.* Enligt punkt 1 i artikeln skall medlemsstaterna se till att de brott som avses i artiklarna 2, 3, 4 och 5 är belagda med effektiva, proportionella och avskräckande straffrättsliga påföljder. I punkt 2 sägs att medlemsstaterna skall se till att de brott som avses i artiklarna 3 och 4 är belagda med straffrättsliga påföljder som innebär ett maximistraff på minst ett till tre års fängelse.

Valet av påföljd och straffskalor överlåts således på medlemsstaterna i fråga om olagligt intrång enligt artikel 2 och anstiftan, medhjälp och försök enligt artikel 5. Bestämmelsen om försvårande omständigheter i artikel 7 nedan gäller visserligen också olagligt intrång som begåtts genom att bryta säkerhetsarrangemang.

Punkt 2 i artikeln innebär att den föreskrivna maximipåföljden för systemstörning enligt artikel 3 och datastörning enligt artikel 4 skall vara fängelse i minst ett år. Den övre gräns på tre år som anges i artikeln är endast en rekommendation.

De gärningar som avses i punkt 2 motsvaras i den finska lagstiftningen av störande av post- och teletrafik med ett maximistraff på fängelse i två år, skadegörelse som riktar sig mot information med ett maximistraff på fängelse i ett år samt det i denna proposition föreslagna brottet systemstörning med ett maximistraff på fängelse i två år.

Artikeln förutsätter således inte ändringar i lagstiftningen.

Artikel 7. *Försvårande omständigheter.* Enligt artikeln skall medlemsstaterna se till att det brott som avses i artikel 2.2 och de brott som avses i artiklarna 3 och 4 är belagda med straffrättsliga påföljder som innebär ett maximistraff på minst två till fem års fängelse, när de begås inom ramen för en sådan kriminell organisation som avses i gemensam åtgärd 98/733/RIF, oberoende av den påföljdsnivå som anges i den gemensamma åtgärden. Enligt artikeln får en medlemsstat även vidta de åtgärder som avses i punkt 1, när brottet har orsakat allvarliga skador eller påverkat väsentliga intressen.

Artikeln innebär att den föreskrivna maximipåföljden för sådant olagligt intrång enligt artikel 2.2 som begås genom intrång i en säkerhetsåtgärd, systemstörning enligt artikel 3 och datastörning enligt artikel 4 skall vara fängelse i minst två år, om gärningen har begåtts inom ramen för en sådan kriminell organisation som avses i artikeln. Detta krav skall förstås så att det nämnda maximistraffet skall föreskrivas åtminstone i ovan nämnda fall men att den nationella bestämmelsen också kan gå utöver detta. Den övre gräns på

fem år som anges i artikeln är endast en rekommendation.

Enligt definitionen i den gemensamma åtgärd 98/733/RIF som det hänvisas till i artikeln avses med kriminell organisation en strukturerad sammanslutning, inrättad för en begränsad tid av mer än två personer som handlar i samförstånd för att begå brott som bestraffas med frihetsberövande eller en frihetsberövande säkerhetsåtgärd på upp till minst fyra år eller ett strängare straff oavsett om brotten är ett mål i sig själv eller ett medel att erhålla materiella fördelar och i förekommande fall ett sätt att otillbörligt påverka offentliga myndighetens verksamhet. En definition som motsvarar artikeln finns i 17 kap. 1 a § 4 mom. i strafflagen.

De gärningar som avses i artikeln motsvaras i den finska lagstiftningen av dataintrång med ett maximistraff på fängelse i ett år, störande av post- och teletrafik med ett maximistraff på fängelse i två år för ett brott enligt grundrekvisitet, skadegörelse som riktar sig mot information med ett maximistraff på fängelse i ett år för ett brott enligt grundrekvisitet samt det i denna proposition föreslagna brottet systemstörning med ett maximistraff på fängelse i två år för ett brott enligt grundrekvisitet.

Straffskalan för grundrekvisitet av störande av post- och teletrafik samt det föreslagna brottet systemstörning uppfyller kraven enligt artikeln. Rekvisitet för dessa allmänna bestämmelser blir också tillämpligt när en gärning har begåtts som ett led i en sådan kriminell organisations verksamhet som avses i bestämmelsen. Artikeln förutsätter således inte att straffskalan ändras i fråga om dessa brott.

När det gäller dataintrång uppfyller lagstiftningen inte kraven enligt artikeln. I propositionen ingår ett förslag enligt vilket till strafflagens 38 kap. fogas en bestämmelse om en grov gärningsform av dataintrång. Enligt paragrafen skall en gärning betraktas som grov om gärningsmannen begår brottet såsom medlem av en i 17 kap. 1 b § avsedd organiserad kriminell sammanslutning eller om brottet begås särskilt planmässigt. Dessutom förutsätts det att gärningen är grov även bedömd som en helhet. Straffskalan föreslås vara fängelse i minst fyra månader och högst två år. Förslaget behandlas mera ingående i detaljmotiveringen till paragrafen. Efter att den föreslagna lagändringen har trätt i kraft uppfyller lagstiftningen till dessa delar kraven i artikeln.

När det gäller det föreskrivna maximistraffet för skadegörelse som riktar sig mot information uppfyller lagstiftningen inte kraven enligt artikeln. Maximistraffet för ett brott enligt grundrekvisitet är fängelse i ett år. Maximistraffet för den grova gärningsformen av brottet är visserligen fängelse i fyra år, men i rekvisitet nämns inte gärningar som begås inom ramen för en kriminell organisation. Eftersom tillämpningsförutsättningarna alltid anges uttömmande i strafflagen i fråga om grova gärningsformer av brott, kan bestämmelsen inte tillämpas på gärningar som begåtts inom ramen för en kriminell organisation. I propositionen ingår ett förslag enligt vilket straffskalan för grundrekvisitet av skadegörelse i 35 kap. 1 § i strafflagen ändras så att maximistraffet höjs från ett till två års fängelse. Förslaget behandlas mera ingående i detaljmotiveringen till paragrafen. Efter att den föreslagna lagändringen har trätt i kraft uppfyller lagstiftningen till dessa delar kraven i artikeln.

Artikel 8. *Juridiska personers ansvar.* Enligt punkt 1 i artikeln skall juridiska personer kunna ställas till ansvar för brott som kriminaliseras i rambeslutet och som begås till deras förmån av en fysisk person som agerar antingen enskilt eller i den juridiska personens namn och har en ledande ställning inom denna, grundad på befogenhet att företräda den juridiska personen, befogenhet att fatta beslut på den juridiska personens vägnar eller befogenhet att utöva kontroll inom den juridiska personen.

Punkt 1 i artikeln motsvarar i sak artikel 12.1 i konventionen.

Enligt punkt 2 i artikeln skall en juridisk person kunna ställas till ansvar för brott som straffbeläggs i enlighet med rambeslutet också när bristande övervakning eller kontroll som skall utföras av en sådan fysisk person som avses i punkt 1 har gjort det möjligt för en fysisk person, som handlar på den juridiska personens vägnar, att begå de brott som straffbeläggs i enlighet med artiklarna 2–5 i rambeslutet till förmån för den juridiska per-

sonen.

Punkt 2 i artikeln motsvarar i sak artikel 12.2 i konventionen.

I punkt 3 konstateras att en juridisk persons ansvar inte skall inverka på det straffrättsliga ansvaret för fysiska personer som har begått brott.

Punkt 3 i artikeln motsvarar i sak artikel 12.4 i konventionen.

Av de skäl som anges i motiveringen till artikel 12 i konventionen förutsätter den nämnda artikeln inte ändringar i lagstiftningen när det gäller de allmänna bestämmelserna om straffansvar för juridiska personer. Av samma skäl förutsätter inte heller den föreliggande artikeln i rambeslutet några ändringar i lagstiftningen. När det gäller de enskilda straffbestämmelserna förutsätts det för att straffansvar för juridiska personer skall kunna tillämpas dessutom att det finns en hänvisningsbestämmelse om saken i strafflagen. Denna fråga behandlas i motiveringen till artikel 9 nedan.

Artikel 9. *Påföljder för juridiska personer.* Enligt punkt 1 i artikeln skall en juridisk person kunna bli föremål för effektiva, proportionella och avskräckande påföljder, som skall innefatta bötesstraff eller administrativa avgifter och som får innefatta andra påföljder.

Artikeln avviker till dessa delar från artikel 12.3 i konventionen, som innehåller motsvarande bestämmelser. Enligt konventionen kan det bli fråga om ansvar av straffrättslig, civilrättslig eller administrativ natur. I rambeslutet sägs att påföljderna skall innefatta bötesstraff eller administrativa avgifter. Enbart ett privaträttsligt skadeståndsansvar är således inte tillräckligt för att uppfylla kraven enligt rambeslutet.

Saken är av betydelse eftersom Finland inte enligt propositionen kommer att utsträcka straffansvaret för juridiska personer till de lindriga gärningsformerna av skadegörelse, störande av post- och teletrafik eller systemstörning på den grunden att detta inte vore ändamålsenligt med hänsyn till gärningarnas karaktär och ringa betydelse. För rambeslutets del kan detta beslut dock inte motiveras enbart med att en juridisk person i Finland alltid kan ställas till skadeståndsansvar för skador som orsakats genom brott.

I artikel 4 i rambeslutet sägs dock att bestämmelsen om datastörning inte behöver tillämpas på sådana fall som är ringa. Bestämmelsen skall tolkas så att detsamma gäller även utsträckande av ansvaret för juridiska personer till de gärningar som avses i artikel 4, också i sådana fall när en ringa gärning i sig är straffbar. En annan tolkning skulle leda till ett slutresultat som strider mot rambeslutets syftemål.

I bestämmelsen om lindrig skadegörelse i 35 kap. 3 § i strafflagen är det uttryckligen fråga om en sådan ringa gärning som avses i artikel 4 i rambeslutet. Därför förutsätter artikeln inte att ansvaret för juridiska personer utsträcks till lindrig skadegörelse. Inte heller artikel 3, som gäller olaglig systemstörning, förpliktar till kriminalisering av ringa fall, varför ansvaret för juridiska personer på samma grunder inte heller behöver utsträckas till lindrigt störande av post- och teletrafik eller det föreslagna nya brottet lindrig systemstörning.

Till övriga delar motsvarar kraven i rambeslutet och konventionen varandra. I punkt 1 i artikeln finns en förteckning med exempel på alternativa påföljder, av vilka en del är främmande för rättssystemet i Finland. Denna omständighet saknar dock betydelse, eftersom bestämmelsen inte är förpliktande till dessa delar. I punkt 2 i artikeln sägs att påföljderna skall vara effektiva, proportionella och avskräckande. Punkt 2 i artikeln motsvarar i sak artikel 13.2 i konventionen.

I motiveringen till artikel 12 i konventionen redogörs för de ändringar som skall göras i den finska lagstiftningen på grund av den ovan nämnda artikeln. Efter att de föreslagna ändringarna har trätt i kraft uppfyller de gällande bestämmelserna även kraven i artiklarna 8 och 9 i rambeslutet.

Artikel 10. *Behörighet.* I punkt 1 a i artikeln sägs att varje medlemsstat skall fastställa sin behörighet beträffande de brott som avses i rambeslutet, när brottet har begåtts helt eller delvis på dess territorium.

Enligt punkt 2 i artikeln skall punkt 1 a tillämpas även i fall där brottslingen är närvarande på medlemsstatens territorium när brottet begås, oavsett om brottet riktar sig mot ett informationssystem på denna medlemsstats territorium eller inte, eller brottet

riktar sig mot ett informationssystem på medlemsstatens territorium, oavsett om brottslingen är närvarande på detta territorium när brottet begås eller inte.

Punkt 1 a i artikeln motsvarar artikel 22.1 a i konventionen. Trots att konventionen inte såsom artikel 10.2 i rambeslutet innehåller någon uttrycklig bestämmelse om tillämpning av territorialitetsprincipen på basis av gärningsorten och den ort där följden av brottet framträdde, uppfyller regleringen även till dessa delar i sak kraven enligt konventionen.

Enligt punkt 1 b i artikeln skall varje medlemsstat fastställa sin behörighet beträffande de brott som avses i rambeslutet, när brottet har begåtts av en av dess medborgare. En i sak identisk bestämmelse finns i artikel 22.1 d i konventionen.

I punkt 1 c i artikeln sägs att varje medlemsstat skall fastställa sin behörighet beträffande de brott som avses i rambeslutet, när brottet har begåtts till förmån för en juridisk person som har sitt huvudkontor på medlemsstatens territorium. I konventionen finns inte någon motsvarande bestämmelse. Inte heller den finska lagstiftningen innehåller någon sådan reglering som skulle motsvara bestämmelsen. Detta saknar dock betydelse eftersom bestämmelsen enligt punkt 5 i artikeln inte behöver tillämpas.

En medlemsstat som enligt sin lagstiftning ännu inte utlämnar eller överlämnar sina egna medborgare skall enligt punkt 3 i artikeln vidta de åtgärder som är nödvändiga för att fastställa sin behörighet i fråga om och, när det är lämpligt, väcka åtal för de brott som avses i rambeslutet, när de har begåtts av en av landets medborgare utanför landets territorium. En i sak identisk bestämmelse finns i artikel 22.3 i konventionen.

I punkt 4 i artikeln finns en bestämmelse om skyldighet för medlemsstaterna att samarbeta när ett brott faller under flera än en medlemsstats behörighet. Bestämmelserna i rambeslutet är mera detaljerade än motsvarande bestämmelser i artikel 22.5 i konventionen. Skillnaden saknar dock betydelse med hänsyn till behovet av att ändra den finska lagstiftningen.

Enligt punkt 5 i artikeln får en medlemsstat besluta att inte eller endast i särskilda fall eller under särskilda omständigheter tillämpa de bestämmelser om behörighet som anges i punkt 1 b och 1 c. Såsom sagts ovan kommer Finland enligt propositionen inte att tillämpa punkt 1 c i artikeln.

Medlemsstaterna skall enligt punkt 6 i artikeln underrätta rådets generalsekretariat och kommissionen när de beslutar att tillämpa punkt 5, i förekommande fall med uppgift om i vilka särskilda fall eller under vilka särskilda omständigheter beslutet gäller. I samband med den rapport om genomförandet av rambeslutet som avses i artikel 12 kommer Finland att så som avses i punkt 6 göra en underrättelse om att Finland inte tillämpar punkt 1 c.

Av de skäl som anges i motiveringen till artikel 22 i konventionen förutsätter den nämnda artikeln inte ändringar i lagstiftningen. Av samma skäl förutsätter inte heller den föreliggande artikeln i rambeslutet några ändringar i lagstiftningen.

Artikel 11. *Utbyte av uppgifter.* Enligt punkt 1 i artikeln skall medlemsstaterna, med iakttagande av bestämmelser om dataskydd, för utbyte av uppgifter om de brott som avses i rambeslutet använda det befintliga nät med operativa kontaktpunkter som kan nås dygnet runt alla dagar i veckan.

Varje medlemsstat skall enligt punkt 2 underrätta rådets generalsekretariat och kommissionen om sin utsedda kontaktpunkt för vidarebefordring till de andra medlemsstaterna.

I Finland är centralkriminalpolisen den kontaktpunkt som avses i artikeln.

Artikel 12. *Genomförande.* Enligt punkt 1 i artikeln skall de åtgärder som rambeslutet förutsätter vidtas senast den 16 mars 2007.

Enligt punkt 2 i artikeln skall medlemsstaterna till rådets generalsekretariat och kommissionen senast nämnda dag överlämna texten till bestämmelser genom vilka de skyldigheter som ålagts dem enligt rambeslutet införlivas med deras nationella lagstiftning. Rådet skall senast den 16 september 2007 på grundval av en rapport som skall utarbetas utifrån information och en skriftlig rapport från kommissionen bedöma i vilken utsträckning bestämmelserna i rambeslutet har följts.

Artikel 13. *Ikraftträdande.* Enligt artikeln träder rambeslutet i kraft samma dag som det

offentliggörs i Europeiska unionens officiella tidning. Rambeslutet har publicerats i EUT L 69/67, 16.3.2005.

3. Lagförslag

3.1. Lag om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i Europarådets konvention om IT-relaterad brottslighet

1 §. Paragrafen innehåller en sedvanlig ikraftträdelsebestämmelse om att de bestämmelser i konventionen som hör till området för lagstiftningen gäller som lag sådana Finland har förbundit sig till dem.

2 §. Enligt bestämmelsen i paragrafen kan närmare bestämmelser om verkställigheten av lagen utfärdas genom förordning av statsrådet.

3 §. Enligt bestämmelsen i paragrafen bestäms om ikraftträdandet av lagen genom förordning av republikens president. Avsikten är att lagen skall träda i kraft samtidigt som konventionen.

3.2. Strafflagen

17 kap. **Om brott mot allmän ordning**

1 a §. *Deltagande i en organiserad kriminell sammanslutnings verksamhet.* För att möjliggöra den hänvisningsteknik som används nedan i 38 kap. 8 a § föreslås det att definitionen av organiserad kriminell sammanslutning i paragrafens 4 mom. överförs till en ny 1 b § och att 4 mom. upphävs. Det gällande 4 mom. hindrar att definitionen i momentet utnyttjas genom hänvisningsteknik. Efter att den föreslagna ändringen har trätt i kraft kan definitionen användas också vid genomförandet av andra rambeslut och i eventuella andra bestämmelser som förutsätter användning av definitionen.

1 b §. *Definition av organiserad kriminell sammanslutning.* Av de orsaker som anges i motiveringen till 1 a § ovan föreslås det att till kapitlet fogas en särskild paragraf som innehåller en definition. Enligt den nuvarande definitionen avses med organiserad kriminell sammanslutning en strukturerad sammanslutning, inrättad för en viss tid, bestående av minst tre personer, som handlar i samförstånd för att begå brott som avses i samma paragrafs 1 mom. Det föreslås att hänvisningen till paragrafens 1 mom. stryks i definitionen när det gäller de brott som begås inom ramen för en sammanslutning. I övrigt är definitionen oförändrad i sak.

8 a §. *Grovt ordnande av olaglig inresa.* Enligt punkt 2 i paragrafen är ordnandet av olaglig inresa grovt, om brottet har begåtts som ett led i en i 1 a § 4 mom. avsedd organiserad kriminell sammanslutnings verksamhet. I propositionen föreslås det att definitionen av organiserad kriminell sammanslutning flyttas från den nämnda 1 a § 4 mom. till en ny 1 b §. Det föreslås därför att också hänvisningen i paragrafens 2 punkt ändras till en hänvisning till den nya definitionsbestämmelsen.

18 a §. *Grov spridning av barnpornografisk bild.* Enligt paragrafens 4 punkt är spridningen av barnpornografisk bild grov, om brottet har begåtts som ett led i en i 1 a § 4 mom. avsedd organiserad kriminell sammanslutnings verksamhet. I propositionen föreslås det att definitionen av organiserad kriminell sammanslutning flyttas från den nämnda 1 a § 4 mom. till en ny 1 b §. Det föreslås att hänvisningen i paragrafens 4 punkt ändras till en hänvisning till den nya definitionsbestämmelsen.

25 kap. **Om brott mot friheten**

3 a §. *Grov människohandel.* Det föreslås att hänvisningen i 1 mom. 4 punkten till en i 17 kap. 1 a § 4 mom. avsedd kriminell sammanslutnings verksamhet ändras till en hänvisning till den föreslagna nya bestämmelsen i 17 kap. 1 b §, som innehåller en definition av en kriminell sammanslutnings verksamhet.

34 kap. **Om allmänfarliga brott**

9 a §. *Orsakande av fara för informationsbehandling.* En heltäckande kriminalisering av de gärningar som avses i artikel 6 i konventionen förutsätter att tillämpningsområdet för 34 kap. 9 a § i strafflagen utvidgas väsentligt. Av de hjälpmedel vid nätbrott som avses i artikel 6 i konventionen täcker den

gällande 9 a § endast tillverkning och spridning av datavirus och andra motsvarande skadliga program. Den innefattar varken program för dataintrång eller fysiska apparater och inte heller import av program eller apparater. Det föreslås att paragrafen ändras så att den innefattar alla de hjälpmedel och gärningssätt som avses i artikel 6 i konventionen, med undantag av innehav, som kriminaliseras särskilt i den föreslagna nya 9 b §. Till följd av de föreslagna ändringarna måste 9 a § skrivas om i sin helhet. Paragrafrubriken behöver dock inte ändras, eftersom den också efter att ändringarna har gjorts ger en tillräckligt bra beskrivning av regleringens skyddsobjekt och syfte.

Enligt den föreslagna paragrafens 1 a punkt är det straffbart att föra in i landet, tillverka, sälja eller annars sprida eller ställa till förfogande skadliga program och andra motsvarande hjälpmedel vid nätbrott i syfte att orsaka skada.

Den detaljerade förteckningen över gärningssätt i paragrafen motsvarar delvis den förteckning som finns i den gällande 9 a §, och syftet är att den skall täcka förutom tillverkning också alla slag av aktiva åtgärder som innebär att datavirus, tekniska apparater eller program för dataintrång kan användas av andra personer.

Att införsel till landet nämns som ett självständigt gärningssätt är nödvändigt i synnerhet med avseende på apparater. Med tillverkning avses t.ex. att skriva nya program eller ändra redan befintliga program så som avses i paragrafen. Med att sälja avses överlåtelse av ett hjälpmedel mot ersättning och med att ställa till förfogande att t.ex. att sätta ut ett hjälpmedel på internet så att det fritt kan kopieras. Med att ställa till förfogande avses också att skapa länkar från en internetsida till en sida där det skadliga programmet är tillgängligt.

Med spridning avses två olika gärningssätt. För det första avses att ett hjälpmedel t.ex. via e-post överlåts till en eller flera andra personer. När det gäller datavirus avses dessutom också att ett virus används så att det sprids till offrens datorer. Bestämmelserna kan till dessa delar delvis medföra överlappning med t.ex. försök till skadegörelse. I en sådan situation åsidosätts dock inte den föreliggande bestämmelsen trots att den är tänkt att vara sekundär, eftersom straffskalan för skadegörelse är lindrigare.

En och samma gärning kan som helhet uppfylla rekvisitet i den föreslagna paragrafen på flera punkter när det gäller ett hjälpmedel vid nätbrott. Gärningsmannen kan t.ex. både tillverka ett hjälpmedel och ställa det till förfogande eller föra in ett större parti hjälpmedel till landet och sälja dem ett och ett. Det är dock i dessa fall fråga om ett enda brott.

När gärningsmannens syfte med tillverkningen eller införseln av ett hjälpmedel vid nätbrott är att själv använda hjälpmedlet för att begå ett brott som avses i 35 kap. 1 § eller 38 kap. 3—5, 7a eller 8 § i strafflagen, innebär tillämpningen av den föreslagna 9 a § i praktiken en kriminalisering av förberedelse till de nämnda brotten. Den föreslagna bestämmelsen är därför av exceptionell natur. Förberedelse till brott bestraffas i allmänhet inte i det straffrättsliga systemet i Finland.

Om den som säljer eller sprider ett hjälpmedel vid nätbrott vet att någon annan kommer att använda hjälpmedlet i motsvarande syfte, kan det beroende på det aktuella fallet vara fråga om antingen ett sådant brott som avses i den föreslagna 9 a § eller om medhjälp till ett sådant brott som avses i 35 kap. 1 § eller i 38 kap. 3—5, 7a eller 8 § i strafflagen.

Överbegreppet hjälpmedel vid nätbrott används inte i själva paragrafen. Föremålet för spridningen eller någon annan åtgärd individualiseras i punkt a i paragrafen utifrån föremålets tekniska konstruktion och det planerade användningsändamålet. Föremålet för brottet kan enligt bestämmelsen vara apparater, datorprogram eller programinstruktioner som har skapats eller anpassats för att äventyra eller skada informationsbehandling eller ett informations- eller kommunikationssystems funktion eller för att bryta eller avkoda det tekniska skyddet vid elektronisk kommunikation eller skyddet för ett informationssystem. Ett hjälpmedel vid nätbrott kan också ha ett eller flera lovliga användningsändamål. Tillämpningen av bestämmelsen förutsätter inte att hjälpmedlets huvudsakliga användningsändamål är att orsaka olägenhet eller skada för informationsbehandling eller ett in-

formations- eller kommunikationssystems funktion. Det räcker att hjälpmedlet uttryckligen har skapats och tillverkats för att kunna användas även för detta ändamål och att ett sådant användningsändamål i respektive fall också har kunnat bevisas.

Tillämpningsområdet för bestämmelsen är brett när det gäller de hjälpmedel som kommer i fråga. Avsikten är att täcka dels hjälpmedel avsedda för dataintrång och ofog i form av ren skadegörelse, dels fysisk apparatur, datorprogram och fragment av programkoder. Tillämpningsområdet begränsas dock avsevärt av det faktum att det förutsätts att avsikten med gärningen är att orsaka olägenhet eller skada. I praktiken kan det vara synnerligen svårt att bevisa ett sådant syfte. Kriterierna när det gäller såväl ett hjälpmedels egenskaper som syftet med det förfarande som anges i paragrafen skall uppfyllas samtidigt för att gärningen skall vara straffbar enligt bestämmelsen. I det följande behandlas först det kriterium som hänför sig till ett hjälpmedels användningsändamål.

För att paragrafen skall bli tillämplig förutsätts det att hjälpmedlet har skapats eller anpassats för att äventyra eller skada informationsbehandling eller ett informations- eller kommunikationssystems funktion eller för att bryta eller avkoda det tekniska skyddet vid elektronisk kommunikation eller skyddet för ett informationssystem. Det blir fråga om att göra en bedömning av ett hjälpmedels tekniska egenskaper och dess planerade användningsändamål. Att prövningen sker utifrån hjälpmedlet betyder att ett visst hjälpmedel antingen är ett sådant hjälpmedel vid nätbrott som avses i paragrafen eller inte. Man kan inte avgöra saken på olika sätt i olika fall om det är fråga om identiska hjälpmedel. Vid bedömningen av användningsändamålet kan beaktas t.ex. om ett program är tänkt att användas utan offrets vetskap.

Ett hjälpmedel kan betraktas som ett sådant hjälpmedel vid nätbrott som avses i bestämmelsen trots att det kan ha dubbla användningsändamål, dvs. trots att det kan användas såväl i klandervärt som i godtagbart syfte. Det att ett hjälpmedel kan ha också andra än klandervärda användningsändamål utesluter således inte straffbarhet. Det behöver inte vara så att hjälpmedlet enbart lämpar sig som hjälpmedel vid nätbrott. Å andra sidan kan ett helt vanligt hjälpmedel inte betraktas som ett hjälpmedel vid nätbrott enbart för att det kan användas också för klandervärda ändamål. Det avgörande är om hjälpmedlet till sina egenskaper är sådant att det är uppenbart att det har skapats eller anpassats för att användas för ett sådant klandervärt syfte som anges i paragrafen.

Typiskt för i synnerhet de hjälpmedel som används vid dataintrång är att de har sådan dubbel användning som anges ovan. Datavirus och andra motsvarande skadliga program är å andra sidan helt klart avsedda att användas enbart för klandervärda ändamål. I det följande granskas det kriterium som hänför sig till ett hjälpmedels användningsändamål med hjälp av praktiska exempel.

Med hjälp av ett bakdörrsprogram kan en utomstående attackerare använda en annan persons dator. Programmet består av två delar. Serverdelen, dvs. det egentliga bakdörrsprogrammet, laddas in i offrets dator utan dennes vetskap, medan klientdelen med användargränssnittet finns i attackerarens dator. Programmet möjliggör en så gott som obegränsad användning av offrets dator, utan normala användarrättighetskontroller. Dessa program kan dock även användas för godtagbara ändamål. Ett program kan installeras med datorinnehavarens vetskap för att möjliggöra fjärranvändning av en dator. Frågan om ett program eller dess serverdel skall betraktas som ett sådant hjälpmedel vid nätbrott som avses i paragrafen skall avgöras utifrån programmets särdrag. Ett bakdörrsprogram kan i princip anses vara ett hjälpmedel vid nätbrott utifrån användningsändamålet, åtminstone i sådana fall när avsikten är att programmet skall installeras och användas utan offrets vetskap.

Med hjälp av ett spionprogram kan en attackerare följa användningen av en annan persons dator. Om offrets dator är kopplad till ett lokalt nät är det möjligt att med programmets hjälp följa också all okrypterad trafik inom detta. Spionprogrammet installeras i smyg i offrets dator. Därefter fungerar programmet utan att datoranvändaren märker det, och det inregistrerar alla funktioner som datoranvändaren utför på datorn. Programmet lagrar den insamlade informationen och

översänder den till attackeraren. Attackeraren kan alternativt också hämta informationen från offrets dator. Om programmet installeras i smyg är det utan tvekan fråga om ett klandervärt användningsändamål. Om ett spionprogram används helt öppet, t.ex. för att övervaka ett företags arbetstagare när dessa har gett sitt samtycke eller för att följa hur trafiken i ett nät fungerar rent tekniskt, är användningsändamålet godtagbart. Frågan om ett program skall betraktas som ett sådant hjälpmedel vid nätbrott som avses i paragrafen skall avgöras utifrån programmets särdrag. Också ett spionprogram kan i princip i allmänhet anses vara ett sådant hjälpmedel vid nätbrott som avses i paragrafen.

Med ordlisteattack avses en intrångsmetod där man försöker lista ut användarens lösenord genom att använda en omfattande ordlista. Det program som används vid en ordlisteattack för att gissa lösenordet kan användas inte bara för straffbart dataintrång utan också för att testa eller lovligt bryta skyddet för ett system. Även program av denna typ har uppenbart två användningsändamål. Också i dessa fall kan det i princip anses vara fråga om ett hjälpmedel vid nätbrott, eftersom de alternativa användningsändamålen uttryckligen hänför sig till intrång.

