

TYÖRYHMÄMIETINTÖ 2003:6

*Tietoverkkorikostyöryhmän  
mietintö*



# KUVAILELEHTI

## OIKEUSMINISTERIÖ

Julkaisun päivämäärä  
16.6.2003

Tekijät (toimielimestä: toimielimen nimi, puheenjohtaja, sihteeri)		Julkaisun laji Työryhmän mietintö	
Tietoverkkorikostyöryhmä Puheenjohtaja: lainsäädäntöjohtaja Jan Törnqvist Sihteeri: lainsäädäntöneuvos Riku Ahola		Toimeksiantaja Oikeusministeriö	
		Toimielimen asettamispäivä 10.12.2002	
Julkaisun nimi Tietoverkkorikostyöryhmän mietintö			
Tiivistelmä			
<p>Työryhmän mietintö sisältää ehdotuksen hallituksen esitykseksi eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen hyväksymisestä sekä rikoslain, pakkokeinolain, esitutkintalain ja kansainvälisestä oikeusavusta rikosasioissa annetun lain muuttamisesta.</p> <p>Mietintöön sisältyvässä esitysluonnoksessa ehdotetaan, että eduskunta hyväksyy yleissopimuksen sekä antaa suostumuksensa eräiden yleissopimuksen nojalla annettavien selitysten ja varaumien tekemiseen. Esitysluonnokseen sisältyy lakiehdotus yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.</p> <p>Esitysluonnoksessa ehdotetaan, että rikoslakiin, pakkokeinolakiin, esitutkintalakiin ja kansainvälisestä oikeusavusta rikosasioissa annettuun lakiin tehdään yleissopimuksen voimaansaattamisesta johtuvat muutokset. Rikoslakiin lisätään uudet tietojärjestelmän häirintää ja tietoverkkorikosvälineen hallussapitoa koskevat säännökset. Tietoverkkorikosvälineen levittämisen osalta nykyinen sääntely laajennetaan kattamaan tietokonevirusten ja muiden vastaavien haittaohjelmien lisäksi myös tietomurtovälineet ja laitteet. Eräiden sopimuksessa tarkoitettujen rikosten yritys säädetään rangaistavaksi. Yhteisövastuu laajennetaan sopimuksen edellyttämällä tavalla. Pakkokeinolakiin lisätään uudet datan takavarikko, säilyttämismääräystä ja tietojärjestelmän haltijan tietojenantovelvollisuutta koskevat säännökset. Esitutkintalakiin lisätään säännös, jonka mukaan todistaja on velvollinen esittämään hallussaan olevan datan tai muun todistusaineiston. Lakiin kansainvälisestä oikeusavusta rikosasioissa tehdään muutos, jonka mukaan datan säilyttämismääräystä koskevan oikeusapupyynnön osalta ei edellytetä kaksoisrangaistavuutta. Lisäksi esitysluonnoksessa ehdotetaan eräitä muita vähäisiä lakimuutoksia, jotka ovat luonteeltaan lähinnä teknisiä.</p>			
Avainsanat: (asiasanat) tietotekniikkarikos, esitutkinta, pakkokeino, rikoksen johdosta tapahtuva luovuttaminen, kansainvälinen oikeusapu			
Muut tiedot HARE OM 029:00/2002			
Sarjan nimi ja numero Oikeusministeriön työryhmämietintöjä 2003:6		ISSN 1458-6452	ISBN 952-466-153-5
Kokonaissivumäärä 166	Kieli suomi	Hinta	Luottamuksellisuus julkinen
Jakaja Edita Prima Oy		Kustantaja Oikeusministeriö	

## PRESENTATIONSBLAD

JUSTITIEMINISTERIET

Utgivningsdatum 17.6.2003

Författare (uppgifter om organet: organets namn, ordförande, sekreterare)		Typ av publikation Arbetsgruppsbetänkande	
Arbetsgruppen för IT-brottslighet Ordförande: lagstiftningsdirektör Jan Törnqvist Sekreterare: lagstiftningsrådet Riku Ahola		Uppdragsgivare Justitieministeriet	
		Datum då organet tillsattes 10.12.2002	
Publikation (även den finska titeln) Tietoverkkorikostyöryhmän mietintö Betänkande av arbetsgruppen för IT-brottslighet			
Referat Arbetsgruppens betänkande innehåller ett förslag till en regeringsproposition till riksdagen om godkännande av den Europarådskonvention som gäller IT-brottslighet och om ändring av strafflagen, tvångsmedelslagen, förundersökningslagen och lagen om internationell rättshjälp i straffrättsliga ärenden.  I det utkast till proposition som ingår i betänkandet föreslås att riksdagen godkänner konventionen och ger sitt samtycke till att vissa förklaringar och reservationer avges med stöd av den. Propositionsutkastet innehåller ett förslag till lag om sättande i kraft av de bestämmelser i konventionen som hör till området för lagstiftningen.  I propositionsutkastet föreslås att i strafflagen, tvångsmedelslagen, förundersökningslagen och lagen om internationell rättshjälp i straffrättsliga ärenden görs de ändringar som följer av konventionens ikraftträdande. Till strafflagen fogas nya bestämmelser om störande av informationssystem och innehav av hjälpmedel vid IT-brott. När det gäller spridning av hjälpmedel vid IT-brott utvidgas den gällande regleringen så att den omfattar inte bara datavirus och andra motsvarande program utan också hjälpmedel som används vid dataintrång samt utrustning. Försök till vissa av de brott som avses i konventionen kriminaliseras. Samfundsansvaret utvidgas så som konventionen förutsätter. Till tvångsmedelslagen fogas nya bestämmelser om beslag av data, förordnande att bevara data och skyldighet för den som innehar ett informationssystem att lämna uppgifter. Till förundersökningslagen fogas en bestämmelse om skyldighet för ett vittne att förete data eller annat bevismaterial som vittnet har i sin besittning. I lagen om internationell rättshjälp i straffrättsliga ärenden görs en ändring enligt vilken dubbel straffbarhet inte förutsätts vid en begäran om rättslig hjälp som gäller ett förordnande att bevara data. Dessutom föreslås i propositionsutkastet en del andra mindre lagändringar av främst teknisk natur.			
Nyckelord datateknikbrott, förundersökning, tvångsmedel, utlämning för brott, internationell rättshjälp			
Övriga uppgifter HARE JM 029:00/2002			
Seriens namn och nummer Justitieministeriets arbetsgruppsbetänkanden 2003:6		ISSN 1458-6452	ISBN 952-466-153-5
Sidoantal 166	Språk finska	Pris	Sekretessgrad offentligt
Distribution Edita Prima Oy		Förlag Justitieministeriet	

## OIKEUSMINISTERIÖLLE

Oikeusministeriö asetti 10 päivänä joulukuuta 2002 työryhmän valmistelemaan Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen voimaansaattamiseksi tarvittavaa lainsäädäntöä ja samalla selvittämään mahdollisia muita rikos- ja rikosprosessilainsäädännön muutostarpeita.

Työryhmän tehtäväksi asetettiin arvioida sopimuksen edellyttämät lainmuutostarpeet sekä samassa yhteydessä tarkastella erityisesti esitutkinta- ja pakkokeinolainsäädännön muutostarpeita laajemminkin erityisesti ottaen huomioon lakien toimivuus informaatioteknisessä ympäristössä. Työryhmän tuli valmistella ehdotuksensa hallituksen esityksen muotoon.

Työryhmän puheenjohtajaksi kutsuttiin lainsäädäntöjohtaja Jan Törnqvist oikeusministeriöstä ja jäseniksi lainsäädäntöneuvos Riku Ahola oikeusministeriöstä, johtava kihlakunnansyyttäjä Antti Pihlajamäki Turun kihlakunnan syyttäjänvirastosta, poliisiylitarkastaja Jouni Vätkki sisäasiainministeriöstä, rikostarkastaja Ari Määttä keskusrikospoliisista, neuvotteleva virkamies Sanna Helopuro liikenne- ja viestintäministeriöstä, asianajaja Satu Tiirikka Suomen Asianajajaliitosta, käräjätuomari Sirpa Ahola Helsingin käräjäoikeudesta sekä Jouni Vätkin varajäseneksi ylikomisario Risto Karhunen sisäasiainministeriöstä. Työryhmän jäsen Riku Ahola toimi samalla myös työryhmän sihteerinä.

Työryhmä on kokoontunut 12 kertaa.

Työryhmän tuli saada työnsä valmiiksi 1 päivään kesäkuuta 2003 mennessä.

Mietintöön on liitetty jäsen Tiirikan lausuma.

Saatuaan työnsä valmiiksi työryhmä kunnioittavasti luovuttaa mietintönsä oikeusministeriölle.

Helsingissä 3 päivänä kesäkuuta 2003

Jan Törnqvist

Riku Ahola

Antti Pihlajamäki

Jouni Vätkki

Ari Määttä

Sanna Helopuro

Satu Tiirikka

Sirpa Ahola



Hallituksen esitys Eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen hyväksymisestä sekä rikoslain, pakkokeinolain, esitutkintalain ja kansainvälisestä oikeusavusta rikosasioissa annetun lain muuttamisesta

## **ESITYKSEN PÄÄASIALLINEN SISÄLTÖ**

Esityksessä ehdotetaan, että eduskunta hyväksyy Budapestissä 23 päivänä marraskuuta 2001 tehdyn Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen sekä antaa suostumuksensa eräiden yleissopimuksen nojalla annettavien selitysten ja varaumien tekemiseen. Yleissopimus on tarkoitus ratifioida kun eduskunta on hyväksynyt sopimuksen. Yleissopimus ei ole vielä tullut kansainvälisesti voimaan.

Esitykseen sisältyy lakiehdotus yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta. Lain voimaantulosta säädetään asetuksella. Lain on tarkoitus tulla voimaan samanaikaisesti kuin yleissopimus tulee voimaan Suomen osalta.

Esityksessä ehdotetaan, että rikoslakiin, pakkokeinolakiin, esitutkintalakiin ja kansainvälisestä oikeusavusta rikosasioissa annettuun lakiin tehdään yleissopimuksen voimaansaattamisesta johtuvat muutokset. Rikoslakiin lisätään uudet tietojärjestelmän häirintää ja tietoverkkorikosvälineen hallussapitoa koskevat säännökset. Tietoverkkorikosvälineen levittämisen osalta nykyinen sääntely laajennetaan kattamaan tietokonevirusten ja muiden vastaavien haittaohjelmien lisäksi myös tietomurtovälineet ja laitteet. Eräiden sopimuksessa tarkoitettujen rikosten yritys säädetään rangaistavaksi. Yhteisövastuu laajennetaan sopimuksen edellyttämällä tavalla. Pakkokeinolakiin lisätään uudet datan takavarikkoa, säilyttämismääräystä ja tietojärjestelmän haltijan tietojenantovelvollisuutta koskevat säännökset. Esitutkintalakiin lisätään säännös, jonka mukaan todistaja on velvollinen esittämään hallussaan olevan datan tai muun todistusaineiston. Lakiin kansainvälisestä oikeusavusta rikosasioissa tehdään muutos, jonka mukaan datan säilyttämismääräystä koskevan oikeusapupyynnön osalta ei edellytetä kaksoisrangaistavuutta. Lisäksi esityksessä ehdotetaan eräitä muita vähäisiä lakimuutoksia, jotka ovat luonteeltaan lähinnä teknisiä. Näiden lakien on tarkoitus tulla voimaan mahdollisimman pian sen jälkeen kun ne on hyväksytty.

**SISÄLLYSLUETTELO**

ESITYKSEN PÄÄASIAALLINEN SISÄLTÖ.....	1
SISÄLLYSLUETTELO.....	2
YLEISPERUSTELUT.....	5
1. Johdanto.....	5
2. Nykytila.....	6
2.1 Johdanto.....	6
2.2 Rikoksentehtävän luovuttaminen.....	6
2.2.1 Lainsäädäntö.....	6
2.2.2 Kansainväliset yleissopimukset.....	7
2.2.3 Kahdenväliset valtiosopimukset.....	7
2.3 Kansainvälinen oikeusapu.....	8
2.3.1 Lainsäädäntö.....	8
2.3.2 Kansainväliset yleissopimukset.....	9
2.3.3 Pohjoismainen yhteistyö.....	9
2.3.4 Kahdenväliset valtiosopimukset.....	10
3. Esityksen tavoitteet ja keskeiset ehdotukset.....	10
4. Esityksen vaikutukset.....	11
5. Asian valmistelu.....	12
6. Muita esitykseen vaikuttavia seikkoja.....	12
6.1 Euroopan Unionin lapsipornografiaa koskeva puitepäätös.....	12
6.2 Euroopan Unionin tietojärjestelmiin kohdistuvia hyökkäyksiä koskeva puitepäätös.....	12
6.3 Tekijänoikeuslaki ja WIPO-sopimukset.....	12
YKSITYISKOHTAISET PERUSTELUT.....	13
1. Yleissopimus ja sen hyväksymisen perustelut.....	13
I luku Käsitteiden käyttö.....	13
Määritelmät (1 artikla).....	13
II luku Kansalliset toimenpiteet.....	14
1 jakso Rikosoikeuden aineelliset säännökset.....	14
1 osasto Datasiirron ja tietojärjestelmien luottamuksellisuuteen, eheyteen.....	14
ja käytettävyyteen kohdistuvat rikokset.....	14
Luvaton tunkeutuminen (2 artikla).....	14
Viestintäsalaisuuden loukkaaminen (3 artikla).....	16
Datan vahingoittaminen (4 artikla).....	17
Tietojärjestelmän häirintä (5 artikla).....	18
Laitteiden väärinkäyttö (6 artikla).....	20
2 osasto Tietokoneavusteiset rikokset.....	22
Tietokoneavusteinen väärennys (7 artikla).....	22
Tietokoneavusteinen petos (8 artikla).....	23
3 osasto Viestin sisältöön liittyvät rikokset.....	24
Lapsipornografiaan liittyvät rikokset (9 artikla).....	24
4 osasto Tekijänoikeusrikokset ja tekijänoikeuden lähioikeuksia koskevat rikokset.....	25
Tekijänoikeusrikokset ja tekijänoikeuden lähioikeuksia koskevat rikokset (10 artikla).....	25
5 osasto Osallisuus, yhteisövastuu ja sanktiot.....	27
Rikoksen yritys sekä avunanto tai yllytys rikokseen (11 artikla).....	27
Yhteisövastuu (12 artikla).....	30
Sanktiot ja muut seuraamukset (13 artikla).....	33
2 jakso Prosessioikeus.....	33
1 osasto Yhteiset määräykset.....	33
Oikeudenkäyntimenettelyä koskevien määräysten soveltamisala (14 artikla).....	33



Soveltamiseen liittyvät rajoitukset ja takeet (15 artikla).....	34
2 osasto Tallennetun datan säilyttämisen nopea varmistaminen.....	35
Tallennetun datan säilyttämisen nopea varmistaminen (16 artikla).....	35
Liikennetietojen säilyttämisen nopea varmistaminen ja osittainen luovutus (17 artikla).....	36
3 osasto Esittämismääräys.....	38
Esittämismääräys (18 artikla).....	38
4 osasto Tallennettuun dataan kohdistuva etsintä ja takavarikko .....	39
Tallennettuun dataan kohdistuva etsintä ja takavarikko (19 artikla).....	39
5 osasto Tiedon hankkiminen datasta reaaliajassa .....	42
Tiedon hankkiminen liikennetiedoista reaaliajassa (20 artikla).....	42
Tiedon hankkiminen viestin sisällöstä (21 artikla) .....	44
3 jakso Lainkäyttövalta .....	46
Lainkäyttövalta (22 artikla).....	46
III luku Kansainvälinen yhteistyö .....	48
1 jakso Yleiset periaatteet .....	48
1 osasto Kansainvälistä yhteistyötä koskevat yleiset periaatteet .....	48
Kansainvälistä yhteistyötä koskevat yleiset periaatteet (23 artikla).....	48
2 osasto Rikoksen johdosta tapahtuvaa luovuttamista koskevat periaatteet.....	48
Rikoksen johdosta tapahtuva luovuttaminen (24 artikla).....	48
3 osasto Keskinäistä oikeusapua koskevat yleiset periaatteet.....	50
Keskinäistä oikeusapua koskevat yleiset periaatteet (25 artikla).....	50
Tietojen antaminen omasta aloitteesta (26 artikla) .....	51
4 osasto Keskinäistä oikeusapua koskeviin pyyntöihin sovellettavat menettelytavat silloin kun niihin ei ole sovellettavissa kansainvälistä sopimusta.....	52
Keskinäistä oikeusapua koskeviin pyyntöihin sovellettavat menettelytavat silloin kun niihin ei ole sovellettavissa kansainvälistä sopimusta (27 artikla).....	52
Tietojen salassapito ja käyttörajoitukset (28 artikla).....	54
2 jakso Erityiset määräykset.....	55
1 osasto Väliaikaisia toimenpiteitä koskeva keskinäinen oikeusapu.....	55
Tallennetun datan säilyttämisen nopea varmistaminen (29 artikla).....	55
Varmistettujen liikennetietojen nopea luovutus (30 artikla).....	57
2 osasto Tutkintaan liittyviä toimivaltuuksia koskeva keskinäinen oikeusapu.....	57
Keskinäinen oikeusapu pääsyn hankkimisessa tallennettuun dataan (31 artikla).....	57
Pääsyn hankkiminen tallennettuun dataan valtion rajojen yli suostumuksesta.....	58
tai silloin kun data on julkista (32 artikla).....	58
Keskinäinen oikeusapu tiedon hankkimisessa liikennetiedoista reaaliajassa (33 artikla).....	58
Keskinäinen oikeusapu tiedon hankkimisessa viestin sisällöstä (34 artikla) .....	59
3 osasto 24-tuntinen jokapäiväinen verkosto .....	59
24-tuntinen jokapäiväinen verkosto (35 artikla) .....	59
Loppumääräykset (IV luku 36 - 48 artiklat).....	60
2. Lakiehdotusten perustelut .....	61
2.1 Laki Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta .....	61
2.2 Rikoslaki.....	61
2.3 Pakkokeinolaki.....	73
2.4 Esitutkintalaki.....	83
2.5 Laki kansainvälisestä oikeusavusta rikosasioissa .....	84
3. Voimaantulo.....	85
4. Eduskunnan suostumuksen tarpeellisuus .....	85
5. Säättämisjärjestys .....	86

LAKIEHDOTUKSET.....	89
1. Laki Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta .....	89
2. Laki rikoslain muuttamisesta .....	89
3. Laki pakkokeinolain muuttamisesta.....	93
4. Laki esitutkintalain muuttamisesta.....	95
5. Laki kansainvälisestä oikeusavusta rikosasioissa annetun lain muuttamisesta.....	96
LIITTEET.....	97
Rinnakkaistekstit .....	97
Sopimusteksti.....	109

## YLEISPERUSTELUT

### 1. Johdanto

Esityksen tarkoituksena on saattaa Budapestissä 23 päivänä marraskuuta 2001 tehty Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus, jäljempänä yleissopimus tai tietoverkkorikossopimus, kansallisesti voimaan Suomessa.

Tietoverkkorikos tarkoittaa yleissopimuksen nimessä samaa asiaa kuin tietotekniikkarikos. Tietotekniikkarikoksella tarkoitetaan yhtäältä rikosta, joka kohdistuu tietojärjestelmään, ja toisaalta rikosta, joka tehdään tietojärjestelmän avulla. Yhteistä näille kahdelle rikostyypille on siten se, että niiden tekoympäristönä on tietojärjestelmä ja niiden tekeminen yleensä edellyttää jonkinlaista asiantuntemusta tietojärjestelmien toiminnasta.

Tietotekniikkarikollisuus aiheuttaa mittavia taloudellisia vahinkoja. Yhteiskunnan perustoiminnot ovat riippuvaisia tietojärjestelmien ja tietoverkkojen häiriöttömästä toiminnasta. Tämän vuoksi tietotekniikkarikollisuudesta aiheutuu myös sellaisia vakavia vahinkoja, jotka eivät ole pelkästään taloudellisia. Tietotekniikkarikollisuus on tyypillisesti rajat ylittävää rikollisuutta. Silloin sen tutkiminen ilman kansainvälistä yhteistyötä on vaikeaa tai mahdotonta.

Tietotekniikkarikoksia koskeva todistusaineisto on yleensä lähes yksinomaan sähköisessä muodossa. Tällaisen todistusaineiston muuntelu ja hävittäminen on poikkeuksellisen helppoa. Tämän vuoksi tutkintatoimenpiteiden nopeus on ratkaisevassa asemassa tutkittaessa tietotekniikkarikoksia. Samoista syistä myös kansainvälisen yhteistyön on oltava nopeaa.

Tietoverkkorikossopimus on ensimmäinen tietotekniikkarikoksia koskeva yleissopimus. Yleissopimuksella ja sen kansallisella voimaansaattamisella pyritään yhteiskunnan suojelemiseen tietotekniikkarikollisuudelta ja sen aiheuttamilta vahingoilta yhtenäistämällä ja laajentamalla sitä koskevia rangaistussäädöksiä sekä tehostamalla rikostutkintaa ja kansainvälistä oikeudellista yhteistyötä.

Yleissopimuksen ovat allekirjoittaneet Euroopan neuvoston jäsenmaiden lisäksi Kanada, Japani, Etelä-Afrikka ja Yhdysvallat. Myös muut valtiot voivat myöhemmin liittyä yleissopimukseen. Yleissopimuksen tarkoituksena ei ole olla kattava ja täysin itsenäinen, vaan sen tarkoituksena on täydentää olemassa olevia sopimuksia tietotekniikkarikoksia ja niiden tutkintaa koskevilla määräyksillä. Yleissopimuksen tavoitteiden kannalta on tärkeää, että mahdollisimman moni valtio liittyy sopimukseen.

Yleissopimus on tämän esityksen liitteenä. Yleissopimuksesta on lisäksi laadittu Euroopan neuvoston ministerikomitean 8 päivänä marraskuuta 2001 hyväksymä selitysmuistio, jäljempänä selitysmuistio. Selitysmuistion sisältöä on selostettu esityksen artiklakohtaisissa perusteluissa. Selitysmuistion osalta on huomattava, että siinä esitetyt tulkinasuositukset eivät ole sitovia. Tietotekniikkaan liittyvien kysymysten osalta esityksen valmistelussa on käytetty hyväksi alan yleistajuisia kirjoituksia (ks. Tietoturva & Yksityisyys, Petteri Järvinen, Porvoo 2002 ja siinä olevat lähteet).

## 2. Nykytila

### 2.1 Johdanto

Voimassaolevaa lainsäädäntöä ja sen suhdetta yleissopimukseen on rikoslain, pakkokeinolain ja esitutkintalain osalta selostettu kattavasti esityksen artiklakohtaisissa perusteluissa. Tämän vuoksi niiden käsitteleminen tässä jaksossa ei ole tarkoituksenmukaista.

Kansainvälinen oikeusapu ja rikoksentekijän luovuttaminen ja kansainvälinen oikeusapu rikosasioissa perustuvat Suomessa useisiin rinnakkaisiin säännöksiin ja kansainvälisiin sopimuksiin. Kokonaiskuvan saamiseksi asiasta sääntelyjärjestelmiä selostetaan seuraavassa yleisemmällä tasolla. Yksittäisten artiklojen osalta voimassaolevia säännöksiä on lisäksi selostettu artiklakohtaisissa perusteluissa.

### 2.2 Rikoksentekijän luovuttaminen

#### 2.2.1 Lainsäädäntö

Rikoksentekijän luovuttamista sääntelevät Suomessa sekä kansallinen lainsäädäntö että kansainväliset sopimukset. Suomessa on voimassa rikoksentekijän luovuttamista koskeva yleislaki sekä pohjoismaiden välistä luovuttamista koskeva erityislaki. Suomi on osapuolena useissa rikoksentekijän luovuttamista sääntelevissä yleissopimuksissa ja myös kahdensivuisissa valtiosopimuksissa.

Rikoksentekijän luovuttamista sääntelevä yleislaki on laki rikoksen johdosta tapahtuvasta luovuttamisesta (456/1970), jäljempänä yleinen luovutuslaki. Valtaosa lain säännöksistä koskee luovuttamista Suomesta. Suomeen luovuttamisen osalta laissa on ainoastaan joitakin menettelyä koskevia säännöksiä. Luovuttamisen edellytykset toisesta valtiosta Suomeen määräytyvät luovuttavan valtion lainsäädännön ja asiaa koskevien sopimusten mukaisesti.

Suomesta luovuttaminen voi yleisen luovutuslain mukaan tulla kyseeseen vaikka mitään luovutussopimusta ei ole. Käytännössä luovutusasioissa noudatetaan vastavuoroisuusperiaatetta vaikka lain sanamuoto ei tätä edellytä. Suomesta luovuttamisen edellytyksenä on yleensä, että rikoksen enimmäisrangaistus Suomessa olisi vähintään vuosi vankeutta. Euroopan Unionin jäsenvaltioon luovutettaessa rangaistuskynnys on kuitenkin vähintään kuusi kuukautta vankeutta silloin kun enimmäisrangaistus pyytäjän lain mukaan on vähintään vuosi vankeutta (4 §). Suomen kansalaista ei saa luovuttaa muutoin kuin oikeudenkäyntiä varten Euroopan Unionin jäsenvaltioon. Silloinkin edellytyksenä on, että rikos on tehty muualla kuin Suomessa ja rikoksen enimmäisrangaistus Suomessa olisi vähintään neljä vuotta vankeutta (2 §). Poliittisesta tai sotilasrikoksesta ei saa pääsääntöisesti luovuttaa (5 ja 6 §). Muu kuin Suomen kansalainen voidaan luovuttaa Suomessa tehdystä rikoksesta vain jos se on tarkoituksenmukaista eikä tuomittava rangaistus olennaisesti poikkea siitä mitä Suomessa tuomittaisiin (3 §). Jos teosta on jo tuomittu rangaistus tai jos syyte on vanhentunut, luovuttaminen ei ole pääsääntöisesti mahdollista (10 §). Luovuttaminen on mahdollista ainoastaan tilapäisesti oikeudenkäyntiä varten, jos henkilöllä on Suomessa jokin rangaistus suorittamatta tai syyte vireillä (11 §). Luovuttaa ei saa, jos se olisi olosuhteisiin nähden kohtuutonta (8 §). Laissa on lisäksi tarkempia säännöksiä luovutusmenettelystä (13 - 25 §).

Suomen ja muiden pohjoismaiden välillä tapahtuvien luovutusten osalta on voimassa laki rikoksen johdosta tapahtuvasta luovuttamisesta Suomen ja muiden pohjoismaiden välillä (270/1960),

jäljempänä pohjoismainen luovutuslaki. Pohjoismaisen luovutuslain taustalla ei ole pohjoismaiden välistä sopimusta. Muissa pohjoismaissa on kuitenkin asiasisällöltään samanlaiset lait.

Pohjoismainen luovutuslaki on joissain suhteissa lievempi kuin yleinen luovutuslaki. Suomesta luovuttamisen edellytyksenä on se, että rikoksesta voi seurata pyytäjän lain mukaan vankeutta. Kaksoisrangaistavuutta ei edellytetä (4 §). Suomen kansalaista ei luovuteta, paitsi jos hän on pysyvästi oleskellut vähintään kaksi vuotta luovutusta pyytävässä valtiossa tai jos rikoksesta säädetty ankarin rangaistus Suomen lain mukaan on vähintään neljä vuotta vankeutta (2 §).

### **2.2.2 Kansainväliset yleissopimukset**

Keskeinen rikoksenteikijän luovuttamista sääntelevä sopimus on rikoksen johdosta tapahtuvaa luovuttamista koskeva eurooppalainen yleissopimus (SopS 32/1971), jäljempänä eurooppalainen luovutus sopimus, ja sen toinen lisäpöytäkirja (SopS 15/1985). Eurooppalaista luovutus sopimusta täydentävät yleissopimus Euroopan Unionin jäsenvaltioiden välillä rikoksen johdosta tapahtuvasta luovuttamisesta (SopS 71/1999) ja yleissopimus yksinkertaistetusta menettelystä Euroopan Unionin jäsenvaltioiden välillä rikoksen johdosta tapahtuvassa luovuttamisessa (SopS 73/1999). Yleiseen luovuttamislakiin on lailla 182/1999 tehty edellä mainittujen sopimusten edellyttämät muutokset ja se vastaa siten sisällöltään sopimusten vaatimuksia.

Suomi on lisäksi liittynyt eräisiin muihin yleissopimuksiin, joihin sisältyy myös rikoksenteikijän luovuttamista koskevia määräyksiä. Näitä ovat esimerkiksi eurooppalainen yleissopimus terrorismin vastustamisesta (SopS 16/1990) ja Yhdistyneiden kansakuntien yleissopimus huumausaineiden ja psykotrooppisten aineiden kauppaa vastaan (SopS 44/1994).

Euroopan Unionin neuvosto on hyväksynyt 13 päivänä kesäkuuta 2002 puitepäätöksen eurooppalaisesta pidätysmääräyksestä ja jäsenvaltioiden välisestä luovuttamismenettelystä (EYVL L 190, 18.7.2002, s. 1). Rikoksen johdosta tapahtuva luovuttaminen jäsenvaltioiden välillä tulee 1 päivä tammikuuta 2004 alkaen tapahtua puitepäätöksen määräysten mukaisesti. Puitepäätöksellä korvataan jäsenvaltioiden välisissä suhteissa muun ohessa eurooppalainen luovutus sopimus. Puitepäätös sallii kuitenkin, että Euroopan Unionin jäsenvaltioina olevien pohjoismaiden kesken luovuttaminen voidaan edelleen hoitaa yhdenmukaiseen pohjoismaiseen lainsäädäntöön perustuvan järjestelmän mukaisesti, jos pohjoismaisen lainsäädännön menettelyt ovat suotuisampia kuin puitepäätöksen mukaiset menettelyt. Puitepäätöksessä luovuttamista koskevat pyynnöt ja päätökset siirretään oikeusviranomaisten tehtäviksi. Oman valtion kansalaiset luovutetaan periaatteessa samoin edellytyksin kuin vieraan valtion kansalaiset. Silloin kun kyseessä on jokin puitepäätöksen 32-kohtaiseen luetteloon sisältyvä rikos, josta voi seurata vapausrangaistus ja jonka enimmäiskesto on vähintään kolme vuotta, luovuttamisesta ei voi kieltäytyä sillä perusteella, että kaksoisrangaistavuuden vaatimus ei täyty tai että kyse on poliittisesta rikoksesta tai että luovutettava on luovuttajamaan kansalainen. Luettelossa mainitaan muun ohessa tietotekniikkarikokset. Puitepäätöksen kansallinen täytäntöönpano Suomessa on kesken.

### **2.2.3 Kahdenväliset valtiosopimukset**

Suomi on tehnyt kahdenvälisiä luovuttamissopimuksia eräiden valtioiden kanssa. Näistä käytännössä tärkeimmät ovat Yhdysvaltojen, Kanadan ja Australian kanssa tehdyt sopimukset. Yhdysvallat ja Kanada ovat allekirjoittaneet myös tässä esityksessä voimaansaattettavan yleissopimuksen. Valmisteilla on myös Euroopan Unionin ja Yhdysvaltojen välinen rikoksenteikijän luovutusta ja oikeusapua koskeva sopimus.

Yleissopimuksen määräyksiä ja Suomen voimassaolevaa oikeutta on selostettu myös 24 artiklan perusteluissa.

## 2.3 Kansainvälinen oikeusapu

### 2.3.1 Lainsäädäntö

Kansainvälistä oikeusapua rikosasioissa sääntelevät Suomessa sekä kansallinen lainsäädäntö että kansainväliset sopimukset. Suomessa on voimassa rikosoikeusapua koskeva yleislaki sekä eräitä erityislakeja. Suomi on osapuolena useissa kansainvälisissä rikosoikeusapua sääntelevissä yleissopimuksissa ja myös kahdenvälisissä valtiosopimuksissa.

Kansainvälistä oikeusapua sääntelevä yleislaki on laki kansainvälisestä oikeusavusta rikosasioissa (4/1994), jäljempänä rikosoikeusapulaki. Se on kansainvälistä rikosoikeusapua koskeva yhtenäinen säännöstö, jonka perusteella Suomen viranomaiset voivat antaa ja pyytää oikeusapua toisen valtion viranomaisilta. Lain periaatteena on, että Suomen viranomaiset voivat suoraan lain nojalla antaa toisen valtion viranomaisille oikeusapua siitä riippumatta, onko Suomen ja oikeusapua pyytäneen valtion välillä voimassa valtiosopimusta. Kaksoisrangaistavuutta edellytetään vain, jos oikeusapupyyntö tarkoittaa tai edellyttää pakkokeinojen käyttöä. Oikeusavun antamisen edellytyksenä ei ole myöskään se, että pyynnön esittänyt valtio antaisi vastaavaa oikeusapua Suomelle. Suomen viranomaiset voivat siten pelkästään rikosoikeusapulain nojalla antaa oikeusapua toisen valtion viranomaiselle. Ehdottomista kieltäytymisperusteista on säännös lain 12 §:ssä. Pykälän 1 momentin mukaan oikeusapua ei anneta, jos oikeusavun antaminen saattaisi loukata Suomen täysivaltaisuutta tai vaarantaa Suomen turvallisuutta taikka muita olennaisia etuja. Oikeusapua ei 2 momentin mukaan myöskään anneta, jos oikeusavun antaminen olisi ristiriidassa ihmisoikeuksia ja perusvapauksia koskevien periaatteiden kanssa taikka jos oikeusavun antaminen muutoin olisi Suomen oikeusjärjestyksen peruseriaatteiden vastaista. Rikosoikeusapulain 13 §:ssä on lisäksi säännökset harkinnanvaraisista kieltäytymisperusteista. Pykälän mukaan oikeusavun antamisesta voidaan kieltäytyä muun ohessa, jos pyynnön perusteena on teko, jota on pidettävä poliittisena rikoksena. Pykälässä on lisäksi muita kieltäytymisperusteita, jotka liittyvät syyteoikeuden vanhentumiseen, vireillä olevaan oikeudenkäyntiin ja vastaaviin seikkoihin. Rikosoikeusapulaissa on lisäksi säännöksiä oikeusavun pyytämisestä toiselta valtiolta. Tältä osin sääntelyssä on lähinnä kyse siitä millä viranomaisella Suomessa on oikeus toimia asiassa. Rikosoikeusapulain nojalla on annettu asetus kansainvälisestä oikeusavusta rikosasioissa (13/1994). Asetus sisältää lakia täydentäviä yksityiskohtaisia säännöksiä oikeusavun antamisesta ja pyytämisestä.

Suomen valtion kansainväliset velvoitteet antaa oikeusapua toiselle valtiolle ja Suomen oikeus saada oikeusapua toiselta valtiolta määräytyvät kansainvälisten sopimusten perusteella. Rikosoikeusapulain 30 §:n mukaan siinä olevien säännösten estämättä kansainvälistä oikeusapua rikosasioissa annetaan myös siten kuin oikeusavun antamisesta on erikseen sovittu tai säädetty. Rikosoikeusapulakia ja kansainvälisiä sopimuksia sovelletaan siten rinnakkain toistensa kanssa.

Suurin osa rikosoikeusapulain säännöksistä koskee sitä, millä edellytyksillä Suomen viranomaiset voivat antaa oikeusapua toisen valtion viranomaisille. Edellytykset, joiden perusteella toiset valtiot antavat oikeusapua, ovat hyvin erilaisia, eikä näitä ole mahdollista säännellä rikosoikeusapulaissa. Oikeusavun antamisen edellytykset saattavat vaihdella myös saman sopimuksen eri osapuolien välillä. Tämä johtuu siitä, että sopimukseen on mahdollista tehdä varauksia ja lisäksi sopimukseen liittyneiden valtioiden sisäinen lainsäädäntö voi poiketa sopimuksen määräyksistä. Silloin kun Suomen viranomaiset pyytävät oikeusapua, ne joutuvat toimimaan Suomen ja vieraan valtion välillä

voimassaolevan kansainvälisen sopimuksen mukaisesti. Näissä tilanteissa ei yleensä ole riittävä, että Suomen viranomaiset soveltavat ainoastaan rikosoikeusapulain säännöksiä.

Säännöksiä kansainvälisestä oikeusavusta sisältyy rikosoikeusapulain lisäksi muun ohessa oikeudenkäymiskaareen, pakkokeinolakiin (450/1987), lakiin oikeudenkäyntiin ja esitutkintaan osallistuvien henkilöiden koskemattomuudesta eräissä tapauksissa (11/1994), entisen Jugoslavian alueella tehtyjä rikoksia käsittelevän sotarikostuomioistuimen toimivallasta ja tuomioistuimelle annettavasta oikeusavusta annettuun lakiin (12/1994) sekä kansainvälisen rikostuomioistuimen Rooman perussäännön lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta ja perussäännön soveltamisesta annettuun lakiin (1284/2000).

### **2.3.2 Kansainväliset yleissopimukset**

Keskeisin Suomessa voimassaoleva rikosoikeusapua koskeva yleissopimus on eurooppalainen yleissopimus keskinäisestä oikeusavusta rikosasioissa (SopS 30/1981), jäljempänä eurooppalainen oikeusapusopimus sekä sen lisäpöytäkirja (SopS 14/1985). Toista lisäpöytäkirjaa Suomi ei ole vielä allekirjoittanut.

Eurooppalainen oikeusapusopimus on Suomessa saatettu voimaan siten, että se kattaa asiasisällöltään eurooppalaisen oikeusapusopimuksen vaatimukset. Tämän vuoksi Suomen viranomainen päätyy käytännössä eurooppalaisen oikeusapusopimuksen mukaiseen lopputulokseen soveltamalla ainoastaan Suomen sisäistä lainsäädäntöä. Kun tämän esityksen artiklakohtaisissa perusteluissa verrataan yleissopimuksen vaatimuksia ja rikosoikeusapulain säännöksiä, tämä vertailu kattaa käytännössä myös eurooppalaisen yleissopimuksen. Rikosoikeusapulaki menee tosin joiltakin osin pidemmälle kuin eurooppalainen oikeusapusopimus. Rikosoikeusapulain mukaan oikeusapua voidaan antaa televalvonnassa ja telekuuntelussa vaikka eurooppalainen yleissopimus ei tätä edellytä.

Suomi on lisäksi liittynyt useisiin muihin yleissopimuksiin, joihin sisältyy myös kansainvälistä rikosoikeusapua koskevia määräyksiä. Näistä tärkeimmät ovat Schengenin yleissopimus (SopS 23/2001), rikoksen tuottaman hyödyn rahanpesua, etsintää, takavarikkoa ja menetetyksi tuomitsemista koskeva yleissopimus (SopS 53/1994) ja Yhdistyneiden kansakuntien yleissopimus huumausaineiden ja psykotrooppisten aineiden kauppaa vastaan (SopS 44/1994).

Euroopan Unionin jäsenvaltiot ovat 29 päivänä toukokuuta 2000 tehneet yleissopimuksen keskinäisestä oikeusavusta rikosasioissa (EYVL C 197, 12.7.2000). Yleissopimus täydentää eurooppalaista rikosoikeusapusopimusta ja se sisältää määräyksiä muun muassa yhteydenpitojärjestyksestä oikeusviranomaisten välillä, todistajien kuulemisesta videokokouksen avulla sekä lisäksi laajat telekuuntelua koskevat määräykset. Yleissopimuksen voimaansaattamista koskeva hallituksen esitys (HE 185/2002) raukesi vuoden 2002 valtiopäivillä. Esitys on tarkoitus antaa uudelleen eduskunnalle kesällä 2003.