Genom s.k. portskanning kan man söka efter säkerhetshål i serverprogram på datorer som kopplats till internet och på detta sätt förbereda dataintrång. Attackeraren försöker inte nödvändigtvis komma in i en bestämd dator utan i vilken oskyddad dator som helst som är tillgänglig. Programmen för portskanning kan dock även användas för godtagbara ändamål, t.ex. portskanning av användarens egen serverdator. Frågan om ett program skall betraktas som ett sådant hjälpmedel vid nätbrott som avses i paragrafen skall avgöras utifrån programmets särdrag. Vid bedömningen skall man ta hänsyn till om den portskanning som programmet utför är avsedd att ske utan offrets vetskap eller med dennes samtycke.

Det finns också olika apparater som kan användas för att göra dataintrång. Bl.a. finns det enheter som registrerar vilka tangenter som trycks ner på ett tangentbord så att informationen senare kan fås ur apparatens minne. Det kan vara fråga om en särskild liten omärkbar apparat som kopplas mellan tangentbordet och centralenheten eller som finns inbyggd i ett specialkonstruerat tangentbord. Apparaten eller tangentbordet installeras i smyg i offrets dator, och den lagrade informationen hämtas senare. Registreringsenheten kan också vara ett program. En väsentlig skillnad mellan apparater och program är att installationen av en apparat förutsätter fysisk tillgång till datorn men inte att skyddet för systemet bryts. Om en apparat har skapats och tillverkats så att den kan användas i smyg är det i allmänhet fråga om ett hjälpmedel vid nätbrott. Om apparaten är tänkt att användas helt öppet för att övervaka arbetstagare eller t.ex. som ett medel för säkerhetskopiering, är användningsändamålet godtagbart. Detta är även fallet om apparaten är skapad för att avslöja olovlig användning av den egna datorn. Apparaterna marknadsförs uttryckligen utifrån det godtagbara användningsändamålet. Frågan om en apparat skall betraktas som ett sådant hjälpmedel vid nätbrott som avses i paragrafen skall avgöras på basis av apparatens särdrag.

Med överbelastningsattack avses att någon avsiktligt blockerar ett informationssystem, t.ex. en e-postserver, eller gör det långsammare. Undantagsvis kan syftet med en överbelastningsattack också vara att lamslå skyddet för det system som är föremål för attacken och därigenom förbereda dataintrång. Tekniskt kan en attack utföras på många olika sätt. Gemensamt för dem alla är att man avsiktligt överbelastar ett system eller systematiskt utnyttjar en teknisk brist, dvs. en sårbarhet, i objektet. Med hjälp av ett program som sänder e-post automatiskt är det t.ex. möjligt att skicka en miljon meddelanden med fingerade avsändaruppgifter till samma server. Om servern inte har skyddats mot sådana attacker kan allvarliga störningar uppstå i dess verksamhet. Det ovan nämnda programmet kan dock användas för helt godtagbara syften, t.ex. för massutskick av e-post för att få fram ett meddelande till flera mottagare. Frågan om ett program skall betraktas som ett sådant hjälpmedel vid nätbrott som avses i paragrafen skall avgöras på basis av programmets särdrag.

Med datavirus avses i allmänspråket ett

program som utan att en datoranvändare vet om det sprider sig från en dator till en annan så att det samtidigt orsakar skador. Virus kan fungera och sprida sig på olika sätt och orsaka olika typer av skador. I branschlitteraturen används olika benämningar för olika typer av virus, såsom makrovirus, e-postvirus och mask. Det finns ingen vedertagen begreppsapparat, men detta saknar betydelse med hänsyn till den nu aktuella bestämmelsen. Syftet med den föreslagna bestämmelsen är att täcka alla slag av datavirus oberoende av hur de fungerar. Bestämmelsen täcker således också skadliga mobiltelefonprogram såsom s.k. mobilvirus, som gör att mobiltelefonen inte fungerar eller annars orsakar störningar i den. Enligt ordalydelsen i bestämmelsen skall föremålet för gärningen ha skapats för att äventyra eller eller skada ett informationssystems funktion. I bestämmelsen nämns för tydlighetens skull att skadan också kan avse informationsbehandling och kommunikationssystem. Den skada eller risk för skada som förutsätts i bestämmelsen kan uppstå på olika sätt beroende på hur viruset fungerar. Viruset kan innehålla en skaderutin så att det t.ex. börjar förstöra filer ett visst datum. Ett virus kan orsaka fel på annat sätt, för eget bruk lägga beslag på resurser i ett informationssystem eller göra systemet långsammare. Ett virus som sprider sig kraftigt orsakar skador redan i sig. Enligt bestämmelsen saknar det sätt på vilket ett virus sprider sig och dess tekniska konstruktion betydelse. Ett virus kan bestå av ett helt program som sprider sig med hjälp av disketter eller sprida sig som programinstruktioner i bifogade filer via e-post. Ett virus kan också ha sådana egenskaper som är typiska för de hjälpmedel som används vid dataintrång. Det kan t.ex. automatiskt sända information till en adress som den som satt viruset i omlopp har bestämt.

När det gäller datavirus motsvarar bestämmelserna den gällande 9 a §. Den nuvarande paragrafen behandlas utförligt också i den regeringsproposition som gäller den (RP 4/1999 rd).

Ett nätbrottsprogram kan gömmas i ett nyttoprogram. En sådan helhet bestående av ett nyttoprogram och ett skadligt program kallas trojansk häst. Syftet med en trojansk häst är att med hjälp av nyttoprogrammet locka offret att själv i sin dator installera det skadliga program som finns gömt i nyttoprogrammet. Om ett hjälpmedel för intrång finns gömt inuti en trojansk häst avslöjar programmets konstruktion i sig dess användningsändamål. T.ex. ett bakdörrs- eller spionprogram som har formen av en trojansk häst har knappast något meningsfullt eller godtagbart användningsändamål. Också när det gäller trojanska hästar skall saken dock alltid avgöras från fall till fall.

Som ett exempel på en situation där prövningen kan vålla problem kan nämnas s.k. profileringsprogram i form av trojanska hästar. Syftet med ett profileringsprogram är att samla information om programmets användare med dennes samtycke. Informationen kan gälla t.ex. vilka internetsidor användaren regelbundet besöker. I utbyte för informationen får användaren gratis i sin användning något nyttoprogram. Den enda skillnaden mellan ett profileringsprogram och ett spionprogram är att profileringsprogrammet ber datoranvändaren om tillstånd före installationen. Om användaren inte ger sitt samtycke installeras inte heller det nyttoprogram som var avsett som belöning. Om användaren av misstag samtycker till installationen påminner verksamheten i hög grad om spionage. Om misstaget helt eller delvis beror på avsiktligt vilseledande handlar det i praktiken om spionage.

Enligt 2 punkten i den föreslagna paragrafen är det straffbart att sprida eller ställa till förfogande anvisningar för tillverkning av datorprogram eller programinstruktioner i syfte att orsaka skada. Bestämmelsen gäller således inte anvisningar för tillverkning av fysisk utrustning.

Med anvisningar avses i paragrafen anvisningar som är tillräckligt detaljerade för att en person som har elementära kunskaper i databehandling utifrån dem kan tillverka t.ex. ett datavirus eller något annat skadligt program. Att sprida sådana anvisningar är åtminstone när det gäller virus lika farligt som att sprida färdiga virus, och ett likadant straffhot bör därför gälla för gärningen. För konsekvensens skull gäller bestämmelsen anvisningar för tillverkning av även andra program än virus. Eftersom en anvisning inte

kan spridas av sig själv på samma sätt som ett färdigt program, orsakar enbart tillverkningen av en anvisning i sig inte sådan fara att det skulle vara skäl att kriminalisera även tillverkning. Virus kan spridas endast med hjälp av datateknik. En anvisning kan däremot spridas också i skriftlig form.

I 1 b-punkten i den föreslagna paragrafen föreskrivs om straff för den som för in i landet, tillverkar, säljer, sprider eller ställer till förfogande andra personers lösenord eller åtkomstkoder eller någon annan motsvarande information om ett informationssystem. Paragrafen är uppbyggd så att förteckningen över gärningssätt är gemensam med 1 a-punkten. Enligt ordalydelsen innefattar paragrafen därför också tillverkning av andra personers lösenord, vilket dock inte torde vara möjligt i praktiken. Enligt förslaget är det inte straffbart att sprida egna lösenord, åtkomstkoder eller motsvarande information. Det är inte heller straffbart att sprida en annan persons lösenord, åtkomstkod eller motsvarande information, om personen i fråga har gett sitt samtycke till det och syftet inte är att orsaka skada så som anges i paragrafen. I praktiken är det också vanligt att man använder andra personers åtkomstkoder och lösenord med deras samtycke.

Med åtkomstkod (access code) avses i paragrafen ett kodnummer eller någon annan kod som används bl.a. i bankautomater och i telefonnätet. Åtkomstkoden är delvis densamma som lösenordet, varmed avses en identifierare med vars hjälp ett informationssystem autentiserar en användare. Ett lösenord och en åtkomstkod består i allmänhet av bokstäver, siffror eller specialtecken.

Begreppet annan information som nämns i paragrafen kan vara t.ex. en användaridentifikation. Användaridentifikationen ger systemet information om vem användaren är, och användaren bevisar sin identitet genom att visa att han eller hon känner till lösenordet. Denna metod används allmänt för att skydda informationssystem mot olovlig användning eftersom den är enkel och billig. Om en utomstående får tillgång till de identifierare som används för att skydda ett system förlorar skyddet sin betydelse. Syftet med den föreslagna bestämmelsen är att förhindra olovlig användning av identifierare genom att göra det straffbart att sprida dem och ställa dem till förfogande i syfte att orsaka skada. Redan ett innehav av identifierare i detta syfte är straffbart med stöd av 9 b §, som behandlas nedan.

I en del system är användaridentifikationen offentlig eller annars sådan att en utomstående lätt kan gissa sig till den. Den kan t.ex. bestå av en del av användarens e-postadress. Det är också förbjudet att sprida och ställa till förfogande dylika offentliga användaridentifikationer i syfte att orsaka skada eller olägenhet. Gärningen kan fullbordas t.ex. när någon samlar in och sammanställer uppgifter om användaridentifikationer från olika offentliga källor och sprider dem i den avsikten att uppgifterna senare skall användas för att begå nätbrott.

Ett lösenord och en användaridentifikation har i allmänhet relevans endast när de förekommer tillsammans och används i ett visst informationssystem. Ett enskilt lösenord utan information om användaridentifikationen eller användaren har inte nödvändigtvis samma betydelse. Eftersom en användaridentifikation så som sagts ovan kan vara offentlig eller i varje fall vara lätt att lista ut, kan redan det att man känner till någon annans lösenord underlätta obehörigt tillträde till ett informationssystem. Eftersom samma personliga lösenord ofta används i olika system kan ett lösenord också ha verkningar som utsträcker sig till flera olika informationssystem. Därför är det också straffbart att i syfte att orsaka olägenhet eller skada sprida redan ett lösenord som tillhör någon annan.

Den identifierare som avses i paragrafen kan dock också bestå av annan information som motsvarar ett lösenord, en åtkomstkod eller en användaridentifikation. Bestämmelsens tillämpningsområde är således oberoende av identifierarens tekniska form samt informationens art och i vilken form den ges. Det enda väsentliga är att den är tänkt att användas som ett lösenord. Det är fråga om sådan information som avses i paragrafen endast om syftet med informationen är autentisering av en person för att få tillträde till ett informationssystem. Också t.ex. ett fingeravtryck eller någon annan biometrisk identifierare i form av data kan vara ett lösenord eller en åtkomstkod.

Med informationssystem avses i paragrafen alla sådana system som behandlar information i form av data. Till dessa delar är tillämpningsområdet brett. T.ex. ett bankautomatkorts åtkomstkod eller lösenord är helt klart sådan information som avses i paragrafen, eftersom den möjliggör användning av en banks informationssystem för banktjänster. Också ett kreditkortsnummer kan vara sådan information som avses i paragrafen, eftersom användningsändamålet även kan ha samband med ett informationssystem. Inom konsumenthandeln kan ett kreditkortsnummer i olika betalningssituationer till sin betydelse jämställas med en användaridentifikation. Trots att betalningen i princip förutsätter innehav av kortet är det tekniskt möjligt att sköta betalningen (t.ex. vid en servicestations kassaterminal) om man känner till kortets nummer och den eventuella koden. Missbruk av ett kreditkortsnummer kan även vara straffbart som betalningsmedelsbedrägeri eller grovt betalningsmedelsbedrägeri enligt 37 kap. 8 och 9 § i strafflagen.

De föreslagna bestämmelserna om lösenord och motsvarande information motsvarar artikel 6.1 a ii i konventionen.

Enligt den föreslagna paragrafen skall spridningen av ett hjälpmedel vid nätbrott eller ett lösenord eller någon annan åtgärd ske i syfte att orsaka olägenhet eller skada för informationsbehandling eller för ett informations- eller kommunikationssystems funktion eller säkerhet. En gärning är inte straffbar om syftet inte är att orsaka skada, även om det hjälpmedel som är föremål för gärningen uppfyller kriterierna för ett hjälpmedel vid nätbrott.

Med skada avses t.ex. att data ändras eller försvinner. Med olägenhet avses t.ex. att ett informationssystem blir långsammare eller att systemets resurser försvagas på något annat sätt. För tydlighetens skull nämns i paragrafen förutom informationssystem också informationsbehandling och kommunikationssystem samt deras säkerhet som potentiella skadeobjekt.

I praktiken används hjälpmedel vid nätbrott allmänt utan att syftet är att orsaka skada. Datasäkerheten är en betydande kommersiell bransch. Planeringen av informationssystem och skydd för sådana kräver kunskap om hur virus och hjälpmedel för dataintrång är konstruerade och hur de fungerar. Hjälpmedel vid nätbrott används för att testa system och program. Förutom dataskyddsföretagen använder också försvarsmakten dessa hjälpmedel i utredningar som gäller IT-krigföring. Också polisen använder hjälpmedlen för att utveckla sina egna metoder. Likaså finns det även inom den vetenskapliga forskningen och undervisningen ett behov av kunskap om dessa hjälpmedel. Därför är det klart att inte heller tillverkning, införsel till landet eller överlåtelse av hjälpmedel eller sådant innehav av hjälpmedel som kriminaliseras i 9 b § i ett ovan nämnt syfte är straffbart enligt de föreslagna paragraferna. T.ex. vid försäljning av utrustning eller program uppfylls rekvisitet om säljaren vet eller kan dra den slutsatsen att köparen kommer att använda utrustningen eller programmet för att begå nätbrott.

Det saknar betydelse vem som har tillverkat eller överlåtit hjälpmedlen. En privatperson som har datorer som hobby kan utan risk för straff tillverka ett virus, om syftet endast är att utveckla den egna programmeringsförmågan. Om viruset tillverkas i syfte att sprida det för kriminellt bruk uppfylls rekvisitet för brott. Det står klart att det i praktiken kan vara förenat med stora bevissvårigheter att utreda vilket syftet med en gärning har varit.

Orsakande av fara för informationsbehandling är straffbart endast om gärningen begås uppsåtligen. I paragrafen förutsätts avsiktsuppsåt när det gäller orsakandet av olägenhet eller skada och till övriga delar s.k. omständighetsuppsåt. På basis av bestämmelsen om rekvisitvillfarelse i strafflagens 4 kap. 1 §, som trädde i kraft vid ingången av 2004, avgörs omständighetsuppsåtet genom rättspraxis. Med omständighetsuppsåt hänvisas till andra element i rekvisitet än följden, t.ex. huruvida gärningsmannen har varit medveten om att hjälpmedlet i fråga uppfyller kriterierna för ett hjälpmedel vid nätbrott eller inte. Uppsåtet skall omfatta alla elementen i rekvisitet.

Som ett exempel på en situation där prövningen innefattar en bedömning av uppsåtet och av hur klandervärt syftet med gärningen har varit kan nämnas ett sådant fall där en

skadlig kod har offentliggjorts i påtryckningssyfte. Typiskt för nätbrotten är att man utnyttjar säkerhetshål i ett informationssystem. Om t.ex. ett kommersiellt serverprogram visar sig innehålla ett sådant säkerhetshål måste tillverkaren av programmet åtgärda det. Med hänsyn till datasäkerheten är det givetvis viktigt att de verktyg som behövs för att lappa säkerhetshålet kan fås till användarna så snabbt som möjligt. En dataamatör som har hittat ett säkerhetshål i ett program kan offentliggöra saken enbart i syfte att utöva påtryckning på programtillverkaren så att denne agerar snabbare. Att offentliggöra en programkod som gör det möjligt att utnyttja säkerhetshålet är att gå ett steg längre i påtryckningsåtgärderna. Offentliggörandet uppfyller i sig ännu inte rekvisitet för brott, om inte den information som offentliggörs är så detaljerad att gärningen undantagsvis kan betraktas som sådan spridning av tillverkningsanvisningar som avses i punkt 2 i paragrafen. Däremot är det klart att de element i rekvisitet som gäller gärningssättet och hjälpmedlet uppfylls om man offentliggör en skadlig kod. Rekvisitet uppfylls dock inte till den del det gäller syftet att orsaka olägenhet eller skada, om koden sänds t.ex. till Kommunikationsverkets CERT-enhet (Computer Emergency Response Team), till vars uppgifter det uttryckligen hör att upptäcka och avvärja hot mot datasäkerheten.

Straffskalan föreslås vara böter eller fängelse i högst två år. Denna skala ger domstolarna tillräckligt med spelrum. De gärningar som avses i paragrafen kan skilja sig avsevärt från varandra när det gäller den skada de orsakar. Den föreslagna straffskalan innebär också att förundersökningsmyndigheterna kan använda behövliga tvångsmedel.

Paragrafen tillämpas inte om strängare eller lika strängt straff föreskrivs för gärningen någon annanstans i lag. Att bestämmelsen är sekundär är i praktiken viktigt i synnerhet med tanke på datavirusen. Om ett virus som spridits har aktiverats och orsakat olägenhet eller skada, kan t.ex. bestämmelserna om störande av post- och teletrafik, systemstörning eller grov skadegörelse tillämpas på gärningen, beroende på om den som tillverkat eller spridit viruset har handlat uppsåtligt eller inte. Också rekvisitet för vanlig skadegörelse åsidosätter den föreslagna bestämmelsen, eftersom det föreslagna maximistraffet för brottet, dvs. fängelse i två år, är detsamma som enligt den föreslagna paragrafen.

Enligt 38 kap. 8 a § i strafflagen är det straffbart att i förtjänstsyfte tillverka eller distribuera ett system för avkodning av det tekniska skyddet för avgiftsbelagda TV-sändningar eller andra motsvarande innehållstjänster. Bestämmelsen överlappar delvis den föreslagna bestämmelsen. Eftersom maximistraffet enligt 38 kap. 8 a § är lägre vad som föreskrivs i 9 a §, åsidosätts den förstnämnda paragrafen om gärningen uppfyller bägge rekvisiten.

Bestämmelsen överlappar också delvis förbudet enligt 6 § i lagen om dataskydd vid elektronisk kommunikation, för vilket enligt lagens 42 § kan dömas till bötesstraff, om inte strängare straff föreskrivs någon annanstans i lag. Enligt det förstnämnda lagrummet är innehav, import, tillverkning och distribution av system för avkodning av det tekniska skyddet vid elektronisk kommunikation eller av en del av ett sådant system förbjudet, om det primära ändamålet med systemet eller dess del är obehörig avkodning av det tekniska skyddet. Kommunikationsverket kan av godtagbara skäl bevilja tillstånd att avvika från detta förbud. Om syftet med gärningen är att orsaka olägenhet eller skada åsidosätter bestämmelsen om orsakande av fara för informationsbehandling i strafflagen den gärning som avses i den nämnda 6 §, eftersom bestämmelsen i strafflagen kan tillämpas oberoende av vilket det primära ändamålet med systemet är. Om syftet däremot inte är att orsaka olägenhet eller skada, är gärningen straffbar endast med stöd av lagen om dataskydd vid elektronisk kommunikation, och då under förutsättning att det primära ändamålet med systemet är obehörig avkodning av det tekniska skyddet. På samma sätt avgörs också förhållandet mellan bestämmelsen i strafflagen och bestämmelsen om olovlig spridning av anordning för avlägsnande av skydd för datorprogram, som kriminaliseras i 56 c § i upphovsrättslagen. Enligt den nämnda paragrafen är det straffbart att till allmänheten sprida eller för spridning till allmänheten i förvärvssyfte inneha en anordning vars enda syfte är att olovligt avlägsna eller

kringgå ett tekniskt hjälpmedel som skyddar datorprogram. Brottsbeteckningen och bestämmelsen har ändrats så att de har denna lydelse genom lagen 821/2005, som trädde i kraft den 1 januari 2006.

I och med de föreslagna ändringarna i 9 a § uppfyller lagstiftningen kraven enligt artikel 6 i konventionen.

9 b §. *Innehav av hjälpmedel vid nätbrott.* Det föreslås att till kapitlet fogas en ny 9 b §, där det föreskrivs om innehav av hjälpmedel vid nätbrott. Enligt den föreslagna paragrafen skall den dömas för innehav av hjälpmedel vid nätbrott som för att orsaka olägenhet eller skada för informationsbehandling eller ett informations- eller kommunikationssystems funktion eller säkerhet innehar sådana apparater, datorprogram eller programinstruktioner som avses i 9 a § 1 a-punkten eller sådana lösenord, åtkomstkoder eller andra motsvarande uppgifter som avses i 9 a § 1 b-punkten. Bestämmelsen gäller således inte innehav av sådana anvisningar för tillverkning av datorprogram eller programinstruktioner som avses i 9 a § 2 punkten. Enbart ett innehav av dylika anvisningar orsakar inte i sig sådan fara att det vore skäl att kriminalisera även den gärningen.

Det föreslås att de hjälpmedel vid nätbrott som kommer i fråga individualiseras genom en hänvisning till 9 a §. På samma sätt som när det gäller 9 a § förutsätts det för att innehavet skall utgöra brott att syftet är att orsaka skada. Rekvisitet behandlas i bägge fallen i motiveringen till den nämnda paragrafen.

Det förutsätts inte nödvändigtvis ett direkt fysiskt innehav för att det skall vara fråga om sådant innehav som avses i den föreslagna paragrafen (HD 2001:91). Rekvisitet kan uppfyllas redan när en person uppenbart har tillgång till och förfogar över ett hjälpmedel eller program, även om detta fysiskt finns någon annanstans. Bestämmelsen gäller således bl.a. sådana situationer när en nätbrottsling utan någons vetskap förvarar program som skall betraktas som nätbrottshjälpmedel exempelvis på minnesområdet i ett företags eller ämbetsverks centraldator eller server.

När ett i sig straffbart innehav av ett föremål har samband med begåendet av ett ännu allvarligare brott har den skyldige i rättspraxis i allmänhet inte tillräknats innehavet särskilt. T.ex. i fallet HD 1980 II 10 tillräknades en person som försökt begå dråp med ett eggvapen inte innehav av vapen på allmän plats. Enligt samma princip skall innehav av ett hjälpmedel vid nätbrott i allmänhet inte betraktas som ett särskilt brott, om innehavaren vid användningen av hjälpmedlet antingen själv har gjort sig skyldig till eller har varit delaktig i något annat brott som bestraffas hårdare.

Straffskalan föreslås vara böter eller fängelse i högst sex månader. Enbart ett innehav av ett hjälpmedel vid nätbrott orsakar inte lika stor fara som t.ex. ett aktivt spridande av motsvarande hjälpmedel. Därför är maximistraffet lindrigare än det som föreslås i 9 a §. Det föreslagna maximistraffet är också lägre än det föreskrivna maximistraffet för försök till dataintrång, vilket motsvarar klandervärdheten hos dessa gärningar.

På samma sätt som 9 a § överlappar den föreslagna bestämmelsen delvis 42 § i lagen om dataskydd vid elektronisk kommunikation. Den sistnämnda bestämmelsen täcker även innehav av system för avkodning av det tekniska skyddet vid elektronisk kommunikation eller av en del av ett sådant system. I fråga om förhållandet mellan dessa bestämmelser och 56 c § i upphovsrättslagen gäller vad som sagts ovan i motiveringen till 9 a §. Obehörigt innehav av ett system för avkodning av det tekniska skyddet för avgiftsbelagda TV-sändningar eller andra motsvarande innehållstjänster kriminaliseras i 6 § 2 mom. i lagen om förbud mot vissa avkodningssystem (1117/2001). Det föreskrivna straffet för gärningen är böter, och eftersom bestämmelsen i den nämnda lagen är sekundär åsidosätts den om gärningen uppfyller rekvisitet både i den och i den föreslagna 9 b §.

I och med den föreslagna paragrafen uppfyller lagstiftningen kraven i artikel 6.1 b i konventionen. Dessutom täcker paragrafen artikel 6.1 a till den del den gäller anskaffning av hjälpmedel vid nätbrott utan att hjälpmedlet samtidigt sprids eller görs tillgängligt. I praktiken täcker straffbarheten för innehav också anskaffning, eftersom hjälpmedlet till följd av anskaffningen alltid också kommer i den persons besittning som har gjort anskaffningen.

13 §. *Straffansvar för juridiska personer.* Paragrafen föreslås bli ändrad så att på orsakande av fara för informationsbehandling tillämpas vad som föreskrivs om straffansvar för juridiska personer. I och med bestämmelsen uppfyller lagstiftningen kraven i artikel 12 i konventionen och artikel 8 i rambeslutet när det gäller detta brott. I det avsnitt som innehåller motiveringen till konventionen och godkännandet av den samt i det avsnitt som hänför sig till det nationella genomförandet av rambeslutet redogörs mera allmänt för hur bestämmelserna förhåller sig till artikel 12 i konventionen och artikel 8 i rambeslutet. I riksdagen behandlas även i samband med regeringens proposition 52/2005 rd ett förslag till ändring av den föreliggande paragrafen. Vid riksdagsbehandlingen bör förslaget samordnas med den ändring som föreslås här (se avsnitt 6. Andra omständigheter som inverkat på propositionens innehåll).

35 kap. **Om skadegörelse**

1 §. *Skadegörelse.* Det föreslås att 1 mom. ändras så att maximistraffet för skadegörelse höjs från nuvarande ett till två års fängelse. I och med bestämmelsen uppfyller lagstiftningen kraven i artikel 7 i rambeslutet.

Enligt artikel 7 i rambeslutet skall det föreskrivas om ett maximistraff på minst två års fängelse för orsakande av skada på datorbehandlingsbara uppgifter, om brottet har begåtts inom ramen för en sådan kriminell organisation som avses i artikeln. När det gäller skadegörelse som riktar sig mot information uppfyller lagstiftningen inte kraven enligt artikeln. Maximistraffet för en gärning enligt grundrekvisitet är fängelse i ett år. Maximistraffet för den grova gärningsformen är visserligen fängelse i fyra år, men i den uttömmande förteckningen över straffskärpningsgrunderna nämns inte den omständigheten att brottet begås som ett led i en kriminell organisations verksamhet.

Det föreslås att det krav som gäller straffskalan i artikel 7 i rambeslutet uppfylls genom att maximistraffet för skadegörelse höjs till fängelse i två år. Den höjda straffskalan gäller givetvis också skadegörelse som begåtts inom ramen för en kriminell organisations verksamhet. Genom den föreslagna ändringen korrigeras också en inkonsekvens i den gällande lagen, dvs. att maximistraffet för dataintrång, som kriminaliseras i 38 kap. 8 § i strafflagen, och maximistraffet för skadegörelse som riktar sig mot information, som kriminaliseras i den föreliggande paragrafens 2 mom., i dag är detsamma, trots att dataintrång inte förutsätter att informationen i ett system skadas. Efter den föreslagna höjningen av maximistraffet åsidosätter bestämmelsen om skadegörelse som riktar sig mot information den sekundära bestämmelsen om dataintrång i de fall när det vid dataintrånget också har förekommit skadegörelse som riktar sig mot information.

För konsekvensens skull föreslås det också att maximistraffet för sådan skadegörelse som avses i paragrafens 1 mom. höjs till fängelse i två år. I annat fall skulle olika straffskalor tillämpas på orsakande av skada på data beroende på om gärningen riktar sig uteslutande mot data eller om den också riktar sig mot lagringsplattformen, dvs. ett datamedium som föremål. I det förstnämnda fallet skulle maximistraffet enligt förslaget vara fängelse i två år men i det sistnämnda fallet enligt paragrafens 1 mom. fängelse i endast ett år, trots att den skada som orsakats de facto kan vara större.

Det föreslås dessutom att paragrafen ändras så att till den fogas ett nytt 3 mom., där det sägs att försök till skadegörelse är straffbart. Artikel 11.2 i konventionen förpliktar till att straffbelägga försök till skadegörelse som riktar sig mot information. Det är dock inte motiverat att straffbelägga endast försök till skadegörelse som riktar sig mot information men inte skadegörelse som riktar sig mot föremål. Därför föreslås det att kriminaliseringen av försök till skadegörelse skall omfatta både paragrafens 1 och 2 mom. I det avsnitt som innehåller motiveringen till konventionen och godkännandet av den redogörs mer allmänt för hur bestämmelserna förhåller sig till artikel 11 i konventionen. Försök till grov skadegörelse är straffbart redan i dag.

8 §. *Straffansvar för juridiska personer.* Enligt den föreslagna nya paragrafen skall på skadegörelse som avses i kapitlets 1 § 2 mom. och på grov skadegörelse som avses i kapitlets 2 §, när den har skett på det sätt som avses i 1 § 2 mom., tillämpas vad som före-

skrivs om straffansvar för juridiska personer. Bestämmelsen gäller således endast grundformen och den grova gärningsformen av skadegörelse som riktar sig mot information. I och med bestämmelsen uppfyller lagstiftningen kraven i artikel 12 i konventionen och artikel 8 i rambeslutet när det gäller dessa brott. I det avsnitt som innehåller motiveringen till konventionen och godkännandet av den samt till de nämnda artiklarna i rambeslutet redogörs mera allmänt för hur bestämmelserna förhåller sig till artikel 12 i konventionen och till artiklarna 8 och 9 i rambeslutet.

38 kap. **Om informations- och kommunikationsbrott**

5 §. *Störande av post- och teletrafik.* Det föreslås att till paragrafen fogas ett nytt 2 mom., enligt vilket försök till störande av post- och teletrafik är straffbart. I och med bestämmelsen uppfyller lagstiftningen kraven enligt artikel 11.2 i konventionen och artikel 5.2 i rambeslutet när det gäller detta brott. I det avsnitt som innehåller motiveringen till konventionen och rambeslutet samt till godkännandet av dem redogörs mera allmänt för hur bestämmelserna förhåller sig till artikel 11 i konventionen och till artikel 5.2 i rambeslutet.

6 §. *Grovt störande av post- och teletrafik.* Det föreslås att till paragrafen fogas ett nytt 2 mom., enligt vilket försök till grovt störande av post- och teletrafik är straffbart. I och med bestämmelsen uppfyller lagstiftningen kraven enligt artikel 11.2 i konventionen och artikel 5.2 i rambeslutet när det gäller detta brott. I det avsnitt som innehåller motiveringen till konventionen och rambeslutet samt till godkännandet av dem redogörs mera allmänt för hur bestämmelserna förhåller sig till artikel 11 i konventionen och till artikel 5 i rambeslutet.

7 §. *Lindrigt störande av post- och teletrafik.* Det föreslås att till paragrafen fogas ett nytt 2 mom., enligt vilket försök till lindrigt störande av post- och teletrafik är straffbart. I och med bestämmelsen uppfyller lagstiftningen kraven enligt artikel 11.2 i konventionen och artikel 5.2 i rambeslutet när det gäller detta brott. I det avsnitt som innehåller motiveringen till konventionen och rambeslutet samt till godkännandet av dem redogörs mera allmänt för hur bestämmelserna förhåller sig till artikel 11 i konventionen och till artikel 5 i rambeslutet.

7 a §. *Systemstörning.* Det föreslås att till kapitlet fogas en ny paragraf där det föreskrivs om systemstörning. Enligt paragrafen skall den dömas för systemstörning som i syfte att orsaka en annan person olägenhet eller ekonomisk skada matar in, överför, skadar, ändrar eller undertrycker data eller på något annat med dessa jämförbart sätt obehörigen hindrar ett informationssystems funktion eller orsakar allvarliga störningar i det. Paragrafen tillämpas endast om inte strängare eller lika strängt straff föreskrivs för gärningen någon annanstans i lag.

I och med bestämmelsen uppfyller lagstiftningen kraven i konventionen när det gäller bestämmelserna om systemstörning i artikel 5 och kraven i rambeslutet när det gäller bestämmelserna om olaglig systemstörning i artikel 3. Av punkterna 65 och 67 i den förklarande rapporten till konventionen framgår att syftet med den nämnda artikeln är att skydda i synnerhet kommunikationssystem mot virus- och överbelastningsattacker. Med överbelastningsattack avses bl.a. avsiktlig överbelastning av det informationssystem som är föremål för attacken, t.ex. en e-postserver, i syfte att hindra dess funktion eller orsaka olägenheter för det.

Den föreslagna paragrafen har ett nära samband med brottet störande av post- och teletrafik. Grundrekvisitet för detta brott finns i 5 § i detta kapitel. För störande av post- och teletrafik döms bl.a. den som genom att ingripa i en för tele- eller radiokommunikationer använd anordnings funktion eller på något annat motsvarande sätt obehörigen hindrar eller stör tele- eller radiokommunikationer. I det avsnitt som innehåller motiveringen till konventionen och godkännandet av den redogörs också för hur bestämmelsen om störande av post- och teletrafik förhåller sig till artikel 5 i konventionen.

Vid störande av post- och teletrafik riktar sig gärningen mot kommunikation, även elektronisk kommunikation som sker genom förmedling av informationssystem. I den föreslagna bestämmelsen om systemstörning

riktar sig gärningen mot ett informationssystem, även informationssystem som förmedlar elektroniska meddelanden.

Eftersom den föreslagna paragrafen är sekundär kommer den i praktiken sannolikt inte att behöva tillämpas särskilt ofta. Om den gärning som avses i paragrafen riktar sig mot elektronisk kommunikation, skall bestämmelserna om störande av post- och teletrafik tillämpas i stället för den föreslagna paragrafen. Som ett typexempel på en gärning som bestämmelsen om störande av post- och teletrafik skall tillämpas på kan nämnas en överbelastningsattack som riktar sig mot en e-postserver eller en server som förmedlar internetsidor.

Den föreslagna nya bestämmelsen är dock nödvändig eftersom de ovan nämnda artiklarna 5 och 3 gäller alla slag av systemstörningar, även sådana som riktar sig mot enskilda datorer och sådana som inte ens indirekt har att göra med överföring av meddelanden. Bestämmelserna om störande av post- och teletrafik täcker således artiklarnas kärnområde och de föreslagna bestämmelserna om systemstörning resten.

Gärningsförteckningen i paragrafen är tänkt att vara så heltäckande som möjligt. Eftersom den tekniska utvecklingen kan leda till att det uppstår nya gärningssätt som man inte i dag kan förutspå har förteckningen dock avsiktligt lämnats öppen. Också andra gärningssätt än de som nämns i paragrafen kan således komma i fråga, om de kan jämföras med dessa. Gemensamt för gärningssätten är att störningen orsakas genom att man använder utomstående data eller genom att man ingriper i innehållet i data som redan finns i systemet. Med data avses här för det första detsamma som i det föreslagna nya 2 mom. i tvångsmedelslagens 4 kap. 1 §, dvs. information som finns i en dator eller något annat motsvarande informationssystem eller på dess lagringsplattform, men dessutom också information som kan matas in i datorn eller systemet eller på lagringsplattformen. Begreppet data behandlas närmare i motiveringen till den nämnda paragrafen.

Med att mata in data avses i paragrafen en attack som orsakar en funktionsstörning i systemet. De data som finns i systemet skadas dock inte på något sätt. Orsaken till funktionsstörningen kan vara en avsiktlig överbelastning eller t.ex. inmatning av data som har sådana egenskaper att de orsakar störningar. Attacken riktar sig således inte mot de data som finns i systemet utan mot systemets funktion.

När det gäller de gärningstyper som innebär att direkt skada eller ändra de data som finns i det angripna systemet motsvarar bestämmelsen ordalydelsen i konventionen. I praktiken har skillnaderna mellan att överföra, skada, ändra och undertrycka data liten betydelse, eftersom redan ändring av en enda bit beroende på det sätt på vilket systemen fungerar i avgörande grad kan påverka hela systemets funktion. För att bestämmelsen skall vara heltäckande förtecknas dock alla gärningstyperna i paragrafen. Ett typexempel på ett gärningssätt av ovan nämnt slag är en attack som genomförs med hjälp av ett datavirus som förstör eller ändrar data eller något annat motsvarande hjälpmedel. Om det attackerade systemets funktion inte hänför sig till överföring av meddelanden blir inte heller de ovan nämnda bestämmelserna om störande av post- och teletrafik tillämpliga. Gärningssättet något annat med dessa jämförbart sätt i den föreslagna bestämmelsen innefattar också att göra det omöjligt att komma åt datorbehandlingsbara uppgifter, som nämns i artikel 3 i rambeslutet.

I paragrafen förutsätts att gärningen är obehörig och begås uppsåtligen i syfte att orsaka olägenhet eller skada samt att ett informationssystems funktion förhindras helt och hållet eller orsakas allvarliga störningar till följd av den. Med allvarliga störningar avses att systemet blir väsentligt långsammare eller att dess funktionssäkerhet blir väsentligt sämre så att systemet inte längre kan användas för sitt normala användningsändamål.

För att en gärning skall vara straffbar som systemstörning förutsätts det att gärningsmannen inte har laglig rätt att företa den. En gärning kan vara behörig t.ex. om den som begår gärningen har fått samtycke till det.

Straffskalan föreslås vara böter eller fängelse i högst två år, vilket motsvarar den i 5 § i detta kapitel föreskrivna skalan för störande av post- och teletrafik.

Bestämmelsen om störande av post- och teletrafik är sekundär och skall tillämpas om

inte strängare eller lika strängt straff föreskrivs för gärningen någon annanstans i lag. Gärningssättet att skada data kan innebära att gärningen samtidigt uppfyller det i 35 kap. 1 § 2 mom. i strafflagen föreskrivna rekvisitet för skadegörelse som riktar sig mot information. I dessa situationer åsidosätts bestämmelsen om störande av post- och teletrafik, eftersom det föreslås ett lika strängt straff för skadegörelse som riktar sig mot information, dvs. fängelse i två år. Bestämmelsen om skadegörelse kan också tillämpas om gärningen inte orsakar störningar så som förutsätts i bestämmelserna om störande av post- och teletrafik och systemstörning.

Enligt paragrafens 2 mom. är också försök till systemstörning straffbart.

7 b §. *Grov systemstörning.* I paragrafen finns en bestämmelse om den grova gärningsformen av systemstörning. Enligt paragrafen skall en gärning betraktas som grov om den vållar synnerligen kännbar olägenhet eller ekonomisk skada eller om den begås särskilt planmässigt. Dessutom skall gärningen vara grov även bedömd som en helhet.

Med synnerligen kännbar ekonomisk skada avses här främst sådana följder för systeminnehavaren som kan mätas i pengar. Förutom direkta anskaffnings-, reparations- och servicekostnader kan ekonomisk skada uppstå t.ex. om offrets system har skadats så att denne tvingas använda ett annat system. Det kan också vara fråga om skador i form av inkomstförluster.

Med synnerligen kännbar olägenhet avses för sin del andra skadeverkningar än sådana som kan mätas i pengar. Om systemet inte går att använda eller om användningen försvåras uppstår det olägenheter, trots att det inte är fråga om direkta ekonomiska skador. Ju längre olägenheten varar desto allvarligare skall den anses vara. Ingen klar gräns kan dras mellan olägenhet och skada, utan de överlappar delvis varandra. Eftersom båda nämns i bestämmelsen saknar gränsdragningen betydelse i praktiken.

Särskild planmässighet kan t.ex. ta sig uttryck i att exceptionellt omfattande och invecklade förberedelser har gjorts eller invecklade åtgärder har vidtagits på förhand i vilseledande syfte för att förhindra att gärningen uppdagas eller för att dölja vinningen av brottet. Specialarrangemang som möjliggör bevisförvanskning eller hindrar att den avslöjas samt organisering som bygger på arbetsfördelning mellan flera personer kan också vara ett uttryck för särskild planmässighet. Som exempel på särskild planmässighet kan nämnas de s.k. distribuerade överbelastningsattackerna. Vid en distribuerad överbelastningsattack laddas det program som används för attacken först in i offrens datorer, varefter attackprogrammen i de olika delarna av nätet aktiveras samtidigt så att de utför den egentliga attacken i ett på förhand bestämt objekt. De distribuerade attackerna är inte bara svåra att skydda sig mot utan de utsätter också de mellanhänder som oavsiktligt deltar i attacken för obefogade brottsmisstankar.

Eftersom den föreslagna paragrafen är sekundär kommer den sannolikt inte att behöva tillämpas särskilt ofta i praktiken. Om den gärning som avses i paragrafen riktar sig mot elektronisk kommunikation, skall bestämmelsen om grovt störande av post- och teletrafik tillämpas i stället för den föreslagna paragrafen.

Straffskalan föreslås vara fängelse i minst fyra månader och högst fyra år, vilket motsvarar den i 6 § i samma kapitel föreskrivna skalan för grovt störande av post- och teletrafik.

Enligt paragrafens 2 mom. är också försök till grov systemstörning straffbart.

8 a §. *Grovt dataintrång.* Det föreslås att till kapitlet fogas en bestämmelse om en grov gärningsform av dataintrång. Enligt 1 mom. skall gärningen betraktas som grov om den begås som ett led i en i 17 kap. 1 b § avsedd organiserad kriminell sammanslutnings verksamhet eller om den begås särskilt planmässigt. Dessutom skall gärningen vara grov även bedömd som en helhet.

I momentets 1 punkt hänvisas till definitionen av organiserad kriminell sammanslutning. Både i den gällande 17 kap. 1 a § och i den föreslagna 17 kap. 1 b § avses med organiserad kriminell sammanslutning en strukturerad sammanslutning, inrättad för en viss tid, bestående av minst tre personer, som handlar i samförstånd för att begå brott.

Innehållet i definitionen behandlas närmare

i de ursprungliga förarbetena till definitionsbestämmelsen (RP 183/1999 rd). Enligt förarbetena till lagen är det omöjligt att på förhand ge det krav på varaktighet som ingår i definitionen ett exakt innehåll. Det är ganska klart att inte ens en verksamhet som pågår i några veckor ännu är varaktig på det sätt som avses i definitionen. Om organisationens verksamhet har pågått i minst ett år är det däremot klart att kravet på varaktighet uppfylls. I fråga om verksamhet som pågått längre än några veckor men mindre än ett år blir man tvungen att från fall till fall avgöra frågan om verksamheten skall anses varaktig.

Sammanslutningen skall också vara organiserad. Minimikravet är att sammanslutningen har någon form av hierarki och arbetsfördelning. För att en sammanslutning skall kunna betraktas som en sådan kriminell organisation som avses i momentet skall den ha en klar ledning, och ledningen skall ha rätt att befalla över dem som befinner sig lägre ner i organisationen. Att organisationen är organiserad innebär också att den har arbetsfördelning. I de allra minsta organisationerna är dessa drag dock inte nödvändigtvis så framträdande.

Också kravet på att brotten skall begås i samförstånd begränsar definitionen. En sammanslutning av personer som visserligen begår brott uppsåtligen men utan att vara medvetna om varandras gärningar betraktas inte som en sådan kriminell organisation som avses i definitionen.

Det bör dessutom noteras att dataintrång skall höra till sammanslutningens typiska verksamhet för att den grund som anges i 1 punkten skall kunna tillämpas.

Med att gärningen begås särskilt planmässigt avses t.ex. att omfattande förberedelser har gjorts före gärningen och att särskilda åtgärder vidtas efteråt för att dölja spåren efter den.

Straffskalan föreslås vara böter eller fängelse i högst två år. Ett maximistraff på två år uppfyller kraven i artikel 7 i rambeslutet.

Enligt 2 mom. är också försök till grovt dataintrång straffbart.

I och med den föreslagna bestämmelsen uppfyller den gällande lagstiftningen i Finland kraven i artikel 7 i konventionen när det gäller den lägsta nivån på maximistraffet för dataintrång.

10 §. *Åtalsrätt.* Det föreslås att paragrafens 2 mom. ändras på grund av de nya straffbestämmelserna om systemstörning. Systemstörning fogas till förteckningen över målsägandebrott i momentet. Straffbestämmelserna om systemstörning skyddar huvudsakligen enskilda intressen. Brottsoffret har de bästa förutsättningarna att avgöra brottets betydelse och sitt behov av straffrättsligt skydd. Därför är det ändamålsenligt att brottet utgör ett målsägandebrott. Det undantag som i dag finns i bestämmelsen och som gäller ett viktigt allmänt intresse samt anställda vid ett teleföretag gäller efter den föreslagna ändringen också systemstörning. I dessa fall hör således även brott som gäller systemstörning under allmänt åtal. De grova gärningsformerna av brott är i allmänhet inte målsägandebrott, eftersom det ofta finns ett klart allmänt intresse av att åtal väcks i dessa fall. Därför föreslås grov systemstörning inte utgöra ett målsägandebrott.

12 §. *Straffansvar för juridiska personer.* Enligt den föreslagna nya paragrafen tillämpas på kränkning av kommunikationshemlighet, grov kränkning av kommunikationshemlighet, störande av post- och teletrafik, grovt störande av post- och teletrafik, dataintrång, grovt dataintrång, systemstörning och grov systemstörning vad som föreskrivs om straffansvar för juridiska personer. I och med bestämmelsen uppfyller lagstiftningen kraven i artikel 12 i konventionen när det gäller dessa brott. Genom den föreslagna ändringen beaktas också kraven i artikel 8 i rambeslutet. I det avsnitt som innehåller motiveringen till konventionen och godkännandet av den samt motiveringen till rambeslutet redogörs mera allmänt för hur bestämmelserna förhåller sig till artikel 12 i konventionen.

49 kap. Om kränkning av vissa immateriella rättigheter

7 §. *Straffansvar för juridiska personer.* Genom lagen om ändring av 49 kap. i strafflagen (822/2005) som trädde i kraft den 1 januari 2006, har till kapitlet fogats nya 4—6 §. Det föreslås därför att den nya bestämmelsen om straffansvar för juridiska

personer tas in som en ny 7 § i kapitlet. Enligt den föreslagna nya paragrafen tillämpas på upphovsrättsbrott vad som föreskrivs om straffansvar för juridiska personer. I och med bestämmelsen uppfyller lagstiftningen kraven i artikel 12 i konventionen när det gäller detta brott. I det avsnitt som innehåller motiveringen till konventionen och godkännandet av den redogörs mera allmänt för hur bestämmelserna förhåller sig till artikel 12 i konventionen.

3.3. Tvångsmedelslagen

4 kap. **Beslag**

1 §. *Förutsättningar för beslag.* Det föreslås att till paragrafen fogas ett nytt 2 mom., där det sägs att bestämmelserna om beslag i 1 mom. också skall tillämpas på data. Syftet med momentet är att för sin del klarlägga vilken ställning data i ett informationssystem har som föremål för beslag. Avsikten med tillägget är inte att ändra innehållet i den gällande rätten, utan syftet är att ordalydelsen i lagen bättre skall stämma överens med vedertagen praxis. Av samma orsak föreslås i 1 mom. en precisering som gäller beslag av handlingar.

Det föreslagna nya momentet innehåller samtidigt en definition av data. Begreppet data används i 4 b §, som gäller föreläggande att säkra data.

Enligt definitionen avses med data information som finns i en dator eller i något annat motsvarande informationssystem eller på dess lagringsplattform. Enligt definitionen är data således information som finns i ett visst slags tekniskt informationssystem.

Definitionen är inte beroende av den tekniska utformningen av det informationssystem i vilket informationen finns. Dator nämns i definitionen enbart som ett lättbegripligt exempel. Informationssystemet skall dock fungera på motsvarande sätt som en dator. Det väsentliga är att informationen behandlas elektroniskt, magnetiskt, optiskt eller på något annat motsvarande tekniskt sätt och vidare att behandlingen huvudsakligen sker självständigt, utan omedelbar medverkan av en människa. Ett kartotek i pappersform är därför inte ett sådant informationssystem som avses i definitionen, och uppgifterna i kartoteket utgör inte data. En elektronisk kalender i en mobiltelefon och anteckningarna i kalendern är däremot sådana data som avses i definitionen, trots att en mobiltelefon inte är en dator i allmänspråklig mening.

Var i systemet informationen finns saknar betydelse med tanke på definitionen. Informationen kan finnas tillfälligt lagrad i systemets primärminne eller permanent lagrad i dess massminne eller överföras mellan systemets olika delar med hjälp av en kommunikationsbuss. Informationen kan dessutom finnas på en diskett, en cd-romskiva eller dvd-skiva, ett minneskort eller någon annan särskild lagringsplattform.

Med information avses i definitionen vilka slags enskilda tecken och teckenuppsättningar samt helheter av sådana som helst. Innehållet i den information som dessa tecken representerar saknar betydelse. Innehållet kan således bestå av text, bild eller ljud eller t.ex. ett datorprogram eller en enskild programinstruktion. Enligt definitionen krävs det således inte något annat innehåll än dessa tecken.

När det gäller de informationssystem som används i dag följer av definitionen att data i praktiken avser information i digital form, dvs. all den information som skall lagras eller presenteras framställs i form av endast två olika tecken, vilket möjliggör en automatiserad teknisk behandling av informationen. Det är dock inte ändamålsenligt att binda definitionen av data till enbart information i digital form, eftersom den tekniska utvecklingen i framtiden kommer att möjliggöra behandling av också annan än digital information i informationssystemen.

Den föreslagna definitionen av data motsvarar definitionen av datorbehandlingsbara uppgifter i konventionen.

Enligt artikel 1 b i konventionen avses med datorbehandlingsbara uppgifter framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett datorsystem, inklusive program som utformats för att få ett datorsystem att utföra en viss funktion. Definitionen behandlas i punkt 25 i den förklarande rapporten. I rapporten sägs att definitionen grundar sig på en definition enligt en ISO-standard. Det väsentliga i definitionen är att informationen finns i elektronisk

eller någon annan sådan form att den som sådan lämpar sig för behandling i ett informationssystem.

Enligt förslaget avses med data information som finns i ett informationssystem eller på dess lagringsplattform. I konventionen avses med datorbehandlingsbara uppgifter information i en form som lämpar sig för behandling i ett informationssystem. Definitionen i förslaget är mer lättförståelig. Sakinnehållet är i praktiken identiskt.

Paragrafens 2 mom. ändrar inte förhållandet mellan beslag och teleavlyssning och -övervakning. Bestämmelserna i tvångsmedelslagens 5 a kap. har enligt lex specialisprincipen i egenskap av särskilda bestämmelser företräde framför bestämmelserna om beslag i lagens 4 kap. till den del det är fråga om meddelanden eller identifieringsuppgifter som avses i 5 a kap. 1 §.

I det föreslagna 3 mom. finns en förtydligande bestämmelse som motsvarar nuläget och enligt vilken bestämmelserna i 4 kap. också skall tillämpas på t.ex. sådana handlingar i form av data som har upprättats med hjälp av ett ordbehandlingsprogram. Bestämmelserna skall till dessa delar vara likadana oberoende av om den handling som skall tas i beslag finns utskriven på papper eller om den t.ex finns lagrad i form av data på en dators hårddisk.

I kapitlets 2 § finns bestämmelser om handlingar som på grund av sitt innehåll inte får tas i beslag i sådana fall när de innehas av den som misstänks för brott eller vissa andra i lagen nämnda personer. Samma bestämmelser gäller också handlingar i form av data. Högsta domstolen har i sitt prejudikat HD 2002:85 klarlagt rättsläget när det gäller beslag av handlingar i form av data och det förbud mot beslag som avses i 4 kap. 2 §. Högsta domstolen ansåg i sitt prejudikat att kopiering av en dators hårdskiva i rättsligt avseende skall anses som beslag, men att polisen dock har rätt att ta en hårdskiva i dess helhet i sin besittning för att söka efter sådant material som skall tas i beslag. Först vid granskningen av kopian är polisen skyldig att undersöka om hårddisken innehåller sådan information som omfattas av förbudet mot beslag. Polisen skall omedelbart återlämna eller förstöra sådana filer som omfattas av förbudet.

Handlingar i form av data innehas av en misstänkt om den dator, det informationssystem eller den särskilda lagringsplattform på vilken uppgifterna finns innehas av den misstänkte, eller om den misstänkte har tillgång till och kan använda uppgifterna oberoende av var de finns rent fysiskt.

I kapitlets 8 § finns bestämmelser om vem som har rätt att öppna ett slutet brev eller en annan sluten enskild handling och undersöka dess innehåll. Inom polisen får enligt bestämmelsen en sådan handling öppnas endast av undersökningsledaren, och jämte denne får endast de som utreder brottet i fråga undersöka handlingen. Samma bestämmelser gäller också handlingar i form av data. I praktiken blir bestämmelsen tillämplig främst vid undersökning av e-postmeddelanden som lagrats i en dator som tillhör en misstänkt.

4 a §. *Skyldighet för innehavare av informationssystem att lämna uppgifter.* I den föreslagna nya paragrafen bestäms om skyldighet för innehavaren av ett informationssystem att lämna uppgifter. Bestämmelserna hänför sig till beslag av data. Syftet med bestämmelserna är att se till att förundersökningsmyndigheten vid undersökning av informationssystem vid behov får hjälp med att bryta eller avkoda skyddet för systemet och med eventuella andra tekniska problem.

Enligt 1 mom. är innehavaren av ett informationssystem, den som svarar för systemet eller någon annan person skyldig att på begäran ge förundersökningsmyndigheten lösenord och andra motsvarande uppgifter som han eller hon innehar och som behövs för att genomföra ett beslag.

Kretsen av personer som är skyldiga att lämna uppgifter har inte i bestämmelsen begränsats till personer i en viss position. Innehavaren av ett informationssystem och den som svarar för systemet nämns endast som typexempel på situationer när bestämmelsen skall tillämpas. Skyldigheten att lämna uppgifter kan således enligt ordalydelsen i paragrafen gälla vem som helst som innehar sådana i bestämmelsen avsedda uppgifter som är nödvändiga för att ta i beslag data. Till dessa delar är bestämmelsens tillämpningsområde brett. Proportionalitetsprincipen, som framgår av 7 kap. 1 a § i tvångsmedelslagen,

begränsar också användningen av en begäran som gäller skyldighet att lämna uppgifter. En begäran får inte framställas om den nytta som kan fås för utredningen av brottet inte står i rimlig proportion till den olägenhet som förorsakas den som begäran riktar sig mot. I praktiken är den olägenhet som personen i fråga orsakas i allmänhet liten, eftersom bestämmelsen oftast uttryckligen blir tillämplig t.ex. på datateknisk personal som arbetar i samma företag som den misstänkte och dessa inte behöver göra något annat än att lämna vissa uppgifter. Syftet med bestämmelsen är att underlätta förundersökningsmyndighetens arbete genom att minska tidsåtgången vid beslag av data. Även den misstänkte och dennes arbetsgivare kan indirekt ha nytta av detta.

Bestämmelserna motsvarar till dessa delar de i artikel 15 i konventionen föreskrivna kraven på att en åtgärd skall vara skälig och att proportionalitetsprincipen skall iakttas.

Skyldigheten att lämna uppgifter kan gälla förutom lösenord också alla andra slag av uppgifter som är nödvändiga för att en åtgärd skall kunna vidtas. Det kan t.ex. vara fråga om uppgifter som behövs för avkodning av ett system eller tekniska data om ett systems egenskaper. Uppgifterna hänför sig således inte direkt till det brott som utreds utan endast till framtagningen av det egentliga bevismaterialet. Skyldigheten kan dock inte gälla t.ex. uppgifter om skapandet av en elektronisk signatur. Den gäller inte heller identifieringsuppgifter, om inhämtandet av uppgifterna skall anses som sådan teleövervakning som avses i lagens 5 a kap. 1 §.

Begäran om uppgifter kan enligt bestämmelsen framställas av den förundersökningsmyndighet som utreder brottet i fråga. Begäran kan även framställas muntligt. Om den som begäran riktar sig mot önskar detta, skall ett skriftligt intyg utfärdas över begäran.

Enligt 2 mom. kan den som vägrar att lämna uppgifter till förundersökningsmyndigheten förhöras i domstol så som bestäms i förundersökningslagens 28 §. Hänvisningen till förundersökningslagen avser både det sätt på vilket förhöret hålls och förutsättningarna för det.

Enligt 3 mom. gäller skyldigheten att lämna uppgifter inte en misstänkt och inte heller en person som med stöd av förundersökningslagens 27 § har rätt eller skyldighet att vägra vittna vid en förundersökning. Den som inte är skyldig att vittna är således enligt bestämmelsen inte heller skyldig att indirekt medverka till utredningen av saken genom att lämna uppgifter enligt 1 mom. På motsvarande sätt kan den som vägrar att lämna uppgifter enligt 3 mom. förhöras i domstol. I dessa fall kan de påtryckningsmedel som bestäms i 17 kap. 37 § i tvångsmedelslagen, dvs. vite och fängelse, användas.

Bestämmelserna motsvarar till dessa delar de i artikel 15 i konventionen föreskrivna kraven på en åtgärds skälighet och domstolskontroll.

I och med den föreslagna paragrafen uppfyller lagstiftningen kraven i artikel 19.4 i konventionen.

4 b §. *Föreläggande att säkra data.* Det föreslås att till kapitlet fogas bestämmelser om föreläggande att säkra data (4 b och 4 c §). Föreläggandet att säkra data är ett nytt tvångsmedel som vid behov kan användas som förberedande åtgärd innan andra tvångsmedel som riktar sig mot data används. Syftet med det är att förhindra att data som är av betydelse för utredning av brott går förlorade eller förändras innan de kan tas i besittning med stöd av andra tvångsmedel.

Enligt 1 mom. kan ett föreläggande att säkra data utfärdas för den som innehar data som kan ha betydelse för utredningen av det brott som undersöks, om det finns skäl att anta att dessa data annars går förlorade eller förändras. Ett föreläggande kan dock inte utfärdas för den som misstänks för brott, eftersom en misstänkt inte enligt de allmänna principerna kan åläggas att medverka till att utreda sin skuld.

Data som är av betydelse för utredningen av ett brott kan tas i beslag genast när lagringsplattformen har hittats. Förundersökningsmyndigheten kan i allmänhet genomföra beslaget redan i det skedet när villkoren för ett föreläggande uppfylls. Föreläggandet kommer därför i praktiken sannolikt endast sällan att användas som en åtgärd som föregår beslag.

Också teleövervakning samt teleavlyssning av t.ex. e-postmeddelanden riktar sig på

grund av det sätt på vilket åtgärderna tekniskt genomförs mot uppgifter som har formen av data. I regel krävs det tillstånd av domstolen för att dessa tvångsmedel skall få användas. Det kan hända att uppgifterna hinner gå förlorade innan man kommer åt dem med stöd av ett domstolstillstånd. Detta kan förhindras genom att ett föreläggande att säkra data utfärdas.

I syfte att säkerställa att föreläggandet vid behov kan användas för att säkra vilket slag av uppgifter som helst som har formen av data föreslås det att tillämpningsområdet för bestämmelserna skall vara brett.

Med data avses enligt det föreslagna 2 mom. i 4 kap. 1 § information som finns i en dator eller i något annat motsvarande informationssystem eller på dess lagringsplattform. Definitionen av data behandlas närmare i detaljmotiveringen till bestämmelsen i fråga.

Föreläggandet skall gälla vissa särskilt angivna data som redan existerar när föreläggandet utfärdas. Detta betyder inte att förundersökningsmyndigheten redan när föreläggandet utfärdas måste kunna ge en fullständig specifikation av uppgifterna. Hur noggrant uppgifterna skall specificeras beror på särdragen i det aktuella fallet. Om t.ex. föreläggandet att säkra data utfärdas för att säkerställa teleövervakning kan de uppgifter som föreläggandet gäller begränsas till trafikuppgifterna för en viss teleadress. Ett föreläggande kan självfallet inte gälla t.ex. en teleoperatörs samtliga trafikuppgifter.