### **2.3.3 Pohjoismainen yhteistyö**

Tiedoksiannosta ja todistelusta on Suomen, Islannin, Norjan, Ruotsin ja Tanskan kesken vuonna 1974 tehty sopimus oikeusavusta tiedoksiannon toimittamisessa ja todistelussa (SopS 26/1975). Tarkemmat sopimuksen soveltamista koskevat säännökset on annettu asetuksessa pohjoismaiden keskeisestä oikeusavusta tiedoksiannon toimittamisessa ja todistelussa (470/1975). Lisäksi Suomessa on voimassa yhteispohjoismaiseen lainsäädäntöön perustuva laki velvollisuudesta saapua toisen pohjoismaan tuomioistuimeen eräissä tapauksissa (349/1975). Kyseiset pohjoismaista

yhteistyötä koskevat säännökset on Suomessa katsottu asemaltaan sellaisiksi, että Suomen viranomaiset voivat soveltaa niitä rinnakkain eurooppalaisen oikeusapusopimuksen ja rikosoikeusapulain kanssa.

### **2.3.4 Kahdenväliset valtiosopimukset**

Suomi on tehnyt joidenkin valtioiden kanssa kahdenvälisiä valtiosopimuksia kansainvälisestä rikosoikeusavusta taikka rikostorjuntaa tai muuta yhteistyötä koskevia sopimuksia, jotka sisältävät määräyksiä kansainvälisestä rikosoikeusavusta. Kyseisiä valtioita ovat Australia, Latvia, Liettua, Puola, Ukraina, Unkari, Venäjä ja Viro. Australiaa lukuun ottamatta mainitut valtiot ovat myös allekirjoittaneet tässä esityksessä voimaansaattettavan yleissopimuksen. Valmisteilla on myös Euroopan Unionin ja Yhdysvaltojen välinen rikoksentehtävän luovutusta ja oikeusapua koskeva sopimus.

Yleissopimuksen määräyksiä ja Suomen voimassaolevaa oikeutta on selostettu myös artiklakohtaisissa perusteluissa.

## **3. Esityksen tavoitteet ja keskeiset ehdotukset**

Esityksen tarkoituksena on saattaa yleissopimus kansallisesti voimaan Suomessa.

Yleissopimuksella ja sen kansallisella voimaansaattamisella pyritään yhteiskunnan suojelemiseen tietotekniikkarikollisuudelta ja sen aiheuttamilta vahingoilta. Lisäksi esityksen tarkoituksena on selventää sähköisessä muodossa olevan todistusaineiston asemaa nykyisessä pääosin esineitä ja paperimuodossa olevia asiakirjoja silmälläpitäen kirjoitetussa pakkokeinolaissa. Tältä osin tavoitteet liittyvät myös muihin rikoksiin kuin tietotekniikkarikoksiin.

Esityksessä ehdotetaan, että eduskunta hyväksyy yleissopimuksen sekä antaa suostumuksensa eräiden yleissopimuksen nojalla annettavien selitysten ja varaumien tekemiseen. Esitykseen sisältyy lakiehdotus yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.

Esityksessä ehdotetaan, että rikoslakiin, pakkokeinolakiin, esitutkintalakiin ja kansainvälisestä oikeusavusta rikosasioissa annettuun lakiin tehdään yleissopimuksen voimaansaattamisesta johtuvat muutokset.

Rikoslakiin ehdotetaan lisättäväksi uudet tietojärjestelmän häirintää ja tietoverkkorikosvälineen hallussapitoa koskevat säännökset. Tietoverkkorikosvälineen levittämisen osalta nykyistä sääntelyä laajennetaan. Rikoslain 38 lukuun ehdotetaan lisättäväksi uusi 7 a §, jonka mukaan tietojärjestelmän häirinnästä tuomitaan se, joka dataa syöttämällä tai eräillä muilla säännöksessä tarkoitetuilla tavoilla estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä. Törkeästä tekemuodosta on säännös 7 b §:ssä. Rikoslain 34 luvun 9 a § vaaran aiheuttamisesta tietojenkäsittelylle ehdotetaan muutettavaksi siten, että se kattaa tietokoneviruksen ja vastaavan haittaohjelman levittämisen lisäksi myös muiden tietoverkkorikosvälineiden kuten tietomurto-ohjelmien, tietomurtolaitteiden ja salasanojen levittämisen. Samaan lukuun ehdotetaan lisättäväksi uusi 9 b §, jossa säädetään rangaistavaksi tietomurtovälineen hallussapito ilman hyväksyttävää syytä.

Eräiden rikosten yritys säädetään rangaistavaksi. Nämä ovat tietovahingonteko (RL 35:1,2) ja sen törkeä tekemuoto, tietoliikenteen häirintä (RL 38:5), törkeä tietoliikenteen häirintä (RL 38:6) sekä lievä tietoliikenteen häirintä (RL 38:7).



Yhteisövastuu ehdotetaan ulotettavaksi eräisiin uusiin rikoksiin. Nämä ovat vaaran aiheuttaminen tietojenkäsittelylle (RL 34:9a), tietoverkkorikosvälineen hallussapito (uusi RL 34:9b), tietovahingonteko (RL 35:1,2), törkeä tietovahingonteko (RL 35:3), viestintäsalaisuuden loukkaus (RL 38:3), törkeä viestintäsalaisuuden loukkaus (RL 38:4), tietoliikenteen häirintä (RL 38:5), törkeä tietoliikenteen häirintä (RL 38:6), tietojärjestelmän häirintä (uusi RL 38:7a), törkeä tietojärjestelmän häirintä (uusi RL 38:7b), tietomurto (RL 38:8) ja tekijänoikeusrikos (RL 49:1).

Pakkokeinolakiin ehdotetaan lisättäväksi uudet datan takavarikkoa, säilyttämismääräystä ja tietojärjestelmän haltijan tietojenantovelvollisuutta koskevat säännökset. Pakkokeinolain 4 lukuun ehdotetaan lisättäväksi uusi 4 a § datan kopioinnista ja takavarikoinnista. Pykälän mukaan kopiointia ei yksin vielä pidetä takavarikkotoimenpiteenä. Tämän vuoksi siihen ei sovelleta takavarikkoa koskevia säännöksiä. Vasta jos data kopioinnin yhteydessä poistetaan alkuperäisestä tallennusalueelta, sitä pidetään takavarikkona. Erottelun perusteena on toimenpiteiden erilainen merkitys toimenpiteen kohteena olevan henkilön kannalta. Ehdotettu sääntely vastaa pääosin nykyisin noudatettua käytäntöä. Lukuun ehdotetaan lisättäväksi uusi 4 b § tietojärjestelmän haltijan tietojenantovelvollisuudesta. Pykälän mukaan tietojärjestelmän haltija on velvollinen antamaan esitutkintaviranomaiselle tämän pyynnöstä tiedossaan olevat datan kopioimiseksi ja takavarikoimiseksi tarpeelliset salasanat ja muut vastaavat tiedot. Pykälän tarkoituksena on helpottaa esitutkintaviranomaisen työtä vähentämällä datan kopiointiin ja takavarikkoon kuluva-aikaa. Lukuun ehdotetaan lisättäväksi uusi 4 c § datan säilyttämismääräyksestä. Se on uusi pakkokeino, jota voidaan tarvittaessa käyttää esitoimenpiteenä ennen muita dataan kohdistuvia pakkokeinoja. Sen tarkoituksena on estää rikostutkinnallisesti merkityksellisen datan häviäminen tai muuttaminen ennen kuin datan haltuunotto on muiden pakkokeinojen nojalla mahdollista.

Esitutkintalain 27 §:ään ehdotetaan lisättäväksi uusi 2 momentti, jonka mukaan todistaja on velvollinen esittämään hallussaan olevan asiakirjan tai muun todistusaineiston. Kansainvälisestä oikeusavusta rikosasioissa annetun lain 15 §:ään lisätään uusi 2 momentti, jonka mukaan datan säilyttämismääräystä koskevan oikeusapupyynnön toimeenpano ei edellytä kaksoisrangaistavuutta. Saman lain 23 §:n 1 momenttia ehdotetaan muutettavaksi siten, että siinä olevaan oikeusapupyynnön perusteella toimeenpantavissa olevien pakkokeinojen luetteloon lisätään tässä esityksessä ehdotettu uusi pakkokeinolain 4 luvun 4 c §:n mukainen datan säilyttämismääräys. Lisäksi esityksessä ehdotetaan eräitä muita vähäisiä lakimuutoksia, jotka ovat luonteeltaan lähinnä teknisiä.

#### **4. Esityksen vaikutukset**

Rikoslakiin lisättävät uudet rikossäännökset parantavat sähköisessä muodossa olevan tiedon ja tiedonvälityksen rikosoikeudellista suojaa. Lisäksi esitys antaa viranomaisille tehokkaammat välineet selvittää tietotekniikkarikollisuutta. Tämän seurauksena rikoksen uhrin oikeusasema paranee.

Kansainvälisen yhteistyön tehostaminen taas osaltaan edistää Suomen viranomaisten mahdollisuuksia selvittää myös sellaisia rajat ylittäviä rikoksia, joiden vahingolliset seuraukset ilmenevät Suomessa.

Esityksen mukaan Suomen on järjestettävä ympärivuorokautinen päivystys huolehtimaan 35 artiklassa tarkemmin selostetuista tehtävistä. Esityksellä saattaa tältä osin olla joitain vähäisiä poliisiin kohdistuvia organisaatio- ja henkilöstövaikutuksia.

Esityksen datan säilyttämismääräystä koskeva uusi pakkokeino kohdistuu käytännössä aina sivulliseen datan haltijaan, yleensä teleoperaattoriin. Esityksen vaikutukset ovat kuitenkin tältäkin osin vain vähäisiä.

Esityksellä ei siten ole merkittäviä henkilöstö- tai organisaatiovaikutuksia eikä myöskään taloudellisia vaikutuksia.

## **5. Asian valmistelu**

Esitys on valmisteltu oikeusministeriön asettamassa työryhmässä. Työryhmän jäseninä ovat olleet oikeusministeriötä, sisäasiainministeriötä, liikenne- ja viestintäministeriötä, keskusrikospoliisia, tuomioistuineläimistöä, syyttäjiä ja asianajajia edustavat henkilöt.

## **6. Muita esitykseen vaikuttavia seikkoja**

### **6.1 Euroopan Unionin lapsipornografiaa koskeva puitepäättös**

Euroopan Unionissa on valmisteilla ehdotus neuvoston puitepäättökseksi lasten seksuaalisen hyväksikäytön ja lapsipornografian torjumisesta. Puitepäättöksen kansallisen täytäntöönpanon yhteydessä Suomen voimassa olevat säännökset on muutettava puitepäättöksen velvoitteiden mukaisiksi. Yleissopimuksen 9 artiklan edellyttämät muutokset toteutetaan puitepäättöksen kansallisen voimaansaattamisen yhteydessä. Asiaa on selostettu tarkemmin 9 artiklan perusteluissa.

### **6.2 Euroopan Unionin tietojärjestelmiin kohdistuvia hyökkäyksiä koskeva puitepäättös**

Euroopan Unionissa on valmisteilla ehdotus tietojärjestelmiin kohdistuvia hyökkäyksiä koskevaksi neuvoston puitepäättökseksi. Puitepäättöksessä on eräitä yleissopimuksessa tarkoitettuja tietotekniikkarikoksia koskevia määräyksiä rangaistusasteikoista. Jos yleissopimus saatetaan kansallisesti voimaan ennen puitepäättöstä, puitepäättöksen edellyttämät rangaistusasteikko vaatimukset on tarkoituksenmukaista ottaa huomioon jo yleissopimuksen voimaansaattamisen yhteydessä. Puitepäättöksen voimaantuloaika ei ole vielä tiedossa.

### **6.3 Tekijänoikeuslaki ja WIPO-sopimukset**

Yleissopimuksen 10 artiklan mukaan osapuolen on huolehdittava muun ohessa siitä, että niin sanottuihin WIPO-sopimukseen perustuvien velvollisuuksien osalta huolehditaan myös eräistä yleissopimuksen edellyttämistä vaatimuksista. Asiaa on selostettu tarkemmin 10 artiklan perusteluissa. Suomi on allekirjoittanut molemmat WIPO-sopimukset mutta ei ole saattanut niitä kansallisesti voimaan. Asiaa koskeva hallituksen esitys on tarkoitus antaa eduskunnalle yhdessä tekijänoikeuslain muuttamista koskevan esityksen kanssa kuluvan vuoden aikana. Mikäli WIPO-sopimukset edellyttävät rikosoikeudellista lisäsääntelyä, yleissopimuksen tekotapaa koskevat vaatimukset huomioidaan WIPO-sopimusten kansallisen täytäntöönpanon yhteydessä.

## YKSITYISKOHTAISET PERUSTELUT

### 1. Yleissopimus ja sen hyväksymisen perustelut

#### I luku Käsitteiden käyttö

##### Määritelmät (1 artikla)

Artikla sisältää sopimuksessa käytettyjä määritelmiä koskevat määräykset.

Artiklan a kohdan mukaan ”tietojärjestelmä” tarkoittaa laitetta tai toisiinsa kytkettyjä tai liitettyjä laitteita, joista yksi tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten. Termillä tarkoitetaan siten sekä yksittäistä laitetta sekä usean toisiinsa kytketyn laitteen muodostamaa kokonaisuutta. Määritelmää käsitellään selitysmuistion kohdissa 23 ja 24. Selitysmuistion mukaan tietojärjestelmä koostuu laitteista ja ohjelmista joilla käsitellään digitaalisessa muodossa olevaa dataa automaattisesti. Laite koostuu yleensä prosessorista ja erilaisista tiettyä erityistehtävää suorittavista oheislaitteista. Tietojenkäsittelyn automaattisuus tarkoittaa sitä, että käsittely tapahtuu ohjelman avulla itsenäisesti ilman ihmisen välitöntä myötävaikutusta. Tietojärjestelmän käsite kattaa myös tietoverkon. Tietoverkolla tarkoitetaan yhteen liitettyjä tietojärjestelmiä. Yhteen liittäminen voidaan toteuttaa teknisesti esimerkiksi sähköisillä tai optisilla johtimilla taikka radioaalloilla. Tietoverkko voi olla maantieteelliseltä alueeltaan pieni lähialueverkko tai maailman kattava kuten internetverkko. Oleellista tietoverkon käsitteen kannalta on ainoastaan se, että sitä käytetään datan siirtämiseen tietoverkon osasta toiseen.

Tietojärjestelmän käsitettä käytetään sopimuksessa muun ohessa rajaamaan tietojärjestelmiin kohdistuvien rikosten osalta rangaistavaksi säädettyjen tekojen kohdetta sekä tietojärjestelmää hyväksikäyttäen tehtävien rikosten osalta niiden tekotapaa. Lisäksi termiä käytetään pakkokeinoja koskevissa sopimuksen määräyksissä rajaamaan pakkokeinon kohdetta.

Artiklan b kohdan mukaan ”data” tarkoittaa sellaisessa muodossa olevia tosiseikkoja, tietoja tai käsitteitä edustavia merkkejä, että ne soveltuvat käsiteltäväksi tietojärjestelmässä, mukaan lukien ohjelmat, joiden avulla tietokone pystyy suorittamaan jonkin toiminnon. Määritelmää käsitellään selitysmuistion kohdassa 25. Selitysmuistion mukaan määritelmä perustuu ISO-standardin mukaiseen määritelmään. Keskeistä määritelmässä on se, että tiedon pitää olla sähköisessä tai muussa sellaisessa muodossa, että se sellaisenaan soveltuu käsiteltäväksi tietojärjestelmässä.

Kyseistä termiä käytetään sopimuksessa rajaamaan tietojärjestelmiin kohdistuvien rikosten osalta rangaistavaksi säädettyjen tekojen kohdetta sekä pakkokeinoja koskevissa sopimuksen määräyksissä rajaamaan pakkokeinon kohdetta.

Artiklan c kohdan mukaan ”palveluntarjoaja” tarkoittaa julkista tai yksityistä yksikköä, joka tarjoaa palveluidensa käyttäjille mahdollisuuden tietojärjestelmän välityksellä tapahtuvaan viestintään, ja muuta yksikköä, joka käsittelee tai tallentaa dataa edellä mainitun palveluntarjoajan tai palveluiden käyttäjien puolesta. Määritelmää käsitellään selitysmuistion kohdissa 26 ja 27. Selitysmuistion mukaan artiklassa tarkoitettu palveluntarjoaja voi olla esimerkiksi viestien siirtoa, verkkoon pääsyä, tietojärjestelmän ylläpitoa tai tietojen tallentamista tarjoava yritys. Pelkkä sisällön tarjoaminen kuten esimerkiksi internetsivujen sisällön tarjonta ei ole kuitenkaan artiklassa tarkoitettua palveluntarjontaa.

Kyseistä termiä käytetään pakkokeinoja koskevissa sopimuksen määräyksissä rajaamaan pakkokeinon kohteena kyseeseen tulevaa luonnollista tai oikeushenkilöä.

Artiklan d kohdan mukaan ”liikennetiedot” tarkoittaa tietojärjestelmän välityksellä siirrettyyn viestiin liittyvää dataa, jonka viestinsiirtoketjuun kuuluva tietoverkko on tuottanut, ja josta ilmenee viestin alkuperä, määränpää, reitti, kellonaika, päivämäärä, koko, kesto, tai siihen liittyvän palvelun tyyppi. Määritelmää käsitellään selitysmuistion kohdissa 28 - 31. Selitysmuistion mukaan artiklassa tarkoitettuja viestin alkuperää tai määränpäättä osittavia liikennetietoja ovat esimerkiksi puhelinnumero, IP-osoite tai muu niihin verrattava teleosoite. Palvelun tyyppiä koskeva tieto tarkoittaa sitä, onko viestinnässä kysymys esimerkiksi sähköpostista, tiedoston siirrosta vai reaaliaikaisesta keskustelusta.

Matkapuhelimen sijaintitieto ei sen sijaan ole määritelmän mukaan artiklassa tarkoitettu liikennetieto.

Kyseistä termiä käytetään pakkokeinoja koskevissa sopimuksen määräyksissä rajaamaan pakkokeinon kohteena kyseeseen tulevia tietoja.

## **II luku Kansalliset toimenpiteet**

### **1 jakso Rikosoikeuden aineelliset säännökset**

#### **1 osasto Datasiirron ja tietojärjestelmien luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat rikokset**

##### **Luvatun tunkeutuminen (2 artikla)**

Artiklan mukaan tahallinen tietojärjestelmään tai sen osaan tunkeutuminen on säädettävä rangaistavaksi teoksi. Sopimuspuoli voi asettaa rangaistavuuden edellytykseksi sen, että rikos on tehty turvajärjestelyt murtamalla, tarkoituksin päästä käsiksi dataan tai muuta epärehellistä tarkoitusta varten tai että se liittyy sellaiseen tietojärjestelmään, joka on kytketty toiseen tietojärjestelmään.

Artiklaa käsitellään selitysmuistion kohdissa 44-50. Selitysmuistion mukaan artiklan tarkoituksena on tietojenkäsittelyrauhan turvaaminen. Riittävästä tietoturvasta huolehtiminen on ensisijainen ja tehokkain keino tavoitteen toteuttamiseksi. Tämän lisäksi tarvitaan myös rikosoikeudellista suojaa. On tärkeää, että tekoon voidaan puuttua mahdollisimman varhaisessa vaiheessa. Puhtaan tietomurron kriminalisointi, ilman että teolta edellytetään mitään erityistä muuta rikollista tarkoitusta, täyttää tämän vaatimuksen parhaiten. Laajaan kriminalisointiin saattaa jäsenvaltioiden mielestä liittyä kuitenkin ongelmia. Tämän vuoksi sopimuksen mukaan jäsenvaltiot voivat asettaa rangaistavuuden edellytykseksi eräitä rajoittavia lisäehtoja.

Teon kohteena voi tulla kyseeseen joko tietojärjestelmä tai sen osa. Tietojärjestelmä on määritelty 1 artiklan a kohdassa. Tekotapana on tunkeutuminen. Tämä edellyttää sitä, että tekijä pääsee jollain keinolla käsiksi tietojärjestelmään tai sen osaan. Pelkkä sähköpostin, tiedoston, evästeen tai muun datan lähettäminen järjestelmään ei ole vielä artiklassa tarkoitettua tunkeutumista. Teon pitää tapahtua oikeudettomasti. Tämän vuoksi on selvää, että järjestelmän haltijan luvalla tapahtuva tietoturvan testaamiseksi tapahtuva murtautuminen tai julkiseksi tarkoitettujen internetsivujen lataaminen ei täytä artiklassa tarkoitettua rikoksen tunnusmerkistöä.

Suomessa voimassa olevat säännökset sopimuksessa tarkoitettua luvaton tunkeutumista vastaavasta rikoksesta sisältyvät rikoslain tietomurtoa koskevaan 38 luvun 8 §:ään. Mainitun lain kohdan 1 momentin mukaan tietomurrosta on tuomittava se, joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen järjestelmän erikseen suojattuun osaan. Saman pykälän 2 momentin mukaan tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon 1 momentissa tarkoitettua tietojärjestelmässä olevasta tiedosta. Pykälän 3 momentin mukaan tietomurron yritys on rangaistava. Pykälän 4 momentin mukaan säännös on toissijainen.

Tietomurtoa koskevilla säännöksillä pyritään lain esitöiden (HE 94/1993) turvaamaan toisaalta tietokonerauhaa eli tietojärjestelmiä ulkopuolista tunkeutumista vastaan ja toisaalta tietokoneyöskentelyn yksityisyyttä sellaista ulkopuolista tarkkailua vastaan, jossa ei ole kysymys salakuuntelusta tai -katselusta.

Rangaistavaa on ensinnäkin tunkeutuminen sellaiseen tietojärjestelmään, johon tunkeutujalla ei ole lainkaan oikeutta päästä. Rangaistavaa on lisäksi tunkeutuminen sellaiseen suojattuun tietojärjestelmän osaan, johon tekijällä ei ole oikeutta mennä, vaikka hänellä onkin oikeus työskennellä järjestelmän muissa osissa.

Tietojärjestelmällä tarkoitetaan säännöksessä sellaista järjestelmää, jossa tietoja käsitellään sähköisesti tai muulla teknisellä keinolla.

Tunkeutuminen tarkoittaa pääsyn hankkimista järjestelmässä käsiteltäviin tietoihin. Kohteena voi olla sekä tietokoneen muistissa tai siirtoväylällä oleva tieto.

Tunkeutumisen tulee tapahtua järjestelmän turvajärjestely murtamalla. Tästä esimerkkinä säännöksessä mainitaan toisen käyttäjätunnuksen käyttäminen. Turvajärjestely on läpäistävä jollain tekijän nimenomaisella toimella. Toiselta luvallisesti saadun käyttäjätunnuksen käyttäminen ei ole siten tietomurtona rangaistavaa.

Säännöksen 2 momentissa kriminalisoidaan edellisen lisäksi tietojärjestelmässä olevien tietojen sieppaaminen teknisen erikoislaitteen avulla. Silloin ei edellytetä varsinaista järjestelmään tunkeutumista, vaan tietomurto toteutetaan esimerkiksi tallentamalla ja analysoimalla tietokoneesta lähtevää niin sanottua hajasäteilyä.

Tekijän tulee olla tahallisuuden edellyttämällä tavalla tietoinen siitä, että hän murtautumalla tunkeutuu oikeudettomasti tietojärjestelmään. Rangaistavaa ei ole se, että joku pääsee tai joutuu vahingossa toisen tietojärjestelmään.

Rikos täyttyy heti kun järjestelmän suojaus on läpäisty. Jos turvajärjestelmä on monivaiheinen, edellytetään että viimeinenkin vaihe on läpäisty. Sitä ennen on kysymys rikoksen yrityksestä.

Tietomurron täytyminen ei edellytä, että järjestelmässä oleviin tietoihin millään tavalla kajotaan. Jos rikos etenee tietojen käyttämiseen tai vahingoittamiseen, tekoon soveltuvat rikoslain 28 luvun säännökset luvattomasta käytöstä tai 35 luvun säännökset vahingonteosta.

Tietomurron yritys on rangaistava. Rangaistavaa on jo yrittää selvittää tietojärjestelmää suojaava käyttäjätunnus tai murtaa muu turvajärjestely, jos teko tehdään tarkoituksin oikeudettomasti tunkeutua tietojärjestelmään. Oikeuskäytännössä on katsottu, että jo pelkkä tietoturva-aukon etsiminen niin sanotulla porttiskannauksella täyttää tietomurron yrityksen tunnusmerkistön (KKO:2003:36). Tietomurron yrityksestä ei sen sijaan ole kysymys silloin, jos joku erehdyksessä pyrkii tietojärjestelmään, johon pääsyyn hänellä ei ole oikeutta.

Tietomurtosäännökset ovat toissijaisia. Jos kysymyksessä on esimerkiksi yritysvakoilua varten tapahtuva tietojärjestelmään tunkeutuminen, tietojärjestelmään tallennettuun tietoon tai itse järjestelmään kohdistuva vahingonteko taikka viestintäsalaisuuden loukkaus, säännökset syrjäytyvät. Luvatonta käyttöä koskeva säännös on sovellettavissa, jos tekijä käyttää tietojärjestelmää jollekin sille ominaisella tavalla, esimerkiksi hankkii itselleen maksullisesta tietopankista tietoja ilmaiseksi. Jos tällainen aikomus on näytettävissä toteen jo tunkeutumisen tapahtuessa, kysymys voi olla luvattoman käytön yrityksestä.

Voimassa olevat säännökset vastaavat artiklan velvoitteita. Ehdotuksen mukaan Suomi antaa 40 artiklan mukaisen selityksen, jonka mukaan se käyttää hyväkseen oikeuttaan asettaa rangaistavuuden edellytykseksi sen, että rikos on tehty turvajärjestelyt murtamalla.

Artikla ei edellytä lainsäädännön muuttamista.

### **Viestintäsalaisuuden loukkaaminen (3 artikla)**

Artiklan mukaan tahallinen ja oikeudeton teknisin keinoin tapahtuva tiedon hankkiminen tietojärjestelmän sisäisestä tai tietojärjestelmien välisestä luottamuksellisen datan siirrosta, sekä tällaista dataa sisältävästä tietojärjestelmästä lähtevästä sähkömagneettisesta säteilystä on säädettävä rangaistavaksi teoksi. Sopimuspuoli voi asettaa rangaistavuuden edellytykseksi sen, että rikos on tehty epärehellisin tarkoituksin, tai että se liittyy sellaiseen tietojärjestelmään, joka on kytketty toiseen tietojärjestelmään.

Artiklaa käsitellään selitysmuistion kohdissa 51-59. Selitysmuistion mukaan artiklan tarkoituksena on turvata yksityisyyden suoja kaiken muotoisessa sähköisessä viestinnässä sen teknisestä toteuttamistavasta riippumatta. Artiklan soveltamisalaan kuuluvat ainoastaan teknisellä keinolla tapahtuvat teot. Teknisellä keinolla viitataan laitteiden ja ohjelmien lisäksi myös salasanan käyttämiseen. Luottamuksellinen datan siirto tarkoittaa kohdeviestintänä tapahtuvaa viestintää. Ratkaisevaa ei ole kuitenkaan käytetyn viestintävälineen luonne vaan itse viestin luottamuksellisuus. Tämän vuoksi myös joukkoviestintävälineessä välitetty luottamuksellinen viesti voi kuulua artiklan soveltamisalaan. Viestintä voi olla tietokoneiden välistä, yhden tietokoneen eri osien välistä ja myös käyttäjän ja tietokoneen välistä. Viestintä voi tapahtua myös radioaaltojen välityksellä. Artikla kattaa myös niin sanottua hajasäteilyä sieppaamalla tapahtuvat teot. Artiklassa edellytetään, että rangaistavaksi säädettävä teko tapahtuu oikeudettomasti. Teon oikeutus voi perustua esimerkiksi toisen osapuolen suostumukseen tai viranomaisen oikeuteen tutkia rikoksia. Artikla ei myöskään koske internetissä käytettävien niin sanottujen evästeiden käyttöä käyttäjien seurantaan.

Suomessa voimassa olevat säännökset sopimuksessa tarkoitettua tekoa vastaavasta rikoksesta sisältyvät rikoslain viestintäsalaisuuden loukkausta koskevan 38 luvun 3 §:ään ja törkeän tekemuodon osalta 4 §:ään. Mainitun 3 §:n 1 momentin mukaan viestintäsalaisuuden loukkauksesta on tuomittava se joka oikeudettomasti avaa toiselle osoitetun kirjeen tai muun suljetun viestin

taikka suojaus murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka hankkii tiedon televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta. Teon katsominen törkeäksi edellyttää 4 §:n mukaan erityisen luottamusaseman hyväksikäyttöä, erityistä suunnitelmallisuutta tai teon kohdistumista erityisen arkaluonteisiin tietoihin. Molempien tekemuotojen yritys on rangaistava.

Säännöksen soveltamisala on laaja. Säännös kattaa datan muodossa olevien viestien lisäksi myös muut viestit niiden muodosta riippumatta. Datan muodossa olevan viestin pitää kuitenkin olla joko ulkopuoliselta suljettu tai televerkossa välitettävänä. Siten esimerkiksi sähköpostiviestin saama suoja perustuu säännöksen eri kohtiin viestin sijaintipaikasta riippuen. Sähköpostiviesti saa televerkossa siirrettävän viestin suojaa silloin kun se on televerkossa ja ulkopuolisilta suojatun viestin suojaa silloin kun se on osapuolen hallinnassa esimerkiksi tietokoneeseen tallennettuna.

Televerkolla tarkoitetaan säännöksessä yleisen televerkon lisäksi myös esimerkiksi yrityksen sisäistä televerkkoa. Televiestillä tarkoitetaan mitä hyvänsä viestiä, joka on säännöksen esimerkkiluettelossa mainitun kaltainen. Vastaavuutta on lain esitöiden mukaan (HE 94/1993) tarkasteltava erityisesti viestin yksityisyyttä silmällä pitäen. Esimerkiksi televerkossa välitettävää joukkoviestintää säännös ei koske. Säännös suojaa viestin sisällön lisäksi myös tietoa viestin lähettämisestä ja vastaanottamisesta. Rangaistavaa on siten esimerkiksi hankkia tieto siitä, mihin numeroon tietystä puhelimesta on soitettu.

Säännös suojaa myös sellaista viestiä, joka sitä mihinkään siirtämättä tallennetaan tietokoneeseen tietyn henkilön tai henkilöpiirin luettavaksi. Rangaistavuuden edellytyksenä on kuitenkin se, että viesti on teknisin keinoin suojattu ulkopuolisilta ja että tiedon hankkiminen viestistä tapahtuu tämä suojaus murtaen. Suojaus murtaen voi lain esitöiden (HE 94/1993) tapahtua vastaavalla tavalla kuin tietomurron osalta. Säännös kattaa siten myös niin sanotun hajasäteilyn hyväksikäytön.

Teon tulee tapahtua oikeudettomasti. Teon oikeutus voi perustua esimerkiksi toisen osapuolen suostumukseen tai viranomaisen oikeuteen tutkia rikoksia.

Voimassa olevat säännökset vastaavat tältä osin artiklan velvoitteita.

Artiklan mukaan osapuoli voi asettaa rangaistavuuden edellytykseksi sen, että rikos on tehty epärehellisin tarkoituksin, tai että se liittyy sellaiseen tietojärjestelmään, joka on kytketty toiseen tietojärjestelmään. Suomella ei ole tarvetta asettaa rangaistavuudelle artiklassa mainittuja lisäedellytyksiä.

Artikla ei edellytä lainsäädännön muuttamista.

### **Datan vahingoittaminen (4 artikla)**

Artiklan 1 kappaleen mukaan tahallinen ja oikeudeton datan vahingoittaminen, tuhoaminen, turmeleminen, muuttaminen tai poistaminen on säädettävä rangaistavaksi teoksi.

Artiklaa käsitellään selitysmuistion kohdissa 60-64. Selitysmuistion mukaan artiklan tarkoituksena on saattaa data samankaltaisen suojan kohteeksi kuin reaali maailman esineet. Tekotapaluettelossa on pyritty kattavuuteen. Tekotavat ovat tämän vuoksi osin päällekkäisiä. Koska esimerkiksi datan poistaminen järjestelmästä ei tarkoita välttämättä datan tuhoamista, molemmat tekotavat on

mainittu erikseen. Samanlaisista vähäisiin merkityseroihin liittyvistä syistä myös datan muuttaminen, turmeleminen ja vahingoittaminen on mainittu artiklassa erillisinä tekoapoina. Yhteistä teko tavoille on se, että teon seurauksena tallennusalustalla oleva data ei ole enää samanlaista kuin ennen tekoa. Tyypillisenä esimerkkinä voidaan mainita dataa muuttavan tietokoneviruksen aiheuttama vahinko. Teon tulee olla oikeudeton ja tahallinen. Teon oikeutus voi perustua käytännössä lähinnä datan haltijan suostumukseen.

Suomessa voimassa olevat säännökset sopimuksessa tarkoitettua datan vahingoittamista vastaavasta rikoksesta sisältyvät rikoslain vahingontekoa koskevaan 35 luvun 1 §:ään. Mainitun pykälän 2 momentin mukaan vahingonteosta on tuomittava se joka toista vahingoittaakseen oikeudettomasti hävittää, turmelee, kätkee tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen.

Lain esitöiden (HE 66/1988) mukaan tietovälineelle tallennetulla tiedolla tarkoitetaan tiedon asiasisältöä eli informaatioita ja asiasisältöä viestittäviä merkkejä eli dataa. Tietovälineellä tarkoitetaan esimerkiksi asiakirjaa, äänilevyä, filmiä, magneettinauhaa tai tietokonelevykettä. Säännös kattaa siten selvästi artiklassa tarkoitettua datan. Toisaalta säännöksen soveltamisalue on artiklan vaatimuksia huomattavasti laajempi.

Vaikka säännöksen tekoapaluettelo ei sanamuodoltaan vastaa artiklassa olevaa luetteloa, lopputulos on kuitenkin sama. Turmelemisella tarkoitetaan säännöksessä datan muuttamista sisällöltään toiseksi taikka täysin epäymmärrettävään tai käyttökelvottomaan muotoon. Säännös kattaa siten kaiken sellaisen dataan kajoamisen, jonka seurauksena tallennusalustalla oleva data joko muuttuu tai häviää. Myös teon oikeudettomuutta ja tahallisuutta koskevat edellytykset ovat samat kuin artiklassa.

Voimassa olevat säännökset vastaavat artiklan velvoitteita.

Artiklan 2 kappaleen mukaan sopimuspuoli voi tehdä varauman, jonka mukaan rangaistavuuden edellytyksenä on, että 1 kappaleessa tarkoitettu teko aiheuttaa huomattavaa vahinkoa. Suomella ei ole tarvetta tehdä 2 kappaleen mukaista varaamaa.

Artikla ei edellytä lainsäädännön muuttamista.

### **Tietojärjestelmän häirintä (5 artikla)**

Artiklan mukaan tahallinen ja oikeudeton tietojärjestelmän toiminnan vakava estäminen dataa syöttämällä, siirtämällä, vahingoittamalla, tuhoamalla, turmelemalla, muuttamalla tai poistamalla on säädetty rangaistavaksi teoksi.

Artiklaa käsitellään selitysmuistion kohdissa 65-70. Selitysmuistion mukaan artiklan tarkoituksena on suojata tietojärjestelmien häiriötöntä toimintaa. Tekoapoina tulevat ensinnäkin kyseeseen järjestelmässä olevaan dataan kajoavat tekoavat eli vahingoittaminen, tuhoaminen, turmeleminen, muuttaminen ja poistaminen. Tältä osin tekoapaluettelo vastaa edellä 4 artiklan yhteydessä käsitellyä datan vahingoittamisen tekoapaluetteloa.

Tämän lisäksi tietojärjestelmän häirintä voidaan tehdä myös dataa syöttämällä tai siirtämällä. Datan syöttämisellä tai siirtämisellä tarkoitetaan artiklassa sellaista hyökkäystä, joka aiheuttaa kohteessa toimintahäiriön kuitenkin siten, että tietojärjestelmässä olevaa dataa ei millään tavalla vahingoiteta. Toimintahäiriö voi seurata tarkoituksellisesta ylikuormituksesta tai esimerkiksi syötettävän datan



häiriöitä aiheuttavista ominaisuuksista. Hyökkäys ei siten kohdistu järjestelmässä olevaan dataan vaan järjestelmän toimintaan. Tällainen esimerkiksi sähköpostipalvelimeen kohdistuva niin sanottu palvelunestohyökkäys mainitaan selitysmuistiossa esimerkkinä artiklan tyypillisestä soveltamistilanteesta.

Artiklan mukaan ainoastaan tietojärjestelmän toiminnan vakava estäminen on säädettävä rangaistavaksi. Vakavuuskynnyksen osapuolet saavat määritellä harkintansa mukaan. Osapuolet voivat siten päättää edellytetäänkö teon seurauksena järjestelmän täydellistä vai osittaista tai pysyvää vai tilapäistä lamaantumista.

Teon tulee olla oikeudeton ja tahallinen. Teon oikeutus voi perustua käytännössä lähinnä datan haltijan suostumukseen. Tahallisuuden osalta on huomattava, että tahallisuuden pitää kattaa myös vahingoittamistarkoitus. Suurien sähköpostimäärien lähettäminen saattaa käytännössä hidastaa sähköpostipalvelimen toimintaa ja aiheuttaa vastaanottajalle haittaa. Tämän artiklan soveltamisalaan tällaisen niin sanotun roskapostin lähettäminen kuuluu ainoastaan, jos sen nimenomaisena tarkoituksena on tietojärjestelmän häirintä. Jos tekijän tarkoituksena sen sijaan on saada kirjoittamansa viesti lähetettyä mahdollisimman monelle vastaanottajalle kyseessä ei ole artiklassa tarkoitettu rikos.

Suomessa voimassa olevat säännökset sopimuksessa tarkoitettua tietojärjestelmän häirintää lähinnä vastaavasta rikoksesta sisältyvät rikoslain tietoliikenteen häirintää koskevaan 38 luvun 5 §:ään. Mainitun lainkohdan mukaan tietoliikenteen häirinnästä on tuomittava se, joka puuttumalla postiliikenteessä taikka tele- tai radioviestinnässä käytettävän laitteen toimintaan, lähettämällä ilkeävaltaisessa tarkoituksessa radiolaitteella tai televerkossa häiritseviä viestejä tai muulla vastaavalla tavalla oikeudettomasti estää tai häiritsee postiliikennettä taikka tele- tai radioviestintää.