När det gäller det kriterium i bestämmelsen som avser risken för att uppgifter går förlorade räcker det att förundersökningsmyndigheten själv bedömer att detta är sannolikt. Redan en liten sannolikhet är tillräcklig för att ett föreläggande skall kunna utfärdas. En teleoperatör är skyldig att utplåna trafikuppgifterna om ett samtal när dessa inte längre behövs för faktureringen. En utomstående kan inte veta vid vilken tidpunkt detta sker. Därför kan trafikuppgifter alltid betraktas som data som riskerar att gå förlorade så som avses i bestämmelsen.

I fråga om uppgifternas betydelse för utredningen av brott är kriteriet för att utfärda ett föreläggande detsamma som vid beslag av föremål eller data.

I praktiken är det ofta svårt att visa vem som de facto äger uppgifterna, och ägoförhållandena saknar också relevans med tanke på den föreslagna bestämmelsen. Det väsentliga är däremot om en person har faktiska möjligheter att fullgöra den skyldighet som avses i föreläggandet. Enligt bestämmelsen är kriteriet för att utfärda ett föreläggande därför att personen i fråga faktiskt har uppgifterna i sin besittning.

Den anhållningsberättigade tjänstemannen är behörig att utfärda ett föreläggande.

Ett föreläggande att säkra data skall på begäran ges skriftligt. I brådskande fall kan man i praktiken gå till väga så att föreläggandet ges muntligt, t.ex. per telefon, och ett skriftligt intyg utfärdas senare. Närmare bestämmelser om registreringen av ett föreläggande att säkra data vid förundersökning finns i förordningen om förundersökning och tvångsmedel (575/1988).

I 2 mom. sägs för tydlighetens skull att ett föreläggande att säkra data också kan gälla trafikuppgifter om meddelanden i form av data. Momentet innehåller samtidigt en definition av trafikuppgifter. Begreppet trafikuppgifter används i 3 mom. Enligt definitionen avses med trafikuppgifter sådana uppgifter som hänför sig till ett meddelande och som gäller meddelandets ursprung, destination, färdväg, storlek, tidpunkt, varaktighet, art och andra motsvarande omständigheter. Som exempel på trafikuppgifter kan nämnas uppringarens eller mottagarens telefonnummer och hur länge samtalet varade eller ett e-postmeddelandes ursprung, destination, avsändningstidpunkt och storlek. Uppgifter om mobiletelefoners läge kan betraktas som sådana motsvarande uppgifter som anges i momentet, och ett föreläggande kan således utfärdas även i fråga om dem. Det är huvudsakligen fråga om samma slags uppgifter som de identifieringsuppgifter som avses i 5 a kap. i tvångsmedelslagen. I 5 a kap. 1 § 2 punkten i tvångsmedelslagen nämns för tydlighetens skull förutom identifieringsuppgifter även uppgifter om mobilteleapparaters läge särskilt (RP 52/2002 rd). När paragrafen ursprungligen stiftades konstaterades det i förarbetena till lagen att begreppet identifieringsuppgifter även utan ett särskilt omnämnande beträffande mobiltelefoner täcker upp-

gifter om var apparaten finns (RP 22/1994 rd).

I 3 mom. anges för tydlighetens skull att huvudregeln är att förundersökningsmyndigheten inte har rätt att med stöd av ett föreläggande att säkra data ta del av innehållet i ett meddelande, trafikuppgifter eller andra lagrade uppgifter. I momentets andra mening finns ett undantag från denna huvudregel. Enligt det har förundersökningsmyndigheten rätt att ta del av de trafikuppgifter som behövs för att identifiera tjänsteleverantörerna, om flera tjänsteleverantörer har deltagit i förmedlingen av ett meddelande.

Undantagsbestämmelsen gäller endast sådana trafikuppgifter som hänför sig till ett meddelande och även då endast de uppgifter som är nödvändiga för att klarlägga meddelandets rutt.

Tjänsteleverantör definieras i artikel 1 c i konventionen. Enligt definitionen avses med tjänsteleverantör en offentlig eller privat enhet som erbjuder användarna av dess tjänster möjlighet att kommunicera med hjälp av ett datorsystem, och varje annan enhet som behandlar eller lagrar datorbehandlingsbara uppgifter för en sådan kommunikationstjänst eller för användarna av en sådan tjänst. Den tjänsteleverantör som avses i artikeln kan vara t.ex. ett företag som tillhandahåller överföring av meddelanden, tillträde till ett nät, underhåll av ett datorsystem eller lagring av uppgifter.

Ett meddelande som förmedlas i ett informationssystem kan passera genom flera teleoperatörers nät. För att förhindra att meddelandet eller trafikuppgifter som gäller det går förlorade är det i dessa fall inte alltid tillräckligt att ett föreläggande att säkra data utfärdas för en av operatörerna i överföringskedjan. För att föreläggandet att säkra data skall kunna riktas till alla dem som deltagit i överföringskedjan behövs det uppgifter om vilka operatörer som har deltagit i överföringen. Dessa trafikuppgifter är sådana i bestämmelsen avsedda uppgifter som behövs för att identifiera tjänsteleverantörer, och förundersökningsmyndighetens rätt att ta del av innehållet i uppgifter gäller endast dem.

I praktiken kan ett föreläggande att säkra data med hänsyn till de situationer som beskrivs ovan utfärdas så att förundersökningsmyndighetens rätt att få uppgifter och föreläggandet gäller alla operatörerna i överföringskedjan, trots att dessa ännu inte kan individualiseras när föreläggandet utfärdas.

Ett föreläggande att säkra data är effektivt endast om den som fått föreläggandet iakttar det. Den som vägrar att iaktta ett föreläggande kan med stöd av 16 kap. 4 § i strafflagen dömas för tredska mot polis. Om föreläggandet riktar sig mot en teleoperatör eller någon annan juridisk person gäller straffhotet den fysiska person som anses vara ansvarig för att föreläggandet fullgörs.

Om ett föreläggande inte kan iakttas t.ex. för att det är tekniskt omöjligt är det klart att något straff inte kan dömas ut. T.ex. när det gäller paketförmedlande nät kan det i praktiken vara omöjligt att klarlägga samtliga tjänsteleverantörer och routrar. En teleoperatör är med stöd av denna bestämmelse inte heller skyldig att ändra de tekniska egenskaperna i systemet.

I och med den föreslagna bestämmelsen, i kombination med 4 c §, som behandlas nedan, uppfyller lagstiftningen kraven i artiklarna 16 och 17 i konventionen.

4 c §. *Varaktigheten av ett föreläggande att säkra data och tystnadsplikt.* Den föreslagna paragrafen kompletterar 4 b § med bestämmelser om att ett föreläggande att säkra data är tidsbegränsat, föreläggandets maximala längd och tystnadsplikt för den som fått ett föreläggande.

Enligt 1 mom. utfärdas ett föreläggande att säkra data för en viss tid, högst tre månader. Tiden kan förlängas med högst tre månader åt gången, om det är nödvändigt för utredningen av brottet. Förutsättningarna för ett föreläggande skall således omprövas med minst tre månaders mellanrum. Däremot föreskrivs det inte om någon maximigräns för föreläggandets totala längd. Också användningen av detta tvångsmedel begränsas dock av proportionalitetsprincipen i 7 kap. 1 a §, som allmänt begränsar användningen av tvångsmedel. Ett föreläggande skall genast upphävas när det inte längre behövs eller när nyttan av det för brottsutredningen inte står i rimlig proportion till den olägenhet som förorsakas den som fått föreläggandet. Ett föreläggande att säkra data skall upphävas såsom obehövligt t.ex. när det har utfärdats som en

förberedande åtgärd för teleövervakning och förundersökningsmyndigheten har fått det begärda tillståndet till teleövervakningen av domstolen och i sin besittning fått data som har frusits med hjälp av föreläggandet. På motsvarande sätt skall åtgärden i en ovan nämnd situation återkallas också när domstolen genom ett lagakraftvunnet beslut har avslagit ansökan om teleövervakning och förundersökningsmyndigheten därför inte längre har någon grund för att hålla föreläggandet i kraft.

Enligt 2 mom. är den som fått ett föreläggande att säkra data skyldig att hemlighålla det. Syftet med bestämmelsen är dels att säkerställa en störningsfri brottsutredning men dels också att skydda den misstänktes integritet. I 3 mom. finns en förtydligande hänvisning där det sägs att till straff för brott mot tystnadsplikten enligt 2 mom. döms enligt bestämmelsen om sekretessbrott i strafflagens 38 kap. 1 § eller enligt bestämmelsen om sekretessförseelse i samma kapitels 2 §, om inte strängare straff för gärningen föreskrivs någon annanstans i lag.

I och med den föreslagna bestämmelsen uppfyller lagstiftningen kraven i artikel 16.2 och 16.3 i konventionen.

15 a §. *Beslut om beslag när en främmande stat har begärt rättshjälp.* Eftersom i lagen föreslås förtydligande bestämmelser om beslag av data, föreslås det för konsekvensens skull att även data fogas till förteckningen över objekt som kan tas i beslag i paragrafens första mening.

3.4. Förundersökningslagen

27 §. Inga ändringar i sak föreslås i paragrafens 1 mom. Det föreslås att till paragrafen fogas ett nytt 2 mom., varvid det nuvarande 2 mom. blir 3 mom.

Enligt det föreslagna 2 mom. är ett vittne som har sådan skyldighet att berätta vad han eller hon vet som avses i 1 mom. dessutom också skyldigt att lägga fram handlingar och annat bevismaterial som vittnet har i sin besittning och som är av betydelse för förundersökningen. En misstänkt har material i form av data i sin besittning om den dator, det informationssystem eller den lagringsplattform där uppgifterna finns är i den misstänktes besittning, eller om den misstänkte har uppgifterna i sin besittning och kan förfoga över dem, oberoende av var de rent fysiskt finns.

Med stöd av den gällande lagen kan handlingar och annat material såsom t.ex. upptagningar i form av data tas i beslag. Om det inte är känt var materialet finns, är den som innehar materialet skyldig att som vittne tala om det. Syftet med den föreslagna bestämmelsen är att klargöra att ett vittne i en ovan nämnd situation är skyldigt att själv lägga fram materialet. Det material som vittnet har lagt fram kan således vid behov också tas i beslag. Ett vittnes skyldighet att lägga fram material begränsas dock av proportionalitetsprincipen. Om det på grund av att materialet är mycket omfattande eller av någon annan motsvarande orsak är exceptionellt besvärligt för ett vittne att själv lägga fram det, är det klart att förundersökningsmyndigheten är skyldig att i mån av möjlighet bistå vittnet t.ex. genom att hämta materialet från den plats där det enligt vittnets uppgift finns.

Det nuvarande 2 mom., som gäller ett vittnes rätt och skyldighet att vägra vittna, blir i och med förslaget 3 mom. Enligt den sista meningen i det nya 3 mom. kan den som avses i 17 kap. 24 § 2 mom. i rättegångsbalken och som kan förpliktas att vid en rättegång besvara frågor som avses i 2 eller 3 mom. i samma paragraf förpliktas att besvara sådana frågor också vid förundersökning. Det föreslås att till momentet fogas ett omnämnande av att en ovan nämnd person också är skyldig att vid förundersökning lägga fram sådana handlingar eller annat bevismaterial som personen innehar och som är av betydelse för förundersökningen.

Om ett vittne vägrar att iaktta skyldigheten att lägga fram material kan vittnet med stöd av det nya 2 mom. i 28 §, som behandlas nedan, inför domstol åläggas att göra detta.

Genom denna bestämmelse och 28 § 2 mom. ändras lagstiftningen så att den motsvarar bestämmelserna om skyldighet att lämna uppgifter i artikel 18 i konventionen.

Den skyldighet att lämna uppgifter som avses i konventionen gäller endast datorbehandlingsbara uppgifter. Enligt förslaget omfattar skyldigheten också handlingar och an-

nat bevismaterial i pappersform. Förslaget går således utöver vad konventionen absolut kräver. Detta är dock nödvändigt med hänsyn till regleringens konsekvens och ändamålsenlighetsgrunder. Det finns inga rationella grunder för att data och t.ex. bevismaterial i pappersform skall behandlas olika i detta avseende. Till dessa delar redogörs för konventionen också i detaljmotiveringen till artikel 18.

28 §. På grund av de föreslagna ändringarna i 27 § som anges ovan föreslås det att hänvisningen till 27 § 2 mom. i paragrafens 1 mom. ändras till en hänvisning till 27 § 3 mom. Ändringen är enbart lagteknisk.

Det föreslås att till paragrafen fogas ett nytt 2 mom., varvid de nuvarande 2 och 3 mom. blir 3 och 4 mom. Enligt det föreslagna 2 mom. kan den behandling inför domstol som avses i 1 mom. användas också när ett vittne vägrar att fullgöra den skyldighet att läggra fram bevismaterial som anges i den föreslagna 27 § 2 mom. Detta betyder att vite enligt 17 kap. 15 § i rättegångsbalken kan användas som påtryckningsmedel, och dessutom kan det i enlighet med den nämnda paragrafen bestämmas att en utmätningsman skall hämta materialet.

När det gäller skyldigheten att lägga fram bevismaterial bör det noteras att fängelse inte kan användas som påtryckningsmedel enligt 17 kap. 37 § i rättegångsbalken, eftersom tillämpningsområdet för den nämnda bestämmelsen begränsar sig endast till muntligt förhör av ett vittne. Detta saknar dock betydelse i praktiken, eftersom man även kan förhöra ett vittne muntligt för att få reda på var materialet finns.

I praktiken kan bestämmelsen bli tillämplig endast i en sådan situation då man på någon grund vet att ett vittne i sin besittning har material som är av betydelse för brottsutredningen. Vittnet kan t.ex. själv ha talat om detta, eller så kan uppgiften grunda sig på vad ett annat vittne har berättat. Som ett typexempel kan nämnas en situation där ett vittne medger att han eller hon har bevismaterial i sin besittning men vägrar att lägga fram materialet med åberopande av ett förbud mot beslag av handlingar.

Bestämmelserna om förfarande och vittnesarvoden i de gällande 2 och 3 mom. blir i och med förslaget 3 och 4 mom. Dessa bestämmelser tillämpas också på domstolsbehandlingar som gäller skyldigheten att lägga fram bevismaterial.

Genom denna bestämmelse och 27 § 2 mom. ändras lagstiftningen så att den motsvarar bestämmelserna om skyldighet att lämna uppgifter i artikel 18 i konventionen. Regleringen motsvarar också de krav som ställs i artikel 15 i konventionen när det gäller åtgärdernas skälighet, iakttagandet av proportionalitetsprincipen och domstolskontroll.

3.5. Lagen om internationell rättshjälp i straffrättsliga ärenden

15 §. *Begränsningar i användningen av tvångsmedel.* Det föreslås att till paragrafen fogas ett nytt 2 mom., varvid de nuvarande 2 och 3 mom. blir 3 och 4 mom. Enligt det föreslagna 2 mom. gäller kravet på dubbel straffbarhet i 1 mom. inte det i denna proposition föreslagna nya föreläggandet att säkra data enligt 4 kap. 4 b § i tvångsmedelslagen.

Föreläggandet att säkra data är ett nytt tvångsmedel som vid behov kan användas som förberedande åtgärd innan andra tvångsmedel som riktar sig mot data vidtas. Syftet med åtgärden är att förhindra att data som är av betydelse för utredningen av ett brott går förlorade eller förändras innan de med stöd av andra tvångsmedel kan tas i besittning och innehållet undersökas.

Det föreslagna undantaget från kravet på dubbel straffbarhet gäller enbart föreläggandet att säkra data och inte de egentliga tvångsmedel som i dessa fall i praktiken regelmässigt följer på det. Syftet med bestämmelserna är att göra förfarandet snabbare och därmed förhindra att uppgifter går förlorade. För att det skall kunna avgöras om kravet på dubbel straffbarhet är uppfyllt krävs det en utredning om det brott som undersöks och en prövning av de omständigheter som inverkar på saken. Om prövningen av en begäran om rättslig hjälp tar lång tid kan det hända att de uppgifter som skall säkras hinner gå förlorade under förfarandets gång. Ett föreläggande att säkra data inverkar dock endast obetydligt på rättigheterna för den som har uppgifterna i sin besittning. Därför är det ändamålsenligt att det inte krävs någon prövning alls av kra-

vet på dubbel straffbarhet vid en dylik förberedande åtgärd vars syfte är att säkra uppgifter. Om man senare under behandlingen av den begäran som gäller det egentliga tvångsmedlet märker att kravet på dubbel straffbarhet inte uppfylls, avslås begäran och föreläggandet att säkra data återkallas.

I och med bestämmelsen uppfyller lagstiftningen kraven i artikel 29.3 i konventionen. Till dessa delar behandlas konventionen i detaljmotiveringen till artikel 29.

23 §. *Användning av tvångsmedel för inhämtande av bevis och för säkerställande av verkställigheten av en förverkandepåföljd.* Det föreslås att 1 mom. ändras så att till förteckningen över tvångsmedel som kan användas på grundval av en begäran om rättshjälp fogas det nya tvångsmedlet föreläggande att säkra data, som i denna proposition föreslås bli intaget i 4 kap. 4 b § i tvångsmedelslagen.

4. Ikraftträdande

Konventionen trädde i kraft internationellt den 1 juli 2004. För Finlands del träder konventionen i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då Finland deponerade sitt godkännandeinstrument.

Enligt propositionen bestäms genom förordning av republikens president om ikraftträdandet av lagen om sättande i kraft av konventionen. Avsikten är att lagen skall träda i kraft samtidigt som konventionen träder i kraft för Finlands del.

Medlemsstaterna skall vidta de åtgärder som är nödvändiga för att följa rambeslutet senast den 16 mars 2007. Senast samma dag skall medlemsstaterna till rådets generalsekretariat och kommissionen överlämna texten till bestämmelser genom vilka de skyldigheter som ålagts dem enligt rambeslutet införlivats med deras nationella lagstiftning. Senast den 16 september 2007 skall rådet utifrån denna information och en skriftlig rapport från kommissionen bedöma i vilken utsträckning skyldigheterna har fullgjorts.

Lagarna om ändring av strafflagen, tvångsmedelslagen, förundersökningslagen och lagen om straffrättslig rättshjälp föreslås träda i kraft så snart som möjligt efter det att de har antagits.

5. Behovet av riksdagens samtycke

Enligt 94 § 1 mom. i grundlagen krävs riksdagens godkännande bl.a. för fördrag och andra internationella förpliktelser som innehåller sådana bestämmelser som hör till området för lagstiftningen. Enligt grundlagsutskottets tolkningspraxis skall en bestämmelse anses höra till området för lagstiftningen, om den gäller utövande eller begränsning av någon grundläggande fri- eller rättighet som är skyddad i grundlagen, om den i övrigt gäller grunderna för individens rättigheter och skyldigheter, om den sak som bestämmelsen gäller enligt grundlagen skall föreskrivas i lag eller om det finns lagbestämmelser om den sak som bestämmelsen gäller eller det enligt rådande uppfattning i Finland skall lagstiftas om saken. Enligt dessa kriterier hör en bestämmelse om en internationell förpliktelse till området för lagstiftningen oavsett om den strider mot eller överensstämmer med en lagbestämmelse i Finland (GrUU 11 och 12/2000 rd).

Konventionen är av sådan natur att den huvudsakligen innehåller bestämmelser som hör till området för lagstiftningen. Konventionens samtliga bestämmelser om brott, tvångsmedel, territoriell tillämpning av strafflagen, utlämning för brott och internationell rättslig hjälp hör till området för lagstiftningen. Ett undantag är artikel 35, som endast gäller ordnande av sådan jour 24 timmar i dygnet som avses i artikeln.

Det föreslås att riksdagen godkänner konventionen så att beslutet om godkännande omfattar konventionen i dess helhet.

Också alla de förklaringar och förbehåll som föreslås i propositionen hör till området för lagstiftningen.

Grundlagsutskottet har ansett det vara på sin plats att riksdagen genom ett särskilt beslut ger sitt samtycke till sådana förklaringar avseende bestämmelser i en överenskommelse som faller under riksdagens kompetens (GrUU 2/1980 rd, GrUU 28/1997 rd och GrUU 36/1997 rd). Avgivandet och återtagandet av förbehåll och andra underrättelser som gäller bestämmelser som hör till områ-

det för lagstiftningen inverkar genom ikraftträdandelagen i form av en blankettlag på innehållet i den rätt som gäller som lag i Finland, och avgivandet eller återtagandet av förbehåll och andra underrättelser är således i detta avseende i sak utövande av lagstiftande makt.

Det krävs således riksdagens samtycke för att Finland skall kunna avge en förklaring enligt artikel 2, dvs. att Finland som villkor för att sådant olagligt intrång som avses i artikeln skall vara straffbart föreskriver att brottet har begåtts genom att bryta ett säkerhetsarrangemang.

Riksdagens samtycke krävs också för

1) förbehållet enligt artikel 11.3 i konventionen om att Finland inte tillämpar de bestämmelser som förpliktar till kriminalisering av försök i punkt 2 i den nämnda artikeln på lindrig skadegörelse och lindrig förfalskning,

2) förbehållet enligt artikel 14.3 a i konventionen om att Finland tillämpar artikel 20 endast på brott som riktar sig mot ett automatiskt databehandlingssystem och som har begåtts med hjälp av en teleterminalutrustning samt på koppleri, övergrepp i rättssak, olaga hot, narkotikabrott och försök till dessa brott samt på förberedelse till brott som begås i terroristiskt syfte och på brott för vilka det föreskrivna strängaste straffet är fängelse i minst fyra år,

3) förbehållet enligt artikel 14.3 b i konventionen om att Finland inte tillämpar de åtgärder som avses i artiklarna 20 och 21 på meddelanden som överförs inom ett datorsystem som drivs för en sluten användargrupp och inte använder allmänna kommunikationsnät och inte är anslutet till ett annat datorsystem, oavsett om detta är offentligt eller enskilt.

6. Behandlingsordning

I propositionen föreslås att de bestämmelser i konventionen som hör till området för lagstiftningen sätts i kraft nationellt genom en s.k. blankettlag. Konventionen innehåller bestämmelser om gärningar som skall straffbeläggas, straffrättsliga tvångsmedel och internationell rättslig hjälp. Vissa av konventionens bestämmelser om tvångsmedel och rättslig hjälp kan vara av betydelse med hänsyn till lagstiftningsordningen. Sådana bestämmelser är bestämmelserna om beslag och kopiering av datorbehandlingsbara uppgifter i artikel 19.3, skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter i artikel 16, skyndsamt säkrande och partiellt röjande av trafikuppgifter i artikel 17 samt frångående av dubbel straffbarhet i artikel 29.3.

Artikel 19.3 i konventionen innehåller bestämmelser om beslag och kopiering av datorbehandlingsbara uppgifter. Eftersom föremålet för beslaget är egendom i form av data hänför sig bestämmelsen till egendomsskyddet enligt grundlagens 15 §. Bestämmelsen motsvarar huvudsakligen gällande praxis i Finland, och den utvidgar inte myndigheternas rätt att ta egendom i beslag. Bestämmelsen utgör därför inte något problem med hänsyn till egendomsskyddet.

Artikel 16 i konventionen innehåller bestämmelser om skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter. Det är fråga om ett nytt tvångsmedel som vid behov kan användas som förberedande åtgärd före andra tvångsmedel som riktar sig mot data. Syftet med tvångsmedlet är att hindra att data som är av betydelse för utredningen av brott går förlorade eller förändras innan de kan tas i besittning med stöd av andra tvångsmedel. Med stöd av bestämmelsen kan den som har datorbehandlingsbara uppgifter i sin besittning tillfälligt förbjudas att utplåna dessa. Eftersom föremålet för åtgärden är egendom i form av data hänför sig paragrafen till egendomsskyddet enligt grundlagens 15 §. Bestämmelsen ingriper dock endast i obetydlig utsträckning i egendomsskyddet. Den föreslagna nya bestämmelsen utgör därför inte något problem med hänsyn till egendomsskyddet.

Artikel 17 i konventionen innehåller bestämmelser om skyndsamt säkrande och partiellt röjande av trafikuppgifter. Enligt artikeln kan en åtgärd som avses i artikel 16 också rikta sig mot ett meddelande som förmedlas med hjälp av ett datorsystem och trafikuppgifter som hänför sig till det. En myndighet har dock i regel inte rätt att ta del av innehållet i ett meddelande, trafikuppgifter eller andra lagrade uppgifter. Det finns emellertid ett undantag från denna huvudregel.

Enligt det skall en myndighet ha rätt att ta del av de trafikuppgifter som behövs för att identifiera tjänsteleverantörerna, om flera tjänsteleverantörer har deltagit i förmedlingen av ett meddelande. Till dessa delar hänför sig bestämmelsen också till det skydd för förtroliga meddelanden som anges i grundlagens 10 §. Enligt grundlagsutskottets tolkningspraxis omfattas trafikuppgifter som gäller ett förtroligt meddelande av skyddet enligt den nämnda 10 §, även om de inte hör till kärnan i denna grundläggande rättighet.

Det ovan nämnda undantaget gäller endast trafikuppgifter som hänför sig till ett meddelande, och även i dessa fall endast sådana uppgifter som är nödvändiga för att klarlägga ett meddelandes rutt. I praktiken betyder detta endast uppgifter om vilka operatörer som har deltagit i förmedlingen av meddelandet. Överlämnandet av sådana uppgifter till myndigheterna kränker i praktiken inte alls eller endast i mycket liten utsträckning den berörda personens integritet. Överlämnandet är dock nödvändigt för att ett föreläggande att säkra uppgifter snabbt skall kunna riktas till alla dem som har deltagit i överföringskedjan. Den föreslagna bestämmelsen utgör därför inte något problem med hänsyn till grundlagens 10 §.

Enligt artikel 29.3 i konventionen får i fråga om besvarande av en framställning om föreläggande att säkra datorbehandlingsbara uppgifter så som avses i artikel 16 dubbel straffbarhet inte uppställas som ett villkor för säkrandet. I praktiken betyder detta bl.a. att en finsk myndighet på framställning av en utländsk myndighet är skyldig att använda det ovan nämnda tvångsmedlet även om den gärning som tvångsmedlet grundar sig på inte skulle vara straffbar enligt finsk lag. Eftersom tvångsmedlet även förutsätter att vissa trafikuppgifter överlämnas hänför sig paragrafen åtminstone i någon mån till Finlands suveränitet enligt grundlagens 1 §.

Enligt 1 § 3 mom. i grundlagen deltar Finland i internationellt samarbete i syfte att säkerställa fred och mänskliga rättigheter samt i syfte att utveckla samhället. Enligt förarbetena till grundlagen har denna bestämmelse betydelse för bedömningen av när en internationell förpliktelse står i konflikt med bestämmelserna om suveränitet i grundlagen. Det är således befogat att utgå från att sådana internationella förpliktelser som är sedvanliga i modernt internationellt samarbete och som endast i ringa utsträckning påverkar statens suveränitet inte direkt kan anses strida mot grundlagens bestämmelser om suveränitet.

Det undantag från kravet på dubbel straffbarhet som förutsätts i artikeln gäller endast säkrande av datorbehandlingsbara uppgifter enligt artikel 16 och inte de egentliga tvångsmedel som i praktiken i regel följer på detta säkrande. Artikelns enda syfte är att genom ett snabbare förfarande förhindra att uppgifter som är av betydelse för utredningen av brott går förlorade. Bestämmelsernas konsekvenser för dem som de riktar sig mot eller t.ex. för teleoperatörer är små, i enlighet med vad som sägs ovan. Ett internationellt samarbete vid utredningen och uppklaringen av nätbrott är ägnad att bidra till uttryckligen en sådan utveckling av samhället som avses i 1 § 3 mom. i grundlagen.

Av dessa orsaker kan bestämmelsen i artikeln inte anses stå i strid med grundlagens 1 §.

Regeringen anser att konventionen kan godkännas med enkel majoritet, och förslaget till lag om sättande i kraft av konventionen kan godkännas i vanlig lagstiftningsordning.

Med stöd av vad som anförts ovan och i enlighet med grundlagens 94 § föreslås att

Riksdagen godkänner Europarådets i Budapest den 23 november 2001 ingångna konvention om IT-relaterad brottslighet,

Riksdagen ger sitt samtycke till att Finland avger en förklaring enligt artikel 2 om att Finland som villkor för att sådant olagligt intrång som avses i artikeln skall vara straffbart föreskriver att brottet har begåtts genom att bryta ett säkerhetsarrangemang,

Riksdagen ger sitt samtycke till att Finland gör ett förbehåll enligt artikel 11.3 om att Finland inte tillämpar bestämmelserna som förpliktar till kriminalisering av försök i punkt 2 i den nämnda artikeln på lindrig skadegörelse och lindrig förfalskning,

Riksdagen ger sitt samtycke till att Finland gör ett förbehåll enligt artikel 14.3 a om att Finland tillämpar artikel 20 endast på brott som riktar sig mot ett automatiskt databehandlingssystem och som har begåtts med hjälp av en teleterminalutrustning samt på koppleri, övergrepp i rättssak, olaga hot, narkotikabrott och försök till dessa brott samt på förberedelse till brott som begås i terroristiskt syfte och på brott för vilka det föreskrivna strängaste straffet är fängelse i minst fyra år,

Riksdagen ger sitt samtycke till att Finland gör ett förbehåll enligt artikel 14.3 b om att Finland inte tillämpar de åtgärder som avses i artiklarna 20 och 21 på meddelanden som överförs inom ett datorsystem som drivs för en sluten användargrupp och inte använder allmänna kommunikationsnät och inte är anslutet till ett annat datorsystem, oavsett om detta är offentligt eller enskilt.

Med stöd av vad som anförts ovan och eftersom konventionen innehåller bestämmelser som hör till området för lagstiftningen, föreläggs Riksdagen samtidigt följande lagförslag:

Lagförslagen

1.

Lag

om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i Europarådets konvention om IT-relaterad brottslighet

I enlighet med riksdagens beslut föreskrivs:

1 §

De bestämmelser som hör till området för lagstiftningen i den i Budapest den 23 november 2001 ingångna konventionen om IT-relaterad brottslighet gäller som lag sådana Finland har förbundit sig till dem.

2 §

Närmare bestämmelser om verkställigheten av denna lag kan utfärdas genom förordning av statsrådet.

3 §

Om ikraftträdandet av denna lag bestäms genom förordning av republikens president.

2.

Lag

om ändring av strafflagen

I enlighet med riksdagens beslut

upphävs i strafflagen av den 19 december 1889 (39/1889) 17 kap. 1 a § 4 mom., sådant det lyder i lag 142/2003,

ändras 17 kap. 8 a § 2 punkten, 18 a § 1 mom. 4 punkten, 25 kap. 3 a § 1 mom. 4 punkten, 34 kap. 9 a och 13 §, 35 kap. 1 § och 38 kap. 10 § 2 mom.,

sådana de lyder, 17 kap. 8 a § 2 punkten, 18 a § 1 mom. 4 punkten och 25 kap. 3 a § 1 mom. 4 punkten i lag 650/2004, 34 kap. 9 a § i lag 951/1999 och 13 § i lag 833/2003, 35 kap. 1 § i lag 769/1990 och 38 kap. 10 § 2 mom. i lag 1118/2001, samt

fogas till 17 kap. en ny 1 b §, till 34 kap. en ny 9 b §, till 35 kap. 1 §, sådan den lyder i lag 769/1990, ett nytt 3 mom., till kapitlet en ny 8 §, till 38 kap. 5 §, sådan den lyder i lag 578/1995, ett nytt 2 mom., till 6 §, sådan den lyder i sistnämnda lag, ett nytt 2 mom. och till 7 §, sådan den lyder i sistnämnda lag, ett nytt 2 mom., till kapitlet nya 7 a, 7 b och 8 a §, varvid den nuvarande 8 a § blir 8 b §, och till kapitlet en ny 12 § samt till 49 kap. en ny 7 § som följer:

17 kap.

Om brott mot allmän ordning

1 b §

Definition av organiserad kriminell sammanslutning

Med organiserad kriminell sammanslutning avses en strukturerad sammanslutning, inrättad för en viss tid, bestående av minst tre personer, som handlar i samförstånd för att begå brott.

8 a §

Grovt ordnande av olaglig inresa

Om vid ordnande av olaglig inresa

— — — — — — — — — — — — — — —

2) brottet har begåtts som ett led i en i 1 b § avsedd organiserad kriminell sammanslutnings verksamhet,

och gärningen även bedömd som en helhet är grov, skall gärningsmannen för *grovt ordnande av olaglig inresa* dömas till fängelse i minst fyra månader och högst sex år.

18 a §

Grov spridning av barnpornografisk bild

Om vid spridning av barnpornografisk bild

— — — — — — — — — — — — — — —

4) brottet har begåtts som ett led i en i 1 b § avsedd organiserad kriminell sammanslutnings verksamhet,

och gärningen även bedömd som en helhet är grov, skall gärningsmannen för *grov spridning av barnpornografisk bild* dömas till fängelse i minst fyra månader och högst sex år.

— — — — — — — — — — — — — — —

25 kap.

Om brott mot friheten

3 a §

Grov människohandel

Om vid människohandel

— — — — — — — — — — — — — — —

4) brottet har begåtts som ett led i en i 17 kap 1 b § avsedd organiserad kriminell sammanslutnings verksamhet,

och gärningen även bedömd som en helhet är grov, skall gärningsmannen för *grov människohandel* dömas till fängelse i minst två och högst tio år.

— — — — — — — — — — — — — —

34 kap.

Om allmänfarliga brott

9 a §

Orsakande av fara för informationsbehandling

Den som för att orsaka olägenhet eller skada för informationsbehandling eller ett informations- eller kommunikationssystems funktion eller säkerhet

1) för in i landet, tillverkar, säljer eller annars sprider eller ställer till förfogande

a) sådana apparater, datorprogram eller programinstruktioner som har skapats eller anpassats för att äventyra eller skada informationsbehandling eller ett informations- eller kommunikationssystems funktion eller för att bryta eller avkoda det tekniska skyddet vid elektronisk kommunikation eller skyddet för ett informationssystem, eller

b) andra personers lösenord eller åtkomstkoder eller andra motsvarande uppgifter om informationssystem, eller

2) sprider eller ställer till förfogande anvisningar för tillverkning av sådana datorprogram eller programinstruktioner som avses i 1 punkten

skall, om inte strängare eller lika strängt straff föreskrivs för gärningen någon annanstans i lag, för *orsakande av fara för informationsbehandling* dömas till böter eller fängelse i högst två år.

9 b §

Innehav av hjälpmedel vid nätbrott

Den som för att orsaka olägenhet eller skada för informationsbehandling eller ett informations- eller kommunikationssystems funktion eller säkerhet innehar sådana apparater, datorprogram eller programinstruktioner som avses i 9 a § 1 a-punkten eller sådana lösenord, åtkomstkoder eller andra motsvarande uppgifter som avses i 9 a § 1 b-punkten, skall för *innehav av hjälpmedel vid nätbrott* dömas till böter eller fängelse i högst sex månader.

13 §

Straffansvar för juridiska personer

På kärnladdningsbrott, på förberedelse till allmänfarligt brott enligt 9 § 2 mom. och på orsakande av fara för informationsbehandling tillämpas vad som föreskrivs om straffansvar för juridiska personer.

35 kap.

Om skadegörelse

1 §

Skadegörelse

Den som obehörigen förstör eller skadar någon annans egendom skall för *skadegörelse* dömas till böter eller fängelse i högst två år.

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

Försök är straffbart.

8 §

Straffansvar för juridiska personer

På skadegörelse som avses i 1 § 2 mom. samt på grov skadegörelse som avses i 2 §, när den har skett på det sätt som avses i 1 § 2 mom., tillämpas vad som föreskrivs om straffansvar för juridiska personer.

38 kap.

Om informations- och kommunikationsbrott

5 §

Störande av post- och teletrafik

— — — — — — — — — — — — — — —

Försök är straffbart.

6 §

Grovt störande av post- och teletrafik

— — — — — — — — — — — — — — —

Försök är straffbart.

7 §

Lindrigt störande av post- och teletrafik

— — — — — — — — — — — — — — —

Försök är straffbart.

7 a §

Systemstörning

Den som i syfte att orsaka en annan person olägenhet eller ekonomisk skada matar in, överför, skadar, ändrar eller undertrycker data eller på något annat med dessa jämförbart sätt obehörigen hindrar ett informationssystems funktion eller orsakar allvarliga störningar i det skall, om inte strängare eller lika strängt straff föreskrivs för gärningen någon annanstans i lag, för *systemstörning* dömas till böter eller fängelse i högst två år.

Försök är straffbart.

7 b §

Grov systemstörning

Om vid systemstörning

1) vållas synnerligen kännbar olägenhet eller ekonomisk skada eller

2) brottet begås särskilt planmässigt

och systemstörningen även bedömd som en helhet är grov, skall gärningsmannen för *grov systemstörning* dömas till fängelse i minst fyra månader och högst fyra år.

Försök är straffbart.

8 a §

Grovt dataintrång

Om vid dataintrång

1) brottet begås som ett led i en i 17 kap. 1 b § avsedd organiserad kriminell sammanslutnings verksamhet eller

2) brottet begås särskilt planmässigt

och dataintrånget även bedömt som en helhet är grovt, skall gärningsmannen för *grovt dataintrång* dömas till böter eller fängelse i högst två år.

Försök är straffbart.

10 §

Åtalsrätt

— — — — — — — — — — — — — — —

Allmänna åklagaren får inte väcka åtal för kränkning av kommunikationshemlighet, grov kränkning av kommunikationshemlighet, systemstörning, dataintrång eller avkodningssystemsbrott, om inte målsäganden anmäler brottet till åtal eller gärningsmannen när brottet begicks var anställd hos en inrättning som utövar allmän post- eller televerksamhet eller om ett synnerligen viktigt allmänt intresse kräver att åtal väcks.

— — — — — — — — — — — — — — —

12 §

Straffansvar för juridiska personer

På kränkning av kommunikationshemlighet, grov kränkning av kommunikationshemlighet, störande av post- och teletrafik, grovt störande av post- och teletrafik, dataintrång, grovt dataintrång, systemstörning och grov systemstörning tillämpas vad som föreskrivs om straffansvar för juridiska personer.

49 kap.

Om kränkning av vissa immateriella rättigheter

7 §

Straffansvar för juridiska personer

På upphovsrättsbrott tillämpas vad som föreskrivs om straffansvar för juridiska personer.

Denna lag träder i kraft den 20 .

3.

Lag

om ändring av 4 kap. i tvångsmedelslagen

I enlighet med riksdagens beslut

ändras i tvångsmedelslagen av den 30 april 1987 (450/1987) 4 kap. 1 § och 15 a § 1 mom., av dem 15 a § 1 mom. sådant det lyder i lag 10/1994, samt

fogas till 4 kap. nya 4 a—4 c § som följer:

4 kap.

Beslag

1 §

Förutsättningar för beslag

Föremål och handlingar får tas i beslag, om det finns skäl att anta att de kan ha betydelse som bevis i brottmål eller att de har avhänts någon genom brott eller att en domstol förklarar dem förverkade.

Vad som bestäms i 1 mom. gäller också information som finns i en dator eller i något annat motsvarande informationssystem eller på dess lagringsplattform *(data)*.

Vad som i detta kapitel bestäms om handlingar tillämpas även på handlingar i form av data.

4 a §

Skyldighet för innehavare av informationssystem att lämna uppgifter

Innehavaren av ett informationssystem, den som svarar för systemet eller någon annan person är skyldig att på begäran ge förundersökningsmyndigheten lösenord och andra motsvarande uppgifter som han eller hon innehar och som behövs för verkställande av beslag. Personen i fråga skall, om han eller hon så önskar, få ett skriftligt intyg över begäran.

Den som vägrar att lämna uppgifterna kan förhöras i domstol så som bestäms i förundersökningslagens 28 §.

Vad som bestäms i 1 och 2 mom. gäller inte en misstänkt och inte heller en person som med stöd av förundersökningslagens 27 § har rätt eller skyldighet att vägra vittna vid en förundersökning.

4 b §

Föreläggande att säkra data

Om det finns skäl att anta att data som kan ha betydelse för utredningen av det brott som undersöks går förlorade eller förändras, kan en anhållningsberättigad tjänsteman ålägga den som innehar eller har bestämmanderätten över dessa data, dock inte den som misstänks för brott, att säkra uppgifterna så att de inte ändras. Personen i fråga skall på begäran få ett skriftligt intyg över föreläggandet.

Vad som bestäms i 1 mom. gäller även sådana uppgifter i anslutning till ett meddelande som förmedlats med hjälp av ett informationssystem vilka anger meddelandets ursprung, destination, färdväg, storlek, tidpunkt, varaktighet, art och andra motsvarande omständigheter *(trafikuppgifter)*.

Förundersökningsmyndigheten har inte med stöd av ett sådant föreläggande att säkra data som avses i 1 mom. rätt att ta del av innehållet i ett meddelande, i trafikuppgifter eller i andra lagrade uppgifter. Om flera tjänsteleverantörer har deltagit i förmedlingen av ett sådant meddelande som avses i 2 mom., har förundersökningsmyndigheten rätt att ta del av de trafikuppgifter som behövs för att identifiera tjänsteleverantörerna.

4 c §

Varaktigheten av ett föreläggande att säkra data samt tystnadsplikt

Ett föreläggande att säkra data utfärdas för viss tid, högst tre månader. Tiden kan förlängas med högst tre månader åt gången, om det är nödvändigt för utredningen av brottet.

Den som fått ett föreläggande att säkra data är skyldig att hemlighålla det.

Till straff för brott mot tystnadsplikt som avses i 2 mom. döms enligt 38 kap. 1 eller 2 § i strafflagen, om inte strängare straff för gärningen föreskrivs någon annanstans i lag.

15 a §

Beslut om beslag när en främmande stat har begärt rättshjälp

Föremål, handlingar och data kan på begäran av en utländsk myndighet tas i beslag, om de kan utgöra bevis i ett brottmål som behandlas av den utländska myndigheten eller om de har avhänts någon genom brott. Ett föremål kan tas i beslag, om det genom ett beslut av en utländsk domstol har förklarats förverkat med anledning av ett brott eller om det med fog kan antas att föremålet med anledning av ett brott kommer att förklaras förverkat i ett mål som behandlas av en utländsk myndighet.

— — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .

4.

Lag

om ändring av 27 och 28 § i förundersökningslagen

I enlighet med riksdagens beslut

ändras i förundersökningslagen av den 30 april 1987 (449/1987) 27 § och 28 § 1 mom., sådana de lyder, 27 § delvis ändrad i lag 462/2003 och 28 § 1 mom. i lag 645/2003, samt

fogas till 28 §, sådan den lyder i lag 692/1997 och i nämnda lag 645/2003, ett nytt 2 mom., varvid de nuvarande 2 och 3 mom. blir 3 och 4 mom., som följer:

27 §

Ett vittne skall sanningsenligt och utan att förtiga något berätta vad han eller hon vet om den sak som undersöks. Om ett vittne dock i en rättegång skulle ha rätt eller skyldighet att vägra vittna, röja en omständighet eller besvara en fråga, ifall åtal väcks för det brott som undersöks, har vittnet samma rätt eller skyldighet också vid en förundersökning.

Ett vittne som har i 1 mom. avsedd skyldighet att berätta vad han eller hon vet är också skyldigt att lägga fram handlingar och annat bevismaterial som vittnet har i sin besittning och som är av betydelse för förundersökningen.

Den som avses i 17 kap. 23 § 1 mom. i rättegångsbalken och som enligt 3 mom. i samma paragraf kan förpliktas att vittna om sådant som skall hållas hemligt har rätt att vittna därom vid förundersökning, om den gäller ett brott för vilket det föreskrivna strängaste straffet är minst sex års fängelse. Den som avses i 17 kap. 24 § 2 mom. i rättegångsbalken och som enligt 4 mom. i samma paragraf kan förpliktas att besvara frågor som avses i 2 eller 3 mom. i paragrafen är skyldig att besvara sådana frågor och att lägga fram handlingar eller annat bevismaterial som personen innehar och som är av betydelse för förundersökningen också vid förundersökning, om den gäller ett brott som avses ovan i detta moment.

28 §

Om det är uppenbart att ett vittne känner till någon omständighet som är av vikt för att skuldfrågan skall kunna utredas eller för att vinningen av ett brott skall kunna spåras och återtas, och om vittnet vägrar att röja denna omständighet trots att han eller hon har skyldighet eller enligt 27 § 3 mom. rätt att göra detta, hålls vittnesförhöret på undersökningsledarens begäran inför domstol.

Vad som bestäms i 1 mom. tillämpas också på ett vittne som vägrar lägga fram en handling eller annat bevismaterial.

— — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .

5.

Lag

om ändring av 15 och 23 § i lagen om internationell rättshjälp i straffrättsliga ärenden

I enlighet med riksdagens beslut

ändras i lagen av den 5 januari 1994 om internationell rättshjälp i straffrättsliga ärenden (4/1994) 23 § 1 mom., sådant det lyder i lag 149/2004, samt

fogas till 15 § ett nytt 2 mom., varvid de nuvarande 2 och 3 mom. blir 3 och 4 mom., som följer:

15 §

Begränsningar i användningen av tvångsmedel

— — — — — — — — — — — — — — —

Vad som bestäms i 1 mom. gäller dock inte ett sådant föreläggande att säkra data som avses i 4 kap. 4 b § i tvångsmedelslagen.

— — — — — — — — — — — — — — —

som har framställts av en utländsk myndighet kan för inhämtande av bevis husrannsakan, beslag och förelägganden att säkra data verkställas, teleavlyssning, teleövervakning och teknisk observation utföras samt täckoperationer och bevisprovokationer genom köp genomföras och signalement upptas, om detta ingår i begäran om rättshjälp eller är nödvändigt för att verkställa begäran.

— — — — — — — — — — — — — — —

23 §

Användning av tvångsmedel för inhämtande av bevis och för säkerställande av verkställigheten av en förverkandepåföljd

På grundval av en begäran om rättshjälp

Denna lag träder i kraft den 20 .

Helsingfors den 29 september 2006

Republikens President

TARJA HALONEN

Justitieminister *Leena Luhtanen*

Bilaga
Parallelltexter

2.

Lag

om ändring av strafflagen

I enlighet med riksdagens beslut

upphävs i strafflagen av den 19 december 1889 (39/1889) 17 kap. 1 a § 4 mom., sådant det lyder i lag 142/2003,

ändras 17 kap. 8 a § 2 punkten, 18 a § 1 mom. 4 punkten, 25 kap. 3 a § 1 mom. 4 punkten, 34 kap. 9 a och 13 §, 35 kap. 1 § och 38 kap. 10 § 2 mom.,

sådana de lyder, 17 kap. 8 a § 2 punkten, 18 a § 1 mom. 4 punkten och 25 kap. 3 a § 1 mom. 4 punkten i lag 650/2004, 34 kap. 9 a § i lag 951/1999 och 13 § i lag 833/2003, 35 kap. 1 § i lag 769/1990 och 38 kap. 10 § 2 mom. i lag 1118/2001, samt

fogas till 17 kap. en ny 1 b §, till 34 kap. en ny 9 b §, till 35 kap. 1 §, sådan den lyder i lag 769/1990, ett nytt 3 mom., till kapitlet en ny 8 §, till 38 kap. 5 §, sådan den lyder i lag 578/1995, ett nytt 2 mom., till 6 §, sådan den lyder i sistnämnda lag, ett nytt 2 mom. och till 7 §, sådan den lyder i sistnämnda lag, ett nytt 2 mom., till kapitlet nya 7 a, 7 b och 8 a §, varvid den nuvarande 8 a § blir 8 b §, och till kapitlet en ny 12 § samt till 49 kap. en ny 7 § som följer:

Gällande lydelse	*Föreslagen lydelse*
17 kap.	
Om brott mot allmän ordning	
1 a §	
Deltagande i en organiserad kriminell sammanslutnings verksamhet	
— — — — — — — — — — — — — —	
Med organiserad kriminell sammanslutning avses en strukturerad sammanslutning, inrättad för en viss tid, bestående av minst tre personer, som handlar i samförstånd för att begå brott som avses i 1 mom.	(upphävs)
	1 b §
	Definition av organiserad kriminell sammanslutning
(ny)	*Med organiserad kriminell sammanslutning avses en strukturerad sammanslutning, inrättad för en viss tid, bestående av minst*

Gällande lydelse	*Föreslagen lydelse*
	tre personer, som handlar i samförstånd för att begå brott.
8 a §	8 a §
Grovt ordnande av olaglig inresa	*Grovt ordnande av olaglig inresa*
Om vid ordnande av olaglig inresa	Om vid ordnande av olaglig inresa
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
2) brottet har begåtts som ett led i en i 1 a § 4 mom. avsedd organiserad kriminell sammanslutnings verksamhet,	2) brottet har begåtts som ett led i en i 1 *b §* avsedd organiserad kriminell sammanslutnings verksamhet,
och gärningen även bedömd som en helhet är grov, skall gärningsmannen för *grovt ordnande av olaglig inresa* dömas till fängelse i minst fyra månader och högst sex år.	och gärningen även bedömd som en helhet är grov, skall gärningsmannen för *grovt ordnande av olaglig inresa* dömas till fängelse i minst fyra månader och högst sex år.
18 a §	18 a §
Grov spridning av barnpornografisk bild	*Grov spridning av barnpornografisk bild*
Om vid spridning av barnpornografisk bild	Om vid spridning av barnpornografisk bild
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
4) brottet har begåtts som ett led i en i 1 a § 4 mom. avsedd organiserad kriminell sammanslutnings verksamhet,	4) brottet har begåtts som ett led i en i 1 *b §* avsedd organiserad kriminell sammanslutnings verksamhet,
och gärningen även bedömd som en helhet är grov, skall gärningsmannen för *grov spridning av barnpornografisk bild* dömas till fängelse i minst fyra månader och högst sex år.	och gärningen även bedömd som en helhet är grov, skall gärningsmannen för *grov spridning av barnpornografisk bild* dömas till fängelse i minst fyra månader och högst sex år.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
25 kap.	25 kap.
Om brott mot friheten	**Om brott mot friheten**
3 a §	3 a §
Grov människohandel	*Grov människohandel*
Om vid människohandel	Om vid människohandel
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
4) brottet har begåtts som ett led i en i 17 kap 1 a § 4 mom. avsedd organiserad kriminell sammanslutnings verksamhet,	4) brottet har begåtts som ett led i en i 17 kap *1 b §* avsedd organiserad kriminell sammanslutnings verksamhet,
och gärningen även bedömd som en helhet är grov, skall gärningsmannen *för grov människohandel* dömas till fängelse i minst två och högst tio år.	och gärningen även bedömd som en helhet är grov, skall gärningsmannen för *grov människohandel* dömas till fängelse i minst två och högst tio år.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —

Gällande lydelse	*Föreslagen lydelse*
34 kap.	
Om allmänfarliga brott	
9 a §	9 a §
Orsakande av fara för informations- behandling	*Orsakande av fara för informationsbehandling*
Den som för att orsaka olägenhet för informationsbehandling eller ett data- eller telesystems funktion,	Den som för att orsaka olägenhet *eller skada* för informationsbehandling eller ett informations- eller *kommunikationssystems* funktion *eller säkerhet*
1) tillverkar eller ställer till förfogande ett sådant datorprogram eller sådana programinstruktioner som har planerats för att äventyra informationsbehandling eller ett data- eller telesystems funktion eller för att skada data eller programvara som ingår i ett sådant system, eller sprider ett sådant datorprogram eller sådana programinstruktioner eller	1) *för in i landet*, tillverkar, *säljer* eller annars sprider eller ställer till förfogande a) sådana *apparater*, datorprogram eller programinstruktioner som har *skapats eller anpassats* för att äventyra *eller skada* informationsbehandling *eller ett informations- eller kommunikationssystems funktion eller för att bryta eller avkoda det tekniska skyddet vid elektronisk kommunikation eller skyddet för ett informationssystem, eller* *b) andra personers lösenord eller åtkomstkoder eller andra motsvarande uppgifter om informationssystem, eller*
2) ställer till förfogande anvisningar för tillverkning av ett sådant datorprogram eller sådana programinstruktioner som avses i 1 punkten eller sprider sådana anvisningar	2) sprider eller ställer till förfogande anvisningar för tillverkning av sådana datorprogram eller programinstruktioner som avses i 1 punkten
skall, om inte strängare eller lika strängt straff föreskrivs för gärningen någon annanstans i lag, för *orsakande av fara för informationsbehandling* dömas till böter eller fängelse i högst två år.	skall, om inte strängare eller lika strängt straff föreskrivs för gärningen någon annanstans i lag, för *orsakande av fara för informationsbehandling* dömas till böter eller fängelse i högst två år.
	9 b §
	Innehav av hjälpmedel vid nätbrott
(ny)	*Den som för att orsaka olägenhet eller skada för informationsbehandling eller ett informations- eller kommunikationssystems funktion eller säkerhet innehar sådana apparater, datorprogram eller programinstruktioner som avses i 9 a § 1 a-punkten eller sådana lösenord, åtkomstkoder eller andra motsvarande uppgifter som avses i 9 a § 1 b-punkten, skall för innehav av hjälpmedel vid nätbrott dömas till böter eller fängelse i högst sex månader.*

Gällande lydelse	*Föreslagen lydelse*
13 §	13 §
Juridiska personers straffansvar	*Straffansvar för juridiska personer*
På kärnladdningsbrott och på förberedelse till allmänfarligt brott enligt 9 § 2 mom. tillämpas vad som bestäms om juridiska personers straffansvar.	På kärnladdningsbrott, på förberedelse till allmänfarligt brott enligt 9 § 2 mom. *och på orsakande av fara för informationsbehandling* tillämpas vad som föreskrivs om straffansvar för juridiska personer.

35 kap.

Om skadegörelse

1 §	1 §
Skadegörelse	*Skadegörelse*
Den som orättmätigt förstör eller skadar någon annans egendom skall för *skadegörelse* dömas till böter eller fängelse i högst ett år.	Den som obehörigen förstör eller skadar någon annans egendom skall för *skadegörelse* dömas till böter eller fängelse i högst *två* år.
För skadegörelse döms också den som för att skada någon orättmätigt förstör, skadar, döljer eller hemlighåller information som har upptagits på ett datamedium eller någon annan upptagning.	För skadegörelse döms också den som för att skada någon obehörigen förstör, skadar, döljer eller hemlighåller information som har upptagits på ett datamedium eller någon annan upptagning.
	Försök är straffbart.
	8 §
	Straffansvar för juridiska personer
(ny)	*På skadegörelse som avses i 1 § 2 mom. samt på grov skadegörelse som avses i 2 §, när den har skett på det sätt som avses i 1 § 2 mom., tillämpas vad som föreskrivs om straffansvar för juridiska personer.*

Gällande lydelse	*Föreslagen lydelse*
38 kap.	
Om informations- och kommunikationsbrott	
5 §	5 §
Störande av post- och teletrafik	*Störande av post- och teletrafik*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
(ny)	*Försök är straffbart.*
6 §	6 §
Grovt störande av post- och teletrafik	*Grovt störande av post- och teletrafik*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
(ny)	*Försök är straffbart.*
7 §	7 §
Lindrigt störande av post- och teletrafik	*Lindrigt störande av post- och teletrafik*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
(ny)	*Försök är straffbart.*
	7 a §
	Systemstörning
(ny)	*Den som i syfte att orsaka en annan person olägenhet eller ekonomisk skada matar in, överför, skadar, ändrar eller undertrycker data eller på något annat med dessa jämförbart sätt obehörigen hindrar ett informationssystems funktion eller orsakar allvarliga störningar i det skall, om inte strängare eller lika strängt straff föreskrivs för gärningen någon annanstans i lag, för systemstörning dömas till böter eller fängelse i högst två år.* *Försök är straffbart.*
	7 b §
	Grov systemstörning
(ny)	*Om vid systemstörning* *1) vållas synnerligen kännbar olägenhet eller ekonomisk skada eller* *2) brottet begås särskilt planmässigt* *och systemstörningen även bedömd som en helhet är grov, skall gärningsmannen för*

Gällande lydelse	*Föreslagen lydelse*
	grov systemstörning dömas till fängelse i minst fyra månader och högst fyra år. *Försök är straffbart.*
	8 a §
	Grovt dataintrång
(ny)	*Om vid dataintrång* *1) brottet begås som ett led i en i 17 kap. 1 b § avsedd organiserad kriminell sammanslutnings verksamhet eller* *2) brottet begås särskilt planmässigt* *och dataintrånget även bedömt som en helhet är grovt, skall gärningsmannen för grovt dataintrång dömas till böter eller fängelse i högst två år.* *Försök är straffbart.*
10 §	10 §
Åtalsrätt	*Åtalsrätt*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Allmänna åklagaren får inte väcka åtal för kränkning av kommunikationshemlighet, grov kränkning av kommunikationshemlighet, dataintrång eller avkodningssystemsbrott, om inte målsäganden anmäler brottet till åtal eller gärningsmannen när brottet begicks var anställd hos en inrättning som utövar allmän post- eller televerksamhet eller om ett synnerligen viktigt allmänt intresse kräver att åtal väcks.	Allmänna åklagaren får inte väcka åtal för kränkning av kommunikationshemlighet, grov kränkning av kommunikationshemlighet, *systemstörning*, dataintrång eller avkodningssystemsbrott, om inte målsäganden anmäler brottet till åtal eller gärningsmannen när brottet begicks var anställd hos en inrättning som utövar allmän post- eller televerksamhet eller om ett synnerligen viktigt allmänt intresse kräver att åtal väcks.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
	12 §
	Straffansvar för juridiska personer
(ny)	*På kränkning av kommunikationshemlighet, grov kränkning av kommunikationshemlighet, störande av post- och teletrafik, grovt störande av post- och teletrafik, dataintrång, grovt dataintrång, systemstörning och grov systemstörning tillämpas vad som föreskrivs om straffansvar för juridiska personer.*

Gällande lydelse	*Föreslagen lydelse*
	49 kap.
	Om kränkning av vissa immateriella rättigheter
	7 §
	Straffansvar för juridiska personer
(ny)	*På upphovsrättsbrott tillämpas vad som föreskrivs om straffansvar för juridiska personer.*
	_____
	Denna lag träder i kraft den 20 .
	_____

3.