Lain esitöiden (HE 94/1993) mukaan säännös koskee postiliikennettä sekä tele- ja radioviestintää kokonaisuudessaan, siis sekä kohde- että joukkoviestintää, esimerkiksi yleisradiotoimintaa. Säännöksen tarkoituksena on siten postiliikenteen lisäksi kattaa kaikenlainen sähköinen viestintä viestien sisällöstä ja viestinnän teknisestä toteuttamistavasta riippumatta. Viestien siirto voi tapahtua johtoja pitkin tai langattomasti. Sillä, onko käytettävä televerkko yleinen vai esimerkiksi yrityksen sisäinen erillisverkko, ei ole merkitystä. Säännöksen soveltamisalaa ei ole rajattu tekotavan osalta muutoin kuin esimerkeillä. Tämän vuoksi sen soveltamisala on laaja koskien artiklassa tarkoitettujen tekojen lisäksi esimerkiksi postilaatikkojen rikkomista ja analogisen televisiolähetyksen häirintää.

Artiklassa tarkoitettujen tekojen kuten palvelunestohyökkäyksen osalta säännös kattaa selkeästi kaikki sellaiset teot, joiden voidaan katsoa kohdistuvan viestintään.

Palvelunestohyökkäyksien kohteena ovat tyypillisesti juuri sähköposti- ja internetpalvelimet sekä muut vastaavat viestien siirtoa, reititystä ja jakelua hoitavat palvelimet.

Nykyinen tietoliikenteen häirintää koskeva sääntely kattaa siten käytännössä artiklan ydinalueen.

Nykyinen säännös kattaa kuitenkin ainoastaan tele- ja radioviestinnän häirinnän. Säännöksen soveltamisala on sinänsä laaja, mutta se rajoittuu ainoastaan viestintään eli viestien siirtämiseen paikasta toiseen. Säännös ei kata sellaista sopimuksessa rangaistavaksi edellytettyä tietojärjestelmän häirintää, jonka ei voida edes välillisesti katsoa häiritsevän viestintää. Joissakin tapauksissa sopimuksessa tarkoitettu tietojärjestelmän häirintä voisi tulla rangaistavaksi rikoslain 35 luvun 1 §:n 2 momentissa säädettynä vahingontekona. Mainittu säännös ei kuitenkaan kata sopimuksessa

tarkoitettua tekoa silloin kun tekotapana on jokin muu kuin suoranainen dataan kajoaminen. Myöskään rikoslain 28 luvun 7 §:ssä tarkoitettu luvaton käyttö ei kata sopimuksessa tarkoitettua tekoa silloin, kun tekotapa ei sisällä suoranaista tietojärjestelmän käyttöä.

Tämän vuoksi artikla edellyttää muutoksia nykyiseen lainsäädäntöön.

Muutoksen toteuttaminen laajentamalla tietoliikenteen häirintää koskevan säännöksen soveltamisala kaikkia tietojärjestelmiä koskevaksi ei ole säännösten viestinnän yleisempään suojaan liittyvä alkuperäinen suojelukohde huomioon ottaen tarkoituksenmukaista. Tämän vuoksi hallituksen esitykseen sisältyy muutosehdotus, jonka mukaan rikoslain 38 lukuun lisättäisiin uudet tietojärjestelmän häirintää koskevat erilliset säännökset.

Ehdotuksen uuden 7 a §:n mukaan tietojärjestelmän häirinnästä tuomittaisiin se, joka toista vahingoittaakseen oikeudettomasti, dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla näihin verrattavalla tavalla estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä. Ehdotukseen sisältyy lisäksi säännös törkeästä tekemuodosta sekä eräitä muita säännöksiä. Ehdotuksen sisältöä on tarkemmin selostettu kyseisen lakiehdotuksen yksityiskohtaisissa perusteluissa.

Ehdotetun muutoksen tultua voimaan voimassa olevat säännökset vastaavat artiklan vaatimuksia.

### **Laitteiden väärinkäyttö (6 artikla)**

Artiklan 1 kappaleen a) kohdan i) alakohdan mukaan sellaisten välineiden ja ohjelmien tuottaminen, myynti, hankkiminen, tuonti, levittäminen tai muu saataville asettaminen, jotka on suunniteltu tai muutettu ensisijaisesti sopimuksen 2-5 artiklan mukaisesti rangaistaviksi säädettyjen rikosten tekemistä varten, on säädettävä rangaistavaksi teoksi. Sama koskee ii) alakohdan mukaan myös sellaista tietojärjestelmän salasanaa tai käyttäjätunnusta tai muuta vastaavaa tietoa, joka mahdollistaa pääsyn tietojärjestelmään tai sen osaan. Lisäksi sopimuksessa edellytetään että edellä kuvatun toiminnan tarkoituksena 2-5 artiklassa tarkoitettujen rikosten tekeminen.

Artiklan 1 kappaleen b) kohdan mukaan, myös edellä a) kohdassa mainittujen tuotteiden hallussapito on säädettävä rangaistavaksi teoksi, jos hallussapidon tarkoituksena on 2-5 artiklassa tarkoitettujen rikosten tekeminen. Sopimuspuoli voi tältä osin asettaa rikosvastuun syntymisen edellytykseksi sen, että tekijän hallussa on useita tällaisia tuotteita.

Artiklan 2 kappaleessa on vielä selvyuden vuoksi määräys, jonka mukaan artiklan määräysten ei katsota perustavan rikosvastuuta muun muassa silloin, kun artiklan 1 kappaleessa tarkoitettun tuotannon, myynnin, hankkimisen, tuonnin, levittämisen tai muun saataville asettamisen tarkoituksena ei ole tehdä tämän yleissopimuksen 2-5 artiklan mukaisesti rangaistavaksi säädettyä rikosta, vaan tietojärjestelmän luvallinen testaus tai suojelu.

Artiklaa käsitellään selitysmuistion kohdissa 71-78. Selitysmuistion mukaan artiklan tarkoituksena on välillisesti ehkäistä varsinaisia tietoverkkorikoksia puuttamalla jo niissä käytettävien välineiden levittämiseen ja hallussapitoon itsenäisellä rikossäännöksellä.

Välineen rikollisena käyttötarkoituksena voi olla yhtä hyvin vahingon aiheuttaminen kuin oikeudeton järjestelmään tunkeutuminen. Artikla kattaa siten virusten ja muiden vastaavien haittaohjelmien lisäksi myös tietomurrossa käytettävät ohjelmat. Artikla kattaa tietokoneohjelmien

lisäksi myös laitteet. Näiden lisäksi artiklaa sovelletaan myös salasanoihin ja muuhun todentamisessa käytettävään dataan.

Välineiden kaksikäyttöisyydestä aiheutuviin ongelmiin on kiinnitetty artiklan valmistelussa erityistä huomiota. Jos pelkästään sellaiset välineet, joiden yksinomainen käyttötarkoitus olisi tietoverkkorikosten tekeminen, olisivat artiklan soveltamisalan piirissä, rikosoikeudellinen suoja kutistuisi käytännössä näyttöongelmien vuoksi lähes olemattomaksi. Tämän vuoksi artikla koskee välineitä, joiden ensisijainen käyttötarkoitus on rikosten tekeminen. Selitysmuistion mukaan ensisijaisella käyttötarkoituksella tarkoitetaan välineen objektiivista käyttötarkoitusta. Kaksikäyttöiset välineet rajautuvat käytännössä tosin tämänkin muotoilun perusteella pääsääntöisesti soveltamisalan ulkopuolelle.

Teon tulee olla oikeudeton ja tahallinen. Oikeutettua on esimerkiksi tietorikosvälineiden levittäminen ja hallussapito tarkoituksin, että niitä käytetään järjestelmien kehittämiseen ja testaamiseen. Sama asia toistetaan vielä artiklan 2 kappaleessa.

Suomessa voimassa olevat säännökset sopimuksessa tarkoitettua laitteiden väärinkäyttöä lähinnä vastaavasta rikoksesta sisältyvät rikoslain vaaran aiheuttamista tietojenkäsittelylle koskevaan 34 luvun 9 a §:ään. Mainitun pykälän 1 kohdan mukaan vaaran aiheuttamisesta tietojenkäsittelylle on tuomittava se, joka aiheuttaakseen haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle valmistaa tai asettaa saataville sellaisen tietokoneohjelman tai ohjelmakäskeyjen sarjan, joka on suunniteltu vaarantamaan tietojenkäsittelyä tai tieto- tai telejärjestelmän toimintaa taikka vahingoittamaan sellaisen järjestelmän sisältämiä tietoja tai ohjelmistoja, tai levittää sellaista tietokoneohjelmaa tai ohjelmakäskeyjen sarjaa. Saman pykälän 2 kohdan mukaan tuomitaan myös se, joka asettaa saataville ohjeen 1 kohdassa tarkoitettun tietokoneohjelman tai ohjelmakäskeyjen sarjan valmistamiseen tai levittää sellaista ohjetta.

Nykyinen säännös kattaa sopimuksessa tarkoitetuista teoista ainoastaan tietokoneviruksen ja vastaavan haittaohjelman valmistamisen ja levittämisen. Nykyinen sääntely ei sen sijaan kata haittaohjelman hallussapitoa. Sopimuksessa tarkoitettuja laitteita tai salasanvoja koskevia säännöksiä voimassaolevissa säännöksissä ei myöskään ole. Sama koskee sellaisia rikosten tekemisessä käytettäviä ohjelmia, jotka eivät ole varsinaisia haittaohjelmia, kuten esimerkiksi tietomurto-ohjelmia.

Tämän vuoksi artikla edellyttää muutoksia nykyiseen lainsäädäntöön.

Hallituksen esitykseen sisältyy ehdotus, jonka mukaan rikoslain 34 lukuun lisätään uudet tietoverkkorikosvälineitä koskevat rikossäännökset siten, että 9 a §:ssä säädetään välineiden valmistamisesta ja levittämisestä sekä uudessa 9 b §:ssä välineiden hallussapidosta.

Ehdotetun 9 a §:n mukaan teon kohteena voi olla laite tai tietokoneohjelma tai ohjelmakäskeyjen sarja, joka on suunniteltu tai muunnettu ensisijaisesti vaarantamaan tai vahingoittamaan tietojenkäsittelyä taikka tieto- tai viestintäjärjestelmän toimintaa taikka tietojärjestelmän suojausten murtamiseen. Säännöksen soveltamisala on tältä osin laaja ja sen tarkoituksena on kattaa yhtäältä tietomurtoihin ja puhtaaseen ilkivaltaiseen vahingontekoon tarkoitettut välineet sekä toisaalta fyysiset laitteet, tietokoneohjelmat ja yksittäiset ohjelmakoodin palaset. Lähtökohtaisesti laajaa soveltamisalaa rajoittaa kuitenkin merkittävästi teolta edellytettävä subjektiivinen vahingoittamis- tai haittaamistarkoitus sekä levittämisen tai muun toimenpiteen kohteena olevalta välineeltä edellytettävä objektiivisesti arvioiden moitittava käyttötarkoitus. Molempien edellytysten pitää täytyä samanaikaisesti, jotta teko olisi säännöksen mukaan rangaistava.

Ehdotetun 9 b §:n mukaan hallussapidosta tuomitaan se, joka ilman hyväksyttävää syytä pitää hallussaan 9 a §:ssä tarkoitettua tietoverkkorikosvälinettä.

Ehdotuksen sisältöä on tarkemmin selostettu kyseisen lakiehdotuksen yksityiskohtaisissa perusteluissa.

Ehdotetun muutoksen tultua voimaan voimassa olevat säännökset vastaavat artiklan vaatimuksia.

Artiklan 3 kappaleen mukaan sopimuspuoli voi tehdä varauman, jonka mukaan se ei sovelle tämän artiklan 1 kappaletta, edellyttäen kuitenkin, että varauma ei koske tämän artiklan 1 kappaleen a kohdan ii alakohdassa tarkoitettujen salasanojen tai käyttäjätunnusten myyntiä, levittämistä tai muuta saataville asettamista.

Suomella ei ole tarvetta tehdä 3 kappaleessa tarkoitettua varaumaa.

## **2 osasto Tietokoneavusteiset rikokset**

### **Tietokoneavusteinen väärennys (7 artikla)**

Artiklan mukaan sellainen tahallisen ja oikeudettoman datan syöttäminen, muuttaminen, tuhoaminen tai poistaminen, jonka tuloksena syntyvä väärä data on tarkoitettu käytettäväksi oikeudellisissa tarkoituksissa harhauttavana todisteena, on säädettävä rangaistavaksi teoksi riippumatta siitä, onko data sellaisenaan luettavissa tai ymmärrettävissä. Sopimuspuoli voi asettaa rikosvastuun syntymisen edellytykseksi sen, että teko on toteutettu petostarkoituksin tai muuta epärehellistä tarkoitusta varten.

Artiklaa käsitellään selitysmuistion kohdissa 81-85. Selitysmuistion mukaan artiklan tarkoituksena on saattaa tietokoneavusteinen väärennys samanlaisen rikosoikeudellisen sääntelyn piiriin kuin tavanomainen väärennys. Artiklan suojelukohteena on siten oikeudellisesti merkityksellisen datan eheys ja luotettavuus.

Tekotapaluettelo vastaa pääosin tietojärjestelmän häirintää koskevan 5 artiklan tekotapaluettelo. Olennaista 7 artiklan osalta on se, että teon seurauksena syntyy väärää dataa, jota voidaan käyttää harhauttavana todisteena oikeudellisessa asiayhteydessä. Sillä, onko teon kohteena yksityinen vai julkinen datan muodossa oleva asiakirja tai muu dokumentti, ei ole sääntelyn kannalta merkitystä.

Suomessa voimassa olevat säännökset sopimuksessa tarkoitettua tietokoneavusteista väärennystä vastaavasta rikoksesta sisältyvät rikoslain väärennystä koskevaan 33 luvun 1 §:ään ja sitä täydentävään määritelmiä koskevaan 6 §:ään. Mainitun rikossäännöksen mukaan väärennyksestä tuomitaan se, joka valmistaa väärän asiakirjan tai muun todistuskappaleen tai väärentää sellaisen käytettäväksi harhauttavana todisteena taikka käyttää väärää tai väärennettyä todistuskappaletta tällaisena todisteena. Määritelmäsäännöksen mukaan todistuskappaleena pidetään myös automaattiseen tietojenkäsittelyyn soveltuvaa tallennetta, jos sitä käytetään tai voidaan käyttää oikeudellisesti merkityksellisenä todisteena oikeuksista, velvoitteista tai tosiasioista.

Säännöksen mukaan tekotapoina tulevat kyseeseen todistuskappaleen valmistaminen tai väärentäminen. Valmistaminen tarkoittaa uuden todistuskappaleen luomista ja väärentäminen jo olemassa olevan todistuskappaleen muuttamista sisällöltään toiseksi. Vähäisenkin muutoksen

tekeminen voi tarkoittaa väärentämistä. Säännöksessä mainitut kaksi tekotapaa kattavat yhdessä selvästi artiklan tekotapaluettelon.

Myös automaattiseen tietojenkäsittelyyn soveltuva tallenne voi olla väärennyksen kohteena. Tällaisena tallenteena pidetään lain esitöiden (HE 66/1988) myös esimerkiksi tietokoneen muistiin konekielisessä muodossa tallennettua informaatiota, jota ei vielä ole näkyvässä ja ymmärrettävässä muodossa tulostettu paperille tai näyttöruudulle. Säännöksessä tarkoitettu tallenne vastaa siten selkeästi väärennyksen kohteen osalta artiklassa tarkoitettua dataa.

Voimassa olevat säännökset vastaavat tältä osin artiklan velvoitteita.

Artikla ei edellytä lainsäädännön muuttamista.

Artiklan viimeisen virkkeen mukaan sopimuspuoli voi asettaa rikosvastuun syntymisen edellytykseksi sen, teko on toteutettu petostarkoituksin tai muuta epärehellistä tarkoitusta varten.

Suomella ei ole tarvetta tehdä tällaista varaumaa.

### **Tietokoneavusteinen petos (8 artikla)**

Artiklan mukaan dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla taikka tietojärjestelmän toimintaa häiritsemällä tehty tahallinen ja oikeudeton taloudellisen vahingon aiheuttamisen toiselle tarkoituksin saada itselle tai toiselle taloudellista hyötyä petoksella tai muulla epärehellisellä keinolla on säädettävä rangaistavaksi teoksi.

Artiklaa käsitellään selitysmuistion kohdissa 86-90. Selitysmuistion mukaan artiklan tarkoituksena on säätää rangaistavaksi sellaiset omaisuusrikokset, jotka toteutetaan dataan tai tietojärjestelmän toimintaan puuttumalla. Tekotapaluettelo vastaa pääosin tietojärjestelmän häirintää koskevan 5 artiklan tekotapaluettelo. Tämän lisäksi artiklassa mainitaan kattavuuden varmistamiseksi myös tietojärjestelmän toiminnan häiritseminen. Olennaista 8 artiklan osalta on se, että teon seurauksena syntyy taloudellista vahinkoa toiselle ja että teko tehdään taloudellisessa hyötymis- tai hyödyttämistarkoituksessa. Selvyyden vuoksi artiklassa todetaan vielä, että teon tulee olla oikeudeton ja tahallinen. Tahallisuuden osalta on huomattava, että tahallisuuden pitää kattaa kaikki tunnusmerkistötekijät.

Suomessa voimassa olevat säännökset sopimuksessa tarkoitettua tietokoneavusteista petosta vastaavasta rikoksesta sisältyvät rikoslain petosta koskevaan 36 luvun 1 §:ään ja erityisesti sen 2 momenttiin. Pykälän perustunnusmerkistön sisältävän 1 momentin mukaan petoksesta tuomitaan se joka, hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä taikka toista vahingoittaakseen, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai jättämään tekemättä jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai sille, jonka eduista tällä on ollut mahdollisuus määrätä.

Tietokoneavusteista tekotapaa koskevan 2 momentin mukaan petoksesta tuomitaan nykyisin voimassa olevan säännöksen mukaan myös se, joka 1 momentissa mainitussa tarkoituksessa tietojenkäsittelylaitteeseen vääriä tietoja syöttämällä tai koneelliseen tietojenkäsittelyyn muuten puuttumalla vääristää tietojenkäsittelyn lopputuloksen ja siten aiheuttaa toiselle taloudellista vahinkoa.

Lisäksi rikoslain 37 luvun 8 §:n mukaan tietoverkossa käytettäväksi soveltuvan maksuvälineen luvaton käyttäminen tai luovuttaminen taikka tilin katteen tai sovitun enimmäisluottorajan ylitys tuomitaan maksuvälinepetoksena.

Sääntelyä on osin tarkoitus muuttaa Euroopan Unionin neuvoston 28 päivänä toukokuuta 2001 hyväksymän muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten ja väärennysten torjunnasta annetun puitepäättöksen kansallisen täytäntöönpanon yhteydessä (HE 2/2003). Eduskunta on hyväksynyt asiaa koskevan hallituksen esityksen, mutta laki ei ole vielä voimassa.

Uuden säännöksen mukaan petoksesta tuomitaan se, joka 1 momentissa mainitussa tarkoituksessa dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttamalla saa aikaan tietojenkäsittelyn lopputuloksen vääristymisen ja siten aiheuttaa toiselle taloudellista vahinkoa.

Ehdotetun muutoksen tultua voimaan voimassa olevat säännökset vastaavat lähes sanatarkasti artiklan vaatimuksia.

### **3 osasto Viestin sisältöön liittyvät rikokset**

#### **Lapsipornografiaan liittyvät rikokset (9 artikla)**

Artiklan 1 kappaleen mukaan seuraavat teot on säädetty rangaistavaksi teoksi:

- a) lapsipornografian tuottamisen tietojärjestelmän välityksellä tapahtuvaa levittämistä varten;
- b) lapsipornografian tarjoamisen tai saataville asettamisen tietojärjestelmän välityksellä;
- c) lapsipornografian levittämisen tai siirtämisen tietojärjestelmän välityksellä;
- d) lapsipornografian hankkimisen omaan tai toisen käyttöön tietojärjestelmän välityksellä;
- e) lapsipornografian hallussapidon tietojärjestelmässä tai tietovälineellä.

Artiklan 2 kappaleen mukaan 1 kappaletta sovellettaessa lapsipornografialla tarkoitetaan myös pornografista kuvatallennetta, jossa esitetään:

- a) alaikäistä seksuaalisessa kanssakäymisessä;
- b) alaikäiseltä näyttävää henkilöä seksuaalisessa kanssakäymisessä;
- c) todellisuudenmukaisia kuvia alaikäisestä seksuaalisessa kanssakäymisessä.

Artiklan 3 kappaleen mukaan 2 kappaletta sovellettaessa alaikäisellä tarkoitetaan jokaista alle 18-vuotiasta henkilöä. Sopimuspuoli voi soveltaa myös alemmää ikärajaa, joka ei kuitenkaan saa olla alempi kuin 16 vuotta.

Suomessa voimassa olevat säännökset sopimuksessa tarkoitettuja lapsipornografiaan liittyviä rikoksia vastaavista rikoksista sisältyvät rikoslain sukupuolisiveellisyyttä loukkaavan kuvan levittämistä koskevaan 17 luvun 18 §:ään ja sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan hallussapitoa koskevaan 19 §:ään. Mainitun 18 §:n mukaan sukupuolisiveellisyyttä loukkaavan kuvan levittämisestä tuomitaan se joka pitää kaupan tai vuokrattavana tai levittää taikka siinä tarkoituksessa valmistaa tai tuo maahan kuvia tai kuvatallenteita, joissa sukupuolisiveellisyyttä loukkaavasti esitetään lasta tai väkivaltaa taikka eläimeen sekaantumista. Mainitun 19 §:n mukaan sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan hallussapidosta tuomitaan se, joka oikeudettomasti pitää hallussaan valokuvaa, videonauhaa, elokuvaa tai muuta todellisuudenmukaista kuvatallennetta, jossa esitetään lasta sukupuoliyhteydessä tai siihen

rinnastettavassa seksuaalisessa kanssakäymisessä taikka muulla sukupuolisiveellisyyttä ilmeisen loukkaavalla tavalla.

Nykyiset säännökset kattavat myös tietojärjestelmän välityksellä tapahtuvan lapsipornografian levittämisen ja hallussapidon. Artikla ei tältä osin edellyttäisi lainsäädännön muuttamista.

Nykyisissä säännöksissä lapsella tarkoitetaan sukupuolisesti vielä osin tai kokonaan kehittymätöntä henkilöä, ohjeellisen ikärajan ollessa hallituksen esityksen perustelujen mukaan 16 vuotta. Artikla sen sijaan edellyttää kiinteää ikärajaa, joka ei saa olla 16 vuotta nuorempi. Tältä osin artikla edellyttää muutoksia voimassa olevaan lainsäädäntöön.

Euroopan Unionissa on valmisteilla ehdotus neuvoston puitepäätökseksi lasten seksuaalisen hyväksikäytön ja lapsipornografian torjumisesta. Puitepäätöksellä velvoitettaisiin jäsenvaltiot kriminalisoimaan tietyt lasten seksuaaliseen hyväksikäyttöön ja lapsipornografiaan liittyvät rikokset ja säättämään niistä tietynsuuruiset rangaistukset. Puitepäätökseen sisältyy 18 vuoden kiinteä ikäraja. Puitepäätöksen kansallisen täytäntöönpanon yhteydessä Suomen voimassa olevat säännökset on muutettava puitepäätöksen velvoitteiden mukaisiksi.

Jotta kyseessä olevia rikossäännöksiä ei tarvitsisi muuttaa kahteen kertaan lyhyen ajan sisällä, nyt käsillä olevan artiklan edellyttämät muutokset on tarkoituksenmukaista toteuttaa samassa yhteydessä kuin puitepäätöksen edellyttämät muutokset. Tässä yhteydessä arvioidaan myös tarve mahdollisen varauman tekemiseen.

#### **4 osasto Tekijänoikeusrikokset ja tekijänoikeuden lähioikeuksia koskevat rikokset**

##### **Tekijänoikeusrikokset ja tekijänoikeuden lähioikeuksia koskevat rikokset (10 artikla)**

Artiklan mukaan eräät tahalliset tekijänoikeuksia ja niiden lähioikeuksia koskevat loukkaukset on säädettävä rangaistaviksi teoiksi silloin, kun ne on tehty tietojärjestelmän avulla. Artiklan soveltamisala on rajattu koskemaan vain tekoja, jotka tehdään kaupallisessa tarkoituksessa. Artikla ei koske tekijänoikeuden moraalisia vaan ainoastaan taloudellisia oikeuksia. Artiklassa tarkoitetut tekijänoikeudet on artiklassa yksilöity tyhjentävästi viittauksella kansainvälisiin tekijänoikeussopimuksiin. Artikla velvoittaa siten vain huolehtimaan siitä, että myös tietojärjestelmien hyväksikäyttöön liittyvät tekotavat otetaan huomioon tekijänoikeussopimuksiin perustuvissa kriminalisoinneissa.

Artiklaa on käsitelty selitysmuistion kohdissa 107-117. Selitysmuistion mukaan juuri tekijänoikeusrikokset ovat teosten digitalisoitumisen ja tästä seuraavan helpon kopioitavuuden vuoksi ylivoimaisesti yleisin internetympäristössä esiintyvä rikostyyppi. Tämän vuoksi on ollut välttämätöntä ottaa sopimukseen myös tekijänoikeuden loukkauksia koskevat säännökset. Artikla ei sen sijaan koske patenttioikeutta eikä tavaramerkkioikeutta.

Artikla velvoittaa kutakin osapuolta ainoastaan viitattujen tekijänoikeussopimusten asettamissa rajoissa. Jos osapuoli ei ole osallisena tekijänoikeussopimuksessa artikla ei velvoita tältä osin lainkaan. Jos osapuoli on tehnyt tekijänoikeussopimukseen varauman, artikla velvoittaa ainoastaan varauman rajoittamassa laajuudessa. Jos osapuoli on aikeissa liittyä tekijänoikeussopimukseen, artikla velvoittaa vasta liittymisajankohdasta lukien. Vaikka artiklan velvoitteet on rajattu vain kaupallisessa tarkoituksessa tehtyihin tekoihin, tämä ei estä osapuolia menemästä pidemmälle.

Artiklassa viitattut kansainväliset sopimukset ovat seuraavat:

1. Bernin yleissopimus kirjallisten ja taiteellisten teosten suojaamisesta vuodelta 1886 (jäljempänä Bernin sopimus);
2. Rooman yleissopimus esittävien taiteilijoiden, äänitteiden valmistajien ja radioyrittäjien suojaamisesta vuodelta 1961 (jäljempänä Rooman sopimus);
3. Sopimus teollis- ja tekijänoikeuksien kauppaan liittyvistä näkökohdista vuodelta 1995 (jäljempänä TRIPS-sopimus);
4. WIPO:n tekijänoikeussopimus vuodelta 1996 ja
5. WIPO:n esitys- ja äänitesopimus vuodelta 1996.

Bernin sopimus (SopS 79/1986) on keskeisin tekijänoikeuksien kansainvälistä suojaa koskeva sopimus. Sopimus on tehty vuonna 1886 ja sitä on tarkistettu keskimäärin joka kahdeskymmenes vuosi. Sopimuksen viimeisin uudistaminen tapahtui Pariisissa vuonna 1971. Bernin sopimuksen pääperiaatteina ovat kansallinen kohtelu ja vähimmäissuoja. Muista sopimusvaltioista kotoisin oleville teoksille on myönnettävä sama suoja kuin omien kansalaisten teoksille. Tärkeimpiin suojatasevelvoitteisiin kuuluvat muun muassa 50 vuoden suoja-aika tekijän kuolinvuodesta laskettuna, kappaleiden valmistamisoikeus, esitysoikeus ja yleisradiooikeus. Bernin sopimusta hallinnoi Maailman henkisen omaisuuden järjestö WIPO (World Intellectual Property Organization). Bernin sopimukseen on liittynyt 149 valtiota. Suomi liittyi sopimukseen vuonna 1928.

Rooman sopimus (SopS 56/1983) on keskeisin lähioikeuksien kansainvälistä suojaa koskeva sopimus. Se on esittävien taiteilijoiden, äänitetuottajien sekä radio- ja televisioyrittäjien oikeuksien perussopimus, jossa kullekin oikeuksien haltijaryhmälle on myönnetty tietyt vähimmäisoikeudet. Sopimus velvoittaa lisäksi antamaan siinä erityisesti taattuun suojaan nähden kansallisen kohtelun. Rooman sopimusta hallinnoivat kolmikantasihteeristönä WIPO, Unesco ja Kansainvälinen työjärjestö. Rooman sopimukseen on liittynyt 68 valtiota. Suomi liittyi sopimukseen vuonna 1983.

TRIPS-sopimus on Maailman kauppajärjestön (WTO) perustamissopimuksen liitesopimus. Sen tarkoituksena on kauppapolitiikan välineenä vahvistaa teollis- ja tekijänoikeuksien maailmanlaajuista suojaa. Tekijänoikeuksien sisällön osalta se vahvistaa Bernin sopimuksen noudattamisen kaikissa WTO:n jäsenvaltioissa. Tämän lisäksi se sisältää määräyksiä muun muassa esittäjien, äänitetuottajien ja yleisradio-organisaatioiden suojasta. Sopimus koskee siten sekä tekijänoikeuksia että lähioikeuksia. Sopimus sisältää myös oikeuksien täytäntöönpanoa koskevia määräyksiä, määräykset riitojen ratkaisemisesta sekä esimerkiksi kaupallista piratismia koskevia pakottavia kriminalisointivelvoitteita. Sopimus sitoo Suomea WTO:n jäsenenä.

WIPO:n tekijänoikeussopimus on Bernin sopimusta täydentävä erityissopimus. Sopimuksella ei muuteta Bernin sopimusta. Myös Bernin sopimukseen kuulumattomat WIPO:n jäsenvaltiot voivat liittyä sopimukseen. WIPO:n tekijänoikeussopimus täydentää Bernin sopimusta takaamalla maailmanlaajuisesti kirjallisten ja taiteellisten teosten tekijöille uusia oikeuksia sekä parantamalla tekijöillä aiemmin olleiden oikeuksien tehokasta käyttämistä.

WIPO:n esitys- ja äänitesopimus on vastaavasti uusi esittävien taiteilijoiden ja äänitetuottajien oikeuksia koskeva sopimus, eikä se vaikuta Rooman sopimuksen soveltamiseen. Myös Rooman sopimukseen kuulumattomat WIPO:n jäsenvaltiot voivat liittyä sopimukseen. WIPO:n esitys- ja äänitesopimuksella parannetaan esittävien taiteilijoiden ja äänitetuottajien oikeuksien maailmanlaajuista suojaa muun muassa takaamalla uusia oikeuksia sekä parantamalla esittävillä taiteilijoilla ja äänitetuottajilla aiemmin olleiden oikeuksien tehokasta käyttämistä.



WIPO-sopimuksilla mukautetaan tekijänoikeuden alan kansainvälistä sopimusjärjestelmää digitaalitekniikkaan ja tietoverkkoihin liittyviin erityiskysymyksiin. Sopimuksissa on erityisesti otettu huomioon tieto- ja viestintätekniikoiden kehityksen ja yhdentymisen vaikutukset kirjallisten ja taiteellisten teosten luomiseen ja käyttämiseen sekä esitysten ja äänitteiden tuottamiseen ja käyttämiseen. Sopimukset sisältävät myös määräyksiä teknisten suojakeinojen sekä oikeuksien hallinnointitietojen oikeudellisesta suojasta.

Suomi on allekirjoittanut molemmat WIPO-sopimukset mutta ei ole saattanut niitä kansallisesti voimaan. Asiaa koskeva hallituksen esitys on tarkoitus antaa eduskunnalle kuluvan vuoden aikana.

Kansallisesti voimaansaatettujen sopimusten edellyttämät säännökset ovat rikossääntelyn osalta tekijänoikeuslaissa ja rikoslaissa.

Voimassa olevat säännökset sopimuksessa tarkoitettuja tekoja vastaavista rikoksista sisältyvät pääosin rikoslain tekijänoikeusrikoksia koskevaan 49 luvun 1 §:ään. Pykälän 1 momentin mukaan tekijänoikeusrikoksesta tuomitaan se, joka ansiotarkoituksessa tekijänoikeuslain säännösten vastaisesti ja siten, että teko on omiaan aiheuttamaan huomattavaa haittaa tai vahinkoa loukatun oikeuden haltijalle, loukkaa toisen oikeutta säännöksessä tarkemmin yksilöityyn tekijänoikeuteen tai tekijänoikeuden lähioikeuteen. Pykälän 2 momentin mukaan myös laittoman kopion levittämistarkoituksessa tapahtuva maahantuonti on rangaistavaa. Lisäksi tekijänoikeuslain 56 a §:ssä on rikkomustyyppinen säännös, jossa ei edellytetä ansiotarkoitusta eikä myöskään huomattavaa vahinkoa.

Säännökset kattavat myös artiklassa tarkoitettut tietojärjestelmän välityksellä tapahtuneet tekijänoikeuden loukkaukset.

Voimassa olevat säännökset vastaavat tältä osin artiklan velvoitteita. Artikla ei edellytä lainsäädännön muuttamista.

Mikäli WIPO-sopimukset edellyttävät rikosoikeudellista lisäsääntelyä, yleissopimuksen tekotapaa koskevien vaatimusten täyttymisestä huolehditaan WIPO-sopimusten kansallisen täytäntöönpanon yhteydessä.

Artiklan 3 kohdan mukaan sopimuspuoli voi tehdä varauman, jonka mukaan se ei sovelle tämän artiklan 1 ja 2 kappaleen mukaista rikosvastuuta rajoitetuissa tapauksissa, edellyttäen kuitenkin, että niillä, joiden oikeuksia on loukattu, on käytettävissään muita tehokkaita oikeussuojakeinoja, eikä varauma merkitse poikkeusta sopimuspuolen kansainvälisistä velvoitteista, jotka perustuvat tämän artiklan 1 ja 2 kappaleessa mainittuihin kansainvälisiin asiakirjoihin.

Suomella ei ole tarvetta tehdä kappaleessa tarkoitettuja varaumia.

## **5 osasto Osallisuus, yhteisövastuu ja sanktiot**

### **Rikoksen yritys sekä avunanto tai yllytys rikokseen (11 artikla)**

Artiklan 1 kappaleen mukaan tahallinen avunanto ja yllytys sopimuksen 2-10 artiklan mukaisiin rikoksiin silloin, kun teon tarkoituksena on aikaansaada rikoksen täytyminen on säädetty rangaistavaksi teoksi.

Artiklan 1 kappaletta on käsitelty selitysmuistion kohdissa 118 ja 119. Selitysmuistion mukaan teon tarkoitusta koskevan lisäedellytyksen vuoksi esimerkiksi rikollista aineistoa sisältävän viestin välittämiseen osallistuva operaattori ei voi joutua pelkästään tällä perusteella rikosoikeudelliseen vastuuseen. Operaattorille ei myöskään synny artiklan perusteella velvollisuutta oma-aloitteisesti valvoa välitettävien viestien sisältöä.

Suomessa nyt voimassa olevat säännökset avunannon ja yllytyksen rangaistavuudesta sisältyvät rikoslain 5 luvun 2 ja 3 §:ään. Rikoslain 5 luvun 2 §:n mukaan rikosvastuu ulottuu aina myös rikokseen yllyttäjään. Yllyttäjä rinnastetaan rangaistavuudessa tekijään. Rikoslain 5 luvun 3 §:n mukaan myös avunanto rikoksen tekemiseen on rangaistavaa. Avunantaja tuomitaan lievennetyn asteikon perusteella.

Voimassa olevat säännökset vastaavat tältä osin artiklan velvoitteita. Artikla ei edellytä lainsäädännön muuttamista.

Artiklan 2 kappaleen mukaan tahallinen yritys sopimuksen 3-5, 7 ja 8 artiklan sekä 9 artiklan 1 kappaleen a ja c kohdan mukaisiin rikoksiin on säädettävä rangaistavaksi teoksi. Artiklan 3 kappaleen mukaan sopimuspuoli voi tehdä varauman, jonka mukaan se ei sovelta kokonaan tai osittain artiklan yrityksen kriminalisointia koskevaa 2 kappaletta.

Artiklan 2 kappaletta on käsitelty selitysmuistion kohdissa 120-122. Selitysmuistion mukaan artiklan 2 kappaleessa on otettu huomioon yrityksen kriminalisointiin liittyvät lainsäädäntötekniset ja muut mahdolliset vaikeudet eri oikeusjärjestelmissä. Tämän vuoksi 2 kappaleen soveltamisala on rajattu vain tiettyihin sellaisiin rikoksiin, joiden osalta yrityksen kriminalisointiin ei pitäisi liittyä erityisiä vaikeuksia. Tämän lisäksi osapuoli voi 2 kappaleen osalta tehdä varauman minkä hyvänsä rikoksen osalta tai tarvittaessa koko kappaleen osalta.

Seuraavien sopimuksessa tarkoitettujen rikosten osalta on artiklan mukaan siten joko tehtävä varauma tai säädettävä yritys rangaistavaksi teoksi, jos se ei sitä jo ole:

- 1) viestintäsalaisuuden loukkaaminen (3 artikla),
- 2) datan vahingoittaminen (4 artikla),
- 3) tietojärjestelmän häirintä (5 artikla),
- 4) tietokoneavusteinen väärennys (7 artikla),
- 5) tietokoneavusteinen petos (8 artikla),
- 6) lapsipornografian tuottaminen (9 artiklan 1 kappaleen a kohta) ja
- 7) lapsipornografian tarjoaminen ja saataville asettaminen (9 artiklan 1 kappaleen b kohta).

Edellä lueteltuja rikoksia vastaavista rikoksista ovat Suomessa voimassaolevien säännösten mukaan yrityksenä rangaistavia:

- 1) viestintäsalaisuuden loukkaus (RL 38:3 §)
- 2) törkeä viestintäsalaisuuden loukkaus (RL 38:4 §)
- 3) törkeä vahingonteko (RL 35:2 §)
- 4) petos (RL 36:1 §) ja
- 5) törkeä petos (RL 36:2 §).

Lisäksi väärennyksen ja törkeän väärennyksen yritys säädetään rangaistavaksi teoksi maksuvälinepetoksia koskevan puitepäätöksen kansallisen täytäntöönpanon yhteydessä (HE 2/2003).

Artikla edellyttää siten varauman tekemistä taikka yrityksen rangaistavuutta koskevan muutoksen tekemistä seuraavien rikoslaisissa säädettyjen rikosten osalta:

- 1) vahingonteko (RL 35:1 §),
- 2) lievä vahingonteko (RL 35:3 §),
- 3) tietoliikenteen häirintä (RL 38:5 §),
- 4) törkeä tietoliikenteen häirintä (RL 38:6 §),
- 5) lievä tietoliikenteen häirintä (RL 38:7 §),
- 6) lievä väärennys (RL 33:3 §),
- 7) sukupuolisiveellisyyttä loukkaavan kuvan levittäminen (RL 17:18 §) ja
- 8) sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan hallussapito (RL 17:19 §).

Lisäksi hallituksen esityksessä ehdotetun tietojärjestelmän häirintää koskevan uuden 38 luvun 7 a §:n ja sen törkeää tekemuotoa koskevan 7 b §:n osalta on tehtävä varauma tai säädettävä yritys rangaistavaksi.