Lag

om ändring av 4 kap. i tvångsmedelslagen

I enlighet med riksdagens beslut

ändras i tvångsmedelslagen av den 30 april 1987 (450/1987) 4 kap. 1 § och 15 a § 1 mom., av dem 15 a § 1 mom. sådant det lyder i lag 10/1994, samt

fogas till 4 kap. nya 4 a—4 c § som följer:

Gällande lydelse	*Föreslagen lydelse*
	4 kap.
	Beslag
1 §	1 §
Förutsättningar för beslag	*Förutsättningar för beslag*
Ett föremål får tas i beslag, om det finns skäl att anta att det kan ha betydelse som bevis i brottmål eller att det har avhänts någon genom brott eller att en domstol förklarar det förbrutet.	Föremål *och handlingar* får tas i beslag, om det finns skäl att anta att de kan ha betydelse som bevis i brottmål eller att de har avhänts någon genom brott eller att en domstol förklarar dem förverkade.
(ny)	*Vad som bestäms i 1 mom. gäller också information som finns i en dator eller i något annat motsvarande informationssystem eller på dess lagringsplattform (data).*
(ny)	*Vad som i detta kapitel bestäms om handlingar tillämpas även på handlingar i form av data.*
	4 a §
	Skyldighet för innehavare av informationssystem att lämna uppgifter
(ny)	*Innehavaren av ett informationssystem, den som svarar för systemet eller någon annan person är skyldig att på begäran ge förundersökningsmyndigheten lösenord och andra motsvarande uppgifter som han eller hon innehar och som behövs för verkställande av beslag. Personen i fråga skall, om han eller hon så önskar, få ett skriftligt intyg över begäran.*
	Den som vägrar att lämna uppgifterna

Gällande lydelse	Föreslagen lydelse
	kan förhöras i domstol så som bestäms i förundersökningslagens 28 §.
	Vad som bestäms i 1 och 2 mom. gäller inte en misstänkt och inte heller en person som med stöd av förundersökningslagens 27 § har rätt eller skyldighet att vägra vittna vid en förundersökning.
	4 b §
	Föreläggande att säkra data
	Om det finns skäl att anta att data som kan ha betydelse för utredningen av det brott som undersöks går förlorade eller förändras, kan en anhållningsberättigad tjänsteman ålägga den som innehar eller har bestämmanderätten över dessa data, dock inte den som misstänks för brott, att säkra uppgifterna så att de inte ändras. Personen i fråga skall på begäran få ett skriftligt intyg över föreläggandet.
(ny)	*Vad som bestäms i 1 mom. gäller även sådana uppgifter i anslutning till ett meddelande som förmedlats med hjälp av ett informationssystem vilka anger meddelandets ursprung, destination, färdväg, storlek, tidpunkt, varaktighet, art och andra motsvarande omständigheter (trafikuppgifter).*
	Förundersökningsmyndigheten har inte med stöd av ett sådant föreläggande att säkra data som avses i 1 mom. rätt att ta del av innehållet i ett meddelande, i trafikuppgifter eller i andra lagrade uppgifter. Om flera tjänsteleverantörer har deltagit i förmedlingen av ett sådant meddelande som avses i 2 mom., har förundersökningsmyndigheten rätt att ta del av de trafikuppgifter som behövs för att identifiera tjänsteleverantörerna.
	4 c §
	Varaktigheten av ett föreläggande att säkra data samt tystnadsplikt
(ny)	*Ett föreläggande att säkra data utfärdas för viss tid, högst tre månader. Tiden kan förlängas med högst tre månader åt gången, om det är nödvändigt för utredningen av brottet.*
	Den som fått ett föreläggande att säkra

Gällande lydelse	*Föreslagen lydelse*
	data är skyldig att hemlighålla det. *Till straff för brott mot tystnadsplikt som avses i 2 mom. döms enligt 38 kap. 1 eller 2 § i strafflagen, om inte strängare straff för gärningen föreskrivs någon annanstans i lag.*
15 a §	15 a §
Beslut om beslag när en främmande stat har begärt rättshjälp	*Beslut om beslag när en främmande stat har begärt rättshjälp*
Föremål eller handlingar kan på begäran av en utländsk myndighet tas i beslag, om de kan utgöra bevis i ett brottmål som behandlas av den utländska myndigheten eller om de har avhänts någon genom brott. Ett föremål kan tas i beslag, om det genom ett beslut av en utländsk domstol har förklarats förverkat med anledning av ett brott eller om det med fog kan antas att föremålet med anledning av ett brott kommer att förklaras förverkat i ett mål som behandlas av en utländsk myndighet.	Föremål, handlingar *och data* kan på begäran av en utländsk myndighet tas i beslag, om de kan utgöra bevis i ett brottmål som behandlas av den utländska myndigheten eller om de har avhänts någon genom brott. Ett föremål kan tas i beslag, om det genom ett beslut av en utländsk domstol har förklarats förverkat med anledning av ett brott eller om det med fog kan antas att föremålet med anledning av ett brott kommer att förklaras förverkat i ett mål som behandlas av en utländsk myndighet.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

———

Denna lag träder i kraft den *20* .

———

4.

Lag

om ändring av 27 och 28 § i förundersökningslagen

I enlighet med riksdagens beslut

ändras i förundersökningslagen av den 30 april 1987 (449/1987) 27 § och 28 § 1 mom., sådana de lyder, 27 § delvis ändrad i lag 462/2003 och 28 § 1 mom. i lag 645/2003, samt

fogas till 28 §, sådan den lyder i lag 692/1997 och i nämnda lag 645/2003, ett nytt 2 mom., varvid de nuvarande 2 och 3 mom. blir 3 och 4 mom., som följer:

Gällande lydelse	*Föreslagen lydelse*
27 §	27 §
Ett vittne skall sanningsenligt och utan att förtiga något uppge vad han vet om den sak som undersöks. Om han dock i en rättegång vore berättigad eller skyldig att vägra vittna, yppa något eller besvara någon fråga, ifall åtal väcks för det brott som undersöks, har han samma rätt respektive skyldighet även vid en förundersökning.	Ett vittne skall sanningsenligt och utan att förtiga något berätta vad han *eller hon* vet om den sak som undersöks. Om ett vittne dock i en rättegång skulle ha rätt eller skyldighet att vägra vittna, röja en omständighet eller besvara en fråga, ifall åtal väcks för det brott som undersöks, har vittnet samma rätt eller skyldighet också vid en förundersökning.
(ny)	*Ett vittne som har i 1 mom. avsedd skyldighet att berätta vad han eller hon vet är också skyldigt att lägga fram handlingar och annat bevismaterial som vittnet har i sin besittning och som är av betydelse för förundersökningen.*
Den som avses i 17 kap. 23 § 1 mom. rättegångsbalken och som enligt 3 mom. i samma paragraf kan förpliktas att vittna om sådant som skall hållas hemligt har rätt att vittna därom vid förundersökning, om den gäller ett brott för vilket det strängaste straffet är minst sex års fängelse. Den som avses i 17 kap. 24 § 2 mom. rättegångsbalken och som enligt 4 mom. i samma paragraf kan förpliktas att besvara frågor som avses i 2 eller 3 mom. i paragrafen är skyldig att besvara sådana frågor också vid förundersökning, om den gäller ett brott som avses ovan i detta moment.	Den som avses i 17 kap. 23 § 1 mom. i rättegångsbalken och som enligt 3 mom. i samma paragraf kan förpliktas att vittna om sådant som skall hållas hemligt har rätt att vittna därom vid förundersökning, om den gäller ett brott för vilket det föreskrivna strängaste straffet är minst sex års fängelse. Den som avses i 17 kap. 24 § 2 mom. i rättegångsbalken och som enligt 4 mom. i samma paragraf kan förpliktas att besvara frågor som avses i 2 eller 3 mom. i paragrafen är skyldig att besvara sådana frågor *och att lägga fram handlingar eller annat bevismaterial som personen innehar och som är av betydelse för förundersökningen* också vid förundersökning, om den gäller ett brott som avses ovan i detta moment.

Gällande lydelse	*Föreslagen lydelse*
28 §	28 §
Om det är uppenbart att ett vittne känner till någon omständighet som är av vikt för att skuldfrågan skall kunna utredas eller för att vinningen av ett brott skall kunna spåras och återtas, och om vittnet vägrar att röja denna omständighet trots att han eller hon har skyldighet eller enligt 27 § 2 mom. rätt att göra detta, hålls vittnesförhöret på undersökningsledarens begäran inför domstol.	Om det är uppenbart att ett vittne känner till någon omständighet som är av vikt för att skuldfrågan skall kunna utredas eller för att vinningen av ett brott skall kunna spåras och återtas, och om vittnet vägrar att röja denna omständighet trots att han eller hon har skyldighet eller enligt 27 § *3 mom.* rätt att göra detta, hålls vittnesförhöret på undersökningsledarens begäran inför domstol.
(ny)	*Vad som bestäms i 1 mom. tillämpas också på ett vittne som vägrar lägga fram en handling eller annat bevismaterial.*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .

———

5.

Lag

om ändring av 15 och 23 § i lagen om internationell rättshjälp i straffrättsliga ärenden

I enlighet med riksdagens beslut

ändras i lagen av den 5 januari 1994 om internationell rättshjälp i straffrättsliga ärenden (4/1994) 23 § 1 mom., sådant det lyder i lag 149/2004, samt

fogas till 15 § ett nytt 2 mom., varvid de nuvarande 2 och 3 mom. blir 3 och 4 mom., som följer:

Gällande lydelse	*Föreslagen lydelse*
15 §	15 §
Begränsningar i användningen av tvångsmedel	*Begränsningar i användningen av tvångsmedel*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
(ny)	*Vad som bestäms i 1 mom. gäller dock inte ett sådant föreläggande att säkra data som avses i 4 kap. 4 b § i tvångsmedelslagen.*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
23 §	23 §
Användning av tvångsmedel för inhämtande av bevis och för säkerställande av verkställigheten av en förverkandepåföljd	*Användning av tvångsmedel för inhämtande av bevis och för säkerställande av verkställigheten av en förverkandepåföljd*
På grundval av en begäran om rättshjälp som har framställts av en utländsk myndighet kan för inhämtande av bevis husrannsakan och beslag verkställas, teleavlyssning, teleövervakning och teknisk observation utföras samt täckoperationer och bevisprovokationer genom köp genomföras och signalement upptas, om detta ingår i begäran om rättshjälp eller är nödvändigt för att verkställa begäran.	På grundval av en begäran om rättshjälp som har framställts av en utländsk myndighet kan för inhämtande av bevis husrannsakan, beslag *och föreläggande att säkra data* verkställas, teleavlyssning, teleövervakning och teknisk observation utföras samt täckoperationer och bevisprovokationer genom köp genomföras och signalement upptas, om detta ingår i begäran om rättshjälp eller är nödvändigt för att verkställa begäran.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —

_____

Denna lag träder i kraft den *20* .

_____

Fördragstext

Konvention om IT-relaterad brottslighet

Ingress

Medlemsstaterna i Europarådet och de övriga stater som har undertecknat denna konvention,

som beaktar att Europarådets syfte är att skapa en fastare enhet mellan dess medlemmar,

som erkänner värdet av att främja samarbete med de övriga stater som är parter i denna konvention,

som är övertygade om nödvändigheten av att, som en prioriterad fråga, driva en gemensam straffrättslig politik som syftar till att skydda samhället mot IT-relaterad brottslighet, bl.a. genom att anta lämplig lagstiftning och främja internationellt samarbete,

som är medvetna om de djupgående förändringar som har föranletts av digitalisering, konvergens och fortgående globalisering av datornät,

som är oroade över faran för att datornät och elektroniska uppgifter också kan användas för att begå brott och att bevisning om sådana brott kan lagras och överföras genom dessa datornät,

som erkänner behovet av samarbete mellan staterna och det privata näringslivet i att bekämpa IT-relaterad brottslighet och behovet av att skydda rättmätiga intressen beträffande användning och utveckling av informationsteknologier,

som anser att en effektiv kamp mot IT-relaterad brottslighet fordrar ett utvidgat, snabbt och väl fungerande internationellt samarbete i straffrättsliga frågor,

som är övertygade om att denna konvention behövs för att avskräcka från gärningar

Convention on cybercrime

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

som riktar sig mot datorsystemens, datornätens och de datorbehandlingsbara uppgifternas förtrolighet, integritet och tillgänglighet, liksom från missbruk av dessa system, nät och uppgifter genom att föreskriva att sådana gärningar kriminaliseras så som det beskrivs i konventionen, och att befogenheter som är tillräckliga för att effektivt bekämpa dessa brott införs, genom att underlätta upptäckt, utredning och lagföring av dem, både på det nationella och det internationella planet och genom att sörja för system för ett snabbt och pålitligt internationellt samarbete,

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

som är medvetna om behovet av att säkerställa en lämplig avvägning mellan intresset av att lag och ordning upprätthålls och respekten för de grundläggande mänskliga rättigheterna så som de garanteras i 1950 års Europarådskonvention om skydd för de mänskliga rättigheterna och de grundläggande friheterna, 1966 års FN-konvention om medborgerliga och politiska rättigheter och andra tillämpliga internationella fördrag om mänskliga rättigheter, som bekräftar allas rätt att utan inblandning hysa åsikter liksom rätten till yttrandefrihet, innefattande frihet att söka, ta emot och sprida information och idéer av alla slag, oberoende av gränser, samt rätten till respekt för privatlivet,

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 också är medvetna om rätten till skydd för personuppgifter, såsom denna rätt tillgodoses exempelvis i 1981 års Europarådskonvention om skydd för enskilda vid automatisk databehandling av personuppgifter,

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 beaktar 1989 års FN-konvention om barnets rättigheter och 1999 års ILO-konvention mot de värsta formerna av barnarbete,

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 beaktar de Europarådskonventioner som finns om samarbete på det straffrättsliga området liksom liknande fördrag mellan Europarådets medlemsstater och andra stater och som understryker att den nu aktuella konventionen är avsedd att komplettera dessa konventioner för att effektivisera brottsut-

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

redningar och rättegångar om brott relaterade till datorsystem och datorbehandlingsbara uppgifter samt möjliggöra insamling av bevis i elektronisk form om brott,

som välkomnar den senaste utvecklingen som ytterligare främjar internationell förståelse och internationellt samarbete i att bekämpa IT-relaterad brottslighet, innefattande åtgärder vidtagna av Förenta nationerna, OECD, Europeiska unionen och G8,

som erinrar om ministerkommitténs rekommendationer nr R (85)10 om praktisk tillämpning av Europeiska konventionen om inbördes rättshjälp i brottmål avseende bevisinsamling vid avlyssning av teleförbindelser, nr R (88)2 om piratverksamhet avseende upphovsrätt och närstående rättigheter, nr R (87)15, som reglerar användningen av personuppgifter i polisiär verksamhet, nr R (95)4 om skydd för personuppgifter inom telekommunikationstjänster med särskild hänvisning till telefoni samt nr R (89)9 om datorrelaterade brott, som ger riktlinjer för nationella lagstiftande församlingar om definition av vissa datorbrott och nr R (95)13 om problem inom straffprocessrätten som hör samman med informationsteknologi,

som beaktar resolution nr 1, antagen av de europeiska justitieministrarna vid deras tjugoförsta konferens i Prag den 10—11 juni 1997, vilken rekommenderar ministerkommittén att stödja det arbete om IT-brottslighet som utförs av Europarådets kommitté för brottsfrågor för att tillnärma olika länders nationella straffrättsliga bestämmelser och möjliggöra användning av effektiva utredningsmetoder i fråga om sådana brott, liksom resolution nr 3, antagen vid de europeiska justitieministrarnas tjugotredje konferens i London den 8—9 juni 2000, vilken uppmanar de förhandlande parterna att fortsätta sina ansträngningar med sikte på att finna lämpliga lösningar för att göra det möjligt för största möjliga antal stater att bli parter i konventionen och erkänner behovet av ett snabbt och effektivt system

make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

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

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

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 effi-

för internationellt samarbete, vari vederbörligen beaktas de särskilda krav som ställs i kampen mot IT-relaterad brottslighet,

som även beaktar den handlingsplan som antogs av Europarådets stats- och regeringschefer vid deras andra toppmöte i Strasbourg den 10—11 oktober 1997 för att söka gemensamma svar på utvecklingen av nya informationsteknologier, som grundar sig på Europarådets normer och värderingar,

har kommit överens om följande.

KAPITEL I

ANVÄNDNING AV TERMER

Artikel 1

Definitioner

I denna konvention används följande definitioner:

a) datorsystem: en apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatiserad behandling av uppgifter.

b) datorbehandlingsbara uppgifter: framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett datorsystem, inklusive program som utformats för att få ett datorsystem att utföra en viss funktion.

c) tjänsteleverantör:

i) en offentlig eller privat enhet som erbjuder användarna av dess tjänster möjlighet att kommunicera med hjälp av ett datorsystem, och

ii) varje annan enhet som behandlar eller lagrar datorbehandlingsbara uppgifter för en sådan kommunikationstjänst eller för användarna av en sådan tjänst.

cient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

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

Have agreed as follows:

CHAPTER I

USE OF TERMS

Article 1

Definitions

For the purposes of this Convention:

a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b) “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c) “service provider” means:

i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service;

d) trafikuppgifter: datorbehandlingsbara uppgifter som hänför sig till ett meddelande som förmedlas med hjälp av ett datorsystem, vilka alstrats av ett datorsystem som ingick i kommunikationskedjan och anger meddelandets ursprung, destination, färdväg, tid, datum, storlek, varaktighet eller typ av underliggande tjänst.

KAPITEL II

ÅTGÄRDER SOM SKALL VIDTAS PÅ NATIONELL NIVÅ

Avsnitt 1

Materiell straffrätt

Avdelning 1

Brott mot datorbehandlingsbara uppgifters och datorsystems förtrolighet, integritet och tillgänglighet

Artikel 2

Olagligt intrång

Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga orättmätigt intrång i hela eller en del av ett datorsystem, när det görs uppsåtligen. En part får uppställa krav på att brottet begås genom intrång i säkerhetsåtgärder med uppsåt att komma över datorbehandlingsbara uppgifter eller med annat brottsligt uppsåt eller mot ett datorsystem som är kopplat till ett annat datorsystem.

Artikel 3

Olaglig avlyssning

Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärningar när de begås uppsåtligen: att med tekniska hjälpmedel orättmätigt avlyssna icke allmänna överföringar av datorbehandlingsbara uppgifter till, från eller inom ett

d) “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

CHAPTER II

MEASURES TO BE TAKEN AT THE NATIONAL LEVEL

Section 1

Substantive criminal law

Title 1

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

Article 2

Illegal access

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

Article 3

Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer

datorsystem, däribland elektromagnetiska emissioner från ett datorsystem med sådana datorbehandlingsbara uppgifter. En part får uppställa krav på att brottet begås med brottsligt uppsåt eller mot ett datorsystem som är kopplat till ett annat datorsystem.

Artikel 4

Datastörning

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärningar när de begås uppsåtligen:

Att orättmätigt skada, radera, försämra, ändra eller undertrycka datorbehandlingsbara uppgifter.

2. En part får förbehålla sig rätten att uppställa krav på att det handlande som anges i punkt 1 medför allvarlig skada.

Artikel 5

Systemstörning

Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärningar när de begås uppsåtligen: att orättmätigt allvarligt hindra ett datorsystems drift genom att mata in, överföra, skada, radera, försämra, ändra eller undertrycka datorbehandlingsbara uppgifter.

Artikel 6

Missbruk av apparatur

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärningar när de begås uppsåtligen och orättmätigt:

a) Att tillverka, försälja, anskaffa för användning, importera, sprida eller på annat sätt tillgängliggöra

system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4

Data interference

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

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

Article 5

System interference

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

Article 6

Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a) the production, sale, procurement for use, import, distribution or otherwise making available of:

i) en apparat vari ingår ett datorprogram som är skapat eller anpassat främst för att begå något av de brott som straffbeläggs i enlighet med artiklarna 2—5,

ii) ett datorlösenord, en åtkomstkod eller liknande datorbehandlingsbara uppgifter som kan ge åtkomst till ett helt datorsystem eller en del därav

med uppsåt att den eller det skall användas för att begå något av de brott som straffbeläggs i enlighet med artiklarna 2—5.

b) Att inneha ett föremål som avses i a i eller a ii ovan med uppsåt att det skall användas för att begå något av de brott som straffbeläggs i enlighet med artiklarna 2—5. En part får i lag uppställa krav på att flera sådana föremål skall innehas för att straffansvar skall gälla.

2. Denna artikel skall inte tolkas som att den ålägger straffansvar i de fall där tillverkning, försäljning, anskaffning för användning, import, spridning eller annat tillgängliggörande eller innehav som avses i punkt 1 i denna artikel inte har till syfte att något av de brott som straffbeläggs i enlighet med artiklarna 2—5 i denna konvention skall begås, såsom exempelvis för att i behörig ordning testa eller skydda ett datorsystem.

3. Varje part får förbehålla sig rätten att inte tillämpa punkt 1 i denna artikel, om förbehållet inte avser försäljning, spridning eller annat tillgängliggörande av föremål som avses i punkt 1 a ii i denna artikel.

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.

Avdelning 2

Datorrelaterade brott

Artikel 7

Datorrelaterad förfalskning

Varje part skall vidta nödvändiga lagstift-

Title 2

Computer-related offences

Article 7

Computer-related forgery

Each Party shall adopt such legislative and

ningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärningar när de begås uppsåtligen och orättmätigt:

Att mata in, ändra, radera eller undertrycka datorbehandlingsbara uppgifter så att icke autentiska uppgifter uppstår med uppsåt att dessa skall beaktas eller ligga till grund för handlande i rättsliga hänseenden som om de vore autentiska, oavsett om uppgifterna är direkt läsbara och begripliga. En part får uppställa krav på bedrägligt uppsåt eller liknande brottsligt uppsåt för att straffansvar skall gälla.

Artikel 8

Datorrelaterat bedrägeri

Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärningar när de begås uppsåtligen och orättmätigt: att förorsaka en annan person förlust av egendom genom att

a) mata in, ändra, radera eller undertrycka datorbehandlingsbara uppgifter,

b) störa ett datorsystems drift,

med bedrägligt eller annat brottsligt uppsåt och orättmätigt skaffa sig s jälv eller en annan person en ekonomisk förmån.

Avdelning 3

Innehållsrelaterade brott

Artikel 9

Brott som hänför sig till barnpornografi

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga följande gärningar när de begås uppsåtligen och orättmätigt:

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

Article 8

Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a) any input, alteration, deletion or suppression of computer data;

b) any interference with the functioning of a computer system,

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

Title 3

Content-related offences

Article 9

Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a) Att framställa barnpornografi i syfte att sprida den med hjälp av datorsystem.

b) Att bjuda ut eller tillgängliggöra barnpornografi med hjälp av datorsystem.

c) Att sprida eller överföra barnpornografi med hjälp av datorsystem.

d) Att anskaffa barnpornografi åt sig själv eller någon annan med
hjälp av datorsystem.

e) Att inneha barnpornografi i ett datorsystem eller i ett medium för lagring av datorbehandlingsbara uppgifter.

2. För de syften som avses i punkt 1 ovan skall termen barnpornografi innefatta pornografiskt material som visuellt avbildar

a) en minderårig som ägnar sig åt handlande med uttrycklig sexuell innebörd,

b) en person som ser ut att vara en minderårig som ägnar sig åt handlande med uttrycklig sexuell innebörd, och

c) realistiska bilder som föreställer en minderårig som ägnar sig åt handlande med uttrycklig sexuell innebörd.

3. För de syften som avses i punkt 2 ovan skall termen minderårig innefatta alla personer under 18 års ålder. En part får dock kräva en lägre åldersgräns, som inte skall vara lägre än 16 år.

4. Varje part får förbehålla sig rätten att, helt eller delvis, inte tillämpa punkt 1 d—e och punkt 2 b—c i denna artikel.

a) producing child pornography for the purpose of its distribution through a computer system;

b) offering or making available child pornography through a computer system;

c) distributing or transmitting child pornography through a computer system;

d) procuring child pornography through a computer system for oneself or for another person;

e) possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:

a) a minor engaged in sexually explicit conduct;

b) a person appearing to be a minor engaged in sexually explicit conduct;

c) realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Avdelning 4

Brott som hänför sig till intrång i upphovsrätt och närstående rättigheter

Artikel 10

Brott som hänför sig till intrång i upphovsrätt och närstående rättigheter

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga intrång i upphovsrätt, som detta begrepp definieras i den partens lagstiftning, enligt de skyldigheter som parten har iklätt sig enligt Parisbeslutet av den 24 juli 1971 om revidering av Bernkonventionen för skydd av litterära och konstnärliga verk, avtalet om handelsrelaterade aspekter av immaterialrätter och WIPO-fördraget om upphovsrätt, med undantag för ideella rättigheter som erkänns i dessa konventioner, när sådana gärningar begås uppsåtligen, i kommersiell skala och med hjälp av ett datorsystem.

2. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga intrång i närstående rättigheter, som dessa definieras i den partens lagstiftning, enligt de skyldigheter den har iklätt sig enligt konventionen om skydd för utövande konstnärer, framställare av fonogram och radioföretag (Romkonventionen), avtalet om handelsrelaterade aspekter av immaterialrätter, WIPO-fördraget om framföranden och fonogram, med undantag för ideella rättigheter som erkänns i dessa konventioner, när sådana gärningar begås uppsåtligen, i kommersiell skala och med hjälp av ett datorsystem.

3. En part får förbehålla sig rätten att inte införa straffansvar enligt punkterna 1 och 2 i denna artikel i begränsad omfattning, under förutsättning att andra effektiva rättsliga åtgärder kan komma i fråga och att förbehållet inte innebär ett avsteg från partens internationella skyldigheter enligt de internationel-

Title 4

Offences related to infringements of copyright and related rights

Article 10

Offences related to infringements of copyright and related rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the interna-

la instrument som nämns i punkterna 1 och 2 i denna artikel.

Avdelning 5

Andra former av ansvar och påföljder

Artikel 11

Försök och medhjälp

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga uppsåtlig medhjälp till något av de brott som straffbeläggs i enlighet med artiklarna 2—10 i denna konvention med uppsåt att begå sådant brott.

2. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att i sin nationella lagstiftning straffbelägga uppsåtligt försök till något av de brott som straffbeläggs i enlighet med artiklarna 3-5, 7, 8 samt 9.1 a och 9.1 c i denna konvention.

3. Varje part får förbehålla sig rätten att, helt eller delvis, inte tillämpa punkt 2 i denna artikel.

Artikel 12

Juridiska personers ansvar

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att tillse att juridiska personer kan ställas till ansvar för gärningar som straffbeläggs i enlighet med denna konvention, om de har begåtts till deras förmån av en fysisk person som handlat individuellt eller som en del av ett organ tillhörande den juridiska personen och som har en ledande ställning inom denna grundad på

a) en fullmakt att företräda den juridiska personen,

tional 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) ett bemyndigande att fatta beslut på den juridiska personens vägnar, eller

c) ett bemyndigande att utöva kontroll inom den juridiska personen.

2. Utöver de fall som avses i punkt 1 i denna artikel skall varje part vidta nödvändiga åtgärder för att tillse att en juridisk person kan ställas till ansvar när bristande övervakning eller kontroll som skall utföras av en sådan fysisk person som avses i punkt 1 i denna artikel gjort det möjligt för en fysisk person, som handlar på den juridiska personens vägnar, att begå brott som straffbeläggs i enlighet med denna konvention till förmån för den juridiska personen.

3. Beroende på principerna i partens rättsordning, får den juridiska personens ansvar vara av straffrättslig, civilrättslig eller administrativ natur.

4. Sådant ansvar skall inte inverka på straffansvaret för de fysiska personer som har gjort sig skyldiga till gjort sig skyldiga till brottet.

Artikel 13

Påföljder och åtgärder

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att tillse att de brott som straffbeläggs i enlighet med artiklarna 2—11 är straffbara med effektiva, proportionella och avskräckande påföljder, innefattande frihetsberövande.

2. Varje part skall tillse att juridiska personer som fälls till ansvar i enlighet med artikel 12 underkastas effektiva, proportionella och avskräckande straffrättsliga eller icke straffrättsliga påföljder eller åtgärder, innefattande ekonomiska påföljder.

b) an authority to take decisions on behalf of the legal person;

c) an authority to exercise control within the legal person.

2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13

Sanctions and measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Avsnitt 2

Processrätt

Avdelning 1

Gemensamma bestämmelser

Artikel 14

De processrättsliga bestämmelsernas räckvidd

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att fastställa de befogenheter och förfaranden som föreskrivs i denna avdelning för särskilt angivna brottsutredningar eller rättsliga förfaranden.

2. Med undantag för vad som särskilt föreskrivs i artikel 21 skall varje part tillämpa de befogenheter och förfaranden som avses i punkt 1 i denna artikel på

a) brott som straffbeläggs i enlighet med artiklarna 2—11 i dennakonvention,

b) andra brott som begåtts med hjälp av ett datorsystem och

c) insamling av bevis i elektronisk form om ett brott.

3. a) Varje part får förbehålla sig rätten att endast tillämpa de åtgärder som avses i artikel 20 på brott eller brottstyper som anges i förbehållet, under förutsättning att omfattningen av dessa brott eller brottstyper inte är mer begränsad än det urval av brott på vilka parten tillämpar de åtgärder som avses i artikel 21. Varje part skall överväga att begränsa ett sådant förbehåll för att möjliggöra bredast möjliga tillämpning av den åtgärd som avses i artikel 20.

b) När en part till följd av begränsningar i sin vid tiden för antagandet av denna konvention gällande lagstiftning inte kan tillämpa de åtgärder som avses i artiklarna 20

Section 2

Procedural law

Title 1

Common provisions

Article 14

Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a) the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b) other criminal offences committed by means of a computer system; and

c) the collection of evidence in electronic form of a criminal offence.

3. a) Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b) Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20

och 21 på meddelanden som överförs inom en tjänsteleverantörs datorsystem, som

i) drivs för en sluten användargrupp, och

ii) inte använder allmänna kommunikationsnät och inte är anslutet till ett annat datorsystem, oavsett om detta är offentligt eller enskilt,

får den parten förbehålla sig rätten att inte tillämpa dessa åtgärder på sådana meddelanden. Varje part skall överväga att begränsa ett sådant förbehåll för att möjliggöra bredast möjliga tillämpning av de åtgärder som avses i artiklarna 20 och 21.

Artikel 15

Villkor och garantier

1. Varje part skall tillse att det för införandet, genomförandet och tillämpningen av de befogenheter och förfaranden som avses i denna avdelning gäller de villkor och garantier som föreskrivs i dess nationella lagstiftning, vilka skall ge ett tillfredsställande skydd för mänskliga rättigheter och friheter, däribland de rättigheter som följer av de åtaganden parten har gjort genom 1950 års Europarådskonvention om skydd för de mänskliga rättigheterna och de grundläggande friheterna, 1966 års FN-konvention om medborgerliga och politiska rättigheter samt andra tillämpliga internationella fördrag om mänskliga rättigheter, och i vilka proportionalitetsprincipen skall vara införlivad.

2. Sådana villkor och garantier skall, när så är lämpligt med tanke på arten av det förfarande eller den befogenhet det gäller, bl.a. innefatta rättslig eller annan oberoende tillsyn, de skäl som motiverar tillämpning samt begränsning av omfattningen och varaktigheten av befogenheten eller förfarandet.