Hallituksen esitykseen sisältyy ehdotus, jonka mukaan seuraavien rikosten osalta yritys säädetään rangaistavaksi:

- 1) vahingonteko (RL 35:1 §),
- 2) tietoliikenteen häirintä (RL 38:5 §) ja
- 3) törkeä tietoliikenteen häirintä (RL 38:6 §),
- 4) lievä tietoliikenteen häirintä (RL 38:7 §),
- 5) tietojärjestelmän häirintä (uusi RL 38:7 a §),
- 6) törkeä tietojärjestelmän häirintä (uusi RL 38:7 b §).

Ehdotetun muutoksen tultua voimaan voimassa olevat säännökset vastaavat tältä osin artiklan vaatimuksia.

Muiden artiklassa tarkoitettujen rikosten osalta Suomi tekee ehdotuksen mukaan varauman. Varauma koskee siten lievää vahingontekoa (RL 35:3 §) ja lievää väärennystä (RL 33:1 §).

Lievän vahingonteon ja väärennyksen osalta yrityksen kriminalisointi ei ole tarkoituksenmukaista, koska se johtaa tekojen vähäisyys huomioon ottaen liian laajaan rikosoikeudelliseen vastuuseen. Lievän väärennyksen osalta on lisäksi huomattava, että väärennysvälineen ja -tarvikkeen hallussapito on rikoslain 33 luvun 4 §:n nojalla rangaistavaa väärennysaineiston hallussapitona.

Euroopan Unionissa on valmisteilla ehdotus neuvoston puitepäätökseksi lasten seksuaalisen hyväksikäytön ja lapsipornografian torjumisesta. Edellä 9 artiklan perusteluissa kerrotuista syistä nyt käsillä olevan artiklan edellyttämät muutokset lapsipornografiarikoksiin on tarkoituksenmukaista toteuttaa samassa yhteydessä kuin puitepäätöksen edellyttämät muutokset. Tässä yhteydessä arvioidaan myös tarve mahdollisen varauman tekemiseen.

Eduskunta on hyväksynyt hallituksen esityksen rikosoikeuden yleisiä oppeja koskevan lainsäädännön uudistamiseksi (HE 44/2002). Esityksessä ehdotetaan, että rikoslakiin otetaan rikosoikeuden yleisiä oppeja eli rikosoikeudellisen vastuun edellytyksiä, vastuuvapausperusteita sekä yritystä ja osallisuutta koskevat säännökset. Nykyiset säännökset ovat aukollisia ja osaksi vanhentuneita. Rikosoikeudellinen laillisuusperiaate ja oikeusturva edellyttävät niiden uudistamista. Siltä osin kuin ehdotetut säännökset ovat kokonaan uusia, ne perustuvat oikeuskäytännössä ja oikeuskirjallisuudessa vakiintuneisiin periaatteisiin. Ehdotetut uudet lait ovat tarkoitetut tulemaan voimaan 1 päivänä tammikuuta 2004. Ehdotuksessa ei ole yleissopimuksen 11 artiklan voimaansaattamisen kannalta merkityksellisiä lakimuutoksia.

## Yhteisövastuu (12 artikla)

Artiklan 1 kappaleen mukaan oikeushenkilö on voitava asettaa vastuuseen sopimuksen mukaan rangaistavaksi säädetystä teosta, jonka luonnollinen henkilö on tehnyt oikeushenkilön hyväksi joko itsenäisesti tai oikeushenkilön nimissä, silloin kun asianomainen henkilö on oikeushenkilössä johtavassa asemassa, joka perustuu valtuutukseen edustaa kyseistä oikeushenkilöä, valtuutukseen tehdä päätöksiä kyseisen oikeushenkilön puolesta tai valtuutukseen harjoittaa oikeushenkilön sisäistä valvontaa. Artiklan 2 kappaleen mukaan oikeushenkilö on voitava asettaa vastuuseen sopimuksen mukaan rangaistavaksi säädetystä teosta myös silloin, kun 1 kappaleessa tarkoitettu luonnollinen henkilö on laiminlyönyt valvonnan, ja kyseisen oikeushenkilön valtuuttaman luonnollisen henkilön on sen vuoksi ollut mahdollista tehdä tämän yleissopimuksen mukaisesti rangaistavaksi säädetty rikos kyseisen oikeushenkilön hyödyksi. Artiklan 4 kappaleessa todetaan selvyuden vuoksi, että oikeushenkilön vastuu ei vaikuta rikoksen tehneen luonnollisen henkilön rikosvastuuseen.

Artiklaa on käsitelty selitysmuistion kohdissa 123 -127. Selitysmuistion mukaan sääntely on sopusoinnussa nykyisin vallitsevan yhteisöjen rikosoikeudellista vastuuta korostavan yleisemmän suuntauksen kanssa. Artikla kattaa aktiivisten tekojen lisäksi myös valvontavelvollisuuden laiminlyönnin.

Seuraavien neljän ehdon pitää täytyä 1 kappaleessa tarkoitettun yhteisövastuun edellytyksenä: yleissopimuksessa tarkoitettu rikos on tehty, rikos on tehty oikeushenkilön hyväksi, tekijä on oikeushenkilössä johtavassa asemassa ja tekijä on tehnyt teon johtavan asemansa luomin valtuutuksin. Artiklan 2 kappale kattaa myös tilanteen, jossa teon tekee oikeushenkilön lukuun muu kuin johtavassa asemassa oleva henkilö, jos johtavassa asemassa olevan henkilön voidaan katsoa laiminlyöneen valvontavelvollisuutensa. Oikeushenkilön lukuun toimivana henkilönä tulee tällöin kyseeseen tyypillisesti esimerkiksi yrityksen työntekijä. Johtavassa asemassa olevan henkilön valvontavelvollisuuden laajuutta on tulkittava siten, että se rajoittuu ainoastaan tavanomaisiin ja normaalilaajuisiin valvontatoimenpiteisiin. Se mitä tämä käytännössä tarkoittaa on ratkaistava tapauskohtaisesti ottaen huomioon esimerkiksi harjoitetun liiketoiminnan laatu ja laajuus.

Suomessa voimassa olevat yleiset säännökset oikeushenkilön rangaistusvastuusta sisältyvät rikoslain 9 lukuun. Yksittäisen rikossäännöksen osalta oikeushenkilön rangaistusvastuun soveltuminen edellyttää sitä, että rikoslaissa on asiaa koskeva viittaussäännös.

Rikoslain 9 luvun 2 §:n 1 momentin mukaan oikeushenkilö tuomitaan yhteisösakkoon, jos sen lakisääteiseen toimielimeen tai muuhun johtoon kuuluva taikka oikeushenkilössä tosiasiallista päätösvaltaa käyttävä on ollut osallinen rikokseen tai sallinut rikoksen tekemisen taikka jos sen toiminnassa ei ole noudatettu vaadittavaa huolellisuutta ja varovaisuutta rikoksen ehkäisemiseksi. Rikokseen osallisen käsitettä käytetään pykälässä sen laajassa merkityksessä siten, että se kattaa myös varsinaisen tekijän vastuun. Saman pykälän 2 momentin mukaan yhteisösakkoon tuomitaan, vaikkei rikosentekijää saada selville tai muusta syystä tuomita rangaistukseen. Luvun 3 §:n mukaan rikos katsotaan oikeushenkilön toiminnassa tehdyksi, jos sen tekijä on toiminut oikeushenkilön puolesta tai hyväksi ja hän kuuluu oikeushenkilön johtoon tai on virka- tai työsuhteessa oikeushenkilöön taikka on toiminut oikeushenkilön edustajalta saamansa toimeksiannon perusteella.

Edellä selostettu sääntely ei kaikilta osin täysin vastaa artiklan sanamuotoa.

Artiklan 1 kappale koskee oikeushenkilön vastuuta silloin, kun johdon edustaja on rikosentekijänä. Kappaleessa on määritelty myös johdon käsite, jonka mukaan oikeushenkilön johtoon kuuluminen voi ilmetä kolmella tavalla. Johtoon kuuluvat ne, joilla on valta edustaa oikeushenkilöä, valtuudet tehdä päätöksiä oikeushenkilön puolesta tai valtuudet harjoittaa valvontaa oikeushenkilössä.

Rikoslain 9 luvussa ei ole tyhjentävää johdon määritelmää. Luvun 2 §:n 1 momentissa oikeushenkilön lakimääräisiin toimielimiin kuuluvien on todettu olevan oikeushenkilön johtoa. Lakimääräisillä toimielimillä tarkoitetaan esimerkiksi yhdistyksen, säätiön tai osakeyhtiön hallitusta, osakeyhtiön hallintoneuvostoa ja toimitusjohtajaa tai kommandiittiyhtiön vastuunalaisia yhtiömiehiä. Tämän lisäksi momentissa todetaan, että myös oikeushenkilön muuhun johtoon kuuluvien toiminta voi perustaa oikeushenkilön vastuun.

Artiklan 1 kappaleen a-kohdan mukaan vastuu tulee ulottaa henkilöön, jonka johtava asema oikeushenkilössä perustuu valtaan edustaa oikeushenkilöä. Suomen oikeuden mukaan sitä, jolla on valta edustaa oikeushenkilöä, ei välttämättä pidetä oikeushenkilön johtoon kuuluvana. Tällaisen henkilön toiminta voi kuitenkin synnyttää oikeushenkilön rangaistusvastuun sitä kautta, että hän on rikoslain 9 luvun 3 §:n 1 momentin mukaisesti toiminut oikeushenkilön edustajalta saamansa toimeksiannon perusteella. Lainsäädäntö täyttää siten tältä osin yleissopimuksen vaatimukset.

Artiklan 1 kappaleen b-kohdan mukaan vastuu tulee ulottaa henkilöön, jonka johtava asema oikeushenkilössä perustuu valtuuksiin tehdä päätöksiä oikeushenkilön puolesta. Rikoslain 9 luvun 2 §:n mukainen päätösvaltaan perustuva vastuu samastaminen edellyttää, että tällaisella henkilöllä täytyy olla paljon itsenäistä päätösvaltaa. On katsottu, että niin sanottuun keskijohtoon kuuluvia ei yleensä voitaisi tässä mielessä pitää 2 §:n tarkoittamassa mielessä johtoon kuuluvina (HE 95/1993). Koska kuitenkin tosiasiallinen vallankäyttö on erikseen mainittu vastuun perustavana seikkana, lainsäädäntö täyttää tältäkin osin yleissopimuksen vaatimukset.

Artiklan 1 kappaleen c-kohdan mukaan vastuu tulee ulottaa henkilöön, jonka johtava asema oikeushenkilössä perustuu valtuuksiin harjoittaa valvontaa oikeushenkilössä. Tällaisia henkilöitä ei Suomessa katsota yleensä oikeushenkilön johtoon kuuluviksi. Heidän tekemänsä rikokset voivat kuitenkin synnyttää oikeushenkilön rangaistusvastuun työntekijäaseman perusteella silloinkin, kun he eivät kuulu oikeushenkilön johtoon.

Artiklan 2 kappaleessa tarkoitettua laiminlyöntiä vastaa rikoslain 9 luvun 2 §:n 1 momenttiin sisältyvä huolellisuus- ja varovaisuusvelvollisuuden rikkomista koskeva säännös. Yleissopimuksessa, toisin kuin Suomen rikoslaissa, laiminlyönti on kuitenkin kytketty 1 kappaleessa tarkoitettuun johtavaan asemaan oikeushenkilössä. Edellä esitetyn mukaisesti kaikki artiklan 1 kappaleessa tarkoitettut henkilöt eivät kuulu rikoslain 9 luvussa tarkoitettulla tavalla oikeushenkilön johtoon. Rikoslain 9 luvun 2 §:n 1 momentin mukaisen laiminlyönnin perusteella syntyvä oikeushenkilön rangaistusvastuu ei edellytä, että rikoksen välittömästi mahdollistaneen laiminlyönnin tekijä olisi kuulunut oikeushenkilön johtoon. Riittää, että jokin laiminlyönti on tehty myös oikeushenkilön johdossa. Säännöksen soveltamisen osalta on lisäksi huomattava, että laiminlyönnin on vähintäänkin täytynyt olennaisesti lisätä mahdollisuutta siihen, että oikeushenkilön toiminnassa on tehty rikos.

Rikoslain 9 luvun 2 §:n 2 momentin mukaan yhteisösakkoon tuomitaan, vaikkei rikosentekijää saada selville tai muusta syystä tuomita rangaistukseen. Suomen oikeuden mukaan oikeushenkilön rangaistusvastuun pääperiaatteet ovat näin jonkin verran laajemmalle meneviä, koska yleissopimus ei edellytä tällaisen anonyymin syyllisyyden ulottamista siinä mainittuihin rikoksiin.

Edellä selostettu yleinen sääntely kattaa siten sisällöltään artiklan vaatimukset. Yhteisövastuu ei kuitenkaan nykyisten säännösten mukaan sovellu yhteenkään artiklassa tarkoitettuun rikokseen. Artikla näyttäisi siten edellyttävän muutoksia nykyiseen lainsäädäntöön ainakin siltä osin kuin rikokset on tehty tietojärjestelmän avustuksella.

Artiklan 3 kappaleen mukaan oikeushenkilön vastuu voi kuitenkin olla rikos-, yksityis- tai hallinto-oikeudellista, jollei sopimuspuolen soveltamista oikeusperiaatteista muuta johdu. Vastuun ei siten artiklan mukaan välttämättä tarvitse olla rikosoikeudellista vaan esimerkiksi yksityisoikeudellinen vahingonkorvausvastuu riittää täyttämään artiklan vaatimukset. Suomessa taas oikeushenkilö voidaan artiklassa tarkoitetuissa tapauksissa aina saattaa vahingonkorvausvastuuseen rikoksella aiheutetuista vahingoista. Tämän johdosta Suomen ei tarvitse tehdä asiassa varaumaa eikä antaa selitystä vaikka lakia ei artiklan vuoksi muutettaisi.

Hallituksen esitykseen sisältyy ehdotus, jonka mukaan oikeushenkilön rangaistusvastuu ulotetaan koskemaan seuraavia rikoksia:

- 1) tietomurto (RL 38:8 §),
- 2) viestintäsalaisuuden loukkaus (RL 38:3 §),
- 3) törkeä viestintäsalaisuuden loukkaus (RL 38:4 §),
- 4) vahingonteko (RL 35:1 §),
- 5) törkeä vahingonteko (RL 35:2 §),
- 6) tietoliikenteen häirintä (RL 38:5 §),
- 7) törkeä tietoliikenteen häirintä (RL 38:6 §),
- 8) tietojärjestelmän häirintä (uusi RL 38:7 a §),
- 9) törkeä tietojärjestelmän häirintä (uusi RL 38:7 b §),
- 10) vaaran aiheuttaminen tietojenkäsittelylle (RL 34:9 a §),
- 11) tietoverkkorikosvälineen hallussapito (RL 34:9 b §) ja
- 12) tekijänoikeusrikos (RL 49:1 §).

Maksuvälinepetoksia koskevan puitepäätöksen kansallisen täytäntöönpanon yhteydessä (HE 2/2003) oikeushenkilön rangaistusvastuu ehdotetaan ulotettavaksi koskemaan väärennystä, törkeää väärennystä, väärennysaineiston hallussapitoa, maksuvälinepetosta, törkeää maksuvälinepetosta ja maksuvälinepetoksen valmistelua. Oikeushenkilön rangaistusvastuu ulotetaan myös petokseen ja törkeään petokseen, jos kyseiset teot tapahtuisivat tietojenkäsittelylaitteeseen vääriä tietoja syöttämällä tai tietojenkäsittelyyn muuten puuttumalla.

Oikeushenkilön rangaistusvastuun ulottaminen vahingonteon ja tietoliikenteen häirinnän lieviin tekemuotoihin ei sen sijaan ole näiden tekojen luonne ja vähäinen merkitys huomioon ottaen tarkoituksenmukaista. Tämän vuoksi näiden osalta voimassa olevaan lakiin ei ehdoteta muutoksia.

Edellä mainitun puitepäätöksen yhteydessä toteutettavien ja nyt ehdotettujen muutoksien tultua voimaan voimassa olevat säännökset vastaavat lievää vahingontekoa ja lievää tietoliikenteen häirintää lukuun ottamatta yleissopimuksen suosituksia.

Euroopan Unionissa on valmisteilla ehdotus neuvoston puitepäätökseksi lasten seksuaalisen hyväksikäytön ja lapsipornografian torjumisesta. Edellä 9 artiklan perusteluissa kerrotuista syistä nyt käsillä olevan artiklan edellyttämät muutokset lapsipornografiarikoksiin on tarkoituksenmukaista toteuttaa samassa yhteydessä kuin puitepäätöksen edellyttämät muutokset.

## **Sanktiot ja muut seuraamukset (13 artikla)**

Artiklan 1 kappaleen mukaan sopimuspuolen on varmistettava se, että 2-11 artiklan mukaisesti rangaistaviksi säädettyihin tekoihin syyllistyneille voidaan määrätä tehokkaat, tekoon nähden oikeassa suhteessa olevat ja riittävät rangaistukset, mukaan luettuna vankeusrangaistus.

Artiklan 2 kappaleen mukaan sopimuspuolen on varmistettava, että 12 artiklan mukaisesti vastuuseen saatetuille oikeushenkilöille voidaan määrätä tehokas, tekoon nähden oikeassa suhteessa oleva ja riittävä rangaistus tai muu sanktio tai seuraamus, mukaan luettuna sakkorangaistus.

Artiklassa seuraamuksien valinta ja asteikot jätetään osapuolien harkintaan. Artiklat eivät edellytä muutoksia lainsäädäntöön.

## **2 jakso Prosessioikeus**

### **1 osasto Yhteiset määräykset**

#### **Oikeudenkäyntimenettelyä koskevien määräysten soveltamisala (14 artikla)**

Artiklassa on määräykset prosessioikeutta koskevan 2 jakson soveltamisalasta sekä kyseistä jaksoa koskevista sallituista varaumista. Artikla koskee sen 1 kappaleen mukaan kaikkia 2 jaksossa säänneltyjä pakkokeinoja eli tallennetun datan säilyttämisen nopeaa varmistamista (16 artikla), liikennetietojen säilyttämisen nopeaa varmistamista ja osittaista luovutusta (17 artikla), esittämismääräystä (18 artikla), tallennettuun dataan kohdistuvaa etsintää ja takavarikkoa (19 artikla), tiedon hankkimista liikennetiedoista reaaliajassa (20 artikla) sekä tiedon hankkimista viestin sisällöstä (21 artikla).

Artiklan 2 kappaleen mukaan pakkokeinoja sovelletaan pääsääntöisesti kaikkiin sopimuksessa rangaistaviksi teoiksi säädettyihin rikoksiin, muihin tietojärjestelmän avulla tehtyihin rikoksiin ja mihin hyvänsä rikokseen liittyvän sähköisessä muodossa olevan todistusaineiston keräämiseen. Tästä pääsäännöstä on poikkeuksena kuitenkin viestin sisältöä koskevan 21 artiklan mukainen oikeus rajoittaa siinä tarkoitettuja pakkokeinoja ainoastaan tiettyihin törkeisiin rikoksiin.

Artiklan 3 kappaleen a) kohdan mukaan sopimuspuoli voi tehdä varauman, jonka mukaan se soveltaa viestin liikennetietoja koskevassa 20 artiklassa tarkoitettuja toimenpiteitä ainoastaan varaumassa yksilöityihin rikoksiin tai rikostyyppeihin, kuitenkin niin että valikoima ei ole suppeampi kuin niiden rikosten valikoima, joihin se soveltaa 21 artiklan nojalla siinä tarkoitettuja pakkokeinoja.

Artiklan 3 kappaleen b) kohdan mukaan sopimuspuoli voi tehdä varauman, jonka mukaan se ei sovelta 20 tai 21 artiklassa tarkoitettuja pakkokeinoja tietojärjestelmän sisäiseen viestintään, jos tietojärjestelmällä on rajattu käyttäjäryhmä ja tietojärjestelmää ei käytetä julkisten tietoverkkojen avulla eikä sitä ole kytketty toiseen julkiseen tai yksityiseen tietojärjestelmään.

Artiklaa käsitellään selitysmuistion kohdissa 140 - 144. Selitysmuistion mukaan pakkokeinojen soveltamisala on laaja koska sopimuksen tarkoituksena on saattaa digitaalisessa muodossa oleva sähköinen todistusaineisto ja sen hankkiminen kaikkien rikosten osalta samaan asemaan kuin tavanomainen todistusaineisto.

Poikkeuksena ovat kuitenkin tiedon hankinta viestin sisällöstä ja sitä koskevista liikennetiedoista. Näitä tietoja koskevien pakkokeinojen osalta osapuolille on varattu mahdollisuus rajoittaa niiden käyttöä. Tämä johtuu kyseisten pakkokeinojen luottamuksellisuutta ja yksityisyyttä loukkaavasta luonteesta. Viestin sisällön selvittäminen merkitsee tuntuvampaa kajoamista henkilön oikeusasemaan kuin pelkkä liikennetietojen selvittäminen. Tämän vuoksi osapuolella ei ole artiklan mukaan oikeutta rajoittaa pakkokeinojen käyttöä liikennetietojen osalta enempää kuin viestin sisällön osalta.

Suljettuja erillisverkkoja koskevan 3 kappaleen b) kohdan tarkoituksena on antaa varaumamahdollisuus sellaisille osapuolille, jotka eivät kansallisen lainsäädäntönsä asettamien rajoitusten vuoksi voi sallia 20 tai 21 artiklassa tarkoitettujen pakkokeinojen käyttöä tällaisissa täysin yksityisissä verkoissa.

Artiklan osalta on vielä huomattava, että siinä määritelty soveltamisala ei kata poliisin rikostiedustelutoimintaa.

Artiklan vaikutukset lainsäädännön muutostarpeisiin määräytyvät yhdessä pakkokeinojen sisältöä koskevien artiklojen kanssa. Tarve mahdollisten varaumien tekemiseen on arvioitu 20 ja 21 artiklan perusteluissa.

### **Soveltamiseen liittyvät rajoitukset ja takeet (15 artikla)**

Artiklassa on yleiset määräykset pakkokeinojen käytössä noudatettavista rajoitusperiaatteista ja oikeusturvatakeista.

Artiklan 1 kappaleen mukaan pakkokeinojen käytössä on noudatettava suhteellisuusperiaatetta ja muutoinkin varmistettava se, ettei pakkokeinojen käyttö ole ristiriidassa kansainvälisiin sopimuksiin perustuvan ihmisoikeuksien ja perusvapauksien suojan kanssa.

Artiklan 2 kappaleen mukaan pakkokeinojen käytössä on varmistettava tarkoituksenmukaiset oikeusturvatakeet, kuten tuomioistuimen valvonta sekä riittävät asialliset ja ajalliset rajoitukset.

Artiklan 3 kappaleen mukaan pakkokeinojen käytössä on otettava huomioon myös sivullisten oikeudet.

Artiklaa käsitellään selitysmuistion kohdissa 145 - 148. Selitysmuistion mukaan sopimuksen edellyttämien rajoitusperiaatteiden ja oikeusturvatakeiden toteuttamistapa kansallisessa lainsäädännössä on artiklassa jätetty tarkoituksellisesti osapuolten harkintaan. Osapuolten oikeusjärjestelmät ovat erilaisia. Tämän vuoksi yksityiskohtaisten määräysten antaminen asiasta ei ole mahdollista. Artiklan 1 kappaleen esimerkkiluettelossa mainitut ihmisoikeussopimukset asettavat sääntelylle minimivaatimukset. Suhteellisuusperiaatteen mukaan käytetyn pakkokeinon ja siitä aiheutuvien haittojen on oltava järkevissä suhteissa tutkittavana olevan rikoksen vahingollisuuteen ja muihin vastaaviin seikkoihin. Suhteellisuusperiaatetta ilmentää myös 21 artiklan mukainen oikeus rajoittaa siinä tarkoitettuja pakkokeinoja ainoastaan tiettyihin törkeisiin rikoksiin. Artiklan 2 kappaleessa tarkoitettuja oikeusturvatakeita ja rajoituksia on mitoitettava niin, että ne ovat järkevissä suhteissa pakkokeinosta aiheutuviin haittoihin. Esimerkiksi viestin sisällön selvittäminen merkitsee tuntuvampaa kajoamista henkilön oikeusasemaan kuin pelkkä viestiä koskeva säilyttämismääräys. Tämän vuoksi myös oikeusturvatakeet ja rajoitukset voivat näiden



pakkokeinojen osalta olla erilaiset. Artiklan 3 kappaleessa tarkoitettu sivullinen voi olla esimerkiksi teleoperaattori. Osapuolten on otettava huomioon pakkokeinojen vaikutukset myös yleisen edun ja sivullisten näkökulmasta ja pyrittävä mahdollisuuksien mukaan pienentämään aiheutuvia haittoja.

Artiklan 1 kappaleessa viitatu kansainväliset sopimukset ovat Suomessa lakina voimassa.

Artiklan suhdetta voimassaolevaan lainsäädäntöön ja ehdotettuihin muutoksiin on käsitelty pakkokeinoja koskevien artiklojen yhteydessä ja lisäksi myös niiden edellyttämien lakimuutosten yksityiskohtaisissa perusteluissa.

## **2 osasto Tallennetun datan säilyttämisen nopea varmistaminen**

### **Tallennetun datan säilyttämisen nopea varmistaminen (16 artikla)**

Artiklassa on määräykset datan säilyttämisvelvollisuudesta. Artiklan 1 kappaleen mukaan viranomaisilla on oltava valtuudet estää rikostutkinnallisesti merkityksellisen datan häviäminen tai muuttaminen ennen kuin datan haltuunotto on muiden pakkokeinojen nojalla mahdollista. Datan säilyminen muuttumattomana voidaan varmistaa erityisellä datan haltijalle annettavalla säilyttämismääräyksellä tai osapuolen harkinnan mukaan jollain muulla tarkoitukseen sopivalla tavalla. Artikla koskee myös liikennetietojen säilyttämistä. Liikennetiedon käsitettä on tarkemmin selostettu jäljempänä 17 artiklan perusteluissa.

Artiklan 2 kappale koskee säilyttämismääräystä ja sen mukaan määräys voidaan antaa sille, jonka hallussa tai hallinnassa data on. Säilyttämismääräyksen määräajan on oltava sen tarkoitus huomioon ottaen riittävän pitkä mutta enintään 90 päivää. Määräaika on kuitenkin mahdollisuus pidentää.

Artiklan 3 kappaleen mukaan datan haltija on velvollinen pitämään edellä tarkoitettun säilyttämismääräyksen salassa.

Artiklan 4 kappaleen mukaan artiklassa tarkoitettuun pakkokeinoon sovelletaan 14 ja 15 artiklan määräyksiä soveltamisalasta, rajoitusperusteista ja oikeusturvatakeista.

Artiklaa käsitellään selitysmuistion kohdissa 149 - 164. Selitysmuistion mukaan sääntelyn tarkoituksena on luoda mahdollisimman vähän datan haltijan oikeuksiin kajoava, nopea ja helppokäyttöinen väline datan eheyden turvaamiseksi vaihtoehtona esimerkiksi datan takavarikolle. Tietoverkkorikollisuuden osalta keskeinen todistusaineisto on monesti datan muodossa. Datan hävittäminen ja muuntelu on teknisesti suhteellisen helppoa ja tietojärjestelmissä olevat datamäärät ovat huomattavan suuria. Tämän vuoksi juuri datan turvaamista koskeva erityisen sääntely on tärkeää. Erityisen tarpeellista tämä on rajat ylittävissä tapauksissa, joissa perinteinen kansainvälinen yhteistyö on monesti aikaa vievien menettelysääntöjen vuoksi hidasta. Jos oikeusapupyynnön tutkiminen kestää kauan, datan muodossa oleva todistusaineisto saattaa hävitä menettelyn aikana. Tässä yhteydessä on huomattava, että kansainvälistä yhteistyötä sääntelevässä 29 artiklan 3 kappaleessa säädetään menettelyn nopeuttamiseksi muun ohessa ettei datan säilyttämismääräystä koskevan oikeusapupyynnön toteuttamiseksi saa edellyttää kaksoisrangaistavuutta.

Artikla koskee ainoastaan jo olemassa olevaa dataa ja sen vaikutukset rajoittuvat ainoastaan siihen. Artiklalla ei ole siten lainkaan vaikutuksia datan haltijan, kuten teleoperaattorin, muihin säännöksiin mahdollisesti perustuviin oikeuksiin tai velvollisuuksiin kerätä ja tallentaa liikennetietoja tai muuta dataa. Artikla koskee vain jo olemassa olevan datan häviämisen estämistä. Artiklan 1 kappaleessa

säilyttämismääräys mainitaan vain esimerkkinä sääntelytavasta, jolla datan muuttumattomuus voidaan turvata. Osapuoli voi toteuttaa sääntelyn teknisesti myös muulla tavalla kuten esimerkiksi datan takavarikkoa tai datan esittämisvelvollisuutta koskevan sääntelyn yhteydessä.

Datan säilyttäminen tarkoittaa artiklassa ainoastaan sen tehokasta suojaamista. Se ei välttämättä edellytä, että datan käyttö olisi kokonaan estettävä. Se, miten riittävän tehokas suojaaminen teknisesti toteutetaan, jätetään artiklassa osapuolten harkintaan. Artiklan mukaan datan säilyttäminen on voitava varmistaa erityisesti silloin, kun viranomaisilla on syytä uskoa, että datan häviäminen tai muuttaminen on erityisen todennäköistä. Tällainen epäily voi perustua esimerkiksi tietoon datan haltijan noudattamista säilytysmääräajoista tai datan säilyttämisessä käytettävän menetelmän epäluotettavuudesta. Säilyttämismääräyksessä tarkoitettu data voi olla joko sen kohteena olevan henkilön tai yrityksen hallussa tai muualla, jos data on kuitenkin kyseisen tahon määräämisvallassa. Osapuolien velvollisuutena on säätää kansallisessa lainsäädännössä säilyttämismääräykselle maksimiaika, joka ei saa olla pidempi kuin artiklassa määrätty 90 päivää. Salassapitovelvollisuutta koskevan määräyksen tarkoituksena on yhtäältä turvata rikostutkinnan häiriötöntä kulkua mutta toisaalta myös suojata epäillyn henkilön yksityisyyttä.

Suomen voimassa olevassa lainsäädännössä ei ole lainkaan artiklassa tarkoitettua datan säilyttämismääräystä vastaavaa sääntelyä. Tämän vuoksi artikla edellyttää muutoksia nykyiseen lainsäädäntöön.

Hallituksen esitykseen sisältyy ehdotus, jonka mukaan pakkokeinolakiin lisätään tämän artiklan ja jäljempänä selostetun 17 artiklan edellyttämät datan säilyttämismääräystä koskevat säännökset. Ehdotettua sääntelyä on tarkemmin selostettu pakkokeinolain 4 luvun säilyttämismääräystä koskevan 4 c §:n ja säilyttämismääräyksen kestoja ja salassapitovelvollisuutta koskevan 4 d §:n yksityiskohtaisissa perusteluissa.

Ehdotetun muutoksen tultua voimaan voimassa olevat säännökset vastaavat tämän artiklan ja myös 17 artiklan vaatimuksia.

### **Liikennetietojen säilyttämisen nopea varmistaminen ja osittainen luovutus (17 artikla)**

Artiklassa on määräykset liikennetietojen säilyttämisestä ja tiettyjen niitä koskevien reittitietojen luovuttamisesta. Kuten edellä 16 artiklan osalta on todettu, siinä tarkoitettu datan säilyttämismääräys koskee myös liikennetietoja. Liikennetieto on määritelty 1 artiklan d kohdassa. Määritelmän mukaan liikennetiedolla tarkoitetaan tietojärjestelmän välityksellä siirrettyyn viestiin liittyvää dataa, jonka viestinsiirtoketjuun kuuluva tietoverkko on tuottanut, ja josta ilmenee viestin alkuperä, määränpää, reitti, kellonaika, päivämäärä, koko, kesto, tai siihen liittyvän palvelun tyyppi. Artiklassa tarkoitettuja viestin alkuperää tai määränpäättä osittavia liikennetietoja ovat esimerkiksi puhelinnumero, IP-osoite tai muu niihin verrattava teleosoite. Palvelun tyyppiä koskeva tieto tarkoittaa sitä onko viestinnässä kysymys esimerkiksi sähköpostista, tiedoston siirrosta vai reaaliaikaisesta keskustelusta.

Artiklan 1 kappaleen a kohdan mukaan liikennetiedot on voitava määrätä nopeasti säilytettäväksi riippumatta siitä, onko viestin siirrossa ollut mukana yksi tai useampi palveluntarjoaja. Artiklan 1 kappaleen b kohdan mukaan viranomaisilla on lisäksi oltava oikeus saada tietoonsa palveluntarjoajien tunnistamiseksi tarvittavat liikennetiedot, jos viestin välittämiseen on osallistunut useampi palveluntarjoaja. Palveluntarjoaja on määritelty 1 artiklan c kohdassa. Määritelmän mukaan palveluntarjoajalla tarkoitetaan julkista tai yksityistä yksikköä, joka tarjoaa palveluidensa

käyttäjille mahdollisuuden tietojärjestelmän välityksellä tapahtuvaan viestintään, ja muuta yksikköä, joka käsittelee tai tallentaa dataa edellä mainitun palveluntarjoajan tai palveluiden käyttäjien puolesta. Artiklassa tarkoitettu palveluntarjoaja voi olla esimerkiksi viestien siirtoa, verkkoon pääsyä, tietojärjestelmän ylläpitoa tai tietojen tallentamista tarjoava yritys.

Artiklan 2 kappaleen mukaan artiklassa tarkoitettuun pakkokeinoon sovelletaan 14 ja 15 artiklan määräyksiä soveltamisalasta, rajoitusperusteista ja oikeusturvatakeista.

Artiklaa käsitellään selitysmuistion kohdissa 165 - 169. Selitysmuistion mukaan liikennetiedot saattavat muodostaa yksinomaisen ja ratkaisevan todistusaineiston siitä, kuka tietoverkkorikoksen on tehnyt. Liikennetietojen säilytysajat saattavat kuitenkin olla esimerkiksi yksityisyyden suojaa painottavien muiden säännösten vuoksi erittäin lyhyet. Tämän vuoksi on tärkeää, että liikennetietojen säilyttäminen voidaan tarvittaessa varmistaa nopeasti ja tehokkaasti.

Artiklassa annetaan erityiset määräykset 16 artiklassa tarkoitettua liikennetietojen säilyttämismääräyksestä. Keskeisin näistä on määräys, jonka mukaan viranomaisilla on oltava oikeus saada tietoonsa palveluntarjoajien tunnistamiseksi tarvittavat liikennetiedot, jos viestin välittämiseen on osallistunut useampi palveluntarjoaja. Tältä osin kyse ei siis ole vain tietojen säilyttämisestä vaan viranomaisen rajoitetusta tiedonsaantioikeudesta.

Tietojärjestelmässä kulkeva viesti saattaa kulkea useiden teleoperaattorien verkkojen kautta. Silloin yhdelle siirtoketjuun osallistuneelle operaattorille osoitettu säilyttämismääräys ei välttämättä riitä viestin tai sen liikennetietojen häviämisen estämiseen. Jotta säilyttämismääräys voitaisiin kohdistaa kaikkiin siirtoketjuun osallistuneisiin tahoihin, tarvitaan tieto siitä mitkä kaikki operaattorit ovat siirtämiseen osallistuneet. Jokaisella operaattorilla on tieto siitä miltä operaattorilta viesti on sille tullut ja tieto siitä mille operaattorille viesti on siltä lähtenyt. Nämä liikennetiedot ovat artiklassa tarkoitettuja palveluntarjoajan tunnistamiseksi tarvittavia tietoja ja vain näiden osalta artikla edellyttää viranomaiselle oikeuden saada tiedon liikennetiedon sisällöstä.

Jos jokaisen siirtoketjussa ilmenevän operaattorin osalta edellytetään uutta juuri sille kohdistettua erillistä määräystä, menettelystä tulee hidas ja tehoton. Tehokkaampaa on antaa säilyttämismääräys esimerkiksi siten, että esitutkintaviranomaisen tiedonsaantioikeus ja säilyttämismääräys kohdistetaan avoimella määräyksellä kaikkiin siirtoketjussa ilmeneviin operaattoreihin vaikkei niitä määräystä annettaessa voida vielä yksilöidä. Myös palveluntarjoajat voidaan velvoittaa osallistumaan siirtoketjun selvittämiseen. Se miten ja kuinka tehokkaasti viestiketjun selvittämistä koskeva sääntely teknisesti toteutetaan jätetään artiklassa kuitenkin osapuolten harkintaan.

Suomen voimassa olevassa lainsäädännössä ei ole lainkaan artiklassa tarkoitettua liikennetietojen säilyttämistä ja viestin reittitietojen luovuttamista vastaavaa sääntelyä.

Tämän vuoksi artikla edellyttää muutoksia nykyiseen lainsäädäntöön.

Hallituksen esitykseen sisältyy ehdotus, jonka mukaan pakkokenolakiin lisätään tämän artiklan ja edellä selostetun 16 artiklan edellyttämät datan säilyttämismääräystä ja viestin reittitietojen luovuttamista koskevat säännökset. Ehdotettua sääntelyä on tarkemmin selostettu pakkokeinolain 4 luvun säilyttämismääräystä koskevan 4 c §:n ja säilyttämismääräyksen kestoja ja salassapitovelvollisuutta koskevan 4 d §:n yksityiskohtaisissa perusteluissa.

Ehdotetun muutoksen tultua voimaan voimassa olevat säännökset vastaavat tämän artiklan ja myös 16 artiklan vaatimuksia.

### 3 osasto Esittämismääräys

#### Esittämismääräys (18 artikla)

Artiklassa on määräykset yleisestä datan esittämisvelvollisuudesta ja erityisestä palveluntarjoajan tilaajatietoja koskevasta esittämisvelvollisuudesta, jonka soveltamisala kattaa datan lisäksi myös muun todistusaineiston.

Artiklan 1 kappaleen a kohdan mukaan datan haltija on velvollinen esittämään hallussaan tai hallinnassaan olevan datan viranomaisen määräyksestä.

Artiklan 1 kappaleen b kohdan mukaan palveluntarjoaja on velvollinen esittämään palveluntarjoajan tarjoamien palveluiden tilaajia koskevia tietoja, jotka eivät ole liikennetietoja tai viestin sisältöä koskevia tietoja ja joita palveluntarjoaja säilyttää tietojärjestelmään tallennettuina tai missä tahansa muussa muodossa.

Palveluntarjoaja on määritelty 1 artiklan c kohdassa. Määritelmän mukaan palveluntarjoajalla tarkoitetaan julkista tai yksityistä yksikköä, joka tarjoaa palveluidensa käyttäjille mahdollisuuden tietojärjestelmän välityksellä tapahtuvaan viestintään, ja muuta yksikköä, joka käsittelee tai tallentaa dataa edellä mainitun palveluntarjoajan tai palveluiden käyttäjien puolesta. Artiklassa tarkoitettu palveluntarjoaja voi olla esimerkiksi viestien siirtoa, verkkoon pääsyä, tietojärjestelmän ylläpitoa tai tietojen tallentamista tarjoava yritys. Tilajia koskevilla tiedoilla tarkoitetaan artiklan mukaan tietoja, joista ilmenevät käytetty viestintäpalvelu, tilaajan henkilö- ja yhteystiedot sekä viestintälaitteiden sijainti.