3. I den utsträckning det är förenligt med allmänintresset, särskilt med sund rättskipning, skall varje part pröva vilken inverkan

and 21 to communications being transmitted within a computer system of a service provider, which system:

i) is being operated for the benefit of a closed group of users, and

ii) does not employ public communications networks and is not connected with another computer system, whether public or private,

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

Article 15

Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall

de befogenheter och förfaranden som avses i denna avdelning har på tredje mans rättigheter, skyldigheter och rättmätiga intressen.

Avdelning 2

Skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter

Artikel 16

Skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att dess behöriga myndigheter genom föreläggande eller på liknande sätt skall kunna åstadkomma skyndsamt säkrande av särskilt angivna datorbehandlingsbara uppgifter, innefattande trafikuppgifter, som har lagrats med hjälp av ett datorsystem, särskilt i de fall där det finns anledning att förmoda att de datorbehandlingsbara uppgifterna löper särskild risk att gå förlorade eller förändras.

2. När en part verkställer punkt 1 i denna artikel genom ett föreläggande till en person om att säkra särskilt angivna lagrade datorbehandlingsbara uppgifter i denna persons besittning eller under denna persons kontroll, skall parten vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att ålägga personen att säkra och bevara de datorbehandlingsbara uppgifterna orubbade så länge som behövs, dock högst 90 dagar, för att göra det möjligt för de behöriga myndigheterna att begära att uppgifterna röjs. En part får föreskriva att ett sådant föreläggande sedan får förnyas.

3. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att ålägga den som har de datorbehandlingsbara uppgifterna i sin vård eller en sådan annan person som skall bevara dem att hemlighålla att sådana åtgärder vidtagits under så lång tid som föreskrivs i dess nationella lagstiftning.

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. Bestämmelserna i artiklarna 14 och 15 skall gälla för de befogenheter och förfaranden som avses i denna artikel.

Artikel 17

Skyndsamt säkrande och partiellt röjande av trafikuppgifter

1. Varje part skall i fråga om trafikuppgifter som skall säkras enligt artikel 16 vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att

a) tillse att ett sådant skyndsamt säkrande av trafikuppgifter kan ske, oavsett om en eller flera tjänsteleverantörer har deltagit i överföringen av meddelandet, och

b) tillse att en tillräcklig mängd trafikuppgifter skyndsamt röjs för partens behöriga myndighet, eller för en person utsedd av denna myndighet, för att parten skall kunna identifiera tjänsteleverantörerna och den väg på vilken meddelandet överfördes.

2. Bestämmelserna i artiklarna 14 och 15 skall gälla för de befogenheter och förfaranden som avses i denna artikel.

Avdelning 3

Skyldighet att lämna uppgifter

Artikel 18

Skyldighet att lämna uppgifter

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att bemyndiga sina behöriga myndigheter att förelägga

a) en person inom dess territorium att lämna ut särskilt angivna datorbehandlingsbara uppgifter som vederbörande har i sin besittning eller under sin kontroll, och som lagras i ett datorsystem eller i ett medium för lagring av datorbehandlingsbara uppgifter, och

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17

Expedited preservation and partial disclosure of traffic data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3

Production order

Article 18

Production order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b) en tjänsteleverantör som erbjuder sina tjänster inom partens territorium att lämna ut abonnentuppgifter som hänför sig till sådana tjänster och som tjänsteleverantören har i sin besittning eller under sin kontroll.

2. Bestämmelserna i artiklarna 14 och 15 skall gälla för de befogenheter och förfaranden som avses i denna artikel.

3. För de syften som avses i denna artikel betyder termen abonnentuppgifter varje information i form av datorbehandlingsbara uppgifter eller uppgifter i annan form som innehas av en tjänsteleverantör och som hänför sig till andra uppgifter om dennes abonnenter än trafikuppgifter eller innehållsuppgifter och genom vilka kan fastställas

a) den typ av kommunikationstjänst som använts, de tekniska åtgärder som vidtagits för dem och tidsperioden för tjänsten,

b) abonnentens identitet, postadress eller geografiska adress, telefonnummer och annat accessnummer, information om fakturering och betalning, som är tillgänglig genom tjänsteavtalet eller tjänstearrangemanget,

c) övriga upplysningar om var kommunikationsutrustningen är belägen som är tillgängliga genom tjänsteavtalet eller tjänstearrangemanget.

Avdelning 4

Husrannsakan och beslag av lagrade datorbehandlingsbara uppgifter

Artikel 19

Husrannsakan och beslag av lagrade datorbehandlingsbara uppgifter

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att bemyndiga sina behöriga myndigheter att genom husrannsakan eller på liknande sätt inom territoriet bereda sig åtkomst till

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

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a) the type of communication service used, the technical provisions taken thereto and the period of service;

b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4

Search and seizure of stored computer data

Article 19

Search and seizure of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a) ett datorsystem eller en del därav och de datorbehandlingsbara uppgifter som lagras däri, och

b) ett medium för lagring av datorbehandlingsbara uppgifter i vilket uppgifter kan vara lagrade.

2. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att tillse att dess myndigheter, när de genom husrannsakan eller på liknande sätt bereder sig åtkomst till ett visst datorsystem eller en del därav enligt punkt 1 a och har anledning att tro att de eftersökta uppgifterna är lagrade i ett annat datorsystem eller en del av ett annat datorsystem inom dess territorium och sådana uppgifter är lagligen åtkomliga eller tillgängliga för det första systemet, skyndsamt skall kunna utvidga husrannsakan eller det liknande sättet till att bereda sig åtkomst till detta andra system.

3. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att bemyndiga sina behöriga myndigheter att beslagta eller på liknande sätt säkra datorbehandlingsbara uppgifter som åtkommits enligt punkterna 1 och 2 i denna artikel. Dessa åtgärder skall innefatta behörighet att

a) beslagta eller på liknande sätt säkra ett datorsystem eller en del därav eller ett medium för lagring av datorbehandlingsbara uppgifter,

b) framställa och behålla en kopia av dessa datorbehandlingsbara uppgifter,

c) bevara de lagrade datorbehandlingsbara uppgifternas integritet,

d) göra de datorbehandlingsbara uppgifterna oåtkomliga eller avlägsna dem från det datorsystem till vilket åtkomst har beretts.

4. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att bemyndiga sina behöriga myndigheter att förelägga en person som har kunskap om ett datorsystems funktion eller om de åtgärder som tillämpas för att skydda de datorbe-

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

handlingsbara uppgifter som finns däri att, i den mån det är skäligt, lämna den information som är nödvändig för att möjliggöra de åtgärder som avses i punkterna 1 och 2 i denna artikel.

5. Bestämmelserna i artiklarna 14 och 15 skall gälla för de befogenheter och förfaranden som avses i denna artikel.

Avdelning 5

Insamling i realtid av datorbehandlingsbara uppgifter

Artikel 20

Insamling i realtid av trafikuppgifter

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att bemyndiga sina behöriga myndigheter att

a) med tekniska hjälpmedel inom partens territorium insamla eller ta upp, och

b) ålägga en tjänsteleverantör, att inom dennes existerande tekniska förmåga

i) att med tekniska hjälpmedel inom partens territorium insamla eller ta upp, eller

ii) att samarbeta med och biträda de behöriga myndigheterna med insamling eller upptagning

av trafikuppgifter i realtid som hör till särskilt angivna meddelanden, som inom partens territorium överförs med hjälp av ett datorsystem.

2. Om en part, beroende på gällande principer i sin nationella rättsordning, inte kan vidta de åtgärder som avses i punkt 1 a i denna artikel, får den i stället vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att med tekniska hjälpmedel inom sitt territorium säkerställa insamling eller upptagning i realtid av trafikuppgifter som hänför sig till särskilt angivna meddelanden

data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5

Real-time collection of computer data

Article 20

Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and

b) compel a service provider, within its existing technical capability:

i) to collect or record through the application of technical means on the territory of that Party; or

ii) to co-operate and assist the competent authorities in the collection or recording of,

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

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

som överförs inom partens territorium.

3. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att ålägga en tjänsteleverantör att hemlighålla det förhållandet att befogenhet som avses i denna artikel utövas och all information som har samband med denna.

4. Bestämmelserna i artiklarna 14 och 15 skall gälla för de befogenheter och förfaranden som avses i denna artikel.

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.

Artikel 21

Avlyssning av innehållsuppgifter

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att, med avseende på vissa allvarliga brott som bestäms i partens nationella lagstiftning, bemyndiga sina behöriga myndigheter att

a) med tekniska hjälpmedel inom partens territorium insamla eller ta upp, och

b) ålägga en tjänsteleverantör, att inom dennes existerande tekniska förmåga

i) att med tekniska hjälpmedel inom partens territorium insamla eller ta upp, eller

ii) att samarbeta med och biträda de behöriga myndigheterna med insamling eller upptagning

i realtid av innehållsuppgifter i särskilt angivna meddelanden inom partens territorium som överförs med hjälp av ett datorsystem.

2. Om en part, beroende på gällande principer i sin nationella rättsordning, inte kan vidta de åtgärder som avses i punkt 1 a ovan, får den i stället vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att med tekniska hjälpmedel inom dess territorium säkerställa insamling eller upptagning i

Article 21

Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and

b) compel a service provider, within its existing technical capability:

i) to collect or record through the application of technical means on the territory of that Party, or

ii) to co-operate and assist the competent authorities in the collection or recording of,

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

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

realtid av innehållsuppgifter i särskilt angivna meddelanden, som överförs inom dess territorium.

3. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att ålägga en tjänsteleverantör att hemlighålla det förhållandet att befogenhet som avses i denna artikel utövas och all information som har samband med denna.

4. Bestämmelserna i artiklarna 14 och 15 skall gälla för de befogenheter och förfaranden som avses i denna artikel.

Avsnitt 3

Domsrätt

Artikel 22

Domsrätt

1. Varje part skall vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att utöva domsrätt över brott som straffbeläggs i enlighet med artiklarna 2—11 i denna konvention, när brottet har begåtts

a) inom dess territorium, eller

b) ombord på ett fartyg som för dess flagg, eller

c) ombord på ett luftfartyg som är registrerat enligt dess lagar, eller

d) av en av dess medborgare, om brottet är straffbart enligt strafflagstiftningen där det begicks eller om brottet inte faller under någon stats territoriella behörighet.

2. Varje part får förbehålla sig rätten att inte alls tillämpa eller att bara i vissa fall och under särskilda förhållanden tillämpa de regler om domsrätt som anges i punkt 1 b - d i denna artikel eller en del av dessa regler.

3. Varje part skall vidta nödvändiga åtgärder för utöva domsrätt över de brott som av-

in its territory through the application of technical means on that territory.

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

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3

Jurisdiction

Article 22

Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a) in its territory; or

b) on board a ship flying the flag of that Party; or

c) on board an aircraft registered under the laws of that Party; or

d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction

ses i artikel 24.1 i denna konvention i de fall då en påstådd gärningsman befinner sig inom dess territorium och parten inte på begäran utlämnar honom eller henne till en annan part endast på grund av hans eller hennes nationalitet.

4. Denna konvention utesluter inte straffrättslig domsrätt som utövas av en part i enlighet med dess nationella lagstiftning.

5. I de fall där mer än en part gör gällande domsrätt över ett påstått brott som straffbeläggs enligt denna konvention, skall de berörda parterna, om så om det är lämpligt, samråda för att avgöra vilken domsrätt som är den lämpligaste för lagföring.

KAPITEL 3

INTERNATIONELLT SAMARBETE

Avsnitt 1

Allmänna principer

Avdelning 1

Allmänna principer för internationellt samarbete

Artikel 23

Allmänna principer för internationellt samarbete

Parterna skall i största möjliga utsträckning samarbeta med varandra i enlighet med bestämmelserna i detta kapitel och genom tillämpning av relevanta internationella instrument om internationellt samarbete i straffrättsliga frågor, gällande överenskommelser som ingåtts på grundval av ensartad eller reciprok lagstiftning samt nationella lagar, för att utreda eller lagföra brott som är relaterade till datorsystem och datorbehandlingsbara uppgifter eller för insamling av bevis i elektronisk form om brott.

over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

CHAPTER III

INTERNATIONAL CO-OPERATION

Section 1

General principles

Title 1

General principles relating to international co-operation

Article 23

General principles relating to international co-operation

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

Avdelning 2

Principer för utlämning

Artikel 24

Utlämning

1. a) Denna artikel tillämpas på utlämning mellan parter för brott som straffbeläggs i enlighet med artiklarna 2—11 i denna konvention, om brotten enligt lagstiftningen i båda de berörda parterna kan bestraffas med frihetsberövande och maximistraffet uppgår till lägst ett år, eller med strängare straff.

b) I de fall där ett annat lägsta straff skall tillämpas enligt en överenskommelse som ingåtts på grundval av ensartad eller reciprok lagstiftning eller ett utlämningsavtal, däribland europeiska utlämningskonventionen (ETS 24), som gäller mellan två eller flera parter, skall det lägsta straff som anges i en sådan överenskommelse eller ett sådant avtal gälla.

2. De brott som avses i punkt 1 i denna artikel skall anses tillhöra de utlämningsbara brotten i ett utlämningsavtal som gäller mellan två eller flera parter. Parterna förbinder sig att ta med sådana brott bland de utlämningsbara brotten i utlämningsavtal som kommer att slutas mellan två eller flera av dem.

3. Om en part som för utlämning ställer som villkor att det finns ett utlämningsavtal mottar en framställning om utlämning från en annan part med vilken den inte har slutit ett sådant avtal, får den betrakta denna konvention som rättslig grund för utlämning för brott som avses i punkt 1 i denna artikel.

4. Parter som för utlämning inte ställer som villkor att utlämningsavtal skall föreligga skall erkänna de brott som avses i punkt 1 i denna artikel som utlämningsbara brott mellan dem.

Title 2

Principles relating to extradition

Article 24

Extradition

1. a) This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b) Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. För utlämning skall gälla de villkor som anges i den anmodade partens lagstiftning eller i gällande utlämningsavtal, däribland de skäl på grund av vilka den anmodade parten får vägra att bevilja utlämning.

6. Om utlämning för brott som avses i punkt 1 i denna artikel vägras endast på grund av den sökta personens nationalitet eller därför att den anmodade parten anser sig ha domsrätt över brottet, skall den anmodade parten efter framställning från den begärande parten hänskjuta ärendet till sina behöriga myndigheter för lagföring och rapportera slutresultatet till den begärande parten i vederbörlig ordning. Myndigheterna skall fatta beslut och genomföra utredningar och lagföring på samma sätt som för andra brott av jämförbar natur enligt den partens lagstiftning.

7. a) Varje part skall vid undertecknandet eller när den deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument meddela Europarådets generalsekreterare namn och adress på de myndigheter som är ansvariga för att göra eller ta emot framställningar om utlämning eller provisoriskt frihetsberövande i avsaknad av avtal.

b) Europarådets generalsekreterare skall upprätta och föra en aktuell förteckning över de myndigheter som utsetts på detta sätt av parterna. Varje part skall tillse att uppgifterna i förteckningen alltid är riktiga.

Avdelning 3

Allmänna principer för ömsesidig rättslig hjälp

Artikel 25

Allmänna principer för ömsesidig rättslig hjälp

1. Parterna skall i största möjliga utsträckning lämna varandra ömsesidig rättslig hjälp för att utreda och lagföra brott som är relaterade till datorsystem och datorbehandlings-

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7. a) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b) The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3

General principles relating to mutual assistance

Article 25

General principles relating to mutual assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences re-

bara uppgifter eller för insamling av bevis i elektronisk form om brott.

2. Varje part skall också vidta nödvändiga lagstiftningsåtgärder och andra åtgärder för att uppfylla åtagandena i artiklarna 27—35.

3. Varje part får i brådskande fall göra framställningar om ömsesidig rättslig hjälp eller sända meddelanden relaterade därtill genom snabba kommunikationsmedel, däribland telefax eller elektronisk post, i den mån sådana medel tillgodoser tillräckliga säkerhetsnivåer och verifiering (däribland användning av kryptering vid behov) med efterföljande formell bekräftelse, i den mån så krävs av den anmodade parten. Den anmodade parten skall godta och besvara framställningar genom sådana snabba kommunikationsmedel.

4. Om inte annat uttryckligen föreskrivs i artiklarna i detta kapitel, skall för ömsesidig rättslig hjälp gälla de villkor som föreskrivs i den anmodade partens lagstiftning eller i tillämpliga avtal om ömsesidig rättslig hjälp, innefattande de skäl på grund av vilka den anmodade parten får avslå en framställning om samarbete. Den anmodade parten får inte vägra rättslig hjälp i fråga om brott som avses i artiklarna 2—11 endast av det skälet att framställningen gäller ett brott som den anser vara ett fiskalt brott.

5. I de fall där den anmodade parten, i enlighet med bestämmelserna i detta kapitel, har rätt att ställa dubbel straffbarhet som villkor för rättslig hjälp, skall det villkoret anses vara uppfyllt, oberoende av om dess lagstiftning placerar brottet inom samma kategori av brott eller rubricerar det med samma termer som den begärande parten, om det handlande som ligger bakom brottet för vilket hjälp har begärts utgör ett brott enligt dess lagstiftning.

lated 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.

Artikel 26

Upplysningar som lämnas på eget initiativ

1. En part får, inom gränserna för sin nationella lagstiftning och utan föregående framställning, överlämna information som erhållits inom ramen för dess egna utredningar till en annan part, när den anser att röjande av sådan information skulle kunna hjälpa den mottagande parten att inleda eller utföra utredningar om och lagföring av brott som är straffbara enligt denna konvention eller som skulle kunna föranleda en framställning av denna part om samarbete med stöd av detta kapitel.

2. Den part som lämnar sådan information får, innan uppgifterna lämnas, begära att de skall hemlighållas eller endast användas på vissa villkor. Om den mottagande parten inte kan tillmötesgå en sådan begäran, skall den meddela den förstnämnda parten, som då skall avgöra om informationen ändå kan överlämnas. Om den mottagande parten tar emot uppgifterna på sådana villkor, är den skyldig att följa dem.

Article 26

Spontaneous information

1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such 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.

Avdelning 4

Förfaranden vid framställningar om ömsesidig rättslig hjälp i avsaknad av tillämpliga internationella avtal

Artikel 27

Förfaranden vid framställningar om ömsesidig rättslig hjälp i avsaknad av tillämpliga internationella avtal

1. Bestämmelserna i punkterna 2—9 i denna artikel skall tillämpas om det saknas gällande avtal eller överenskommelse om ömsesidig rättslig hjälp på grundval av ensartad eller reciprok lagstiftning mellan de berörda parterna. Bestämmelserna i denna artikel skall inte tillämpas när det finns ett sådant avtal, en sådan överenskommelse eller sådan lagstiftning, såvida inte de berörda

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

parterna kommer överens om att tillämpa någon del eller hela återstoden av denna artikel i deras ställe.

2. a) Varje part skall utse en eller flera centralmyndigheter som skall ansvara för att sända och besvara framställningar om ömsesidig rättslig hjälp, verkställa sådana framställningar eller remittera dem till de myndigheter som är behöriga att verkställa dem.

b) Centralmyndigheterna skall kommunicera direkt med varandra.

c) Varje part skall vid undertecknandet eller när den deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument meddela Europarådets generalsekreterare namn och adress på de myndigheter som utses enligt denna punkt.

d) Europarådets generalsekreterare skall upprätta och föra en aktuell förteckning över de centralmyndigheter som utsetts på detta sätt av parterna. Varje part skall tillse att uppgifterna i förteckningen alltid är riktiga.

3. Framställningar om ömsesidig rättslig hjälp enligt denna artikel skall göras i enlighet med det förfarande som anges av den begärande parten, utom när det är oförenligt med den anmodade partens lagstiftning.

4. Den anmodade parten får, utöver de skäl för avslag som anges i artikel 25.4, avslå en framställning om hjälp, om

a) framställningen gäller ett brott som den anmodade parten betraktar som ett politiskt brott eller ett brott med anknytning till ett politiskt brott, eller

b) den anmodade parten anser att verkställande av framställningen sannolikt kan inkräkta på dess suveränitet, säkerhet, allmänna rättsprinciper eller andra viktiga intressen.

5. Den anmodade parten får uppskjuta verkställandet av en framställning

of the remainder of this article in lieu thereof.

2. a) Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b) The central authorities shall communicate directly with each other;

c) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d) The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3. Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4. The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b) it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

5. The requested Party may postpone action on a request if such action would preju-

om det skulle inkräkta på brottsutredningar eller lagföring som utförs av dess myndigheter.

6. Innan den anmodade parten avslår en framställning eller uppskjuter hjälp, skall den, där så är lämpligt efter att ha samrått med den begärande parten, pröva om framställningen kan bifallas till en del eller med förbehåll för sådana villkor som den anmodade parten anser vara nödvändiga.

7. Den anmodade parten skall ofördröjligen underrätta den begärande parten om utfallet av en framställning om hjälp. Skälen för avslag eller uppskjutande av hjälpen skall anges. Den anmodade parten skall också underrätta den begärande parten om de skäl som omöjliggör verkställandet av framställningen eller sannolikt kan försena det avsevärt.

8. Den begärande parten får anhålla om att den anmodade parten hemlighåller att en framställning har gjorts med stöd av detta kapitel liksom dess syfte, utom i den mån det är nödvändigt för dess verkställande att röja uppgiften. Om den anmodade parten inte kan tillmötesgå anhållan om hemlighållande, skall den ofördröjligen meddela den begärande parten, som då skall avgöra om framställningen ändå skall verkställas.

9. a) I brådskande fall får framställningar om ömsesidig rättslig hjälp eller därtill hörande meddelanden sändas direkt av den begärande partens rättsliga myndigheter till motsvarande myndighet i den anmodade parten. I dessa fall skall en kopia samtidigt sändas till den anmodade partens centralmyndighet via den begärande partens centralmyndighet.

b) En framställning eller ett meddelande enligt denna punkt får göras via Internationella kriminalpolisorganisationen (Interpol).

c) Om en framställning görs i enlighet med a i denna punkt och myndigheten inte är behörig att handlägga den, skall den remittera framställningen till behörig nationell

dice criminal investigations or proceedings conducted by its authorities.

6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9. a) In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b) Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c) Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the compe-

myndighet och direkt meddela den begärande parten att så har skett.

d) En framställning eller ett meddelande enligt denna punkt som inte innefattar tvångsåtgärder får sändas direkt av den begärande partens behöriga myndigheter till den anmodade partens motsvarande myndigheter.

e) Varje part får vid undertecknandet av konventionen eller när den deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument meddela Europarådets generalsekreterare att framställningar enligt denna punkt av effektivitetsskäl skall ställas direkt till dess centralmyndighet.

Artikel 28

Sekretess och begränsningar i fråga om användning

1. Bestämmelserna i denna artikel skall tillämpas om det saknas gällande avtal eller överenskommelse om ömsesidig rättslig hjälp på grundval av ensartad eller reciprok lagstiftning mellan de berörda parterna. Bestämmelserna i denna artikel skall inte tillämpas när det finns ett sådant avtal, en sådan överenskommelse eller sådan lagstiftning, såvida inte de berörda parterna kommer överens om att tillämpa någon del eller hela återstoden av denna artikel i deras ställe.

2. Den anmodade parten får göra lämnande av upplysningar eller material som svar på en framställning beroende av att de

a) hemlighålls i de fall framställningen om ömsesidig rättslig hjälp inte kan verkställas om så inte är fallet, eller

b) inte används för andra utredningar eller annan lagföring än som anges i framställningen.

3. Om den begärande parten inte kan uppfylla ett villkor som anges i punkt 2 i denna

tent national authority and inform directly the requesting Party that it has done so.

d) Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

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

Article 28

Confidentiality and limitation on use

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a) kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b) not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2,

artikel, skall den genast meddela den andra parten, som då skall avgöra om upplysningarna ändå kan överlämnas. Om den begärande parten godtar villkoret, är den bunden av det.

4. En part som lämnar upplysningar eller material med ett förbehåll som avses i punkt 2 i denna artikel får begära att den andra parten förklarar hur den har använt upplysningarna eller materialet med avseende på detta villkor.

Avsnitt 2

Särskilda bestämmelser

Avdelning 1

Ömsesidig rättslig hjälp med provisoriska åtgärder

Artikel 29

Skyndsamt säkrande av lagrade datorbehandlingsbara uppgifter

1. En part får anmoda en annan part att genom föreläggande eller på annat sätt åstadkomma skyndsamt säkrande av uppgifter som lagrats med hjälp av ett datorsystem inom den andra partens territorium och beträffande vilka den begärande parten avser att överlämna en framställning om rättslig hjälp med husrannsakan eller motsvarande åtkomst, beslag eller motsvarande säkringsåtgärd eller röjande av uppgifterna.

2. En framställning om säkrande som görs med stöd av punkt 1 i denna artikel skall innehålla följande:

a) Namnet på den myndighet som begär säkrandet.

b) Den gärning som är föremål för brottsutredning eller lagföring och ett sammandrag omständigheterna.

c) De lagrade datorbehandlingsbara uppgifter som skall säkras och deras förhållande till brottet.

it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4. Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2

Specific provisions

Title 1

Mutual assistance regarding provisional measures

Article 29

Expedited preservation of stored computer data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2. A request for preservation made under paragraph 1 shall specify:

a) the authority seeking the preservation;

b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c) the stored computer data to be preserved and its relationship to the offence;

d) Alla tillgängliga upplysningar som identifierar den som vårdar de lagrade datorbehandlingsbara uppgifterna eller var datorsystemet finns.

e) Upplysning om varför säkrandet är nödvändigt.

f) Uppgift om att parten avser att överlämna en framställning om rättslig hjälp med husrannsakan eller motsvarande åtkomst, beslag eller motsvarande säkringsåtgärd eller röjande av de lagrade datorbehandlingsbara uppgifterna.

3. När den anmodade parten mottar en framställning från en annan part, skall den vidta alla lämpliga åtgärder för att skyndsamt säkra de särskilt angivna uppgifterna i enlighet med sin nationella lagstiftning. I fråga om besvarande av en framställning skall dubbel straffbarhet inte uppställas som ett villkor för säkrandet.

4. En part som ställer dubbel straffbarhet som villkor för att besvara en framställning om rättslig hjälp med husrannsakan eller motsvarande åtkomst, beslag eller motsvarande säkringsåtgärd eller röjande av lagrade uppgifter får, med avseende på andra brott än de som straffbeläggs i enlighet med artiklarna 2—11 i denna konvention, förbehålla sig rätten att avslå en framställning om säkrande enligt denna artikel, om den har skäl att tro att villkoret om dubbel straffbarhet inte kan uppfyllas när uppgifterna skall röjas.

5. Härutöver får en framställning om säkrande avslås endast om

a) framställningen gäller ett brott som den anmodade parten betraktar som ett politiskt brott eller ett brott med anknytning till ett politiskt brott, eller

b) den anmodade parten anser att verkställande av framställningen sannolikt kan inkräkta på dess suveränitet, säkerhet, allmänna rättsprinciper eller andra viktiga intressen.

6. Om den anmodade parten anser att säk-

d) any available information identifying the custodian of the stored computer data or the location of the computer system;

e) the necessity of the preservation; and

f) that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5. In addition, a request for preservation may only be refused if:

a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

6. Where the requested Party believes that

rande inte kommer att trygga den framtida tillgängligheten till uppgifterna eller hota sekretessen för, eller på annat sätt störa den begärande partens brottsutredning, skall den ofördröjligen meddela den begärande parten, som då får avgöra om framställningen ändå skall verkställas.

7. Ett säkrande som verkställs som svar på en framställning som avses i punkt 1 i denna artikel skall gälla under en period om minst 60 dagar, för att den begärande parten skall kunna överlämna en framställning om husrannsakan eller liknande åtkomst, beslag eller liknande säkringsåtgärd eller röjande av uppgifterna. Sedan en sådan framställning mottagits, skall uppgifterna bevaras i avvaktan på ett beslut om framställningen.

Artikel 30

Skyndsamt röjande av säkrade trafikuppgifter

1. Om den anmodade parten, vid verkställandet av en framställning enligt artikel 29 om att säkra trafikuppgifter som rör ett särskilt angivet meddelande, upptäcker att en tjänsteleverantör i en annan stat har medverkat i överföring av meddelandet, skall den anmodade parten snabbt röja en tillräcklig mängd trafikuppgifter för den begärande parten för att identifiera tjänsteleverantören och den väg på vilken meddelandet har överförts.

2. Röjande av trafikuppgifter enligt punkt 1 i denna artikel får underlåtas endast om

a) framställningen gäller ett brott som den anmodade parten betraktar som ett politiskt brott eller ett brott med anknytning till ett politiskt brott, eller

b) den anmodade parten anser att verkställande av framställningen sannolikt kan inkräkta på dess suveränitet, säkerhet, allmänna rättsprinciper eller andra viktiga intressen.

preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

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

Article 30

Expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2. Disclosure of traffic data under paragraph 1 may only be withheld if:

a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

Avdelning 2

Ömsesidig rättslig hjälp med utredningsbefogenheter

Artikel 31

Ömsesidig rättslig hjälp med åtkomst till lagrade datorbehandlingsbara uppgifter

1. En part får anmoda en annan part att genom husrannsakan eller på liknande sätt skaffa åtkomst till, genom beslag eller liknande åtgärd säkra eller att röja uppgifter som lagrats med hjälp av ett datorsystem inom den anmodade partens territorium, däribland uppgifter som har säkrats enligt artikel 29.

2. Den anmodade parten skall besvara framställningen med tilllämpning av de internationella instrument, överenskommelser och lagar som avses i artikel 23 och i enlighet med andra tillämpliga bestämmelser i detta kapitel.

3 Framställningen skall besvaras skyndsamt när

a) det finns skäl att tro att uppgifterna i fråga löper särskild risk att gå förlorade eller förändras, eller

b) de instrument, överenskommelser och lagar som avses i punkt 2 i denna artikel på annat sätt föreskriver skyndsamt samarbete.

Artikel 32

Gränsöverskridande åtkomst till lagrade datorbehandlingsbara uppgifter med samtycke eller i de fall de är allmänt tillgängliga

En part får utan tillstånd av en annan part

a) bereda sig åtkomst till lagrade datorbehandlingsbara uppgifter som är allmänt tillgängliga (öppna källor), oavsett var uppgifterna befinner sig geografiskt, eller

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) genom ett datorsystem inom sitt territorium bereda sig åtkomst till eller ta emot lagrade datorbehandlingsbara uppgifter som finns hos en annan part, om den förstnämnda parten erhåller lagligt och frivilligt samtycke av den person som har laglig rätt att röja uppgifterna för parten via det datorsystemet.

Artikel 33

Ömsesidig rättslig hjälp med insamling i realtid av trafikuppgifter

1. Parterna skall lämna varandra rättslig hjälp med insamling i realtid av trafikuppgifter som hör till särskilt angivna meddelanden som överförs med hjälp av ett datorsystem inom deras territorier. Med beaktande av bestämmelserna i punkt 2 i denna artikel, skall för denna hjälp gälla de villkor och förfaranden som anges i den nationella lagstiftningen.

2. Varje part skall lämna sådan hjälp åtminstone med avseende på brott för vilka insamling i realtid av trafikuppgifter skulle vara möjlig i ett motsvarande nationellt fall.

Artikel 34

Ömsesidig rättslig hjälp med avlyssning av innehållsuppgifter

Parterna skall, i den utsträckning det är tillåtet enligt gällande avtal och nationell lagstiftning, lämna varandra rättslig hjälp i fråga om insamling eller upptagning i realtid av innehållsuppgifter i särskilt angivna meddelanden som överförs med hjälp av ett datorsystem.

Avdelning 3

Nätverk (24/7)

Artikel 35

Nätverk (24/7)

1. Varje part skall utse en kontaktpunkt

b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33

Mutual assistance in the real-time collection of traffic data

1. The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34

Mutual assistance regarding the interception of content data

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

Title 3

24/7 Network

Article 35

24/7 Network

1. Each Party shall designate a point of

som skall vara tillgänglig 24 timmar om dygnet sju dagar i veckan för att säkerställa omedelbar hjälp vid utredning och lagföring av brott som är relaterade till datorsystem och datorbehandlingsbara uppgifter eller för insamling av bevis i elektronisk form om brott. Denna hjälp skall innefatta underlättande av eller, om det är tillåtet i partens nationella lagar och praxis, direkt vidtagande av följande åtgärder:

a) tillhandahållande av teknisk rådgivning,

b) säkrande av uppgifter i enlighet med artiklarna 29 och 30, samt

c) insamling av bevis, tillhandahållande av rättslig information och lokalisering av misstänkta.

2. a) En parts kontaktpunkt skall kunna skyndsamt kommunicera med en annan parts kontaktpunkt.

b) Om en parts utsedda kontaktpunkt inte tillhör partens myndighet eller myndigheter som ansvarar för internationell rättslig hjälp eller utlämning, skall kontaktpunkten tillse att den är i stånd att skyndsamt samverka med en eller flera sådana myndigheter.

3. Varje part skall tillse att utbildad och välutrustad personal är tillgänglig för att underlätta nätverkets verksamhet.

KAPITEL IV

SLUTBESTÄMMELSER

Artikel 36

Undertecknande och ikraftträdande

1. Denna konvention skall stå öppen för undertecknande av Europarådets medlemsstater och de icke-medlemsstater som har deltagit i utarbetandet av konventionen.

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 coordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

CHAPTER IV

FINAL PROVISIONS

Article 36

Signature and entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2. Denna konvention skall ratificeras, godtas eller godkännas. Ratifikations-, godtagande- eller godkännandeinstrument skall deponeras hos Europarådets generalsekreterare.

3. Denna konvention träder i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då fem stater, varav minst tre medlemsstater i Europarådet, har uttryckt sitt samtycke till att vara bundna av konventionen i enlighet med bestämmelserna i punkterna 1 och 2 i denna artikel.

4. För en signatärstat som senare uttrycker sitt samtycke till att vara bunden av konventionen träder denna i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då den har uttryckt sitt samtycke till att vara bunden av konventionen i enlighet med bestämmelserna i punkterna 1 och 2 ovan.

Artikel 37

Anslutning till konventionen

1. Efter det att det att denna konvention har trätt i kraft kan Europarådets ministerkommitté efter samråd med konventionsstaterna och med deras enhälliga samtycke inbjuda en stat som inte är medlem av Europarådet och som inte har deltagit i konventionens utarbetande att ansluta sig till konventionen. Beslutet skall fattas med den majoritet som anges i artikel 20 d i Europarådets stadga och i enhällighet av ombuden för de konventionsstater som är berättigade att delta i ministerkommittén.

2. För en stat som ansluter sig till konventionen enligt punkt 1 ovan träder den i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter dagen för deponeringen av anslutningsinstrumentet hos Europarådets generalsekreterare.

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.

Artikel 38

Territoriell tillämpning

1. En stat kan när den undertecknar konventionen eller deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument ange för vilket eller vilka territorier konventionen skall gälla.

2. En stat kan vid en senare tidpunkt genom en förklaring ställd till Europarådets generalsekreterare utsträcka tillämpningen av konventionen till ett annat territorium som anges i förklaringen. I förhållande till ett sådant territorium träder konventionen i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då generalsekreteraren mottog förklaringen.

3. En förklaring som avgivits enligt de båda föregående punkterna kan, med avseende på ett territorium som har angivits i förklaringen, återtas genom ett meddelande ställt till Europarådets generalsekreterare. Återtagandet börjar gälla den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då generalsekreteraren mottog meddelandet.

Article 38

Territorial application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Artikel 39

Konventionens verkan

1. Konventionens syfte är att komplettera tillämpliga multilaterala eller bilaterala fördrag eller överenskommelser mellan parterna, däribland bestämmelserna i följande instrument:

— Europeiska utlämningskonventionen, öppnad för undertecknande i Paris den 13 december 1957 (ETS nr 24).

— Europeiska konventionen om inbördes rättshjälp i brottmål, öppnad för undertecknande i Strasbourg den 20 april 1959 (ETS nr 30).

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);

— Tilläggsprotokollet till europeiska konventionen om inbördes rättshjälp i brottmål, öppnad för undertecknande i Strasbourg den 17 mars 1978 (ETS nr 99).

2. Om två eller flera parter redan har ingått en överenskommelse eller slutit ett fördrag om frågor som behandlas i denna konvention eller på annat sätt reglerat sina inbördes förhållanden beträffande sådana frågor, eller om de i framtiden gör det, skall de också ha rätt att tillämpa överenskommelsen eller fördraget i fråga eller att reglera sina förhållanden i enlighet därmed. Om parter emellertid reglerar sina förhållanden beträffande frågor som behandlas i konventionen på annat sätt än det som regleras häri, skall de göra detta på ett sätt som inte är oförenligt med konventionens syften och principer.

3. Ingenting i konventionen skall inverka på en parts övriga rättigheter, begränsningar, skyldigheter eller ansvar.

Artikel 40

Förklaringar

En stat får vid undertecknandet eller när den deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument, genom ett skriftligt meddelande ställt till Europarådets generalsekreterare meddela att den begagnar sig av möjligheten att kräva ytterligare rekvisit enligt vad som anges i artiklarna 2, 3, 6.1 b, 7, 9.3 och 27.9 e.

Artikel 41

Tillämpning på federala stater

1. En federal stat får förbehålla sig rätten att åta sig skyldigheter enligt kapitel II i konventionen som är förenliga med grundprinciperna för förhållandet mellan dess centralregering och delstaterna och andra liknande territoriella enheter under förutsättning att den fortfarande kan samarbeta enligt kapitel III.

— the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40

Declarations

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

Article 41

Federal clause

1. A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2. När en federal stat gör ett förbehåll enligt punkt 1, får den inte tillämpa villkoren i förbehållet för att undanta eller väsentligen minska sina skyldigheter att vidta åtgärder enligt kapitel II. Den skall generellt sörja för vidsträckta och effektiva rättsliga medel för att de åtgärder som avses i kapitel II skall kunna verkställas.

3. Med avseende på de bestämmelser i denna konvention vilkas tillämpning faller under behörigheten hos delstaterna eller andra territoriella enheter, vilka inte enligt federationens konstitutionella system är skyldiga att vidta lagstiftningsåtgärder, skall den federala regeringen underrätta delstaternas behöriga myndigheter om bestämmelserna med sin välvilliga rekommendation och uppmana dem att vidta lämpliga åtgärder för att ge bestämmelserna verkan.

Artikel 42

Förbehåll

En stat får när den undertecknar konventionen eller deponerar sitt ratifikations-, godtagande-, godkännande- eller anslutningsinstrument genom ett skriftligt meddelande ställt till Europarådets generalsekreterare förklara att den begagnar sig av de möjligheter att göra förbehåll som anges i artiklarna 4.2, 6.3, 9.4, 10.3, 11.3, 14.3, 22.2, 29.4 och 41.1. Inget annat förbehåll får göras.

Artikel 43

Förbehållens status och återtagande

1. En part som har gjort ett förbehåll i enlighet med artikel 42 får helt eller delvis återta det genom ett meddelande till Europarådets generalsekreterare. Återtagandet börjar gälla den dag då generalsekreteraren mottog meddelandet. Om det i meddelandet anges att återtagandet av ett förbehåll skall börja gälla den dag som anges i meddelandet och denna dag infaller senare än den dag

2. When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3. With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42

Reservations

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

Article 43

Status and withdrawal of reservations

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date

då generalsekreteraren mottog meddelandet, skall återtagandet gälla från den senare dagen.

2. En part som har gjort ett förbehåll som avses i artikel 42 skall återta detta, helt eller delvis, så snart som omständigheterna så medger.

3. Europarådets generalsekreterare får regelbundet fråga parter som har gjort ett eller flera förbehåll som avses i artikel 42 om möjligheterna att de återtar dem.

Artikel 44

Ändringar

1. Ändringar i denna konvention får föreslås av en part och skall av Europarådets generalsekreterare meddelas dess medlemsstater, de icke-medlemsstater som har deltagit i utarbetandet av konventionen samt stater som har anslutit sig till eller inbjudits att ansluta sig till konventionen i enlighet med bestämmelserna i artikel 37.

2. Ändringsförslag från en part skall tillställas Europarådets kommitté för brottsfrågor, som skall avge yttrande över den föreslagna ändringen till ministerkommittén.

3. Ministerkommittén skall överväga den föreslagna ändringen och kommitténs för brottsfrågor yttrande och får, efter samråd med de icke-medlemsstater som är parter i konventionen, anta ändringen.

4. Text till ändringar som har antagits av ministerkommittén i enlighet med punkt 3 i denna artikel skall meddelas parterna för godtagande.

5. En ändring som har antagits i enlighet med punkt 3 i denna artikel skall träda i

specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3. The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44

Amendments

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5. Any amendment adopted in accordance with paragraph 3 of this article shall come

kraft den trettionde dagen efter det att samtliga parter har meddelat generalsekreteraren sitt godtagande av ändringen.

Artikel 45

Tvistlösning

1. Europarådets kommitté för brottsfrågor skall hållas underrättad om tolkningen och tillämpningen av konventionen.

2. Om en tvist skulle uppstå mellan parter om tolkningen eller tillämpningen av denna konvention, skall de söka lösa tvisten genom förhandling eller andra fredliga medel efter deras eget val, inbegripet hänskjutande av tvisten till Europarådets kommitté för brottsfrågor, till en skiljedomstol vars avgöranden skall vara bindande för parterna, eller till Internationella domstolen, efter överenskommelse mellan de berörda parterna.

Artikel 46

Samråd mellan parterna

1. Parterna skall på lämpligt sätt regelbundet samråda i syfte att underlätta följande:

a) konventionens faktiska tillämpning och genomförande, innefattande identifiering av problem på området liksom verkan av förklaringar eller förbehåll som gjorts enligt konventionen,

b) informationsutbyte om rättslig, politisk eller teknisk utveckling av betydelse på området för IT-relaterade brott och bevisinsamling i elektronisk form,

c) prövning av möjliga tillägg till och ändringar av konventionen.

2. Europarådets kommitté för brottsfrågor skall fortlöpande informeras om utfallet av det samråd som avses i punkt 1ovan.

3. Europarådets kommitté för brottsfrågor skall på lämpligt sätt främja samråd som av-

into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45

Settlement of disputes

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46

Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

a) the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b) the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c) consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The CDPC shall, as appropriate, facilitate the consultations referred to in para-

ses i punkt 1 i denna artikel och vidta nödvändiga åtgärder för att biträda parterna i deras strävanden att komplettera eller ändra konventionen. Senast tre år efter konventionens ikraftträdande skall Europarådets kommitté för brottsfrågor i samarbete med parterna genomföra en granskning av konventionens samtliga bestämmelser och, vid behov, rekommendera lämpliga ändringar.

4. Utom i de fall de bärs av Europarådet, skall kostnader som uppstår vid genomförandet av bestämmelserna i punkt 1 ovan bäras av parterna på ett sätt som de skall komma överens om.

5. Parterna skall biträdas av Europarådets sekretariat i att utföra sina funktioner enligt denna artikel.

graph 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.

Artikel 47

Uppsägning

1. En part får när som helst säga upp konventionen genom ett meddelande ställt till Europarådets generalsekreterare.

2. Uppsägningen börjar gälla den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då generalsekreteraren mottog meddelandet.

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.

Artikel 48

Meddelanden

Europarådets generalsekreterare skall meddela medlemsstaterna, de icke-medlemsstater som har deltagit i utarbetandet av konventionen och de stater som har anslutit sig till den eller inbjudits att ansluta sig till den om

a) undertecknanden,

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) deponering av ratifikations-, godtagande-, godkännande- och anslutningsinstrument,

c) dag för konventionens ikraftträdande enligt artiklarna 36 och 37,

d) förklaringar enligt artikel 40 eller förbehåll enligt artikel 42,

e) andra handlingar, underrättelser eller meddelanden som rör konventionen.

Till bekräftelse härav har undertecknade, därtill vederbörligen bemyndigade, undertecknat denna konvention.

Upprättad i Budapest den 23 november 2001 på engelska och franska, vilka båda texter är lika giltiga, i ett enda exemplar, som skall deponeras i Europarådets arkiv. Europarådets generalsekreterare skall översända bestyrkta kopior till varje medlemsstat i Europarådet, de icke-medlemsstater som har deltagit i utarbetandet av konventionen och till de stater som har inbjudits att ansluta sig till den.

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.

RÅDETS RAMBESLUT

2005/222/RIF

av den 24 februari 2005

om angrepp mot informationssystem

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA RAMBESLUT

med beaktande av Fördraget om Europeiska unionen, särskilt artiklarna 29, 30.1 a, 31.1 e och 34.2 b i detta,

med beaktande av kommissionens förslag,

med beaktande av Europaparlamentets yttrande [(1)], och

av följande skäl:

(1) Syftet med detta rambeslut är att förbättra samarbetet mellan rättsliga och andra behöriga myndigheter, inbegripet polismyndigheter och andra specialiserade brottsbekämpande organ i medlemsstaterna, genom tillnärmning av medlemsstaternas strafflagstiftning på området för angrepp mot informationssystem.

(2) Det har konstaterats att det förekommer angrepp mot informationssystem, särskilt till följd av hotet från den organiserade brottsligheten, och det finns en stigande oro för terroristattacker mot de informationssystem som ingår i medlemsstaternas vitala infrastruktur. Detta utgör ett hot mot skapandet av ett säkrare informationssamhälle och ett område med frihet, säkerhet och rättvisa och kräver därför motåtgärder på EU-nivå.

(3) Ett effektivt svar på dessa hot kräver en samlad syn på nät- och informationssäkerhet, vilket betonas i handlingsplanen Europe, i kommissionens meddelande ”Nät- och informationssäkerhet: förslag till en europeisk strategi” och i rådets resolution av den 28 januari 2002 om en gemensam inställning och särskilda åtgärder på området för nät- och informationssäkerhet[(2)].

(4) Behovet av att ytterligare öka medvetenheten om problemen som har att göra med informationssäkerhet och ge praktisk hjälp har också betonats i Europaparlamentets resolution av den 5 september 2001.

(5) Stora klyftor och skillnader i medlemsstaternas lagstiftning på detta område kan försvåra kampen mot organiserad brottslighet och terrorism och komplicera ett effektivt polisiärt och rättsligt samarbete när det gäller angrepp mot informationssystem. De moderna informationssystemens nationsöverskridande och gränslösa karaktär innebär att angrepp mot sådana system ofta är gränsöverskridande, vilket understryker det trängande behovet av ytterligare insatser för att tillnärma strafflagstiftningen på detta område.

---

(1) EUT C 300 E, 11.12.2003, s. 26.
(2) EGT C 43, 16.2.2002, s. 2.

(6) Rådets och kommissionens handlingsplan för att på bästa sätt genomföra bestämmelserna i Amsterdamfördraget om upprättande av ett område med frihet, säkerhet och rättvisa[1], Europeiska rådet i Tammerfors den 15–16 oktober 1999, Europeiska rådet i Santa Maria da Feira den 19–20 juni 2000, kommissionen i ”Resultattavlan” och Europaparlamentet i sin resolution av den 19 maj 2000 anger eller uppmanar till lagstiftningsåtgärder mot högteknologisk brottslighet, inklusive gemensamma definitioner, kriminaliseringar och påföljder.

(7) Det arbete som utförs av internationella organisationer, särskilt Europarådets insatser för tillnärmning av strafflagstiftning och G8:s arbete för gränsöverskridande samarbete på området för högteknologisk brottslighet, måste kompletteras genom att det fastställs en gemensam strategi på detta område inom Europeiska unionen. Detta krav utvecklades ytterligare i kommissionens meddelande till rådet, Europaparlamentet, Ekonomiska och sociala kommittén och Regionkommittén ”Ett säkrare informationssamhälle – ökad säkerhet i informationsinfrastrukturen och bekämpning av datorrelaterad brottslighet”.

(8) Strafflagstiftningen om angrepp mot informationssystem bör tillnärmas i syfte att få till stånd största möjliga polisiära och rättsliga samarbete när det gäller brott som hänför sig till angrepp mot informationssystem och att bidra till kampen mot organiserad brottslighet och terrorism.

(9) Alla medlemsstater har ratificerat Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter. Personuppgifter som behandlas i samband med genomförandet av detta rambeslut bör skyddas i enlighet med principerna i den nämnda konventionen.

(10) Gemensamma definitioner på detta område, särskilt av informationssystem och datorbehandlingsbara uppgifter, betyder mycket för att säkra att detta rambeslut tillämpas enhetligt i medlemsstaterna.

(11) Det finns ett behov av att fastställa en gemensam inställning i fråga om brottsrekvisit, genom att gemensamt kriminalisera olagligt intrång i informationssystem, olaglig systemstörning och olaglig datastörning.

(12) För att kunna bekämpa IT-relaterad brottslighet bör varje medlemsstat säkerställa effektivt rättsligt samarbete avseende brott vilka bygger på de typer av handlande som avses i artiklarna 2, 3, 4 och 5.

(13) Det finns ett behov av att undvika att kriminaliseringen går för långt, särskilt i fråga om ringa fall, liksom att undvika att kriminalisera rättighetshavare och behöriga personer.

(14) Det finns ett behov av att medlemsstaterna föreskriver påföljder för angrepp mot informationssystem. Dessa påföljder skall vara effektiva, proportionella och avskräckande.

(15) Det är lämpligt att föreskriva strängare påföljder när ett angrepp mot ett informationssystem sker inom ramen för en sådan kriminell organisation som avses i gemensam åtgärd 98/733/RIF av den 21 december 1998 om att göra deltagande i en kriminell organisation i Europeiska unionens medlemsstater till ett brott [2]. Det är också lämpligt att föreskriva strängare påföljder när ett sådant angrepp har orsakat allvarliga skador eller har påverkat väsentliga intressen.

---

(1) EGT C 19, 23.1.1999, s. 1.
(2) EGT L 351, 29.12.1998, s. 1.

(16) Åtgärder bör även förutses för samarbete mellan medlemsstaterna, i syfte att säkra effektiva insatser mot angrepp mot informationssystem. Medlemsstaterna bör därför för utbyte av uppgifter använda sig av det befintliga nät med operativa kontaktpunkter som omnämns i rådets rekommendation av den 25 juni 2001 om kontaktpunkter som upprätthåller ett öppethållande dygnet runt för bekämpning av högteknologisk brottslighet [1].

(17) Eftersom målen för detta rambeslut, nämligen att se till att angrepp mot informationssystem i medlemsstaterna blir föremål för effektiva, proportionella och avskräckande straffrättsliga påföljder och att förbättra och uppmuntra rättsligt samarbete genom att undanröja eventuella komplikationer, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna, då bestämmelserna måste vara gemensamma och förenliga med varandra, och de därför bättre kan uppnås på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i EG-fördraget. I enlighet med proportionalitetsprincipen i samma artikel går detta rambeslut inte utöver vad som är nödvändigt för att uppnå dessa mål.

(18) I detta rambeslut respekteras de grundläggande rättigheter och iakttas de principer som erkänns genom artikel 6 i fördraget om Europeiska unionen och återspeglas i Europeiska unionens stadga om de grundläggande rättigheterna, framför allt i kapitlen II och VI i denna.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Definitioner

I detta rambeslut används följande beteckningar med de betydelser som här anges:

a) informationssystem: en apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av datorbehandlingsbara uppgifter, samt datorbehandlingsbara uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av dessa för att de skall kunna drivas, användas, skyddas och underhållas.

b) datorbehandlingsbara uppgifter: framställning av fakta, information eller begrepp i en form som lämpar sig för behandling i ett informationssystem, inklusive program som lämpar sig för att få ett informationssystem att utföra en viss uppgift.

c) juridisk person: enhet som har sådan status enligt tillämplig lagstiftning, med undantag av stater eller andra offentliga organ vid utövandet av de befogenheter som de har i egenskap av statsmakter samt internationella offentliga organisationer.

d) orättmätigt: intrång eller störning som sker utan tillstånd från ägaren eller annan rättighetshavare till systemet eller del av detta eller som inte medges i den nationella lagstiftningen.

Artikel 2

Olagligt intrång i informationssystem

1. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att straffbelägga uppsåtligt orättmätigt intrång i ett informationssystem som helhet eller en del av ett sådant system, åtminstone i fall som inte är ringa.

2. Varje medlemsstat får besluta att det handlande som avses i punkt 1 skall kriminaliseras endast när brottet begås genom intrång i en säkerhetsåtgärd.

(1) EGT C 187, 3.7.2001, s. 5.

Artikel 3

Olaglig systemstörning

Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att det är straffbart att uppsåtligen allvarligt hindra eller avbryta driften av ett informationssystem genom att mata in, överföra, skada, radera, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter, när gärningen utförs orättmätigt, åtminstone i fall som inte är ringa.

Artikel 4

Olaglig datastörning

Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att det är straffbart att uppsåtligen radera, skada, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem, när gärningen utförs orättmätigt, åtminstone i fall som inte är ringa.

Artikel 5

Anstiftan, medhjälp och försök

1. Varje medlemsstat skall straffbelägga anstiftan av och medhjälp till brott som avses i artiklarna 2, 3 och 4.

2. Varje medlemsstat skall straffbelägga försök till de brott som avses i artiklarna 2, 3 och 4.

3. Varje medlemsstat får besluta att inte tillämpa punkt 2 för de brott som avses i artikel 2.

Artikel 6

Påföljder

1. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 2, 3, 4 och 5 är belagda med effektiva, proportionella och avskräckande straffrättsliga påföljder.

2. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att de brott som avses i artiklarna 3 och 4 är belagda med straffrättsliga påföljder som innebär ett maximistraff på minst ett till tre års fängelse.

Artikel 7

Försvårande omständigheter

1. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att det brott som avses i artikel 2.2 och de brott som avses i artiklarna 3 och 4 är belagda med straffrättsliga påföljder som innebär ett maximistraff på minst två till fem års fängelse, när de begås inom ramen för en sådan kriminell organisation som avses i gemensam åtgärd 98/733/RIF, oberoende av den påföljdsnivå som anges i den gemensamma åtgärden.

2. En medlemsstat får även vidta de åtgärder som avses i punkt 1, när brottet har orsakat allvarliga skador eller påverkat väsentliga intressen.

Artikel 8

Juridiska personers ansvar

1. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att juridiska personer kan ställas till ansvar för brott som avses i artiklarna 2, 3, 4 och 5 och som begås till deras förmån av en person som agerar antingen enskilt eller som en del av den juridiska personens organisation och har en ledande ställning inom den juridiska personen, grundad på

a) befogenhet att företräda den juridiska personen, eller

b) befogenhet att fatta beslut på den juridiska personens vägnar, eller

c) befogenhet att utöva kontroll inom den juridiska personen.

2. Utöver de fall som anges i punkt 1 skall medlemsstaterna se till att en juridisk person

kan ställas till ansvar när brister i övervakning eller kontroll som skall utföras av en sådan person som avses i punkt 1 har gjort det möjligt för en person som är underställd den juridiska personen att till förmån för denna juridiska person begå de brott som avses i artiklarna 2, 3, 4 och 5.

3. En juridisk persons ansvar enligt punkterna 1 och 2 skall inte utesluta lagföring av fysiska personer som är gärningsmän vid, anstiftare av eller medhjälpare till de brott som avses i artiklarna 2, 3, 4 och 5.

Artikel 9

Påföljder för juridiska personer

1. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att en juridisk person som har fällts till ansvar i enlighet med artikel 8.1 kan bli föremål för effektiva, proportionella och avskräckande påföljder, som skall innefatta bötesstraff eller administrativa avgifter och som får innefatta andra påföljder, som

a) fråntagande av rätt till offentliga förmåner eller stöd,

b) tillfälligt eller permanent näringsförbud,

c) rättslig övervakning, eller d) rättsligt beslut om upplösning av verksamheten.

2. Varje medlemsstat skall vidta de åtgärder som är nödvändiga för att se till att en juridisk person som har fällts till ansvar i enlighet med artikel 8.2 kan bli föremål för effektiva, proportionella och avskräckande påföljder eller åtgärder.

Artikel 10

Behörighet

1. Varje medlemsstat skall fastställa sin behörighet beträffande de brott som avses i artiklarna 2, 3, 4 och 5, när brottet har begåtts

a) helt eller delvis på dess territorium, eller

b) av en av dess medborgare, eller

c) till förmån för en juridisk person som har sitt huvudkontor på medlemsstatens territorium.

2. Varje medlemsstat skall vid fastställandet av sin behörighet enligt punkt 1 a se till att behörigheten innefattar fall där

a) brottslingen är fysiskt närvarande på medlemsstatens territorium när brottet begås, oavsett om brottet riktar sig mot ett informationssystem på denna medlemsstats territorium eller inte, eller

b) brottet riktar sig mot ett informationssystem på medlemsstatens territorium, oavsett om brottslingen är fysiskt närvarande på detta territorium när brottet begås eller inte.

3. En medlemsstat som enligt sin lagstiftning ännu inte utlämnar eller överlämnar sina egna medborgare skall vidta de åtgärder som är nödvändiga för att fastställa sin behörighet i fråga om och, när det är lämpligt, väcka åtal för de brott som avses i artiklarna 2, 3, 4 och 5, när de har begåtts av en av landets medborgare utanför landets territorium.

4. När ett brott faller under fler än en medlemsstats behörighet och vilken som helst av dessa stater kan lagföra brottet på grundval av samma omständigheter, skall de berörda medlemsstaterna samarbeta för att avgöra vilken av dem som skall lagföra brottslingarna, för att, om möjligt, centralisera lagföringen till en enda medlemsstat. I detta syfte kan medlemsstaterna anlita de organ eller mekanismer som inrättats inom Europeiska unionen för att underlätta samarbetet mellan deras rättsliga myndigheter och samordningen av deras verksamhet. Följande omständigheter får beaktas i successiv ordning:

— Medlemsstaten skall vara den inom vars territorium brotten har begåtts enligt punkt 1 a och punkt 2.

— Medlemsstaten skall vara den i vilken gärningsmannen är medborgare.

— Medlemsstaten skall vara den på vars territorium gärningsmannen påträffats.

5. En medlemsstat får besluta att inte eller endast i särskilda fall eller under särskilda omständigheter tillämpa de bestämmelser om behörighet som anges i punkt 1 b och 1 c.

6. Medlemsstaterna skall underrätta rådets generalsekretariat och kommissionen när de beslutar att tillämpa punkt 5, i förekommande fall med uppgift om i vilka särskilda fall eller under vilka särskilda omständigheter beslutet gäller.

Artikel 11

Utbyte av uppgifter

1. 1För utbyte av uppgifter om de brott som avses i artiklarna 2, 3, 4 och 5 skall medlemsstaterna, med iakttagande av bestämmelser om dataskydd, säkerställa att de använder det befintliga nät med operativa kontaktpunkter som kan nås dygnet runt alla dagar i veckan.

2. Varje medlemsstat skall underrätta rådets generalsekretariat och kommissionen om sin utsedda kontaktpunkt för utbyte av uppgifter om brott som avser angrepp mot informationssystem. Generalsekretariatet skall vidarebefordra dessa uppgifter till de andra medlemsstaterna.

Artikel 12

Genomförande

1. Medlemsstaterna skall vidta de åtgärder som är nödvändiga för att följa bestämmelserna i detta rambeslut senast den 16 mars 2007.

2. Senast den 16 mars 2007 skall medlemsstaterna till rådets generalsekretariat och kommissionen överlämna texten till bestämmelser genom vilka de skyldigheter som ålagts dem enligt detta rambeslut införlivas med deras nationella lagstiftning. Senast den 16 september 2007 skall rådet, på grundval av en rapport som skall utarbetas utifrån information och en skriftlig rapport från kommissionen, bedöma i vilken utsträckning medlemsstaterna har följt bestämmelserna i detta rambeslut.

Artikel 13

Ikraftträdande

Detta rambeslut träder i kraft samma dag som det offentliggörs i Europeiska unionens officiella tidning.

Utfärdat i Bryssel den 24 februari 2005.

På rådets vägnar
N. SCHMIT
Ordförande