Artiklan 2 kappaleen mukaan artiklassa tarkoitettujen velvollisuuden osalta ovat voimassa myös 14 ja 15 artiklan määräykset soveltamisalasta, rajoitusperusteista ja oikeusturvatakeista.

Artiklaa käsitellään selitysmuistion kohdissa 170 - 183. Selitysmuistion mukaan sääntelyn tarkoituksena on luoda mahdollisimman vähän datan haltijan oikeuksiin kajoava väline datan muodossa olevan todistusaineiston hankkimiseksi vaihtoehtona esimerkiksi datan takavarikolle.

Artikla koskee ainoastaan jo olemassa olevaa dataa tai tietoja sellaisina kun ne ovat. Artiklan nojalla ei siten esimerkiksi voida velvoittaa teleoperaattoria tai muuta tahoa keräämään tai tallentamaan mitään tietoja tai varmistumaan tietojen oikeellisuudesta. Esittämismääräyksessä tarkoitettu data voi olla joko sen kohteena olevan henkilön tai yrityksen hallussa tai muualla, jos data on kuitenkin kyseisen tahon määräämisvallassa. Esittämismääräyksessä voidaan antaa tarkempia määräyksiä siitä, missä muodossa data tai muut tiedot on esitettävä. Tilajia koskevat tiedot on tarkoitettu tulkittavaksi siten laajasti, että niillä tarkoitetaan esimerkiksi maksullisten palveluiden lisäksi myös sellaisia tilajia koskevia tietoja, jotka käyttävät palveluita ilmaiseksi. Käytännössä tiedot ovat joko tiettyä henkilöä koskevia tietoja tämän käyttämistä palveluista ja niihin liittyvistä tarkemmista tiedoista tai tiettyä palvelua koskevia tietoja siitä kuka palvelun käyttäjä on ja mitkä ovat hänen tarkemmat henkilö- ja yhteystietonsa. Tärkeä rajoitusperuste on se, että tiedot eivät voi koskaan olla liikennetietoja tai viestin sisältöä koskevia tietoja. Artikla ei myöskään oikeuta summittaiseen tietojen keräämiseen, vaan tiedon tarve on kyettävä riittävän tarkasti yksilöimään jo esittämismääräystä annettaessa. Artiklan 2 kappaleessa viitatu rajoitusperusteet ja oikeusturvatakeet voidaan mitoittaa eri tilanteissa eri tavalla ottaen huomioon esimerkiksi esitettävien tietojen luonne ja luovutusvelvollisen tahon asema.

Suomessa artiklan määräyksiä lähinnä vastaava säännös on esitutkintalain 27 §, jonka mukaan todistajan on totuudenmukaisesti ja mitään salaamatta ilmaistava, mitä hän tietää tutkittavasta asiasta. Säännöksen sanamuodon mukaan säännös tarkoittaa kuitenkin ainoastaan velvollisuutta suullisesti kertoa tiedoistaan. Käytännössä todistaja voi luonnollisesti vapaaehtoisesti esittää hallussaan olevan aineiston. Lisäksi nykyisen lain nojalla asiakirja tai muu aineisto kuten esimerkiksi datan muodossa oleva tallenne voidaan takavarikoida. Jos aineiston säilytyspaikka ei ole tiedossa, aineiston haltija on todistajana velvollinen kertomaan sen. Vasta oikeudenkäynnissä todistaja voidaan oikeudenkäymiskaaren 17 luvun 12 §:n nojalla velvoittaa esittämään hallussaan oleva aineisto. Vastaavaa säännöstä esitutkintalaissa ei ole.

Vaikka nykyinen sääntely varsinkin käytännön tarpeet huomioonottaen täyttäisikin pitkälti artiklan vaatimukset, artiklan sanamuoto ja voimassa oleva lainsäädäntö eroavat kuitenkin tosistaan.

Tämän vuoksi artikla edellyttää muutoksia nykyiseen lainsäädäntöön.

Hallituksen esitykseen sisältyy ehdotus, jonka mukaan esitutkintalakiin lisätään artiklan edellyttämät säännökset todistusaineiston esittämisvelvollisuudesta. Ehdotettua sääntelyä on tarkemmin selostettu esitutkintalain 27 §:ää ja 28 §:ää koskevan muutosehdotuksen perusteluissa.

Ehdotetun muutoksen tultua voimaan voimassa olevat säännökset vastaavat artiklan vaatimuksia.

#### **4 osasto Tallennettuun dataan kohdistuva etsintä ja takavarikko**

##### **Tallennettuun dataan kohdistuva etsintä ja takavarikko (19 artikla)**

Artiklassa on määräykset datan etsinnästä ja takavarikosta.

Artiklan 1 kappaleen mukaan viranomaisilla on oltava joko etsinnällä tai muulla vastaavalla toimenpiteellä oikeus hankkia pääsy tietojärjestelmään ja sen osaan, muuhun vastaavaan datan tallennusalueeseen sekä niissä olevaan dataan.

Artiklan 2 kappaleen mukaan etsintä tai muu toimenpide on voitava nopeasti laajentaa alkuperäisestä kohteesta toiseen kohteeseen, jos etsittävän datan havaitaan olevan sieltä laillisesti saatavissa ensin mainitun kohteen avulla.

Artiklan 3 kappaleen mukaan viranomaisella on oltava oikeus takavarikoimalla tai muulla vastaavalla tavalla turvata tietojärjestelmä ja sen osa, muu vastaava datan tallennusalueeseen sekä niissä oleva data. Data on lisäksi voitava kopioida ja poistaa tietojärjestelmästä tai estää sen käyttö.

Artiklan 4 kappaleen mukaan henkilö, jolla on tietoa tietojärjestelmän toiminnasta tai siihen sisältyvän datan suojaamisesta on velvollinen esittämään tarvittavat tiedot 1 ja 2 kappaleessa tarkoitettun etsinnän toimittamiseksi.

Artiklan 5 kappaleen mukaan artiklassa tarkoitettujen toimenpiteiden osalta ovat voimassa myös 14 ja 15 artiklan määräykset soveltamisalasta, rajoitusperusteista ja oikeusturvatakeista.

Artiklaa käsitellään selitysmuistion kohdissa 184 - 204. Selitysmuistion mukaan artiklan tarkoituksena on harmonisoida datan etsintää ja takavarikkoa koskeva sääntely ja saattaa se

osapuolten kansallisessa lainsäädännössä samanlaisen sääntelyn piiriin kuin esimerkiksi esineiden etsintä ja takavarikko. Datan aineettomasta luonteesta johtuen erityiset dataa koskevat säännökset ovat tarpeellisia. Artiklan 1 kappaleessa tarkoitettu etsintä voi kohdistua tietojärjestelmän lisäksi myös sen osaan, kuten esimerkiksi erilliseen tallennuslaitteeseen tai muuhun tallennusalueeseen kuten esimerkiksi CD-levykkeeseen. Jos etsittävän datan sisältönä on esimerkiksi sähköpostiviesti, osapuolien on itse harkittava sovelletaanko asiassa datan etsintää vai luottamuksellisen viestin sisällön selvittämistä koskevia säännöksiä. Artiklan 2 kappaleessa tarkoitettu laajentaminen on mahdollista ainoastaan kyseisen sopimuspuolen alueella olevaan tietojärjestelmään tai sen osaan. Artikla ei siten oikeuta rajat ylittävään datan etsintään. Se, miten laajentaminen teknisesti toteutetaan, jätetään artiklassa osapuolien harkintaan. Oleellista on se, että laajentaminen pitää tehdä nopeasti. Artiklan 3 kappaleessa tarkoitetuilla toimenpiteillä on kaksi erillistä tarkoitusta. Datan turvaamisella ja kopioimisella pyritään todisteiden keräämiseen. Jos datan kopiointi ei ole mahdollista, koko tallennusalue on voitava takavarikoida. Datan poistamisella ja käytön estämisellä pyritään lähinnä estämään datan käyttö vahingollisiin tarkoituksiin. Datan poistaminen ei tarkoita datan lopullista tuhoamista vaan ainoastaan siirtämistä tallennusalueelta toiselle. Datan käytön estäminen voidaan toteuttaa esimerkiksi salaamalla data tai muulla tarkoituksenmukaisella tavalla. Artiklan 4 kappaleessa tarkoitettujen järjestelmän haltijan ja muun henkilön tietojenantovelvollisuuden tarkoituksena helpottaa ja nopeuttaa viranomaisen työtä. Tästä saattaa olla välillisesti hyötyä myös epäillylle ja hänen työnantajalleen. Tietojenantovelvollisuutta rajoittaa kuitenkin kohtuullisuuden vaatimus. Se, mitä eri tilanteissa on pidettävä kohtuullisena, on ratkaistava tapauskohtaisesti. Artiklan 5 kappaleessa tarkoitettuna rajoitusperusteena voi tulla kyseeseen esimerkiksi tietojenantovelvolliselle maksettava kohtuullinen korvaus. Se, ilmoitetaanko epäillylle artiklan mukaisten pakkokeinojen käytöstä ja missä vaiheessa tämä mahdollisesti tehdään, jätetään artiklassa osapuolten harkintaan.

Suomessa datan etsintää koskevaa artiklan 1 kappaletta ja etsinnän laajentamista koskevaa 2 kappaletta vastaavaa erityistä sääntelyä ei ole. Datan etsintää koskevat välillisesti samat pakkokeinot lain 5 luvun yleiset etsintää koskevat säännökset kuin fyysisen esineen etsintää. Etsinnälle asetetaan lainsäädännössä lisäehtoja, jos toimenpide kohdistuu kotirauhaan, yksityisyyden suojaan tai henkilön fyysiseen koskemattomuuteen.

Etsittävä data sijaitsee aina fyysisellä tallennusalueella kuten tietokoneen kovalevyllä. Tallennusalueen sijainti määrää siten sen etsintätoimenpiteen, jonka nojalla tallennusalueesta ja sen sisältämää dataa päästään tutkimaan. Jos tallennusalueesta on esimerkiksi kotirauhan suojaamalla alueella, datan etsiminen siitä edellyttää esivaiheena kotietsinnän edellytysten täyttymistä. Jos tallennusalueesta on henkilön salkussa, datan etsiminen edellyttää vastaavasti henkilöntarkastuksen edellytysten täyttymistä. Molemmat edellä mainitut pakkokeinot edellyttävät rikosta, jonka rangaistusmaksimi on vähintään 6 kuukautta vankeutta. Sen jälkeen, kun tallennusalueesta on päästy edellä mainituilla etsintätoimenpiteillä käsiksi, sen sisältöä voidaan tutkia. Tallennusalueesta ja siinä oleva data voidaan tässä yhteydessä myös takavarikoida.

Jos tutkinnan kohteena olevan henkilön tietokone on esimerkiksi lähiverkon kautta kytketty toiseen tietokoneeseen ja henkilölle kuuluvaa dataa on tallennettu siihen, myös tätä dataa voidaan tutkia ilman uutta kotietsintämääräystä. Uusi määräys tarvitaan vasta, jos etsinnän laajentaminen edellyttää fyysistä pääsyä toiseen kotirauhalta suojattuun paikkaan, kuin mistä alkuperäisessä määräyksessä oli kysymys. Silloinkin kun uusi määräys tarvitaan, etsintä voidaan laajentaa nopeasti, koska kotietsinnästä päättää pidättämiseen oikeutettu virkamies ja kiireellisessä tapauksessa siitä voi päättää poliisimies.

Artiklan datan etsintää koskevan 1 kappaleen ja etsinnän laajentamista koskevan 2 kappaleen määräykset eivät siten edellytä etsintää koskevien pakkokeinolain säännösten muuttamista.

Suomessa datan takavarikkoa koskevaa artiklan 3 kappaletta lähinnä vastaava sääntely on pakkokeinolain esineiden ja asiakirjojen takavarikkoa koskevissa säännöksissä. Erityisiä tietojärjestelmää ja siinä olevaan dataa koskevia säännöksiä ei Suomen lainsäädännössä takavarikon osalta kuitenkaan ole.

Tietojärjestelmä, sen osa ja muu tallennusalue sekä niissä oleva data voidaan artiklan edellyttämällä tavalla turvata esineen takavarikkoa koskevien säännösten nojalla. Pakkokeinolain 4 luvun 1 §:n mukaan esine voidaan takavarikoida, jos on syytä olettaa, että se voi olla todisteena rikosasiassa tai on rikoksella joltakulta viety taikka että tuomioistuimien julistaa sen menetetyksi. Saman luvun 2 §:ssä on lisäksi säännökset sellaisista asiakirjoista, joita ei saa niiden sisällön vuoksi takavarikoida silloin, kun ne ovat epäillyn tai eräiden muiden määrättyjen henkilöiden hallussa. Sama sääntely koskee myös datan muodossa olevia asiakirjoja. Luvun 10 §:n mukaan takavarikko voidaan myös toteuttaa niin, että esine jätetään sen omistajan hallintaan esimerkiksi sinetöitynä ja omistajaa kielletään käyttämästä sitä. Siitä, että koko esine voidaan takavarikoida, seuraa se, että myös siinä oleva data voidaan takavarikoida.

Artiklan mukaan data on lisäksi voitava kopioida ja poistaa tietojärjestelmästä tai datan käyttö on voitava estää. Tältäkin osin oikeus artiklassa tarkoitettuihin toimenpiteisiin voidaan johtaa esineen takavarikkoa koskevasta sääntelystä. Mainittujen toimenpiteiden oikeudellinen luonne on kuitenkin osin epäselvä. Korkein oikeus on ratkaisussaan 2002:85 katsonut muun ohessa, että jo pelkkä datan kopiointi on takavarikkotoimenpide, vaikka kopioinnin kohteena oleva kiintolevy olisi palautettu sen omistajalle. Tapausta on tarkemmin selostettu pakkokeinolain 4 luvun 4 a §:n perusteluissa. Tapauksesta ilmenee, että esineiden takavarikkoa silmällä pitäen kirjoitettu sääntely ei ole vaikeuksitta sovellettavissa tietojärjestelmässä olevaan dataan.

Suomessa järjestelmän haltijan ja muun henkilön tietojenantovelvollisuutta koskevaa 4 kappaletta lähinnä vastaava sääntely on esitutkintalain 27 §:ssä, jonka mukaan todistajan on totuudenmukaisesti ja mitään salaamatta ilmaistava, mitä hän tietää tutkittavasta asiasta. Säännöksen sanamuodon mukaan säännös tarkoittaa lähinnä velvollisuutta kertoa tutkittavasta rikoksesta eikä niinkään artiklassa tarkoitettulla tavalla tietojärjestelmän ominaisuuksista. Mainittu pykälä on tältä osin tulkinnanvarainen eikä asiaa koskevaa oikeuskäytäntöä ole.

Vaikka nykyinen sääntely varsinkin käytännön tarpeet huomioonottaen täyttäisikin pitkälti artiklan datan takavarikkoa koskevan 3 kappaleen ja järjestelmän haltijan tietojenantovelvollisuutta koskevan 4 kappaleen vaatimukset, artiklan sanamuoto ja voimassa oleva lainsäädäntö eroavat kuitenkin tältä osin tosistaan. Lisäksi voimassa oleva sääntely on molempien kappaleiden osalta osin tulkinnanvaraista.

Tämän vuoksi artikla edellyttää näiltä osin muutoksia nykyiseen lainsäädäntöön.

Hallituksen esitykseen sisältyy ehdotus, jonka mukaan pakkokeinolakiin lisätään artiklan edellyttämät säännökset datan takavarikosta ja järjestelmän haltijan tietojenantovelvollisuudesta.

Ehdotettua sääntelyä on tarkemmin selostettu pakkokeinolain datan takavarikkoa koskevan 4 luvun 4 a §:n ja datan haltijan tietojenantovelvollisuutta koskevan 4 b §:n yksityiskohtaisissa perusteluissa.

Ehdotetun muutoksen tultua voimaan voimassa olevat säännökset vastaavat artiklan vaatimuksia.

## **5 osasto Tiedon hankkiminen datasta reaaliajassa**

### **Tiedon hankkiminen liikennetiedoista reaaliajassa (20 artikla)**

Artiklassa on määräykset reaaliaikaisesta liikennetietojen hankkimisesta.

Artiklan 1 kappaleen a) kohdan mukaan viranomaisilla on oltava oikeus hankkia tai tallentaa teknisin keinoin liikennetietoja tietojärjestelmän avulla siirretyistä yksilöidyistä viesteistä. Myös palveluntarjoaja on saman kappaleen b) kohdan mukaan voitava velvoittaa joko itse hankkimaan liikennetietoja tai avustamaan viranomaisia.

Artiklan 2 kappaleen mukaan osapuolen ei tarvitse noudattaa a) kohtaa, jos se ei sen vakiintuneiden oikeusperiaatteiden mukaan ole mahdollista.

Artiklan 3 kappaleen mukaan palveluntarjoaja on velvollinen pitämään toimenpiteen salassa.

Artiklan 4 kappaleen mukaan artiklassa tarkoitettujen pakkokeinon osalta ovat voimassa myös 14 ja 15 artiklan määräykset soveltamisalasta, rajoitusperusteista ja oikeusturvatakeista.

Liikennetieto on määritelty 1 artiklan d kohdassa. Määritelmän mukaan liikennetieto tarkoittaa tietojärjestelmän välityksellä siirrettyyn viestiin liittyvää dataa, jonka viestinsiirtoketjuun kuuluva tietoverkko on tuottanut ja josta ilmenee viestin alkuperä, määränpää, reitti, kellonaika, päivämäärä, koko, kesto, tai siihen liittyvän palvelun tyyppi.

Palveluntarjoaja on määritelty 1 artiklan c) kohdassa. Määritelmän mukaan palveluntarjoaja tarkoittaa julkista tai yksityistä yksikköä, joka tarjoaa palveluidensa käyttäjille mahdollisuuden tietojärjestelmän välityksellä tapahtuvaan viestintään, ja muuta yksikköä, joka käsittelee tai tallentaa dataa edellä mainitun palveluntarjoajan tai palveluiden käyttäjien puolesta.

Artiklaa käsitellään selitysmuistion kohdissa 205 - 227. Selitysmuistion mukaan liikennetiedot saattavat muodostaa ratkaisevan tai yksinomaisen todistusaineiston siitä, kuka tietoverkkorikoksen on tehnyt. Liikennetietojen säilytysajat saattavat kuitenkin olla erittäin lyhyet. Tämän vuoksi on tärkeää, että liikennetietoja voidaan hankkia reaaliaikaisesti. Artiklan 1 kappaleessa tarkoitettu tietojärjestelmän käsite on laaja. Tietojärjestelmän käsitettä on tarkemmin käsitelty 1 artiklan a) kohdan perusteluissa. Se kattaa kaikki tietoverkot niiden teknisestä toteuttamistavasta riippumatta. Merkitystä ei ole myöskään sillä, onko tietoverkko yksityisessä vai julkisessa omistuksessa. Reaaliaikaisuudella tarkoitetaan liikennetietojen hankkimista viestinnän aikana. Viranomaisen toimivallan näkökulmasta se tarkoittaa oikeutta saada vasta tulevaisuudessa syntyviä liikennetietoja. Selvyyden ja kattavuuden vuoksi hankkiminen ja tallentaminen mainitaan artiklassa erikseen. Pakkokeinon perusteena oleva rikos ja siihen liittyvä viestintä on voitava yksilöidä riittävällä tarkkuudella. Artikla ei siten oikeuta keräämään suuria määriä liikennetietoja pelkästään tarkoituksin saada tietoja joistakin mahdollista rikoksista. Artiklan 1 kappaleen a) kohdasta seuraa, että viranomaisella on oltava myös riittävät tekniset valmiudet hankkia liikennetietoja. Artiklan 1 kappaleen b) kohdan mukainen operaattorin avustusvelvollisuus sen sijaan rajoittuu vain sen olemassa oleviin teknisiin valmiuksiin. Edellä mainitut a) ja b) kohta eivät ole toisensa poissulkevia, vaan artiklan lähtökohtana on se, että ne täydentävät toisiaan ja niitä sovelletaan rinnakkain. Artiklan 2 kohdan mukaan osapuolen ei kuitenkaan tarvitse noudattaa a) kohdan



mukaista velvollisuutta. Silloin osapuolen on velvoitettava operaattorit huolehtimaan myös niiden teknisistä valmiuksista kerätä liikennetietoja. Artikla koskee vain osapuolen alueella tapahtuvaa viestintää. Tämän edellytyksen täyttää kuitenkin jo se, että viestintä kulkee osapuolen alueen läpi. Artiklan 3 kappaleessa tarkoitettun salassapitovelvollisuuden tarkoituksena on varmistaa toimenpiteen tehokkuus. Salassapitovelvollisuuden lakitekkinen toteutus jätetään artiklassa osapuolten harkintaan. Salassapitovelvollisuuden kestolle voidaan asettaa kohtuullinen aikarajoitus. Artiklan 4 kappaleessa viitatu rajoitusperusteet ja oikeusturvatakeet voidaan mitoitaa esimerkiksi sen mukaan kuinka paljon toimenpide loukkaa sen kohteena olevan yksityisyyttä.

Liikennetiedon määritelmää käsitellään selitysmuiston kohdissa 28 - 31. Selitysmuiston mukaan artiklassa tarkoitettuja viestin alkuperää tai määränpäättä osittavia liikennetietoja ovat esimerkiksi puhelinnumero, IP-osoite tai muu niihin verrattava teleosoite. Palvelun tyyppiä koskeva tieto tarkoittaa sitä, onko viestinnässä kysymys esimerkiksi sähköpostista, tiedoston siirrosta vai reaaliaikaisesta keskustelusta.

Palveluntarjoajan määritelmää käsitellään selitysmuiston kohdissa 26 ja 27. Selitysmuiston mukaan artiklassa tarkoitettu palveluntarjoaja voi olla esimerkiksi viestien siirtoa, verkkoon pääsyä, tietojärjestelmän ylläpitoa tai tietojen tallentamista tarjoava teleyritys tai muu yritys.

Suomessa voimassa olevat säännökset artiklan määräyksiä vastaavasta pakkokeinosta ovat pakkokeinolain 5 a luvun televalvontaa koskevissa säännöksissä. Televalvonnalla tarkoitetaan pakkokeinolaissa samaa kuin artiklassa liikennetietojen hankkimisella.

Televalvontaa koskevien säännösten osalta on vireillä lakiuudistus (HE 52/2002). Eduskunta on hyväksynyt lakiehdotuksen ja sen on tarkoitus tulla voimaan viimeistään 1.1.2004. Seuraavassa selostetaan voimassaolevan lain säännöksiä sellaisina kun ne ovat edellä hyväksytyssä lakiehdotuksessa.

Pakkokeinolain 5 a luvun 3 §:n mukaan esitutkintaviranomaisella on oikeus tiettyjä rikoksia tutkittaessa hankkia tuomioistuimen luvalla salassa pidettäviä televiestin tunnistamistietoja.

Tunnistamistiedot tarkoittavat viestin lähettäjän tai vastaanottajan puhelinnumeroa tai vastaavaa osoitetietoa, yhteyden kestoa ja tapahtuma-aikaa sekä muuta vastaavaa tietoa. Myös matkapuhelinlaitteen yksilöinti- ja sijaintitieto ovat tunnistamistietoja.

Tutkittava rikos voi olla automaattiseen tietojenkäsittelyjärjestelmään kohdistunut rikos, joka on tehty telepäätelaitetta käyttäen, paritus, oikeudenkäytössä kuultavan uhkaaminen, laitton uhkaus, huumausainerikos ja näiden yritys sekä terroristisessa tarkoituksessa tehtävän rikoksen valmistelu. Lisäksi pakkokeino voidaan käyttää, jos rikoksesta säädetty ankarin rangaistus on vähintään 4 vuotta vankeutta. Lisäedellytyksenä on vielä se, että tiedoilla voidaan olettaa olevan erittäin tärkeä merkitys rikoksen selvittämiseksi. Lisäedellytystä ei kuitenkaan ole, jos asianomistajan suostumuksella pakkokeino kohdistetaan tämän itse käyttämään teleliittymään.

Tunnistamistietoja voidaan hankkia ainoastaan sellaisesta televiestistä, joka on lähetetty tai vastaanotettu yleisen viestintäverkon tai siihen liitetyn viestintäverkon kautta (PKL 5a:1 §). Yleinen viestintäverkko tarkoittaa verkkoa, jonka käyttäjäpiiriä ei ole etukäteen rajoitettu. Erillisverkon sisäinen viestintä rajautuu siten soveltamisalan ulkopuolelle, jos verkkoa ei ole liitetty yleiseen viestintäverkkoon. Sääntely kattaa perinteisen puhelinviestinnän ja dataviestinnän.

Tuomioistuimen luvassa pakkokeinon kohteena olevat tunnistamistiedot on yksilöitävä. Yksilöintiperusteena voi olla epäillyn hallussa oleva tai todennäköisesti käyttämä teleliittymä, sähköpostiosoite tai muu vastaava teleosoite sekä telepäätelaitte. Yksilöintiperuste on siten teleosoitteiden osalta avoin.

Lupa voidaan myöntää yhdeksi kuukaudeksi kerrallaan (PKL 5a:7§). Lupa voidaan myöntää myös myöntämisaikajaksoksi edeltäneeseen aikaan. Silloin erityistä määräaika ei ole ja ajanjakso voi olla pidempi. Kiireellisessä tapauksessa luvan voi väliaikaisesti myöntää myös pidättämiseen oikeutettu virkamies (PKL 5a:5§).

Pakkokeinon käytöstä on ilmoitettava epäilylle vasta esitutkinnan päätyttyä (PKL 5a:11§). Tämän vuoksi on selvää, että myös teleoperaattori on velvollinen pitämään asian salassa, vaikka nimenomaista säännöstä asiasta ei ole.

Teleoperaattori on viestintämarkkinalain 95 §:n mukaan velvollinen varustamaan verkkonsa siten, että tunnistamistietojen hankkiminen on mahdollista, sekä pakkokeinolain 5 a luvun 9 §:n nojalla muutoinkin avustamaan esitutkintaviranomaista.

Pakkokeinolain rajoitusperusteet ja oikeusturvatakeet ovat sopusoinnussa artiklan 4 kappaleessa viitattujen 14 ja 15 artiklan määräysten kanssa. Lain säännökset kattavat muutoinkin artiklan vaatimukset. Voimassa olevat säännökset vastaavat siten artiklan velvoitteita.

Artikla ei edellytä lainsäädännön muuttamista.

Yleissopimuksen 14 artiklan 3 kappaleen a) kohdan mukaan sopimuspuoli voi tehdä varauman, jonka mukaan se soveltaa tässä artiklassa tarkoitettuja toimenpiteitä ainoastaan varaumassa yksilöityihin rikoksiin tai rikostyyppeihin, kuitenkin niin että valikoima ei ole suppeampi kuin niiden rikosten valikoima, joihin se soveltaa 21 artiklan nojalla siinä tarkoitettuja pakkokeinoja.

Ehdotuksen mukaan Suomi tekee 14 artiklan 3 kappaleen a) kohdan mukaisen varauman, jonka mukaan se soveltaa toimenpiteitä ainoastaan automaattiseen tietojenkäsittelyjärjestelmään kohdistuneeseen rikokseen, joka on tehty telepäätelaitetta käyttäen, paritukseen, oikeudenkäytössä kuultavan uhkaamiseen, laittomaan uhkaukseen, huumausainerikokseen ja näiden yritykseen sekä terroristisessa tarkoituksessa tehtävän rikoksen valmisteluun ja rikoksiin, joista säädetty ankarin rangaistus on vähintään 4 vuotta vankeutta.

Yleissopimuksen 14 artiklan 3 kappaleen b) kohdan mukaan sopimuspuoli voi tehdä varauman, jonka mukaan se ei sovelta tässä artiklassa tai 21 artiklassa tarkoitettuja pakkokeinoja tietojärjestelmän sisäiseen viestintään, jos tietojärjestelmällä on rajattu käyttäjäryhmä ja tietojärjestelmää ei käytetä julkisten tietoverkkojen avulla eikä sitä ole kytketty toiseen julkiseen tai yksityiseen tietojärjestelmään.

Ehdotuksen mukaan Suomi tekee tämän artiklan osalta 14 artiklan 3 kappaleen b) kohdan mukaisen varauman.

### **Tiedon hankkiminen viestin sisällöstä (21 artikla)**

Artiklassa on määräykset reaaliaikaisesta viestin sisältöä koskevan tiedon hankkimisesta.

Artiklan 1 kappaleen a) kohdan mukaan viranomaisilla on oltava oikeus hankkia tai tallentaa teknisin keinoin tietoja tietojärjestelmän avulla siirrettyjen yksilöityjen viestien sisällöstä. Artiklaa sovelletaan ainoastaan tiettyjen kansallisen lainsäädännön määrittämien törkeiden rikosten osalta. Myös palveluntarjoaja on saman kappaleen b) kohdan mukaan voitava velvoittaa joko itse hankkimaan tietoja tai avustamaan viranomaisia.

Artiklan 2 kappaleen mukaan osapuolen ei tarvitse noudattaa a) kohtaa, jos se ei sen vakiintuneiden oikeusperiaatteiden mukaan ole mahdollista.

Artiklan 3 kappaleen mukaan palveluntarjoaja on velvollinen pitämään toimenpiteen salassa.

Artiklan 4 kappaleen mukaan artiklassa tarkoitettun pakkokeinon osalta ovat voimassa myös 14 ja 15 artiklan määräykset soveltamisalasta, rajoitusperusteista ja oikeusturvatakeista.

Artiklaa käsitellään selitysmuistion kohdissa 205 - 215 ja 228 - 231. Selitysmuistion mukaan artiklassa tarkoitettu pakkokeino on tarpeellinen samoista syistä kuin perinteinen puhelin kuuntelu. Jos tietoja ei voida hankkia reaaliaikaisesti esimerkiksi tekeillä olevien rikosten tutkinnassa, rikoksiin puuttuminen ennen vahinkojen syntymistä on vaikeaa tai mahdotonta. Artiklan rakenne ja säänneltävät asiat ovat lähes samat kuin edellä 20 artiklassa. Se, mitä selitysmuistiossa on edellä kerrotulla tavalla sanottu liikennetietojen hankinnasta, koskee siten myös tätä artiklaa.

Suomessa voimassa olevat säännökset artiklan määräyksiä vastaavasta pakkokeinosta ovat pakkokeinolain 5 a luvun telekuuntelua koskevista säännöksistä.

Telekuuntelua koskevien säännösten osalta on vireillä lakiuudistus (HE 52/2002). Eduskunta on hyväksynyt lakiehdotuksen ja sen on tarkoitus tulla voimaan viimeistään 1.1.2004. Seuraavassa selostetaan voimassaolevan lain säännöksiä sellaisina kuin ne ovat edellä hyväksytyssä lakiehdotuksessa.

Pakkokeinolain 5 a luvun 2 §:n mukaan esitutkintaviranomaisella on oikeus tiettyjä törkeitä rikoksia tutkittaessa tuomioistuimen luvalla kuunnella ja tallentaa televiestejä niiden sisällön selvittämiseksi.

Pykälässä on rikosnimikekohtainen tyhjentävä luettelo rikoksista, joiden osalta pakkokeinoa voidaan käyttää. Niitä ovat esimerkiksi maan- ja valtiopetosrikokset, henkirikokset, törkeät vapautteen kohdistuvat rikokset, eräät törkeät vaarantamisrikokset, eräät törkeät varallisuusrikokset, törkeä huumausainerikos ja eräät törkeät ammattimaiset talousrikokset sekä näiden yritys. Lisäedellytyksenä on vielä se, että tiedoilla voidaan olettaa olevan erittäin tärkeä merkitys rikoksen selvittämiseksi.

Tietoja voidaan hankkia ainoastaan sellaisen televiestin sisällöstä, joka on lähetetty tai vastaanotettu yleisen viestintäverkon tai siihen liitetyn viestintäverkon kautta (PKL 5a:1 §). Yleinen viestintäverkko tarkoittaa verkkoa, jonka käyttäjäpiiriä ei ole etukäteen rajoitettu. Erillisverkon sisäinen viestintä rajautuu siten soveltamisalan ulkopuolelle, jos verkkoa ei ole liitetty yleiseen viestintäverkkoon. Sääntely kattaa perinteisen puhelinviestinnän ja dataviestinnän.

Tuomioistuimen luvassa pakkokeinon kohteena oleva viestintä on yksilöitävä. Yksilöintiperusteena voi olla epäillyn hallussa oleva tai todennäköisesti käyttämä teleliittymä, sähköpostiosoite tai muu vastaava teleosoite sekä telepääte laite. Yksilöintiperuste on siten teleosoitteiden osalta avoin.

Lupa voidaan myöntää yhdeksi kuukaudeksi kerrallaan (PKL 5a:7§). Tuomioistuin voi liittää lupaan muitakin rajoituksia ja ehtoja.

Pakkokeinon käytöstä on ilmoitettava epäilylle vasta esitutkinnan päätyttyä (PKL 5a:11§). Tämän vuoksi on selvää, että myös teleoperaattori on velvollinen pitämään asian salassa vaikka nimenomaista säännöstä asiasta ei ole.

Teleoperaattori on viestintämarkkinalain 95 §:n mukaan velvollinen varustamaan verkkonsa siten, että tietojen hankkiminen viestin sisällöstä on mahdollista sekä pakkokeinolain 5 a luvun 9 §:n nojalla muutoinkin avustamaan esitutkintaviranomaista.

Pakkokeinolain rajoitusperusteet ja oikeusturvatakeet ovat sopusoinnussa artiklan 4 kappaleessa viitattujen 14 ja 15 artiklan määräysten kanssa. Lain säännökset kattavat muutoinkin artiklan vaatimukset. Voimassa olevat säännökset vastaavat siten artiklan velvoitteita.

Artikla ei edellytä lainsäädännön muuttamista.

Yleissopimuksen 14 artiklan 3 kappaleen b) kohdan mukaan sopimuspuoli voi tehdä varauman, jonka mukaan se ei sovelta tässä artiklassa tai 20 artiklassa tarkoitettuja pakkokeinoja tietojärjestelmän sisäiseen viestintään, jos tietojärjestelmällä on rajattu käyttäjäryhmä ja tietojärjestelmää ei käytetä julkisten tietoverkkojen avulla eikä sitä ole kytketty toiseen julkiseen tai yksityiseen tietojärjestelmään.

Ehdotuksen mukaan Suomi tekee tämän artiklan osalta 14 artiklan 3 kappaleen b) kohdan mukaisen varauman.

### **3 jakso Lainkäyttövalta**

#### **Lainkäyttövalta (22 artikla)**

Artiklassa on määräykset yleissopimukseen perustuvien rikossäännösten alueellisesta soveltamisalasta.

Artiklan 1 kappaleen a) - c) kohtien mukaan osapuolen rikossäännöksiä on voitava soveltaa silloin kun rikos on tehty sen alueella (a), sen lippua käyttävässä aluksessa (b) tai sen lakien mukaan rekisteröidyssä ilma-aluksessa (c).

Artiklan 1 kappaleen d) kohdan mukaan osapuolen rikossäännöksiä on voitava soveltaa silloin kun rikoksentehtäjä on sen kansalainen, jos rikos on rangaistava myös tekopaikan lain mukaan, tai kun rikos on tehty millekään valtiolle kuulumattomalla alueella.

Artiklan 2 kappaleen mukaan osapuoli voi tehdä varauman, jonka mukaan se ei sovelta tai soveltaa ainoastaan tiettyihin tapauksiin tai tietyin edellytyksin artiklan 1 kappaleen b - d kohtiin tai johonkin niistä sisältyviä lainkäyttövaltaa koskevia määräyksiä.

Artiklan 3 kappaleen mukaan osapuolen rikossäännöksiä on voitava soveltaa silloin kun epäilty rikoksentehtäjä tavataan sen alueella eikä se rikoksen johdosta tapahtuvaa luovuttamista koskevan pyynnön saatuaan luovuta häntä toiselle sopimuspuolelle pelkästään hänen kansalaisuutensa perusteella.

Artiklan 4 kappaleessa todetaan selvyyden vuoksi, ettei artiklassa oleva soveltamisalaluettelo ole tyhjentävä eikä artikla siten estä säätämästä kansallisessa lainsäädännössä muihin edellytyksiin perustuvia soveltamisalasäännöksiä.

Artiklan 5 kappaleessa on määräys neuvotteluvollisuudesta sen tilanteen varalle, että useampi sopimuspuoli ilmoittaa aikomuksestaan käyttää lainkäyttövaltaansa samassa rikoksessa.

Artiklaa käsitellään selitysmuistion kohdissa 232 - 239. Selitysmuistion mukaan soveltamisalamääräykset perustuvat 1 kappaleen a) - c) kohtien osalta alueperiaatteeseen ja sen johdannaisiin sekä d) kohdan osalta kansalaisuusperiaatteeseen. Artiklan 3 kappaleen määräys taas perustuu rikosentekijän luovuttamisessa sovellettavaan "luovuta tai rankaise" -periaatteeseen. Artiklan 2 kohdan mukainen varaumaoikeus koskee vain siinä mainittuja b - d kohtia. Artiklan 1 kappaleen a) kohdan ja 3 kappaleen osalta varaumaa ei voi tehdä. Artiklan 5 kohdassa tarkoitettu neuvotteluvollisuus ei ole ehdoton. Asiasta on neuvoteltava, jos se katsotaan tarkoituksenmukaiseksi.

Suomessa voimassa olevat säännökset rikoslain soveltamisalasta ovat rikoslain 1 luvussa.

Artiklan 1 kappaleen a) kohtaa vastaava säännös on luvun 1 §, jonka mukaan Suomessa tehtyyn rikokseen sovelletaan Suomen lakia. Rikos katsotaan luvun 10 §:n mukaan tehdyksi sekä siellä, missä rikollinen teko suoritettiin, että siellä, missä rikoksen tunnusmerkistön mukainen seuraus ilmeni.

Artiklan 1 kappaleen b) ja c) kohtaa vastaava säännös on luvun 2 §, jonka mukaan suomalaisessa aluksessa tai ilma-aluksessa tehtyyn rikokseen sovelletaan Suomen lakia. Pääsääntöisesti Suomen lakia sovelletaan silloinkin kun alus on vieraan valtion alueella tai sen yläpuolella.

Artiklan 1 kappaleen d) kohtaa vastaava säännös on luvun 6 §, jonka mukaan Suomen kansalaisen Suomen ulkopuolella tekemään rikokseen sovelletaan Suomen lakia. Lisäedellytyksenä 11 §:n mukaan on se, että rikos on myös tekopaikan lain mukaan rangaistava ja siitä olisi voitu tuomita rangaistus myös tämän vieraan valtion tuomioistuimessa. Rikoksesta ei silloin Suomessa saa tuomita ankarampaa seuraamusta kuin siitä tekopaikan laissa säädetään. Jos rikos on tehty millekään valtiolle kuulumattomalla alueella, rangaistavuuden edellytyksenä on 6 §:n mukaan, että teosta Suomen lain mukaan saattaa seurata yli kuuden kuukauden vankeusrangaistus. Kaikkien yleissopimuksessa tarkoitettujen rikosten rangaistusmaksimi on vähintään vuosi vankeutta.

Artiklan 3 kohtaa vastaava säännös on luvun 8 §, jonka mukaan Suomen ulkopuolella tehtyyn rikokseen, josta Suomen lain mukaan saattaa seurata yli kuuden kuukauden vankeusrangaistus, sovelletaan Suomen lakia, jos valtio, jonka alueella rikos on tehty, on pyytänyt rikoksen syytteenpanoa suomalaisessa tuomioistuimessa tai rikoksen johdosta esittänyt pyynnön rikosentekijän luovuttamisesta, mutta pyyntöön ei ole suostuttu.

Artiklan 4 ja 5 kohdalla ei ole välitöntä merkitystä lainsäädännön kannalta.

Voimassa olevat säännökset vastaavat siten artiklan velvoitteita.

Artikla ei edellytä lainsäädännön muuttamista.

Suomella ei ole tarvetta artiklan 2 kohdassa tarkoitettua varaumaa.

### **III luku Kansainvälinen yhteistyö**

#### **1 jakso Yleiset periaatteet**

##### **1 osasto Kansainvälistä yhteistyötä koskevat yleiset periaatteet**

###### **Kansainvälistä yhteistyötä koskevat yleiset periaatteet (23 artikla)**

Artiklassa on määräykset koko III luvussa säänneltyä kansainvälistä yhteistyötä koskevista yleisistä periaatteista. Artiklan määräykset koskevat siten sekä rikoksen johdosta tapahtuvaa luovuttamista että keskinäistä oikeusapua. Artiklan mukaan osapuolet toimivat yhteistyössä luvun määräysten mukaisesti ja soveltavat asiaa koskevia sopimuksia ja kansallista lainsäädäntöään mahdollisimman laajasti tietojärjestelmiin liittyvien rikosten tutkintaan ja oikeudenkäyntiin tai minkä hyvänsä rikoksen sähköisessä muodossa olevan todistusaineiston keräämiseen.

Artiklaa käsitellään selitysmuistion kohdissa 241 - 244. Selitysmuistion mukaan artiklasta ilmenee kolme yleisempää periaatetta. Ensimmäisen periaatteen mukaan osapuolien on pyrittävä kansainvälisessä yhteistyössä soveltamaan eri oikeuslähteitä mahdollisimman laajasti. Toiseksi sopimuksessa säännelty kansainvälinen yhteistyö kattaa tietoverkkorikosten lisäksi myös muuhun rikokseen liittyvän sähköisessä muodossa olevan todistusaineiston hankkimisen. Kolmanneksi sopimuksen 3 luvun määräykset eivät syrjäytä muissa yleissopimuksissa tai kahdenvälisissä sopimuksissa olevia samaa asiaa koskevia määräyksiä.

Sopimuksen 3 luvun määräykset koskevat ainoastaan rikosten tutkintaa ja oikeudenkäyntiä. Ne eivät siten koske esimerkiksi rikostiedustelutoimintaa.

##### **2 osasto Rikoksen johdosta tapahtuvaa luovuttamista koskevat periaatteet**

###### **Rikoksen johdosta tapahtuva luovuttaminen (24 artikla)**

Artiklassa on rikoksen johdosta tapahtuvaa luovuttamista koskevat määräykset.

Artiklan 1 kappaleen a kohdan mukaan artiklaa sovelletaan ainoastaan 2 - 11 artiklan mukaisesti rangaistavaksi säädettyjen rikosten johdosta tapahtuvaan luovuttamiseen. Edellytyksenä on lisäksi, että rikokset ovat molempien osapuolten lainsäädännön mukaan rangaistavia ja että enimmäisrangaistus on sekä pyynnön esittävän että pyynnön vastaanottavan valtion lain mukaan vähintään vuosi vankeutta. Saman kappaleen b kohdan mukaan artiklan mukainen enimmäisrangaistusta koskeva ehto kuitenkin syrjäytyy, jos muussa osapuolta sitovassa sopimuksessa oleva määräys tältä osin poikkeaa artiklan määräyksestä.

Artiklan 2 kappaleen mukaan 1 kappaleessa tarkoitettujen rikosten katsotaan sisältyvän osapuolten välisiin luovuttamissopimuksiin rikoksina, joiden osalta tekijä voidaan luovuttaa. Osapuolet sitoutuvat myös sisällyttämään nämä rikokset myöhemmin tehtäviin luovuttamissopimuksiin.

Artiklan 3 kappaleen mukaan osapuoli voi pitää tätä yleissopimusta luovuttamisen oikeusperustana, jos se asettaa rikoksen johdosta tapahtuvan luovuttamisen ehdoksi sitä koskevan kahdenvälisen

sopimuksen olemassaolon. Jos osapuoli ei edellytä edellä tarkoitettua erityisen sopimuksen olemassaoloa, se katsoo 4 kappaleen mukaan 1 kappaleessa tarkoitettuja rikokset sellaisiksi, joiden johdosta rikoksentekijä voidaan luovuttaa.

Artiklan 5 kappaleen mukaan luovuttamiseen sovelletaan pyynnön vastaanottavan osapuolen lainsäädännön tai sitä sitovan luovuttamissopimuksen ehtoja. Tämä koskee myös kieltäytymisperusteita.

Artiklan 6 kappale koskee tilannetta, jossa sopimuspuoli kieltäytyy luovutuksesta pelkästään pyynnön kohteena olevan henkilön kansalaisuuden perusteella tai koska se katsoo kyseisen rikoksen kuuluvan lainkäyttövaltaansa. Pynnön vastaanottanut sopimuspuoli on silloin velvollinen saattamaan asian toimivaltaisten viranomaisten käsiteltäväksi syytteen nostamista varten pyynnön esittäneen sopimuspuolen pyynnöstä, ja ilmoittamaan käsittelyn lopputuloksesta pyynnön esittäneelle sopimuspuolelle.

Artiklan 7 kappaleessa on määräykset luovuttamisasioista vastaavan viranomaisen nimeämisestä ja näistä viranomaisista ylläpidettävästä rekisteristä.

Artiklaa käsitellään selitysmuistion kohdissa 245 - 252. Selitysmuistion mukaan 1 kappaleessa luovuttamisen edellytyksenä oleva rangaistuskynnys on tarpeellinen, koska osa kyseeseen tulevista rikoksista saattaa olla suhteellisen lieviä. Oleellista ei silloin ole se, mitä teosta voitaisiin käytännössä tuomita vaan sovellettava asteikko. Artiklan 2 kappale ei edellytä sitä, että kaikista mainituista rikoksista olisi aina luovutettava vaan sitä, että luovuttamisen pitää olla mahdollista. Artiklan 3 kappale ei velvoita niitä osapuolia, joihin sitä sovelletaan vaan antaa ainoastaan siinä määrätyn oikeuden. Artiklan 4 kappale on sen sijaan velvoittava. Artiklan 5 kappale koskee myös kieltäytymisperusteita, jotka perustuvat osapuolta sitovaan luovuttamissopimukseen. Artiklan 6 kohta perustuu "luovuta tai rankaise" -periaatteeseen. Artiklan 7 kappaleen tarkoituksena on helpottaa ja varmistaa osapuolten tiedonsaantia.

Suomessa voimassa olevat säännökset rikoksentekijän luovuttamisesta sisältyvät lakiin rikoksen johdosta tapahtuvasta luovuttamisesta, joka on asiaa koskeva yleislaki, eräisiin erityislakeihin sekä Suomessa voimaansaatettuihin yleissopimuksiin ja kahdenvälisiin sopimuksiin. Voimassaolevan oikeuden sisältöä on tältä osin selostettu myös yleisperusteluissa.

Artikla sisältää määräyksiä yleissopimuksessa tarkoitettujen rikosten perusteella tapahtuvasta luovuttamisesta sopimuspuolten välillä voimassa olevien luovutussopimusten mukaisesti tai jos tällaista ei ole, tämän sopimuksen mukaisesti.

Artiklan 1 kappaleessa tarkoitettuja rikokset ovat sellaisia, joiden perusteella Suomen lainsäädännön mukaan voidaan säännönmukaisesti luovuttaa. Kun luovutukseen voidaan lisäksi 5 kappaleen mukaan liittää pyynnön vastaanottaneen lainsäädännön tai soveltamien luovutussopimusten mukaisia ehtoja, artikla on muutoinkin sopusoinnussa Suomen voimassaolevan oikeuden kanssa.

Artiklan 6 kappaleen osalta on huomattava, että Suomen perustuslain 9 §:n mukaan Suomen kansalaista ei saa vasten tahtoaan luovuttaa tai siirtää toiseen maahan. Yleisen luovuttamislain 2 §:n mukaan Suomen kansalaista ei saa luovuttaa. Muihin pohjoismaihin Suomen kansalainen voidaan luovuttaa eräin edellytyksin. Oikeudenkäyntiä varten Suomen kansalainen voidaan määrätyn edellytyksin luovuttaa Euroopan Unionin jäsenvaltioon. Suomen kansalainen voidaan rikoslain 1 luvun 6 §:n mukaan tuomita Suomessa rangaistukseen Suomen ulkopuolella tekemästään rikoksesta, jos teko on rangaistava myös tekopaikan lain mukaan. Lisäksi on huomattava, että

Suomen lakia sovelletaan 1 luvun 8 §:n mukaan, jos valtio, jonka alueella rikos on tehty, on pyytänyt rikoksen syytteenpanoa suomalaisessa tuomioistuimessa tai rikoksen johdosta esittänyt pyynnön rikosentekijän luovuttamisesta, mutta pyyntöön ei ole suostuttu. Säännös edellyttää kaksoisrangaistavuutta ja sitä, että teosta Suomen lain mukaan saattaa seurata yli kuusi kuukautta vankeutta.

Artiklan 7 kappaleessa tarkoitettu viranomainen Suomessa on oikeusministeriö.

Sopimuksen määräykset eivät ole ristiriidassa Suomen voimassa olevan oikeuden kanssa.

### **3 osasto Keskinäistä oikeusapua koskevat yleiset periaatteet**

#### **Keskinäistä oikeusapua koskevat yleiset periaatteet (25 artikla)**

Artiklassa on määräykset keskinäistä oikeusapua koskevista yleisistä periaatteista.

Artiklan 1 kappaleen mukaan osapuolet antavat mahdollisimman laajaa oikeusapua tietojärjestelmiin liittyvien rikosten tutkinnassa ja oikeudenkäynnissä tai minkä hyvänsä rikoksen sähköisessä muodossa olevan todistusaineiston keräämisessä ja 2 kappaleen mukaan varmistavat sopimuksen noudattamisen tarvittaessa lainsäädännöllisin tai vastaavin toimenpitein.

Artiklan 3 kappaleen mukaan osapuoli voi kiireellisessä tapauksessa esittää oikeusapupyynnön sähköpostilla tai muulla vastaavalla nopealla tavalla. Pyyntöön on silloin myös vastattava nopealla tavalla.

Artiklan 4 kappaleen mukaan oikeusapuun sovelletaan pyynnön vastaanottavan osapuolen lainsäädännön tai sitä sitovan keskinäistä oikeusapua koskevan sopimuksen ehtoja. Tämä koskee myös kieltäytymisperusteita. Kieltäytyä ei saa 2 - 11 artiklassa tarkoitettujen rikosten osalta pelkästään sillä perusteella, että osapuoli pitää rikosta verorikoksena.

Artiklan 5 kappaleen mukaan kaksoisrangaistavuutta koskeva edellytys täyttyy rikosnimikkeestä ja rikoksen luokittelusta riippumatta, jos teko on sama.

Artiklaa käsitellään selitysmuistion kohdissa 253 - 259. Selitysmuistion mukaan artiklan 1 kappaleen mukainen soveltamisala on sama kuin 23 artiklassa ja kattaa siten 14 artiklassa tarkoitettut tilanteet. Artiklan 2 kappale velvoittaa osapuolia huolehtimaan siitä, että toimenpiteille on kansallisessa lainsäädännössä riittävä oikeudellinen perusta. Artiklan nopeutettua tietovälinettä koskeva 3 kappale on tarpeellinen, koska rikostutkinnalle merkityksellinen data saattaa muutoin hävitä oikeusapumenettelyn aikana. Siihen, voidaanko oikeusapupyynnö tehdä puhelimitse, selitysmuistiossa ei oteta kantaa. Artiklan 4 kappale ei oikeuta asettamaan sellaisia ehtoja, jotka ovat ristiriidassa yleissopimuksen nimenomaisen määräyksen kanssa. Artiklan 5 kappaleen tarkoituksena on estää osapuolia tulkitsemasta kaksoisrangaistavuutta koskevaa vaatimusta liian tiukasti.

Suomessa voimassa olevat säännökset keskinäisestä oikeusavusta sisältyvät rikosoikeusapulakiin, joka on keskinäistä oikeusapua koskeva yleislaki, eräisiin erityislakeihin sekä Suomessa voimaansaatettuihin yleissopimuksiin ja kahdenvälisiin sopimuksiin. Voimassa olevan oikeuden sisältöä on tältä osin selostettu myös yleisperusteluissa.



Artikla sisältää yleisiä määräyksiä keskinäisestä oikeusavusta tietoverkkorikosten sekä sähköisessä muodossa olevan todistusaineiston osalta voimassa olevien oikeusapusopimusten mukaisesti, tai jos tällaista ei ole, tämän sopimuksen mukaisesti.

Oikeusavun antaminen 1 kappaleessa tarkoitetuissa tapauksissa on rikosoikeusapulain mukaan säännönmukaisesti mahdollista.

Artiklan 3 kappaletta vastaava sääntely on rikosoikeusapulain 7 §:ssä. Pykälän mukaan vieraan valtion viranomaisen Suomen viranomaiselle osoittama oikeusapupyynnö voidaan tehdä kirjallisesti, teknisenä tallenteena tai suullisesti ja se voidaan lähettää myös sähköisenä viestinä. Jos pyynnön tai siihen liittyvän asiakirjan oikeaperäisyydestä tai sisällöstä syntyy epäilystä, voi oikeusministeriö tai toimivaltainen viranomainen pyytää, että pyyntö vahvistetaan tarvittavilta osilta kirjallisesti. Oikeusapupyynnöä ja siihen liittyviä asiakirjoja ei tarvitse laillistaa. Artiklassa tarkoitettu nopeutetun viestintäkeinin käyttäminen on siten mahdollista rikosoikeusapulain mukaan.

Artiklan 4 kappaleen verorikoksia ja 5 kappaleen kaksoisrangaistavuutta koskevilla määräyksillä ei ole Suomen kannalta merkitystä. Rikosoikeusapulain mukaan oikeusapua annetaan myös silloin, kun pyyntö koskee verorikosta. Kaksoisrangaistavuutta arvioitaessa ratkaisevaa ei rikosoikeusapulain 15 §:n 1 momentin mukaan ole se, miten teko on otsikoitu oikeusapupyynnössä.

### **Tietojen antaminen omasta aloitteesta (26 artikla)**

Artiklassa on määräykset osapuolen oma-aloitteisesta tietojenanto-oikeudesta. Artiklan 1 kappaleen mukaan osapuoli voi ilman pyyntöäkin antaa toiselle osapuolelle rikostutkintaa hyödyttäviä tietoja. Artiklan 2 kappaleen mukaan tietojen luovuttaja voi asettaa tiedoille käyttörajoituksia, joita vastaanottajan on noudatettava.

Artiklaa käsitellään selitysmuistion kohdissa 260 ja 261. Selitysmuistion mukaan artikla ei velvoita osapuolia antamaan tietoja vaan antaa siihen oikeuden. Artikla on tarpeellinen, koska eräiden valtioiden osalta oma-aloitteinen tietojenanto-oikeus edellyttää erityistä sopimusmääräystä. Artiklan mukaan tietojenanto tapahtuu osapuolen lainsäädännön asettamissa rajoissa.

Silloin kun Suomi on tietoja luovuttavana osapuolena, tietoja annetaan Suomen lainsäädännön asettamissa rajoissa. Suomen lainsäädäntö ei aseta yleisiä esteitä artiklassa tarkoitettulle tietojenvaihdolle. Viranomaisen julkisuudesta annetun lain (621/1993) 30 §:n mukaan myös salassa pidettäviä tietoja voidaan antaa ulkomaan viranomaiselle silloin, kun luovuttaminen perustuu Suomea sitovaan sopimukseen.

Silloin, kun Suomi on tietoja vastaanottavana osapuolena, viranomainen on oikeutettu ja velvollinen noudattamaan asetettuja salassapito- ja muita ehtoja rikosoikeusapulain 27 §:n nojalla. Pykälän 2 momentin mukaan viranomaisen on Suomen lain lisäksi noudatettava oikeusapua antavan osapuolen asettamia ehtoja.

Tämän vuoksi ja kun artikla ei ole velvoittava, sen hyväksymiseen ei liity Suomen kannalta ongelmia.

#### **4 osasto Keskinäistä oikeusapua koskeviin pyyntöihin sovellettavat menettelytavat silloin kun niihin ei ole sovellettavissa kansainvälistä sopimusta**

#### **Keskinäistä oikeusapua koskeviin pyyntöihin sovellettavat menettelytavat silloin kun niihin ei ole sovellettavissa kansainvälistä sopimusta (27 artikla)**

Artiklaa sovelletaan 1 kappaleen mukaan vain jos osapuolten välillä ei ole erillistä asiaa koskevaa sopimusta.

Artiklan 2 kappaleessa on määräykset oikeusapuasioista vastaavan keskusviranomaisen nimeämisestä ja näistä ylläpidettävästä rekisteristä. Artiklan mukaan keskusviranomaiset ovat suoraan yhteydessä toisiinsa.

Artiklan 3 kappaleen mukaan oikeusapupyynnö on pantava täytäntöön pyytäjän täsmentämien menettelytapojen mukaisesti, paitsi jos ne ovat vastaanottajan lainsäädännön vastaisia.

Artiklan 4 kappaleen mukaan oikeusavusta voi 25 artiklan 4 kappaleessa olevien perusteiden lisäksi kieltäytyä vain, jos vastaanottaja pitää rikosta poliittisena rikoksena tai jos oikeusavun antaminen vaarantaisi vastaanottajan merkittäviä etuja. Artiklassa viitatus 25 artiklan 4 kappaleen mukaan oikeusapuun sovelletaan pyynnön vastaanottavan osapuolen lainsäädännön tai sitä sitovan keskinäistä oikeusapua koskevan sopimuksen ehtoja. Tämä koskee myös kieltäytymisperusteita.

Artiklan 5 kappaleen mukaan oikeusavun antamista voidaan lykätä vastaanottajan rikostutkintaan liittyvillä perusteilla.

Artiklan 6 kappaleen mukaan pyytäjän kanssa on neuvoteltava pyynnön rajoittamisesta ennen kuin vastaanottaja kieltäytyy oikeusavusta tai lykkää sen antamista.

Artiklan 7 kappaleen mukaan vastaanottaja ilmoittaa viipymättä pyytäjälle asian lopputuloksesta. Oikeusavun lykkääminen tai epääminen on perusteltava. Pyytäjälle on myös ilmoitettava, jos oikeusavun antaminen osoittautuu mahdottomaksi tai viivästyy olennaisesti.

Artiklan 8 kappaleen mukaan osapuoli voi pyytää, että oikeusapupyynnö pidetään salassa. Jos pyynnön vastaanottanut sopimuspuoli ei voi noudattaa salassapitoa koskevaa pyyntöä, se ilmoittaa tästä viipymättä pyynnön esittäneelle sopimuspuolelle, joka sitten päättää tulisiko pyyntö siitä huolimatta panna täytäntöön.

Artiklan 9 kappaleessa on määräykset oikeusapupyynnön toimittamisesta. Kappaleen a kohdan mukaan pyyntö voidaan kiireellisissä ja eräissä muissa tapauksissa lähettää keskusviranomaisen sijasta tai ohella suoraan toimivaltaiselle viranomaiselle. Kappaleen c kohdassa on tähän liittyen määräykset pyynnön ohjaamisesta oikealle viranomaiselle. Kappaleen e kohdan mukaan osapuoli voi ilmoittaa, että tehokkuussyistä tämän kappaleen mukaiset pyynnöt tulee osoittaa sen keskusviranomaiselle.

Artiklaa käsitellään selitysmuistion kohdissa 262 - 274. Selitysmuistion mukaan artiklan soveltamisalan rajaaminen ainoastaan tilanteisiin, joissa muuta sopimusta ei ole, perustuu tarkoituksenmukaisuusyyihin. Osapuolten on helpompi soveltaa jo olemassa olevia sopimuksia ja samalla vältetään päällekkäisistä sopimuksista mahdollisesti aiheutuvat ristiriidat. Artiklaa eivät siten sovelleta esimerkiksi eurooppalaisen oikeusapusopimuksen ja sen lisäpöytäkirjan osapuolet.

Artiklan soveltaminen syrjäytyy myös myöhemmin mahdollisten tehtävien sopimusten perusteella. Artikla sisältää ainoastaan yleisiä oikeusavussa noudatettavia periaatteita koskevia määräyksiä. Artiklan 2 kohdan mukainen keskusviranomaisen välityksellä tapahtuva oikeusapu on diplomaattista reittiä huomattavasti tehokkaampi toimintatapa. Artiklan 3 kohdan tarkoituksena on varmistaa se, että oikeusaputeitse hankittu todistusaineisto on muodollisesti pätevä myös esimerkiksi vastaanottajan tuomioistuimessa. Artiklan 4 kohdan mukaisia kieltäytymisperusteita ei saa tulkita niin laajasti, että ne käytännössä estävät oikeusavun saamisen. Artiklan 5 kohdan mukainen lykkääminen ja 6 kohdan mukaiset rajoitukset on tarkoitettu tarkoituksenmukaiseksi vaihtoehdoksi oikeusavusta kieltäytymiselle. Artiklan 7 kohdan perusteluvollisuuden tarkoituksena on edistää osapuolten tiedonsaantia ja siten mahdollisuuksia kehittää yhteistyötä. Artiklan 8 kohdassa tarkoitettua salassapidon kohteena on vain pyyntö ja sen sisältö. Salassapitovelvollisuutta ei pyynnössä pidä asettaa niin laajaksi, että se vaikeuttaa tai tekee mahdottomaksi toimenpiteen toteuttamisen.

Artiklan 1 kappaleesta seuraa, että artiklaa ei sovelleta lainkaan Suomen ja esimerkiksi eurooppalaisen oikeusapusopimuksen osapuolina olevien valtioiden kesken.

Artiklan 2 kappaleessa tarkoitettu keskusviranomainen on Suomessa rikosoikeusapulain 3 §:n mukaan oikeusministeriö.

Artiklan 3 kappaletta vastaava säännös on rikosoikeusapulain 11 §:ssä. Pykälän 1 momentin mukaan oikeusapupyynnön toimeenpanossa voidaan noudattaa pyynnössä esitettyä erityistä muotoa tai menettelyä, jos tätä ei voida pitää Suomen lainsäädännön vastaisena.

Artiklan 4 kappaletta vastaava säännös on ensinnäkin rikosoikeusapulain ehdottomia kieltäytymisperusteita koskevassa 12 §:ssä. Pykälän 1 momentin mukaan oikeusapua ei anneta, jos oikeusavun antaminen saattaisi loukata Suomen täysivaltaisuutta tai vaarantaa Suomen turvallisuutta taikka muita olennaisia etuja. Oikeusapua ei 2 momentin mukaan myöskään anneta, jos oikeusavun antaminen olisi ristiriidassa ihmisoikeuksia ja perusvapauksia koskevien periaatteiden kanssa taikka jos oikeusavun antaminen muutoin olisi Suomen oikeusjärjestyksen peruseriaatteiden vastaista. Rikosoikeusapulain 13 §:ssä on lisäksi säännökset harkinnanvaraisista kieltäytymisperusteista. Pykälän mukaan oikeusavun antamisesta voidaan kieltäytyä muun ohessa, jos pyynnön perusteena on teko, jota on pidettävä poliittisena rikoksena. Pykälässä on lisäksi muita kieltäytymisperusteita, jotka liittyvät syyteoikeuden vanhentumiseen, vireillä olevaan oikeudenkäyntiin ja vastaaviin seikkoihin.

Artiklan 5 kappaletta vastaava säännös on rikosoikeusapulain 13 §:n 2 momentissa. Säännöksen mukaan oikeusapupyynnön toimeenpanoa voidaan lykätä, jos pyynnön toimeenpano saattaisi haitata tai viivästyttää rikostutkintaa, esitutkintaa taikka oikeudenkäyntiä Suomessa.

Artiklan 7 kappaletta vastaava säännös on rikosoikeusapulain 9 §:ssä. Pykälän 3 momentin mukaan pyynnön esittäneen vieraan valtion viranomaiselle on viipymättä ilmoitettava, jos oikeusapupyyntöä ei voida täyttää tai jos pyynnön täytäntöönpano viivästyy. Samalla on mainittava pyynnön täyttämättä jättämisen peruste taikka viivästyksen syyt. Saman pykälän 2 momentin mukaan pyynnön esittänyttä vieraan valtion viranomaista on viipymättä pyydettyä täydentämään pyyntöä taikka antamaan asiassa lisäselvityksiä, jos oikeusapupyyntö tai siihen liitetyt asiakirjat ovat niin puutteelliset, että pyyntöä ei voida täyttää.

Artiklan 6 kappaleen neuvotteluvollisuutta vastaavaa nimenomaista säännöstä rikosoikeusapulaissa ei ole. Edellä selostettujen 9 §:n mukaisten ilmoitusten yhteydessä osapuolen

kanssa voidaan kuitenkin myös neuvotella ja ohjata tämä muuttamaan hakemustaan. Suomen viranomaisen on tältä osin noudatettava myös suoraan yleissopimuksen määräyksiä. Rikosoikeusapulain muuttaminen tämän kaltaisen vähäisen ristiriidan vuoksi ei ole tarpeellista eikä tarkoituksenmukaista.

Artiklan 8 kappaleen osalta on huomattava, että määräys ei velvoita oikeusapupyynnön salassapitoon vaan ainoastaan ilmoittamaan, jos salassapitopyyntöön ei voida suostua. Määräys on muutenkin Suomen kannalta ongelmaton, koska kansainvälinen oikeusapupyyntö on Suomessa esitutkintaan liittyvänä asiakirjana salainen.

Artiklan 9 kappaletta vastaava säännös on rikosoikeusapulain 4 §. Pykälän mukaan vieraan valtion viranomaisen pyyntö oikeusavun antamisesta lähetetään oikeusministeriölle tai tehdään suoraan sille viranomaiselle, jonka toimivaltaan pyynnön täyttäminen kuuluu. Jos oikeusapupyyntö on lähetetty oikeusministeriölle, ministeriön tulee viipymättä toimittaa pyyntö sille viranomaiselle, jonka toimivaltaan pyynnön toimeenpano kuuluu, jos pyynnön täyttäminen ei kuulu oikeusministeriön toimivaltaan. Suomella ei ole tarvetta tehdä kappaleen e kohdan mukaista ilmoitusta.

### **Tietojen salassapito ja käyttörajoitukset (28 artikla)**

Artiklaa sovelletaan 1 kappaleen mukaan vain, jos osapuolten välillä ei ole erillistä asiaa koskevaa sopimusta.

Artiklan 2 kappaleen mukaan pyynnön vastaanottaja voi asettaa tietojen tai aineiston antamisen ehdoksi, että tiedot pidetään salassa, jos pyyntöön ei muutoin voida suostua, tai että tietoja ei käytetä muuhun kuin pyynnössä mainittuun rikostutkintaan tai rikosoikeudenkäyntiin.

Artiklan 3 kappaleen mukaan pyynnön esittäjän on ilmoitettava vastaanottajalle, jos se ei voi noudattaa ehtoa. Jos pyynnön esittäjä hyväksyy ehdon, tämä sitoo sitä.

Artiklan 4 kappaleen mukaan ehdon asettaja on oikeutettu pyynnöstä saamaan tietoja luovutetun aineiston käyttötarkoituksesta.

Artiklaa käsitellään selitysmuistion kohdissa 275 - 280. Selitysmuistion mukaan artiklan eräänä tarkoituksena on suojata arkaluonteisia tietoja esimerkiksi yksityisyyden suojaan liittyvissä tilanteissa. Artiklan soveltamisala on rajoitettu samoista syistä kuin 27 artiklassa. Esimerkkinä 2 kappaleessa tarkoitettu salassapitoa välttämättä edellyttävästä tiedosta mainitaan luottamuksellisen tietolähteen henkilöllisyyden suojaaminen. Käyttötarkoituksen rajoittamisen osalta voi olla käytännössä mahdotonta varmistaa se, ettei aineistoa esimerkiksi oikeudenkäynnin julkisuuden seurauksena joudu käytettäväksi myös muuhun kuin pyynnössä tarkoitettuun tarkoitukseen. Artiklan 4 kappaleen tarkoituksena on se, että ehdon asettaja voi valvoa ehdon noudattamista.

Artiklan 1 kappaleesta seuraa, että artiklaa ei sovelleta lainkaan Suomen ja esimerkiksi eurooppalaisen oikeusapusopimuksen ja sen lisäpöytäkirjan osapuolina olevien valtioiden kesken.

Artiklan 2 - 4 kohtia vastaava säännös, silloin kun Suomi on tietojen pyytäjänä, on rikosoikeusapulain 27 §:ssä. Sen 2 momentin mukaan oikeusavussa on noudatettava, mitä Suomen ja vieraan valtion välillä voimassa olevassa sopimuksessa taikka oikeusapua antaneen valtion

asettamissa ehdoissa on määrätty salassapidosta, vaitiolovelvollisuudesta, tietojen käytön rajoituksista taikka luovutetun aineiston palauttamisesta tai hävittämisestä. Suomi voi siten 3 kohdassa tarkoitettulla tavalla sitovasti hyväksyä asetetun ehdon. Rikosoikeusapulain 27 a §:ssä säännellään tietojen luovuttamista Suomesta toiseen valtioon. Pykälän mukaan vieraan valtion oikeusapupyynnön perusteella saadaan luovuttaa myös salassa pidettäviä tietoja sisältäviä asiakirjoja käytettäväksi todisteena rikosasiassa, jollei tiedon tai asiakirjan luovuttamista ulkomaille tai käyttämistä todisteena ole laissa kielletty tai rajoitettu.

## **2 jakso Erityiset määräykset**

### **1 osasto Väliaikaisia toimenpiteitä koskeva keskinäinen oikeusapu**

#### **Tallennetun datan säilyttämisen nopea varmistaminen (29 artikla)**

Artiklassa on määräykset datan säilyttämismääräystä koskevasta oikeusavusta. Datan säilyttämismääräys on esitykseen sisältyvä uusi pakkokeino, jota voidaan tarvittaessa käyttää esitoimenpiteenä ennen muita dataan kohdistuvia pakkokeinoja. Sen tarkoituksena on estää rikostutkinnallisesti merkityksellisen datan häviäminen tai muuttaminen ennen kuin datan haltuunotto on muiden pakkokeinojen nojalla mahdollista. Datan säilyttämismääräystä on tarkemmin selostettu 16 artiklan ja pakkokeinolain 4 luvun 4 c §:n perusteluissa.

Artiklan 1 kappaleen mukaan osapuoli voi pyytää toista osapuolta antamaan datan säilyttämismääräyksen. Edellytyksenä on, että osapuoli aikoo esittää datan haltuunottoa koskevan oikeusapupyynnön.

Artiklan 2 kappaleessa on yksityiskohtaiset määräykset pyynnössä esitettävistä tiedoista.

Artiklan 3 kappaleen mukaan pyynnön vastaanottaja toteuttaa pyynnön viipymättä eikä kaksoisrangaistavuutta saa vaatia toimenpiteen edellytyksenä.

Artiklan 4 kappaleen mukaan osapuoli, joka edellyttää kaksoisrangaistavuutta datan haltuunottoa koskevien pakkokeinojen käytön edellytyksenä voi tehdä varauman, jonka mukaan se edellyttää kaksoisrangaistavuutta myös datan säilyttämismääräyksen osalta. Varauma ei saa kuitenkaan koskea sopimuksen 2 - 11 artiklassa tarkoitettuja rikoksia.

Artiklan 5 kappaleen mukaan oikeusavusta voi datan säilyttämismääräyksen osalta kieltäytyä vain, jos pyynnön vastaanottaja pitää rikosta poliittisena rikoksena tai jos oikeusavun antaminen vaarantaisi vastaanottajan merkittäviä etuja.

Artiklan 6 kappaleen mukaan osapuoli on velvollinen ilmoittamaan toiselle osapuolelle, jos se katsoo, että datan säilyttämismääräys ei toimi tehokkaasti, vaarantaa rikostutkinnan salassapidon tai aiheuttaa muuta haittaa.

Artiklan 7 kappaleen mukaan datan säilyttämismääräys on pidettävä voimassa vähintään 60 päivää. Jos datan haltuunottoa koskeva pyyntö esitetään tässä ajassa, säilyttämismääräys on pidettävä voimassa siihen saakka kunnes datan haltuunottoa koskeva päätös on tehty.

Artiklaa käsitellään selitysmuistion kohdissa 282 - 289. Selitysmuistion mukaan artiklan tarkoituksena on luoda yhtäältä erittäin nopea ja toisaalta mahdollisimman vähän kohteena olevan

henkilön oikeuksiin kajoava väline sähköisessä muodossa olevan todistusaineiston häviämisen estämiseen. Artikla on tarpeellinen, koska todistusaineiston hävittäminen on helppoa ja perinteinen oikeusapuyhteistyö saattaa kestää suhteellisen kauan. Samoista syistä artiklan 2 kappaleessa edellytetään vain vähimmäistiedot, joiden perusteella oikeusapupyynnö voidaan ratkaista. Kaksoisrangaistavuutta ei saa 3 kohdan mukaan vaatia toimenpiteen edellytyksenä, koska sen tutkiminen on tyypillisesti aikaa vievää. Artiklan 4 kohdan mukaista varaumaa ei saa tehdä 2 - 11 artiklassa tarkoitettujen rikosten osalta, koska edellytys täyttyy käytännössä niiden osalta joka tapauksessa. Muilla kuin artiklan 5 kohdassa mainituilla perusteilla pyynnöstä ei voi kieltäytyä. Artiklan 6 kohta on tarpeellinen, koska datan säilyttämismääräys saattaa vasta sen täytäntöönpanon yhteydessä osoittautua päätarkoituksenmukaiseksi.

Rikosoikeusapulain 23 §:ssä on pakkokeinoja koskeva säännös. Koska datan säilyttämismääräys on uusi pakkokeino, sitä ei erikseen mainita 23 §:ssä. Artiklan 1 kappale edellyttää siten edellä mainitun pykälän muuttamista. Hallituksen esitykseen sisältyy ehdotus, jonka mukaan pykälän 1 momenttia muutetaan siten, että siinä olevaan oikeusapupyynnön perusteella toimeenpantavissa olevien pakkokeinojen luetteloon lisätään tässä esityksessä ehdotettu uusi pakkokeinolain 4 luvun 4 b §:n mukainen datan säilyttämismääräys. Ehdotuksen tultua voimaan voimassa olevat säännökset vastaavat artiklan 1 kappaletta.

Artiklan 3 kappaleen mukaan kaksoisrangaistavuutta ei saa vaatia toimenpiteen edellytyksenä. Rikosoikeusapulain 15 §:n 1 momentin mukaan oikeusapupyynnön tarkoittamia tai edellyttämiä pakkokeinoja ei saa käyttää, jos se ei Suomen lain mukaan olisi sallittua, jos pyynnön perusteena oleva teko olisi tehty Suomessa vastaavissa olosuhteissa. Voimassaoleva oikeus ei tältä osin ole sopusoinnussa artiklan vaatimusten kanssa.

Hallituksen esitykseen sisältyy ehdotus, jonka mukaan rikosoikeusapulain 15 §:ään lisätään uusi 2 momentti, jonka mukaan 1 momentissa sanottu ei koske datan säilyttämismääräystä. Tältä osin on huomattava, että ehdotettu säännös koskee rikosoikeusapulain laajan soveltamisalan vuoksi myös yleissopimuksen ulkopuolisia valtioita. Ehdotuksen tultua voimaan voimassa olevat säännökset vastaavat artiklan 3 kappaletta.

Artiklan 5 kappaletta vastaava säännös on ensinnäkin rikosoikeusapulain ehdottomia kieltäytymisperusteita koskevassa 12 §:ssä. Pykälän 1 momentin mukaan oikeusapua ei anneta, jos oikeusavun antaminen saattaisi loukata Suomen täysivaltaisuutta tai vaarantaa Suomen turvallisuutta taikka muita olennaisia etuja. Oikeusapua ei 2 momentin mukaan myöskään anneta, jos oikeusavun antaminen olisi ristiriidassa ihmisoikeuksia ja perusvapauksia koskevien periaatteiden kanssa taikka jos oikeusavun antaminen muutoin olisi Suomen oikeusjärjestyksen peruseriaatteiden vastaista. Rikosoikeusapulain 13 §:ssä on lisäksi säännökset harkinnanvaraisista kieltäytymisperusteista. Pykälän mukaan oikeusavun antamisesta voidaan kieltäytyä muun ohessa, jos pyynnön perusteena on teko, jota on pidettävä poliittisena rikoksena. Pykälässä on lisäksi muita kieltäytymisperusteita, jotka liittyvät syyteoikeuden vanhentumiseen, vireillä olevaan oikeudenkäyntiin ja vastaaviin seikkoihin.

Artiklan 2, 6 ja 7 kohdat ovat sellaisenaan soveltamiskelpoisia ja suomalaiset viranomaiset voivat näiltä osin noudattaa suoraan sopimuksen määräyksiä.

Muilta osin rikosoikeusapulain muuttaminen ei siten ole artiklan perusteella tarpeellista.

Ehdotuksen mukaan Suomi ei tee 4 kappaleessa tarkoitettua varaumaa, koska järkeviä perusteita säännellä asiaa eri rikostyyppien osalta eri tavalla ei ole. Ratkaisu on sopusoinnussa myös sen

rikosoikeusapulaista ilmenevän periaatteen kanssa, että Suomi pyrkii antamaan oikeusapua mahdollisimman laajasti. Ratkaisu tarkoittaa sitä, että Suomi ulottaa kaksoisrangaistavuutta koskevan poikkeuksen pidemmälle kuin mitä yleissopimus välttämättä edellyttää.

### **Varmistettujen liikennetietojen nopea luovutus (30 artikla)**

Artiklassa on määräykset viestin reittitietojen nopeaa luovutusta koskevasta oikeusavusta. Kyseessä on hallituksen esitykseen sisältyvä ja 29 artiklassa tarkoitettuun datan säilyttämismääräykseen kiinteästi liittyvä uusi toimenpide, jonka tarkoituksena on varmistaa se, että datan säilyttämismääräys voidaan nopeasti kohdistaa oikeisiin tahoihin silloin kun viestin välittämiseen on osallistunut useita eri valtioissa olevia palveluntarjoajia. Artikla koskee ainoastaan viestiin liittyviä liikennetietoja ja niidenkin osalta ainoastaan sellaisia tietoja, jotka ovat välttämättömiä viestin reitin selvittämiseksi. Käytännössä tämä tarkoittaa ainoastaan tietoa siitä, mitkä operaattorit ovat osallistuneet viestin välittämiseen. Reittitietojen luovutusvelvollisuutta on tarkemmin selostettu 17 artiklan ja pakkokeinolain 4 luvun 4 c §:n perusteluissa.

Artiklan 1 kappaleen mukaan osapuoli luovuttaa oma-aloitteisesti palveluntarjoajan ja viestin reitin tunnistamiseksi tarvittavat liikennetiedot datan säilyttämismääräystä pyytäneelle osapuolelle, jos se havaitsee, että pyynnön kohteena olevan viestin siirtoon on osallistunut toisessa valtiossa oleva palveluntarjoaja.

Artiklan 2 kappaleen mukaan oikeusavusta voi reittitietojen luovuttamisen osalta kieltäytyä vain jos pyynnön vastaanottaja pitää rikosta poliittisena rikoksena tai jos oikeusavun antaminen vaarantaisi vastaanottajan merkittäviä etuja.

Artiklaa käsitellään selitysmuistion kohdissa 290 - 291. Selitysmuistion mukaan artiklan tarkoituksena on huolehtia liikennetietoihin kohdistuvan säilyttämismääräyksen käytettävyydestä myös silloin kun viestintä on rajat ylittävää. Luovutettavien tietojen avulla toimenpiteen pyytäjä voi nopeasti tehdä uuden säilyttämismääräystä koskevan oikeusapupyynnön myös toiselle valtiolle, jonka kautta viesti on kulkenut.

Artiklan 1 kappaleen edellyttämää muutosta rikosoikeusapulain 23 §:ään on selostettu 29 artiklan perusteluissa. Siinä selostettu muutos kattaa myös tämän artiklan vaatimukset.

Artiklan 2 kappaletta vastaavaa säännös on rikosoikeusapulain 12 ja 13 pykälässä. Myös näiden pykäläen sisältöä on selostettu 29 artiklan perusteluissa.

Muilta osin artikla on sellaisenaan soveltamiskelpoinen ja suomalaiset viranomaiset voivat noudattaa tältä osin suoraan sopimuksen määräyksiä. Rikosoikeusapulain muuttaminen edellä 30 artiklan yhteydessä selostettujen muutosten lisäksi ei ole tarpeellista.

### **2 osasto Tutkintaan liittyviä toimivaltuuksia koskeva keskinäinen oikeusapu**

#### **Keskinäinen oikeusapu pääsyn hankkimisessa tallennettuun dataan (31 artikla)**

Artiklassa on määräykset datan etsintää ja takavarikkoa koskevasta oikeusavusta.

Artiklan 1 kappaleen mukaan osapuoli voi pyytää toiselta osapuolelta tämän alueella olevan datan etsintää, takavarikkoa tai muuta vastaavaa pakkokeinoa. Määräys koskee myös säilyttämismääräyksen kohteena olevaa dataa.

Artiklan 2 kappaleen mukaan pyynnön vastaanottaja vastaa pyyntöön soveltamalla 23 artiklassa tarkoitettuja kansainvälisiä asiakirjoja, järjestelyjä ja lainsäädäntöä, sekä muiden tämän luvun asiaan liittyvien määräysten mukaisesti.

Artiklan 3 kappaleen mukaan pyyntöön vastataan nopeutettua menettelyä noudattaen, jos datan häviäminen tai muuttaminen on erityisen todennäköistä. Myös muissa osapuolta sitovissa sopimuksissa olevia määräyksiä on tämän lisäksi noudatettava.

Artiklaa käsitellään selitysmuistion kohdassa 292. Selitysmuistion mukaan viranomaisella on 19 artiklan mukainen oikeus datan etsintään ja takavarikkoon vain oman valtion alueella. Nyt käsillä olevan artiklan tarkoituksena on saattaa samat toimenpiteet myös kansainvälisen oikeusavun piiriin.

Artiklan 1 kappaleessa tarkoitettut pakkokeinot ovat sellaisia, joiden osalta oikeusapua voidaan rikosoikeusapulain 23 §:n mukaan Suomessa säännönmukaisesti antaa. Datan takavarikon osalta hallituksen esitykseen sisältyy ehdotus, jonka mukaan pakkokeinolain 4 luvun oikeusapuna annettavaa takavarikkoa koskevaa 15 a §:ää muutetaan siten, että siinä olevaan takavarikoitavissa olevien objektien luetteloon lisätään selvyyden vuoksi myös data.

Artiklan 2 ja 3 kappaleet ovat sellaisenaan soveltamiskelpoisia ja suomalaiset viranomaiset voivat noudattaa näiltä osin lain säännösten lisäksi suoraan sopimuksen määräyksiä.

Rikosoikeusapulain muuttaminen artiklan perusteella ei ole tarpeellista.

### **Pääsyn hankkiminen tallennettuun dataan valtion rajojen yli suostumuksesta tai silloin kun data on julkista (32 artikla)**

Artiklan a kohdan mukaan osapuoli voi ilman toisen osapuolen lupaa hankkia datan muodossa olevia tietoja silloin kun ne ovat julkisia.

Artiklan b kohdan mukaan osapuoli voi hankkia datan muodossa olevia tietoja asianomaisen henkilön suostumuksella vaikka tiedot eivät olisikaan sen alueella.

Artiklaa käsitellään selitysmuistion kohdissa 293 ja 294. Selitysmuistion mukaan sopimuksen valmistelussa oli tarkoitus säätää huomattavasti pidemmälle menevistä oikeuksista hankkia datan muodossa olevia tietoja toisen valtion alueella. Tämä osoittautui kuitenkin mahdottomaksi ja nyt käsillä olevassa artiklassa on sääntely, jonka kaikki osapuolet kykenivät vaikeuksista hyväksymään.

Artiklan mukaiset oikeudet ovat Suomen näkökulmasta itsestään selviä eikä niiden soveltamiseen liity siten mitään ongelmia.

### **Keskinäinen oikeusapu tiedon hankkimisessa liikennetiedoista reaaliajassa (33 artikla)**

Artiklassa on määräykset televalvontaa vastaavaa pakkokeinoa koskevasta oikeusavusta. Kyseessä olevaa pakkokeinoa on tarkemmin selostettu 20 artiklan perusteluissa.



Artiklan mukaan osapuolet antavat televalvonnassa oikeusapua ainakin sellaisten rikosten tutkinnassa, joiden osalta televalvonta on mahdollista kansallisissa tapauksissa. Muilta osin sovellettavat ehdot ja menettelyt määräytyvät kansallisen lainsäädännön mukaan.

Artiklaa käsitellään selitysmuistion kohdissa 295 ja 296. Selitysmuistion mukaan liikennetietojen usein lyhyiden säilytysaikojen vuoksi on tärkeää, että liikennetietoja voidaan hankkia reaaliaikaisesti myös silloin kun viestintä on rajat ylittävää. Artiklan 2 kappaletta on tulkittava siten, että siinä suositellaan osapuolille mahdollisimman laajan oikeusavun hyväksymistä tämän artiklan osalta.

Artiklassa tarkoitettu pakkokeino on sellainen, jonka nojalla oikeusapua voidaan Suomessa rikosoikeusapulain 23 §:n mukaan säännönmukaisesti antaa samoin edellytyksin kuin sitä voidaan käyttää kansallisestikin. Voimassaolevaa oikeutta on tältä osin selostettu 20 artiklan perusteluissa. Suomi tekee ehdotuksen mukaan varauman, jonka mukaan se soveltaa kansallisesti mainittua pakkokeinoa ainoastaan tiettyihin nimettyihin rikoksiin. Myös varaumaa on selostettu tarkemmin 20 artiklan perusteluissa.

### **Keskinäinen oikeusapu tiedon hankkimisessa viestin sisällöstä (34 artikla)**

Artiklassa on määräykset telekuuntelua vastaavaa pakkokeinoa koskevasta oikeusavusta. Kyseessä olevaa pakkokeinoa on tarkemmin selostettu 21 artiklan perusteluissa.

Artiklan mukaan osapuolet antavat toisilleen keskinäistä oikeusapua reaaliaikaiseksi tiedon hankkimiseksi tietojärjestelmän välityksellä siirrettyjen yksilöityjen viestien sisällöstä siinä määrin kuin se on niiden soveltamien sopimusten ja kansallisen lainsäädännön mukaan sallittua.

Artiklaa käsitellään selitysmuistion kohdassa 297. Selitysmuistion mukaan oikeusavun antaminen tämän pakkokeinon osalta on jätetty toimenpiteen luonteen vuoksi osapuolten kansallisessa lainsäädännössä ratkaistavaksi.

Tämän artiklan ja edellä selostetun 33 artiklan osalta on huomattava, että eurooppalaisessa oikeusapusopimuksessa ei ole määräyksiä televalvonnasta eikä telekuuntelusta. Euroopan Unionin oikeusapusopimuksessa sen sijaan on. Euroopan Unionin oikeusapusopimus on yleisperusteluissa kerrotulla tavalla tarkoitus saattaa Suomessa voimaan niin pian kuin se on mahdollista.

Artiklassa tarkoitettu pakkokeino on kuitenkin sellainen, jonka osalta oikeusapua voidaan Suomessa suoraan rikosoikeusapulain 23 §:n mukaan säännönmukaisesti antaa samoin edellytyksin kuin sitä voidaan käyttää kansallisestikin.

### **3 osasto 24-tuntinen jokapäiväinen verkosto**

#### **24-tuntinen jokapäiväinen verkosto (35 artikla)**

Artiklassa on määräykset erityisen yhteyspisteen nimeämisestä ja tehtävistä.

Artiklan 1 kappaleen mukaan osapuoli nimeää yhteyspisteen, jonka tehtävänä on avustaa ja mahdollisuuksien mukaan toimia sopimukseen perustuvissa oikeusapuasioissa. Toimipisteen tulee

olla käytettävissä joka päivä vuorokauden ympäri. Toimipisteen tehtäviin kuuluvat tekninen apu, datan säilyttämisen varmistaminen, todisteiden kerääminen, oikeudellisten tietojen antaminen ja epäiltyjen paikantaminen.

Artiklan 2 kappaleen mukaan yhteyspisteellä tulee olla valmiudet nopeutettuun viestintään toisen osapuolen yhteyspisteen kanssa ja tarvittaessa oman maan oikeusapuviranomaisten kanssa.

Artiklan 3 kappaleen mukaan yhteyspisteen henkilökunnalla tulee olla riittävä koulutus ja toimintavalmius.

Artiklaa käsitellään selitysmuistion kohdissa 298 - 302. Selitysmuistion mukaan tietoverkkorikollisuuden tutkinta saattaa edellyttää erittäin nopeaa kansainvälistä yhteistyötä. Artiklassa tarkoitettulla yhteyspisteellä on siten ratkaiseva merkitys yleissopimuksen mukaisten tavoitteiden toteutumisen kannalta. Yhteyspisteen tehtävänä on joko huolehtia tai itse toteuttaa artiklassa säädetyt tehtävät. Se mihin organisaatioon yhteyspiste sijoitetaan on jätetty osapuolten harkintaan. Sijoittamisesta päätettäessä on otettava huomioon se, että yhteyspisteellä on hyvin eriluonteisia tehtäviä. Artiklan 3 kappale tarkoittaa käytännössä ainakin tehokkaita viestintävälineitä ja riittävän kielitaitoista henkilökuntaa.

Suomi nimeää artiklassa tarkoitetuksi yhteyspisteeksi keskusrikospoliisin.

### **Loppumääräykset (IV luku 36 - 48 artiklat)**

Yleissopimuksen 4 luvussa on määräykset sopimuksen allekirjoittamisesta ja voimaantulosta (36 artikla), sopimukseen liittymisestä (37 artikla), alueellisesta soveltamisesta (38 artikla), sopimuksen vaikutuksista (39 artikla), selityksistä (40 artikla), liittovaltioita koskevasta varaumamahdollisuudesta (41 artikla), muista varaumista (42 artikla), varaumien voimassaolosta ja peruuttamisesta (43 artikla), sopimuksen muuttamisesta (44 artikla), riitojen ratkaisusta (45 artikla) sopimuspuolten välisistä neuvotteluista (46 artikla), sopimuksen irtisanomisesta (47 artikla) ja ilmoituksista (48 artikla). Artikloja käsitellään selitysmuistion kohdissa 303 - 330. Loppumääräykset ovat pääosin tavanomaisia Euroopan neuvoston yleissopimukseen liitettäviä määräyksiä.

Yleissopimus tulee 36 artiklan mukaan voimaan seuraavan kuukauden ensimmäisenä päivänä, kun on kulunut kolme kuukautta siitä päivästä, jona viisi valtiota, mukaan lukien kolme Euroopan neuvoston jäsenvaltiota, on ilmaissut suostumuksensa tulla yleissopimuksen sitomaksi 1 ja 2 kappaleen määräysten mukaisesti. Sellaisen allekirjoittajavaltion osalta, joka myöhemmin ilmaisee suostumuksensa tulla yleissopimuksen sitomaksi, se tulee voimaan seuraavan kuukauden ensimmäisenä päivänä, kun on kulunut kolme kuukautta siitä päivästä, jona se on ilmaissut suostumuksensa tulla yleissopimuksen sitomaksi.

Yleissopimuksen 40 artiklassa on määräykset selityksistä. Artiklan mukaan selitys voi koskea osapuolen asettamia lisäehtoja 2 ja 3 artiklan, 6 artiklan 1 kappaleen b kohdan, 9 artiklan 3 kappaleen ja 27 artiklan 9 kappaleen e kohdan määräysten mukaisesti. Ehdotuksen mukaan Suomi antaa 2 artiklan mukaisen selityksen. Suomen antaman selityksen ja muiden mahdollisten selitysten sisältöä on tarkemmin selostettu kyseisten artiklojen perusteluissa.

Yleissopimuksen 42 artiklassa on tyhjentävä luettelo sallituista varaumista. Artiklan mukaan sallittuja varaumia ovat 4 artiklan 2 kappaleen, 6 artiklan 3 kappaleen, 9 artiklan 4 kappaleen, 10

artiklan 3 kappaleen, 11 artiklan 3 kappaleen, 14 artiklan 3 kappaleen, 22 artiklan 2 kappaleen, 29 artiklan 4 kappaleen ja 41 artiklan 1 kappaleen mukaiset varaumat.

Ehdotuksen mukaan Suomi tekee 11 artiklan 3 kappaleen ja 14 artiklan 3 kappaleen a ja b kohdan mukaiset varaumat. Suomen tekemien varaumien ja muiden mahdollisten varaumien sisältöä on tarkemmin selostettu kyseisten artiklojen perusteluissa.

Yleissopimuksen 45 artiklassa on määräykset sopimuksesta aiheutuvien riitojen ratkaisusta.

Artiklan mukaan pyrkivät ratkaisemaan mahdolliset riidat neuvotteluin tai muulla valitsemallaan rauhanomaisella keinolla. Artiklan määräys on suositusluonteinen eikä velvoita Suomea alistumaan mihinkään erityiseen riidanratkaisumenettelyyn.

## **2. Lakiehdotusten perustelut**

### **2.1 Laki Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta**

*1 §. Yleissopimuksen voimaansaattaminen.* Pykälä sisältää tavanomaisen voimaantulosäännöksen, jonka mukaan yleissopimuksen lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

*2 §. Asetuksenantovaltuus.* Pykälä sisältää säännöksen, jonka mukaan tarkempia säännöksiä lain täytäntöönpanosta voidaan antaa valtioneuvoston asetuksella.

*3 §. Voimaantulo.* Pykälä sisältää säännöksen, jonka mukaan lain voimaantulosta säädetään tasavallan presidentin asetuksella. Laki on tarkoitettu tulemaan voimaan samanaikaisesti kuin yleissopimus.

## **2.2 Rikoslaki**

### **34 luku Yleisvaarallisista rikoksista**

*9 a § Vaaran aiheuttaminen tietojenkäsittelylle.* Lukuun ehdotetaan lisättäväksi uudet tietoverkkorikosvälineitä koskevat rikossäännökset siten, että 9 a §:ssä säädetään välineiden valmistamisesta ja levittämisestä sekä uudessa 9 b §:ssä välineiden hallussapidosta. Nykyinen 9 a § kattaa tietoverkkorikosvälineistä ainoastaan tietokonevirusten ja muiden vastaavien haittaohjelmien valmistuksen ja levittämisen. Se ei sen sijaan kata tietomurto-ohjelmia eikä fyysisiä laitteita eikä myöskään ohjelmien tai laitteiden hallussapitoa. Ehdotetun muutoksen seurauksena 9 a § on kirjoitettava kokonaan uudelleen. Pykälän otsikkoa ei tarvitse sen sijaan muuttaa, koska se muutoksen jälkeenkin kuvaa hyvin sääntelyn suojelukohdetta ja tarkoitusta.

Ehdotetun pykälän 1 kohdan a) kohdassa säädetään rangaistavaksi haittaohjelmien ja muiden vastaavien tietoverkkorikosvälineiden vahingoittamistarkoituksessa tapahtuva maahantuonti, valmistaminen, myyminen, levittäminen ja saataville asettaminen.

Pykälän yksityiskohtainen tekoapaluettelo vastaa pääosin nykyisessä 9 a §:ssä olevaa luetteloa ja sen tarkoituksena on kattaa valmistamisen ohella kaikki sellaiset aktiiviset toimenpiteet, joiden seurauksena tietokonevirus, tekninen laite tai tietomurto-ohjelma voi siirtyä muiden henkilöiden käytettäväksi. Maahantuonnin mainitseminen itsenäisenä tekotapana on tarpeellista erityisesti

laitteiden osalta. Valmistamisella tarkoitetaan esimerkiksi uuden ohjelman kirjoittamista tai olemassa olevan ohjelman muuttamista pykälässä tarkoitettuna kaltaiseksi. Myymisellä tarkoitetaan välineen vastikkeellista luovutusta ja saataville asettamisella välineen laittamista esimerkiksi internet-sivulle halukkaiden vapaasti kopioitavaksi. Levittäminen tarkoittaa kahta erilaista tekotapaa. Ensinnäkin se tarkoittaa välineen vastikkeetonta luovuttamista esimerkiksi sähköpostin välityksellä toiselle henkilölle tai henkilöille. Tämän lisäksi se tarkoittaa tietokonevirusten osalta myös viruksen käyttämistä levittämällä sitä uhrien koneisiin. Sääntely saattaa tältä osin johtaa osittaiseen päällekkäisyyteen esimerkiksi vahingonteon yrityksen kanssa, jolloin nyt käsillä oleva toissijaiseksi tarkoitettu säännös ei väisty. Samaa tietoverkkorikosvälinettä koskeva tekokokonaisuus saattaa myös täyttää useamman kohdan ehdotetun pykälän tunnusmerkistöstä. Tekijä voi esimerkiksi syöllistyä saman välineen valmistamiseen ja saataville asettamiseen taikka suuren väline-erän maahantuontiin ja niiden yksittäin tapahtuvaan myymiseen. Kyse on silloin kuitenkin vain yhdestä rikoksesta.

Itse pykälässä ei käytetä yläkäsitettä tietoverkkorikosväline. Levittämisen ja muun toimenpiteen kohde on pykälän a) kohdassa yksilöity sen teknisen rakenteen ja objektiivisen käyttötarkoituksen perusteella. Säännöksen mukaan kohteena voi olla laite tai tietokoneohjelma tai ohjelmakäskyjen sarja, joka on suunniteltu tai muunnettu ensisijaisesti vaarantamaan tai vahingoittamaan tietojenkäsittelyä taikka tieto- tai viestintäjärjestelmän toimintaa taikka tietojärjestelmän suojausten murtamiseen.

Säännöksen soveltamisala on tältä osin laaja ja sen tarkoituksena on kattaa yhtäältä tietomurtoihin ja puhtaaseen ilkeilyyn vahingontekoon tarkoitettuja välineitä sekä toisaalta fyysiset laitteet, tietokoneohjelmat ja yksittäiset ohjelmakoodin palaset. Lähtökohtaisesti laajaa soveltamisalaa rajoittaa kuitenkin merkittävästi teolta edellytettävä subjektiivinen vahingoittamis- tai haittaamistarkoitus sekä levittämisen tai muun toimenpiteen kohteena olevalta välineeltä edellytettävä moitittava käyttötarkoitus. Molempien edellytysten pitää täytyä samanaikaisesti, jotta teko olisi säännöksen mukaan rangaistava. Seuraavassa tarkastellaan ensin välineen käyttötarkoitukseen liittyvää edellytystä.

Jos väline on sellainen, että sitä voidaan käyttää sekä säännöksessä tarkoitettuihin moitittaviin tarkoituksiin että muihin hyväksyttäviin tarkoituksiin, välineen ensisijainen käyttötarkoitus ratkaisee sen, onko välinettä pidettävä säännöksessä tarkoitettuna tietoverkkorikosvälineenä vai ei. Välineen ensisijainen käyttötarkoitus on ratkaistava objektiivisella ja välinekohtaisella harkinnalla. Objektiivinen harkinta tarkoittaa tässä sitä, että esimerkiksi sillä, miten välineen käyttäjä itse on subjektiivisesti mieltänyt välineen luonteen, ei ole ratkaisevaa merkitystä. Välinekohtainen harkinta taas tarkoittaa sitä, että tietty väline joko on pykälässä tarkoitettu tietoverkkorikosväline tai se ei ole sellainen. Ratkaisu ei voi eri tilanteissa olla erilainen, jos väline on täysin sama. Säännöstä on tältä osin tulkittava varovaisesti. Ensisijainen käyttötarkoitus on selvästi lähempänä yksinomaista kuin pääasiallista käyttötarkoitusta. Joidenkin välineiden osalta ratkaisu saattaa olla vaikea. Epäselvissä tapauksissa asia on ratkaistava syytetyn eduksi. Jos välineen vaihtoehtoinen käyttötarkoitus on hyväksyttävä, tämän pykälän mukainen tunnusmerkistö ei täyty, vaikka kyseistä välinettä levitettäisiinkin sinänsä moitittavien tarkoituksien.

Sääntely vastaa tältä osin yleissopimuksen 6 artiklan 1 kappaleen a) kohdan 1) alakohtaa, jonka mukaan artiklan soveltamisala määräytyy välineen ensisijaisen käyttötarkoituksen perusteella. Sopimuksen sanamuodossa ei tosin käytetä käsitettä objektiivinen käyttötarkoitus. Selitysmuistion 73 kohdan mukaan ensisijaisella käyttötarkoituksella tarkoitetaan kuitenkin nimenomaan välineen objektiivista käyttötarkoitusta. Selitysmuistiossa todetaan myös, että kaksikäyttöiset välineet rajautuvat tämän vuoksi pääsääntöisesti soveltamisalan ulkopuolelle.

Erityisesti tietomurtojen tekemisessä käytettävät välineet ovat tyypillisesti edellä kuvatulla tavalla kaksikäyttöisiä. Toisaalta tietokonevirukset ja muut vastaavat haittaohjelmat ovat varsin selkeästi tarkoitettuja käytettäväksi ainoastaan moitittaviin käyttötarkoituksiin. Seuraavassa tarkastellaan välineen käyttötarkoitukseen liittyvää edellytystä eräiden käytännön esimerkkien avulla.

Takaoviohjelmiston avulla uhrin tietokone voidaan ottaa ulkopuolisen hyökkääjän käyttöön. Ohjelmisto muodostuu kahdesta osasta. Palvelinosa eli varsinainen takaoviohjelma asennetaan salaa uhrin koneelle ja asiakasosa, jossa on ohjelman käyttöliittymä, sijaitsee hyökkääjän koneella. Ohjelmiston avulla hyökkääjä voi käyttää uhrin konetta lähes rajoituksetta ilman normaalia käyttöoikeustarkistusta. Tällaista ohjelmistoa voidaan kuitenkin käyttää myös hyväksyttävään käyttötarkoitukseen. Jos asentaminen ei tapahdu salaa, ohjelmaa voidaan käyttää tietokoneen etäkäyttöohjelmiana. Ohjelman erityispiirteiden avulla on ratkaistava onko ohjelmistoa tai sen palvelinosaa pidettävä pykälässä tarkoitettuna tietoverkkorikosvälineenä. Lähtökohtana voidaan takaoviohjelmiston osalta pitää sitä, että kyseessä ei ole pykälässä tarkoitettu tietoverkkorikosväline.

Vakoiluohjelman avulla hyökkääjä voi seurata uhrin koneen käyttöä. Jos uhrin kone on lähiverkossa, ohjelmalla on mahdollista seurata myös kaikkea lähiverkon salaamatonta liikennettä. Vakoiluohjelma asennetaan salaa uhrin koneelle. Sen jälkeen se toimii käyttäjän huomaamatta ja pitää kirjaa kaikesta mitä käyttäjä tietokoneella tekee. Ohjelma tallentaa keräämänsä tiedot, jonka jälkeen ne joko lähetetään hyökkääjälle tai hyökkääjä käy hakemassa tallenteen uhrin koneelta. Jos ohjelma asennetaan uhrin koneeseen salaa, käyttötarkoitus on selvästi moitittava. Jos vakoiluohjelmaa käytetään avoimesti, esimerkiksi yrityksen työntekijöiden valvontaan näiden suostumuksella taikka verkkoliikenteen teknisen toimintakyvyn seuraamiseen, käyttötarkoitus on hyväksyttävä. Ohjelman erityispiirteiden avulla on ratkaistava, onko ohjelmaa pidettävä pykälässä tarkoitettuna tietoverkkorikosvälineenä. Lähtökohtana voidaan vakoiluohjelman osalta pitää sitä, että kyseessä ei ole pykälässä tarkoitettu tietoverkkorikosväline.

Sanakirjahyökkäyksellä tarkoitetaan murto menetelmää, jossa käyttäjän salasana pyritään arvaamaan laajan sanalistan avulla kokeilemalla. Sanakirjahyökkäyksessä käytettävää salasanan arvausohjelmaa voidaan käyttää rikollisen tietomurron lisäksi myös järjestelmän suojauksen testaamiseen ja järjestelmän oikeutettuun murtamiseen. Tämänkin tyyppinen ohjelma on selvästi kaksikäyttöinen. Se, onko ohjelma pykälässä tarkoitettu tietoverkkorikosväline, on ratkaistava käyttötarkoituksen ensisijaisuuden perusteella. Lähtökohtana voidaan tässä pitää sitä, että se on tietoverkkorikosväline, koska vaihtoehtoiset käyttötarkoituksetkin liittyvät nimenomaan murtautumiseen. Ainoastaan suostumukseen perustuva oikeuttamisperuste tekee niistä hyväksyttäviä. Asia on kuitenkin käytännössä ratkaistava tapauskohtaisesti kunkin ohjelman erityispiirteet huomioon ottaen. Salasan arvausohjelmaa muistuttaa läheisesti ohjelma, joka käy kokeilemalla läpi kaikki mahdolliset merkkijhdistelmät.

Niin sanottu porttiskannaus on menetelmä, jossa tietomurtoa valmistellaan etsimällä internetverkkoon kytketyissä koneissa olevien palvelinohjelmien tietoturva-aukkoja. Hyökkääjä ei välttämättä pyri tietyn uhrin koneelle vaan mihin hyvänsä löytämäänsä suojaamattomaan koneeseen. Porttiskannauksessa käytettävää ohjelmaa voidaan kuitenkin käyttää myös hyväksyttäviin tarkoituksiin, kuten esimerkiksi oman palvelinkoneen porttiskannaukseen. Ohjelman erityispiirteiden avulla on ratkaistava onko ohjelmaa pidettävä pykälässä tarkoitettuna tietoverkkorikosvälineenä.

Tietomurtojen tekemiseen voidaan käyttää myös laitetta. Näppäintallennin on laite, joka tallentaa

käyttäjän näppäimen painallukset siten, että ne voidaan jälkikäteen palauttaa laitteen muistista. Näppäintallennin voi olla erillinen huomaamaton pieni laite, joka kytketään näppäimistön ja keskusyksikön väliin tai se voi olla sisäänrakennettuna erityisnäppäimistöön. Laite tai erityisnäppäimistö asennetaan uhrin koneeseen salaa ja tallennetut tiedot käydään keräämässä myöhemmin. Näppäintallennin voi olla myös ohjelma. Olennainen ero laitteen ja ohjelman välillä on se, että laitteen asentaminen edellyttää fyysistä pääsyä tietokonelaitteen luokse, mutta se ei edellytä tietojärjestelmän suojauksen murtamista. Jos laitetta käytetään salaa, käyttötarkoitus on selvästi moitittava. Jos laitetta käytetään avoimesti työntekijöiden valvontaan tai esimerkiksi varmuuskopiointivälineenä, käyttötarkoitus on hyväksyttävä. Samaten käyttötarkoitus on hyväksyttävä, jos laitetta käytetään oman tietokoneen luvottoman käytön paljastamiseen. Laitteita markkinoidaan nimenomaan niiden hyväksyttävien käyttötarkoitusten perusteella. Laitteen erityispiirteiden avulla on ratkaistava, onko ohjelmaa pidettävä pykälässä tarkoitettuna tietoverkkorikosvälineenä. Lähtökohtana voidaan näppäimistöallentimien osalta pitää sitä, että kyseessä ei ole pykälässä tarkoitettu tietoverkkorikosväline.

Myös vahingoittamistarkoituksessa käytettävät välineet voivat olla kaksikäyttöisiä.

Palvelunestohyökkäys tarkoittaa kohteena olevan tietojärjestelmän kuten sähköpostipalvelimen toiminnan tarkoituksellista estämistä tai hidastamista. Palvelunestohyökkäystä voidaan poikkeuksellisesti käyttää myös tietomurron esivaiheena, lamauttamaan kohteena olevan järjestelmän suojaus. Hyökkäystekniikoita on lukuisia. Yhteistä niille on järjestelmän tahallinen ylikuormitus tai kohteessa olevan teknisen puutteen eli haavoittuvuuden järjestelmällinen hyväksikäyttö. Palvelunestohyökkäykseen voidaan käyttää sähköpostia automaattisesti lähettävää ohjelmaa. Ohjelman avulla voidaan lähettää esimerkiksi miljoona keksityillä lähettäjätiedoilla varustettua viestiä samalle palvelimelle. Jos palvelinta ei ole suojattu tällaista hyökkäystä vastaan sen toiminta saattaa häiriintyä vakavasti. Mainittua ohjelmaa voidaan kuitenkin käyttää täysin hyväksyttäviin käyttötarkoituksiin kuten sähköpostin joukkolähetykseen tarkoituksin saada viesti perille usealle vastaanottajalle. Ohjelman erityispiirteiden avulla on ratkaistava, onko ohjelmaa pidettävä pykälässä tarkoitettuna tietoverkkorikosvälineenä. Lähtökohtana voidaan mainitun ohjelman osalta pitää sitä, että kyseessä ei ole pykälässä tarkoitettu tietoverkkorikosväline.

Yleensä vahingoittamistarkoituksessa käytettävät välineet eivät ole kaksikäyttöisiä.

Tietokoneviruksella tarkoitetaan yleiskielessä sellaista ohjelmaa, joka leviää käyttäjän huomaamatta koneelta toiselle aiheuttaen samalla vahinkoa. Viruksen toiminta- ja leviämistapa sekä sen aiheuttama vahinko voivat olla erilaisia. Erilaisista viruksista käytetään alan kirjoituksissa eri nimikkeitä kuten makrovirus, sähköpostivirus ja mato. Käsitteistö ei ole vakiintunutta eikä sillä ole käsiteltävänä olevan säännöksen kannalta merkitystä. Ehdotetun säännöksen tarkoituksena on kattaa kaikki tietokonevirukset niiden toimintatavasta riippumatta. Säännöksen sanamuodon mukaan levittämisteon kohteen on oltava suunniteltu vaarantamaan tai aiheuttamaan vahinkoa tietojärjestelmän toiminnalle. Myös tietojen käsittely ja viestintäjärjestelmä mainitaan säännöksessä selvyuden vuoksi mahdollisen vahingon kohteena. Säännöksessä edellytetty vahinko tai sen vaara voi syntyä viruksen toimintatavasta riippuen eri tavoilla. Virus voi sisältää niin sanotun vahinkorutiinin, jolloin se esimerkiksi tietyssä päivämääränä ryhtyy tuhoamaan tiedostoja. Se voi muulla tavalla aiheuttaa virheitä, vallata tietojärjestelmän voimavaroja omaan käyttöönsä tai hidastaa tietojärjestelmän toimintaa. Voimakkaasti leviävä virus aiheuttaa vahinkoa pelkällä olemassaolollaan. Viruksen leviämistapa ja tekninen rakenne voi säännöksen mukaan olla minkäläinen hyvänsä. Se voi olla levykkeiden välityksellä leviävä kokonainen ohjelma tai sähköpostissa leviävä liitetiedoston sisällä oleva ohjelmakäskeyjen sarja. Viruksessa voi myös olla tietomurtovälineelle tyypillisiä ominaisuuksia. Se saattaa esimerkiksi lähettää automaattisesti tietoja

liikkeellelaskijan määrittämään osoitteeseen.

Tietokonevirusten osalta sääntely vastaa nykyisessä 9 a §:ssä olevaa sääntelyä. Nykyistä pykälää on selostettu seikkaperäisesti myös sitä koskevassa hallituksen esityksessä (HE 4/1999).

Tietoverkkorikosohjelma voidaan piilottaa hyötyohjelman sisään. Tällaista hyöty- ja haittaohjelman muodostamaa kokonaisuutta kutsutaan troijalaiseksi. Troijalaisen tarkoituksena on hyötyohjelman avulla houkutella uhri itse asentamaan siihen piilotettu haittaohjelma koneelleen. Edellä kuvatulla tavalla tietyn tyyppiset tietomurtojen tekemiseen käytetyt ohjelmat eivät yleensä käytännössä niiden kaksikäyttöisyyden vuoksi täytä tietoverkkorikoslain tunnusmerkkejä. Tilanne muuttuu kuitenkin ratkaisevasti, jos murtoväline on piilotettuna troijalaiseen. Silloin ohjelman ensisijainen käyttötarkoitus on pääteltävissä suoraan ohjelman rakenteesta. Jos esimerkiksi takaovi- tai vakoiluohjelma on troijalaisessa muodossa, ohjelmalle on vaikea löytää enää mitään mielekäästä hyväksyttävää käyttötarkoitusta. Troijalaisenkin osalta asia on kuitenkin ratkaistava aina tapauskohtaisesti kokonaisharkinnalla.

Esimerkkinä ongelmallisesta harkintatilanteesta voidaan mainita troijalaisessa muodossa oleva niin sanottu profiointiohjelma. Profiointiohjelman tarkoituksena on kerätä tietoa ohjelman käyttäjästä tämän suostumuksella. Kerättävät tiedot voivat koskea esimerkiksi internetsivuja, joilla käyttäjä säännöllisesti vierailee. Vastineeksi tiedoista käyttäjä saa jonkun hyötyohjelman käyttöönsä ilmaiseksi. Profiointiohjelman ja vakoiluohjelman ero on ainoastaan siinä, että profiointiohjelma pyytää käyttäjän suostumuksen ennen kuin se antaa asentaa itsensä käyttäjän koneelle. Jos käyttäjä ei suostu asennukseen, myöskään palkinnoksi tarkoitettua hyötyohjelmaa ei asenneta. Jos käyttäjä suostuu asennukseen erehdyksessä toiminta muistuttaa läheisesti vakoilua. Jos erehdys johtuu osin tai kokonaan tietoisesta harhaanjohtamisesta ero vakoiluun on käytännössä olematon.

Ehdotetun pykälän 2 kohdassa säädetään rangaistavaksi pykälän 1 kohdassa tarkoitettun tietokoneohjelman tai ohjelmakäskeyjen sarjan valmistusohjeen vahingoittamistarkoituksessa tapahtuva levittäminen ja saataville asettaminen. Säännös ei siten koske fyysisen laitteen valmistusohjetta.

Ohjeella tarkoitetaan pykälässä sellaista ohjetta, joka on niin yksityiskohtainen, että vähänkin tietojenkäsittelyyn perehtynyt henkilö pystyy sen perusteella valmistamaan esimerkiksi tietokoneviruksen tai muun haittaohjelman. Tällaisen ohjeen levittäminen on ainakin virusten osalta vaarallisuudeltaan melkein rinnastettavissa valmiin viruksen levittämiseen, joten teon on oltava samanlaisen rangaistusuhan alainen. Johdonmukaisuuden vuoksi säännös koskee myös muiden ohjelmien kuin virusten valmistusohjeita. Koska ohje ei voi levitä itsestään samalla tavoin kuin valmis ohjelma, ei pelkkä ohjeen valmistaminen vielä aiheuta sellaista vaaraa, että myös valmistaminen olisi syytä säätää rangaistavaksi. Kun viruksen levittäminen on mahdollista vain tietotekniikkaa hyväksi käyttäen, ohjetta voidaan levittää myös kirjallisessa muodossa.

Ehdotetun pykälän 1 kohdan b) kohdassa säädetään rangaistavaksi tietojärjestelmän salasanan tai käyttäjätunnuksen taikka muun vastaavan tiedon maahantuonti, valmistaminen, myyminen, levittäminen ja saataville asettaminen. Tekotapaluettelo on pykälän rakenteesta johtuen yhteinen a) kohdan kanssa. Tämän vuoksi pykälän sanamuoto kattaa myös salasanan valmistamisen, joka ei kuitenkaan käytännössä liene mahdollista.

Käyttäjätunnuksella tarkoitetaan pykälässä sellaista tunnusta, jonka perusteella tietojärjestelmä yksilöi käyttäjän. Salasanalla tarkoitetaan sellaista tunnusta, jonka perusteella tietojärjestelmä todentaa käyttäjän. Käyttäjä kertoo järjestelmälle käyttäjätunnuksella kuka on ja todistaa

henkilöllisyytensä osoittamalla tuntevansa salasanan. Mainittu menetelmä on sen yksinkertaisuuden ja edullisen hinnan vuoksi yleinen tapa suojata tietojärjestelmä luvattomalta käytöltä. Jos sivullinen saa suojauksessa käytetyt tunnukset tietoonsa, suojaus menettää merkityksensä. Ehdotetun säännöksen tarkoituksena on ehkäistä tunnusten luvattonta käyttöä säätämällä niiden levittäminen ja saataville asettaminen rangaistavaksi teoksi. Pelkkä tunnusten hankkiminen ei siten vielä ole tämän pykälän nojalla rangaistavaa.

Salasana koostuu yleensä kirjaimista, numeroista tai erikoismerkeistä. Pykälässä tarkoitettu tunnus voi olla kuitenkin myös salasanaa ja käyttäjätunnusta vastaava muu tieto. Säännöksen soveltamisala on siten riippumaton tunnuksen teknisestä rakenteesta tai tiedon laadusta ja esittämistavasta. Oleellista on vain tiedon salasanaa vastaava käyttötarkoitus. Tietoa on pidettävä pykälässä tarkoitettuna tietona vain, jos sen käyttötarkoituksena on henkilön todentaminen tietojärjestelmään pääsyn edellytyksenä.

Tietojärjestelmällä tarkoitetaan pykälässä kaikkia sellaisia järjestelmiä, joissa käsitellään datan muodossa olevia tietoja. Soveltamisala on tältä osin laaja. Esimerkiksi pankkiautomaattikortin salasana on selkeästi pykälässä tarkoitettu tieto, koska juuri sen avulla käyttäjä pääsee käyttämään pankin pankkipalveluja tarjoavaa tietojärjestelmää. Sen sijaan luottokortin numero ei ole pykälässä tarkoitettu tieto, koska sen käyttötarkoitus ei liity tietojärjestelmään.

Sääntely vastaa salasanojen ja vastaavien tietojen osalta yleissopimuksen 6 artiklan 1 kappaleen a) kohdan 2) alakohtaa.

Ehdotetun pykälän mukaan tietoverkkorikosvälineen ja salasanan levittämisen tai muun toimenpiteen on tapahduttava tarkoituksin aiheuttaa haittaa tai vahinkoa tietojenkäsittelylle taikka tieto- tai viestintäjärjestelmän toiminnalle tai turvallisuudelle. Vaikka teon kohteena oleva väline täyttäisi tietoverkkorikosvälineen tunnusmerkit teko ei ole rangaistava jos vahingoittamistarkoitus puuttuu.

Vahingolla tarkoitetaan esimerkiksi datan muuttumista ja häviämistä. Haitalla tarkoitetaan esimerkiksi tietojärjestelmän toiminnan hidastumista tai järjestelmän voimavarojen muuta heikentymistä. Selvyyden vuoksi pykälän sanamuodossa mainitaan vahingon mahdollisena kohteena tietojärjestelmän lisäksi myös tietojenkäsittely ja viestintäjärjestelmä sekä näiden turvallisuus.

Tietoverkkorikosvälineiden käyttö ilman vahingoittamistarkoitusta on käytännössä yleistä. Tietoturvallisuus on merkittävä kaupallinen toimiala. Tietojärjestelmien ja niiden suojauksen suunnittelu edellyttää tietoa viruksista, tietomurtovälineistä ja niiden toimintatavoista. Järjestelmien ja ohjelmien testauksessa käytetään tietoverkkorikosvälineitä. Tietoturvayritysten lisäksi tietoverkkorikosvälineitä käytetään puolustusvoimissa tutkittaessa tietoverkkosodankäyntiä. Myös poliisi käyttää tietoverkkorikosvälineitä kehittäessään omia menetelmiään. Tämän vuoksi on selvää, että myöskään välineiden valmistaminen, maahantuonti ja luovuttaminen tällaisessa tarkoituksessa ei ole ehdotetun pykälän mukaan rangaistava teko. Jos kysymys on esimerkiksi laitteen tai ohjelman myymisestä, myyjän velvollisuutena on selvittää ostajan käyttötarkoitus.

Sillä, mikä taho tietoverkkorikosvälineitä valmistaa tai luovuttaa, ei ole merkitystä. Myös yksityinen alan harrastaja voi valmistaa viruksen, jos tarkoituksena on ainoastaan omien ohjelmointitaitojen kehittäminen. Jos virus valmistetaan levittämistarkoituksessa, rikoksen tunnusmerkistö täyttyy. Selvää on, että teon tarkoituksen selvittämiseen saattaa käytännössä liittyä vaikeita näyttöongelmia.



Pykälässä tarkoitettu teko edellyttää tahallisuutta. Tahallisuus määritellään uudessa rikoslain 3 luvun 6 §:ssä, jonka eduskunta on hyväksynyt ja jonka on tarkoitus tulla voimaan vuoden 2004 alussa (HE 44/2002). Mainitussa pykälässä säädetään vain seuraustahallisuudesta ja sen mukaan tekijä on aiheuttanut tunnusmerkistön mukaisen seurauksen tahallaan, jos hän on tarkoittanut aiheuttaa seurauksen taikka pitänyt seurauksen aiheutumista varmana tai varsin todennäköisenä. Seuraus on aiheutettu tahallaan myös, jos tekijä on pitänyt sitä tarkoittamaansa seuraukseen varmasti liittyvänä. Niin sanottu olosuhdetahallisuus jäisi tunnusmerkistöerehdystä koskevan säännöksen perusteella oikeuskäytännössä arvioitavaksi. Olosuhdetahallisuudella viitataan muihin tunnusmerkistötekijöihin kuin seuraukseen, kuten esimerkiksi tekijän tietoisuuteen siitä, täyttääkö kyseessä oleva väline tietoverkkorikosvälineen tunnusmerkit. Tahallisuuden on ulotuttava kaikkiin tunnusmerkistötekijöihin.

Esimerkkinä tahallisuuden ja tarkoituksen moitittavuuden arviointiin liittyvästä harkintatilanteesta voidaan mainita haittakoodin julkaiseminen painostustarkoituksessa. Tietoverkkorikollisuudessa käytetään tyypillisesti hyväksi tietokone-ohjelmissa olevia tietoturva-aukkoja. Jos esimerkiksi kaupallisessa palvelinohjelmassa ilmenee tällainen tietoturva-aukko, ohjelman valmistaja joutuu paikkaamaan aukon. Tietoturvan kannalta on luonnollisesti tärkeää, että paikkausväline saatetaan ohjelman käyttäjille mahdollisimman nopeasti. Asiasta kiinnostunut alan harrastaja saattaa tietoturva-aukon löydettyään tehdä asiasta julkisen yksinomaisena tarkoituksenaan painostaa ohjelman valmistajaa nopeaan toimintaan. Vielä pidemmälle menevä painostustoimenpide on sellaisen ohjelmakoodin julkaiseminen, jonka avulla tietoturva-aukkoa voidaan hyödyntää. Tietoturva-aukon julkaiseminen ei vielä täytä rikoksen tunnusmerkistöä ellei tekoa voida julkaisutiedon seikkaperäisyyden vuoksi poikkeuksellisesti katsoa pykälän 2 kohdassa tarkoitetuksi valmistusohjeen levittämiseksi. Sen sijaan haittakoodin julkaiseminen täyttää tunnusmerkistön tekotapaa ja tietoverkkorikosvälinettä koskevat osat selvästi. Myöskään tahallinen vahingoittamistarkoitus ei poistu pelkästään sillä perusteella, että tekijä ei ole tätä seurausta nimenomaan tahtonut. Jos seuraus on teko-olosuhteet huomioon ottaen tekijän tarkoittamaan seuraukseen varmuudella liittyvä, myös tahallisuuden vaatimus täyttyy. Tilanne on luonnollisesti kokonaan toinen, jos haittakoodi esimerkiksi lähetetään Viestintäviraston CERT-yksikköön (Computer Emergency Response Team), jonka tehtäviin tietoturvauhkien havainnointi ja ratkaisu nimenomaan kuuluu.

Rangaistusasteikoksi ehdotetaan sakkoa tai vankeutta enintään kaksi vuotta. Asteikko antaa tuomioistuimelle riittävästi liikkumavaraa. Pykälässä tarkoitettut teot voivat olla vaarallisuudeltaan hyvin erilaisia. Ehdotetun asteikon seurauksena esitutkintaviranomaisen käytössä ovat myös tarpeelliset pakkokeinot.

Pykälää ei sovelleta, jos teosta muualla laissa säädetään ankarampi tai yhtä ankara rangaistus. Toissijaisuussäännös on käytännössä tärkeä erityisesti tietokonevirusten osalta. Jos levittämisen kohteena ollut virus on aktivoitunut ja aiheuttanut haittaa tai vahinkoa, viruksen valmistajan tai levittäjän tahallisuudesta riippuen tekoon saattavat tulla sovellettaviksi esimerkiksi tietoliikenteen häirintää, tietojärjestelmän häirintää tai törkeää vahingontekoa, koskevat säännökset. Tavallinen vahingonteko sen sijaan syrjäytyy, koska sen rangaistusmaksimi on pienempi.

Maksullisessa televisiolähetyksessä tai muussa vastaavassa sisältöpalvelussa käytettävän teknisen suojauksen purkavan järjestelmän ansiotarkoituksessa tapahtuva valmistaminen ja levittäminen on rangaistavaa tämän luvun 8 a §:n mukaan. Säännös on osin päällekkäinen nyt ehdotetun säännöksen kanssa. Koska 8 a §:n rangaistusmaksimi on pienempi kuin 9a §:n, se väistyy, jos teko täyttää molemmat tunnusmerkistöt.

Pykälällä yhdessä 9 b §:n kanssa saatetaan lainsäädäntö vastaamaan yleissopimuksen 6 artiklan vaatimuksia.

*9 b § Tietoverkkorikosvälineen hallussapito.* Lukuun ehdotetaan lisättäväksi uusi pykälä, jossa säädetään tietoverkkorikosvälineen hallussapidosta. Ehdotetun pykälän mukaan tietoverkkorikosvälineen hallussapidosta tuomitaan se, joka ilman hyväksyttävää syytä pitää hallussaan edellä 9 a §:n 1) kohdassa tarkoitettua laitetta, tietokoneohjelmaa, ohjelmakäskeyjen sarjaa tai tietoa. Säännös ei siten koske viitatus pykälän 2 kohdassa tarkoitettua valmistusohjetta. Pelkkä ohjeen hallussapito ei vielä aiheuta sellaista vaaraa, että myös se olisi syytä säätää rangaistavaksi.

Hallussapidon kohteena kyseeseen tulevat tietoverkkorikosvälineet on yksilöity viittauksella 9 a §:ään. Tunnusmerkistöä on tältä osin selostettu 9 a §:n perusteluissa.

Rangaistavuuden poistaa se, että hallussapitoon on hyväksyttävä syy. Hallussapitokielto on siten samalla tavalla suhteellinen kuin väärennysaineiston osalta rikoslain 33 luvun 4 §:ssä (24.8.1990/769), jota on tarkemmin selostettu mainitun pykälän perusteluissa (HE 66/1988 s.116). Hallussapidon hyväksyttävyyttä arvioitaessa on käytännössä arvioitava sitä, kuinka todennäköisesti välinettä kyseisessä hallussapitotapauksessa käytettäisiin vahingoittamistarkoituksessa. Mitä todennäköisempää tämä on, sitä vankempia perusteita hallussapitoon vaaditaan ja sitä harvemmin hallussapito jää rankaisematta. Kysymys on viimekädessä hallussapitajan esittämän perusteen ja sen uskottavuuden arvioimisesta. Ehdotuksen tarkoituksena ei ole puuttua todistustaakkasäännöksiin. Säännös ei kuitenkaan edellytä näyttöä vahingoittamistarkoituksesta. Riittävä on se, että hallussapitaja ei kykene esittämään hyväksyttävää syytä hallussapidolleen.

Niin kuin edellä 9 a §:n perusteluissa on selostettu tietoverkkorikosvälineiden hallussapito ilman vahingoittamistarkoitusta on käytännössä yleistä. Tietojärjestelmien ja niiden suojauksen suunnittelu edellyttää virusten ja tietomurtovälineiden hallussapitoa. Tietoturvayritysten lisäksi välineitä pitävät hallussaan esimerkiksi poliisi ja tietoturvaviranomaiset. Sillä, mikä taho välineitä pitää hallussaan, saattaa olla merkitystä harkittaessa hallussapidon hyväksyttävyyttä. Alan harrastajalta voidaan edellyttää painavampia perusteita hallussapitoon kuin esimerkiksi tietoturvan ammattilaiselta. Käytännössä säännös tulee todennäköisimmin sovellettavaksi sellaisessa tilanteessa, jossa henkilön hallusta löydetään useita tietoverkkorikosvälineitä, joista vain osaa tiedetään käytetyn vahingoittamistarkoituksessa. Niidenkin välineiden osalta, joita ei ole käytetty, henkilö voidaan tuomita ehdotetun 9 §:n nojalla hallussapidosta. Samassa tilanteessa kaikki välineet voidaan myös takavarikoida.

Pykälässä tarkoitettu teko edellyttää tahallisuutta.

Rangaistusasteikoksi ehdotetaan sakkoa tai vankeutta enintään yksi vuosi. Pelkkä tietorikosvälineen passiivinen hallussapito ei aiheuta samanlaista vaaraa kuin esimerkiksi vastaavan välineen aktiivinen levittäminen. Tämän vuoksi asteikko on rangaistuksen enimmäismäärän osalta lievempi kuin 9 a §:n asteikko.

Yleisten rikosoikeudellisten periaatteiden nojalla hallussapitorikoksesta ei tuomita erikseen, jos hallussapitaja itse on välinettä käyttäessään syyllistynyt joko tekijänä tai osallisena 9 a §:ssä säädettyyn tai johonkin muuhun rikokseen.

Televiestinnässä käytettävän teknisen suojauksen purkavan järjestelmän oikeudeton hallussapito on kielletty yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta annetun lain (565/1999) 5 §:ssä ja säädetty rangaistavaksi saman lain 27 §:n 1 momentin 1 kohdassa. Maksullisen televisiolähetyksessä tai muussa vastaavassa sisältöpalvelussa käytettävän teknisen suojauksen purkavan järjestelmän oikeudeton hallussapito on kielletty eräiden suojauksen purkajärjestelmien kieltämisestä annetun lain (1117/2001) 3 §:ssä ja säädetty rangaistavaksi saman lain 6 §:n 2 momentissa. Vaikka edellä mainitut säännökset ovat osin päällekkäisiä nyt ehdotetun säännöksen kanssa ne ovat molemmat toissijaisia ja siten väistyvät, jos teko täyttää molemmat tunnusmerkistöt.

Ehdotetulla pykälällä saatetaan lainsäädäntö vastaamaan yleissopimuksen 6 artiklan 1 kappaleen b) kohdan vaatimuksia. Lisäksi pykälä kattaa myös 6 artiklan 1 kappaleen a) kohdan siltä osin kuin siinä on kyse tietoverkkorikosvälineen hankinnasta käytettäväksi siten, että välinettä ei samalla levitetä tai aseteta saataville. Käytännössä hallinnan kriminalisointi kattaa myös hankkimisen, koska hankkimisen seurauksena väline päättyy aina myös hankinnan suorittaneen henkilön hallintaan.

*13 § Oikeushenkilön rangaistusvastuu.* Ehdotetun uuden pykälän mukaan vaaran aiheuttamiseen tietojenkäsittelylle ja tietoverkkorikosvälineen hallussapitoon sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään. Säännöksellä saatetaan lainsäädäntö vastaamaan tietoverkkorikosvälineitä koskevien rikosten osalta yleissopimuksen 12 artiklan vaatimuksia. Sääntelyn suhdetta yleissopimuksen 12 artiklaan on selostettu yleisemmin yleissopimuksen ja sen hyväksymisen perusteluita koskevassa osassa.

### **35 luku Vahingonteosta**

*1 § Vahingonteko.* Pykälään ehdotetaan lisättäväksi uusi 3 momentti, jonka mukaan 2 momentissa tarkoitettun tietovahingonteon yritys on rangaistava. Säännös ei siten koskisi 1 momentissa tarkoitettua esineeseen kohdistuvaa vahingontekoa. Säännöksellä saatetaan lainsäädäntö vastaamaan tietotallenteeseen kohdistuvan vahingonteon osalta yleissopimuksen 11 artiklan 2 kohdan vaatimuksia. Sääntelyn suhdetta yleissopimuksen 11 artiklaan on selostettu yleisemmin yleissopimuksen ja sen hyväksymisen perusteluita koskevassa osassa. Törkeän vahingonteon yritys on säädetty rangaistavaksi 1 päivänä helmikuuta 2003 voimaan tulleella lailla (17/2003).

*8 § Oikeushenkilön rangaistusvastuu.* Ehdotetun uuden pykälän mukaan luvun 1 §:n 2 momentissa tarkoitettuun vahingontekoon ja 3 §:ssä tarkoitettuun törkeään vahingontekoon, siltä osin kuin pykälää sovelletaan 2 momentissa tarkoitettuihin tekoihin, sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään. Säännös koskee siten ainoastaan tietovahingonteon normaalia ja törkeää tekemuotoa. Säännöksellä saatetaan lainsäädäntö vastaamaan näiden rikosten osalta yleissopimuksen 12 artiklan vaatimuksia. Sääntelyn suhdetta yleissopimuksen 12 artiklaan on yleisemmin selostettu yleissopimuksen ja sen hyväksymisen perusteluita koskevassa osassa.

### **38 luku Tieto- ja viestintärikoksista**

*5 § Tietoliikenteen häirintä.* Pykälään ehdotetaan lisättäväksi uusi 2 momentti, jonka mukaan tietoliikenteen häirinnän yritys on rangaistava. Säännöksellä saatetaan lainsäädäntö vastaamaan kyseisen rikoksen osalta yleissopimuksen 11 artiklan 2 kohdan vaatimuksia. Sääntelyn suhdetta yleissopimuksen 11 artiklaan on selostettu yleisemmin yleissopimuksen ja sen hyväksymisen perusteluita koskevassa osassa.

*6 § Törkeä tietoliikenteen häirintä.* Pykälään ehdotetaan lisättäväksi uusi 2 momentti, jonka mukaan törkeän tietoliikenteen häirinnän yritys on rangaistava. Säännöksellä saatetaan lainsäädäntö vastaamaan kyseisen rikoksen osalta yleissopimuksen 11 artiklan 2 kohdan vaatimuksia. Sääntelyn suhdetta yleissopimuksen 11 artiklaan on selostettu yleisemmin yleissopimuksen ja sen hyväksymisen perusteluita koskevassa osassa.

*7 § Lievä tietoliikenteen häirintä.* Pykälään ehdotetaan lisättäväksi uusi 2 momentti, jonka mukaan lievän tietoliikenteen häirinnän yritys on rangaistava. Säännöksellä saatetaan lainsäädäntö vastaamaan kyseisen rikoksen osalta yleissopimuksen 11 artiklan 2 kohdan vaatimuksia. Sääntelyn suhdetta yleissopimuksen 11 artiklaan on selostettu yleisemmin yleissopimuksen ja sen hyväksymisen perusteluita koskevassa osassa.

*7 a § Tietojärjestelmän häirintä.* Lukuun ehdotetaan lisättäväksi uusi pykälä, jossa säädetään tietojärjestelmän häirinnästä. Pykälän mukaan tietojärjestelmän häirinnästä tuomitaan se, joka toista vahingoittaakseen oikeudettomasti dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla näihin verrattavalla tavalla estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä. Pykälää sovelletaan ainoastaan, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta.

Säännöksellä saatetaan lainsäädäntö vastaamaan yleissopimuksen tietojärjestelmän häirintää koskevan 5 artiklan vaatimuksia. Selitysmuistion kohdista 65 ja 67 ilmenee, että mainitun artiklan tarkoituksena on suojata erityisesti viestintäjärjestelmiä virus- ja palvelunestohyökkäyksiltä. Palvelunestohyökkäyksellä tarkoitetaan esimerkiksi kohteena olevan tietojärjestelmän kuten sähköpostipalvelimen tahallista ylikuormittamista tarkoituksena estää sen toiminta tai aiheuttaa sille haittaa.

Ehdotettu pykälä liittyy läheisesti tietoliikenteen häirintää koskevaan rikokseen, jonka perustunnusmerkistö on tämän luvun 5 §:ssä. Tietoliikenteen häirinnästä tuomitaan muun ohessa se, joka puuttumalla tele- tai radioviestinnässä käytettävän laitteen toimintaan tai muulla vastaavalla tavalla oikeudettomasti estää tai häiritsee tele- tai radioviestintää. Tietoliikenteen häirinnän suhdetta yleissopimuksen 5 artiklaan on käsitelty myös yleissopimuksen ja sen hyväksymisen perusteluita koskevassa osassa.

Tietoliikenteen häirinnässä teon kohteena on viestintä, mukaan lukien tietojärjestelmien välityksellä tapahtuva sähköinen viestintä. Ehdotetussa tietojärjestelmän häirinnässä teon kohteena on tietojärjestelmä, mukaan lukien sähköisiä viestejä välittävät tietojärjestelmät.

Käytännössä nyt ehdotettua pykälää joudutaan todennäköisesti sen toissijaisuuden vuoksi soveltamaan vain harvoin. Jos pykälässä tarkoitettu teko kohdistuu sähköiseen viestintään, tietoliikenteen häirintää koskevat säännökset syrjäyttävät ehdotetun pykälän. Tyypillisenä esimerkkinä tietoliikenteen häirinnän soveltamisalaan kuuluvasta teosta voidaan mainita sellainen palvelunestohyökkäys, joka kohdistuu sähköpostipalvelimeen tai internetsivuja välittävään palvelimeen.

Ehdotettu uusi säännös on kuitenkin tarpeellinen koska mainittu 5 artikla koskee kaikentyyppistä tietojärjestelmän häirintää, myös sellaista joka kohdistuu yksittäiseen tietokoneeseen ja sellaista joka ei edes välillisesti liity viestien siirtoon. Tietoliikenteen häirintää koskeva sääntely kattaa siten artiklan ydinalueen ja ehdotettu tietojärjestelmän häirintää koskeva sääntely loput.

Pykälässä on tekotapaluettelo, jonka tarkoituksena on olla kattava. Koska teknisen kehityksen vuoksi saattaa syntyä sellaisia uusia tekotapoja, joita nyt ei osata ennakoida, luettelo on kuitenkin tarkoituksellisesti jätetty avoimeksi. Tekotapa voi siten olla muukin kuin luettelossa mainittu, jos se on niihin verrattava. Yhteistä tekotavoille on se, että niissä häiriö aiheutetaan joko kohteena olevan järjestelmän ulkopuolista dataa hyväksikäyttäen tai järjestelmässä jo olevan datan sisältöön puuttumalla. Datalla tarkoitetaan tässä ensinnäkin samaa kuin pakkokeinolain 4 luvun 1 §:n 2 momentissa eli tietokoneessa tai vastaavassa tietojärjestelmässä olevaa tietoa, mutta sen lisäksi myös siihen syötettävissä olevaa tietoa. Datan käsitettä on tarkemmin selostettu mainitun pykälän perusteluissa.

Datan syöttämisellä tarkoitetaan pykälässä sellaista hyökkäystä, joka aiheuttaa kohteessa toimintahäiriön kuitenkin siten, että tietojärjestelmässä olevaa dataa ei millään tavalla vahingoiteta. Toimintahäiriö voi seurata tarkoituksellisesta ylikuormituksesta tai esimerkiksi syötettävän datan häiriöitä aiheuttavista ominaisuuksista. Hyökkäys ei siten kohdistu järjestelmässä olevaan dataan vaan järjestelmän toimintaan.

Kohteena olevassa järjestelmässä olevan datan suoranaista vahingoittamista tai muuttamista tarkoittavat tekotyypit vastaavat yleissopimuksen sanamuotoa. Datan siirtämisen, vahingoittamisen, muuttamisen ja poistamisen väliset erot ovat käytännössä merkitykseltään vähäiset, koska tietojärjestelmien toimintatavasta johtuen jo yhden bitin muuttaminen saattaa vaikuttaa ratkaisevasti koko tietojärjestelmän toimintaan. Kattavuuden vuoksi kaikki tekotyypit on kuitenkin lueteltu pykälässä. Tyypillinen esimerkki mainitun kaltaisesta tekotavasta on dataa tuhoavan tai muuttavan tietokoneviruksen tai muun vastaavan välineen avulla toteutettu hyökkäys. Jos hyökkäyksen kohteena olevan järjestelmän toiminta ei liity viestien siirtoon, edellä käsitelty tietoliikenteen häirintä ei silloin myöskään tule sovellettavaksi.

Pykälässä edellytetään, että teko on tehty vahingoittamistarkoituksessa ja että sen seurauksena tietojärjestelmän toiminta joko estyy kokonaan tai häiriintyy vakavasti. Vakavalla häiriöllä tarkoitetaan järjestelmän toiminnan sellaista olennaista hidastumista tai toimintavarmuuden olennaista heikkenemistä, ettei järjestelmää voida enää käyttää sen normaalin käyttötarkoituksen edellyttämällä tavalla.

Tietojärjestelmän häirinnän rangaistavuus edellyttää, että tekijällä ei ole laillista oikeutta ryhtyä tekoonsa. Teon voi tehdä oikeudenmukaiseksi esimerkiksi loukatun suostumus.

Rangaistusasteikoksi ehdotetaan sakkoa tai vankeutta enintään kaksi vuotta, joka on sama kuin tämän luvun 5 §:ssä säädetyn tietoliikenteen häirinnän asteikko.

Jos tekotapana on datan vahingoittaminen, teko täyttää samalla myös rikoslain 35 luvun 1 §:n 2 momentissa tarkoitetun tietovahingon tunnusmerkistön. Silloin tekoon sovelletaan tietojärjestelmän häirintää koskevaa säännöstä, koska sen rangaistusasteikko on ankarampi. Toisaalta, jos dataa vahingoitetaan siten, että tietoliikenteen tai tietojärjestelmän häirinnän edellyttämät häiriöseuraukset eivät toteudu, tekoon voidaan soveltaa vahingontekoa koskevaa säännöstä.

Pykälän 2 momentin mukaan myös tietojärjestelmän häirinnän yritys on rangaistava.

*7 b § Törkeä tietojärjestelmän häirintä.* Pykälässä on tietoliikenteen häirinnän törkeää tekemuotoa koskeva säännös. Pykälän mukaan tekoa on pidettävä törkeänä jos sillä aiheutetaan erityisen

tuntuva haittaa tai taloudellista vahinkoa taikka jos se tehdään erityisen suunnitelmallisesti. Lisäksi teon pitää olla myös kokonaisuutena arvostellen törkeä.

Erityisen tuntuvalta taloudellisella vahingolla tarkoitetaan tässä lähinnä teolla aiheutetun seuraamuksen rahassa mitattavia vaikutuksia tietojärjestelmän haltijalle. Välittömien hankinta-, korjaus- ja huoltokustannusten lisäksi taloudellista vahinkoa voi syntyä siitä, että uhri joutuu käyttämään oman vahingoittuneen järjestelmänsä sijasta toista järjestelmää. Vahinkoa voi syntyä myös menetettyinä tuloina. Erityisen tuntuvalta haitalla taas tarkoitetaan aiheutetun seuraamuksen muita kuin rahassa mitattavia vahingollisia vaikutuksia. Tietojärjestelmän käyttömahdollisuuksien menettäminen tai heikkeneminen aiheuttaa uhrille haittaa vaikkei kyse olisikaan suoranaisesta taloudellisesta vahingosta. Mitä pidempään haitta kestää sen vakavampana sitä on pidettävä. Haitan ja vahingon välinen ero ei ole selkeä vaan ne ovat osin päällekkäisiä. Koska molemmat mainitaan säännöksessä asialla ei ole käytännössä merkitystä.

Erityisellä suunnitelmallisuudella tarkoitetaan varsinaista tekoa edeltäviä laajoja valmistelutoimenpiteitä sekä erityisiä toimia teon jälkeen jälkien peittämiseksi. Esimerkkinä erityisestä suunnitelmallisuudesta voidaan mainita niin sanottu hajautettu palvelunestohyökkäys. Hajautetulla palvelunestohyökkäyksellä tarkoitetaan hyökkäystä, jossa hyökkäykseen käytetty ohjelma ensin asennetaan uhrin koneisiin, minkä jälkeen verkon eri osissa sijaitsevat hyökkäysohjelmat aktivoidaan samanaikaisesti suorittamaan varsinainen hyökkäys ennalta määrättyyn kohteeseen. Hajautetun hyökkäyksen erityispiirre sen lisäksi, että sitä vastaan suojautuminen on vaikeaa, on se, että se altistaa hyökkäykseen tahattomasti osallistuvat välikädet aiheettomille rikosepäilyille.

Käytännössä nyt ehdotettua pykälää joudutaan todennäköisesti sen toissijaisuuden vuoksi soveltamaan vain harvoin. Jos pykälässä tarkoitettu teko kohdistuu sähköiseen viestintään, törkeää tietoliikenteen häirintää koskeva säännös syrjäyttää ehdotetun pykälän.

Rangaistusasteikoksi ehdotetaan vankeutta vähintään neljä kuukautta ja enintään kaksi vuotta, joka on sama kuin tämän luvun 6 §:ssä säädetyn törkeän tietoliikenteen häirinnän asteikko.

Pykälän 2 momentin mukaan myös törkeän tietojärjestelmän häirinnän yritys on rangaistava.

*10 § Syyteoikeus.* Uusien tietojärjestelmän häirintää koskevien rikossäännösten vuoksi pykälän 2 momenttia ehdotetaan muutettavaksi. Momentin sisältämään asianomistajarikosten luetteloon lisätään tietojärjestelmän häirintä ja törkeä tietojärjestelmän häirintä. Tietojärjestelmän häirintää koskevilla rikossäännöksillä suojataan pääasiassa yksityistä etua. Rikoksen uhrilla on parhaat edellytykset arvioida rikoksen merkitys ja se haluaako hän rikosoikeudellista suojaa. Tämän vuoksi on tarkoituksenmukaista säätää niistä asianomistajarikoksista. Nykyinen säännöksessä oleva tärkeää yleistä etua ja teleyrityksen työntekijää koskeva poikkeus koskee ehdotetun muutoksen jälkeen myös tietojärjestelmän häirintää. Näissä tilanteissa myös tietojärjestelmän häirintää koskevat rikokset ovat siten virallisen syytteen alaisia.

*12 § Oikeushenkilön rangaistusvastuu.* Ehdotetun uuden pykälän mukaan viestintäsalaisuuden loukkaukseen, törkeään viestintäsalaisuuden loukkaukseen, tietoliikenteen häirintään, törkeään tietoliikenteen häirintään, tietomurtoon, tietojärjestelmän häirintään ja törkeään tietojärjestelmän häirintään sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään. Säännöksellä saatetaan lainsäädäntö vastaamaan näiden rikosten osalta yleissopimuksen 12 artiklan vaatimuksia. Sääntelyn suhdetta yleissopimuksen 12 artiklaan on yleisemmin selostettu yleissopimuksen ja sen hyväksymisen perusteluita koskevassa osassa.

## 49 luku Eräiden aineettomien oikeuksien loukkaamisesta

*4 § Oikeushenkilön rangaistusvastuu.* Ehdotetun uuden pykälän mukaan tekijänoikeusrikokseen sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään. Säännöksellä saatetaan lainsäädäntö vastaamaan näiden rikosten osalta yleissopimuksen 12 artiklan vaatimuksia. Sääntelyn suhdetta yleissopimuksen 12 artiklaan on yleisemmin selostettu yleissopimuksen ja sen hyväksymisen perusteluita koskevassa osassa.

### 2.3 Pakkokeinolaki

#### 4 luku Takavarikko

*1 § Takavarikon edellytykset.* Pykälään ehdotetaan lisättäväksi uusi 2 momentti, jonka tarkoituksena on selventää tietojärjestelmässä olevan datan asemaa takavarikon kohteena. Lisäyksen tarkoituksena ei ole muuttaa voimassa olevan oikeuden sisältöä vaan saattaa lain sanamuoto paremmin vastaamaan vakiintunutta käytäntöä. Samasta syystä 1 momenttiin ehdotetaan lisättäväksi asiakirjan takavarikkoa koskeva tarkennus.

Ehdotetussa 2 momentissa on nykytilaa vastaava selventävä säännös, jonka mukaan myös data voi olla takavarikon kohteena. Momentti sisältää samalla datan määritelmän. Määritelmää käytetään datan takavarikkoa koskevassa 4 a §:ssä lähinnä selventämään säännöksen sisältöä ja datan säilyttämismääräystä koskevassa 4 b §:ssä lisäksi rajoittamaan säännöksen soveltamisalaa.

Määritelmän mukaan datalla tarkoitetaan tietoa, joka on tietokoneessa tai muussa vastaavassa tietojärjestelmässä taikka sen tallennusalustalla. Määritelmän mukaan data on siten tietynlaisessa teknisessä tietojärjestelmässä olevaa tietoa.

Määritelmä on riippumaton tiedon sijaintiympäristönä olevan tietojärjestelmän teknisestä toteuttamistavasta. Tietokone mainitaan määritelmässä ainoastaan helposti ymmärrettävänä esimerkkinä. Tietojärjestelmän pitää kuitenkin olla toimintatavaltaan tietokonetta vastaava. Olennaista on se, että tietoja käsitellään sähköisesti, magneettisesti, optisesti tai jollain muulla vastaavalla teknisellä keinolla, ja lisäksi se, että käsittely tapahtuu pääosin itsenäisesti ilman ihmisen välitöntä myötävaikutusta. Paperimuodossa oleva tietokortisto ei tämän vuoksi ole määritelmässä tarkoitettu tietojärjestelmä eikä siinä oleva tieto ole dataa. Matkapuhelimen sähköinen kalenteri ja siinä olevat merkinnät sen sijaan ovat määritelmässä tarkoitettua dataa, vaikka matkapuhelin ei ole yleiskielen tarkoittamassa merkityksessä tietokone.

Tiedon sijaintipaikalla tietojärjestelmässä ei ole määritelmän kannalta merkitystä. Tieto voi olla tilapäisesti järjestelmän keskusmuistissa, pysyvästi järjestelmän massamuistissa tai siirtoväylällä matkalla järjestelmän osasta toiseen. Lisäksi tieto voi olla levykkeellä, CD-levyllä tai muulla erillisellä tallennusalustalla.

Tiedolla tarkoitetaan määritelmässä mitä hyvänsä yksittäistä merkkiä, merkkijoukkoa tai niiden muodostamaa kokonaisuutta. Merkkien edustaman tiedon sisällöllä ei ole merkitystä. Sisältö voi siten yhtä hyvin olla teksti, kuva tai ääni taikka esimerkiksi tietokoneohjelma tai yksittäinen ohjelmakäske. Datalla ei tarvitse määritelmän mukaan siten olla muuta sisältöä kuin siinä olevat merkit.

Nykyisin käytössä olevien tietojärjestelmien osalta määritelmästä seuraa, että data tarkoittaa käytännössä digitaalisessa muodossa olevaa tietoa eli sellaista tietoa, jossa kaikki tallennettava tai esitettävä tieto esitetään ainoastaan kahden erilaisen merkin avulla ja jonka automaattinen tekninen käsittely on tämän vuoksi mahdollista. Datan määritelmän sitominen pelkästään tiedon digitaaliseen muotoon ei ole kuitenkaan tarkoituksenmukaista, koska tulevaisuudessa tekniikan kehittyessä tietojärjestelmissä voidaan käsitellä muutakin kuin digitaalista tietoa.

Ehdotettu datan määritelmä vastaa yleissopimuksessa olevaa datan määritelmää.

Yleissopimuksen 1 artiklan b) kohdan mukaan data tarkoittaa sellaisessa muodossa olevia tosiseikkoja, tietoja tai käsitteitä edustavia merkkejä, että ne soveltuvat käsiteltäväksi tietojärjestelmässä, mukaan lukien ohjelmat, joiden avulla tietokone pystyy suorittamaan jonkin toiminnon. Määritelmää käsitellään selitysmuistion kohdassa 25. Selitysmuistion mukaan määritelmä perustuu ISO-standardin mukaiseen määritelmään. Keskeistä määritelmässä on se, että tiedon pitää olla sähköisessä tai muussa sellaisessa muodossa, että se sellaisenaan soveltuu käsiteltäväksi tietojärjestelmässä.

Ehdotuksen mukaan datalla tarkoitetaan tietoja, jotka ovat tietojärjestelmässä tai sen tallennusalustalla. Yleissopimuksen mukaan datalla tarkoitetaan tietoja, jotka ovat sellaisessa muodossa, että ne soveltuvat käsiteltäväksi tietojärjestelmässä. Ehdotuksen mukainen datan määritelmä on helpommin ymmärrettävä. Lopputulos on käytännössä täysin sama.

Ehdotetussa 3 momentissa on nykytilaa vastaava selventävä säännös, jonka mukaan myös datan muodossa olevaan asiakirjaan sovelletaan 4 luvun 2 ja 8 §:n asiakirjan takavarikointia rajoittavia säännöksiä. Mainittujen rajoitussäännösten tarkoitus huomioon ottaen on selvää, että sääntelyn pitää olla tältä osin samanlainen riippumatta siitä, onko takavarikoitava asiakirja paperilla vai esimerkiksi datana tietokoneen kiintolevyllä.

Momentissa viitatussa 4 luvun 2 §:ssä on säännökset sellaisista asiakirjoista, joita ei saa niiden sisällön vuoksi takavarikoida silloin, kun ne ovat epäillyn tai eräiden muiden määrättyjen henkilöiden hallussa. Sama sääntely koskee myös datan muodossa olevia asiakirjoja.

Datan muodossa oleva asiakirja on epäillyn hallussa, jos tietokone, tietojärjestelmä tai erillinen tallennusalusta, jolla data sijaitsee on epäillyn hallussa, tai jos data on sen fyysisestä sijainnista riippumatta epäillyn hallinnassa ja käytettävissä. Datan kopiointia ja takavarikkoa on tarkemmin selostettu 4 a §:n perusteluissa.

Momentissa viitatussa 8 §:ssä on säännökset siitä, kenellä on oikeus avata suljettu kirje tai muu suljettu yksityinen asiakirja sekä tutkia sen sisältöä. Säännöksen mukaan avaamisoikeus on poliisin henkilökunnasta vain tutkinnan johtajalla ja tutkimisoikeus tämän lisäksi vain kyseessä olevan rikoksen tutkijoilla. Sama sääntely koskee myös datan muodossa olevia asiakirjoja. Käytännössä säännös tulee sovellettavaksi lähinnä tutkittaessa epäillyn tietokoneella tallennettuna olevia sähköpostiviestejä.

*4 a § Datan kopiointi ja takavarikointi.* Ehdotettu uusi pykälä sisältää dataan kohdistuvaa kopiointia ja takavarikkoa koskevat säännökset, joiden tarkoituksena on selventää nykyistä esineiden takavarikkoa silmälläpitäen kirjoitettua sääntelyä.



Ehdotetun säännöksen suhdetta yleissopimuksen 19 artiklan 3 kohtaan on selostettu yleissopimuksen ja sen hyväksymisen perusteluita koskevassa osassa.

Esineen takavarikko toteutetaan ottamalla esine pois sen omistajalta ja siirtämällä se esitutkintaviranomaisen haltuun. Datan osalta samaan lopputulokseen päästään kun datasta tehdään alkuperäisen kanssa identtinen kopio sekä tallennetaan se toiselle tallennusallustalle ja kopioitu data samalla poistetaan alkuperäisestä tallennusallustasta. Tämän toimenpiteen jälkeen data on ainoastaan esitutkintaviranomaisen hallussa. Datan osalta voidaan menetellä kuitenkin myös siten, että se kopioidaan ilman että alkuperäistä dataa poistetaan.

Koska tarve datan poistamiseen riippuu eri perusteista kuin viranomaisen tarve kopioida ja tutkia dataa, nämä kaksi toimenpidettä ja niiden edellytykset on tarkoituksenmukaista erottaa toisistaan datan takavarikkoa koskevassa säännöksessä. Lisäksi toimenpiteiden merkitys on niiden kohteena olevan henkilön kannalta erilainen. Datan poistaminen merkitsee huomattavasti tuntuvampaa kajoamista epäillyn oikeuksiin kuin pelkkä datan kopioiminen. Datan poistamisen seurauksena henkilö menettää datan muodossa olevan omaisuutensa hallinnan ja sen seurauksena mahdollisuuden käyttää sitä. Datan kopioinnista seuraa ainoastaan se, ettei datan muodossa oleva tieto sen jälkeen ole enää henkilön yksinomaisessa hallinnassa. Toimenpide kohdistuu tällöin lähinnä henkilön yksityisyyden suojaan.

Pykälän 1 momentti koskee datan kopiointia. Ehdotetun säännöksen mukaan data voidaan kopioida ja tallentaa toiselle tallennusallustalle, jos on syytä olettaa, että se voi olla todisteena rikosasiassa. Pelkkää datan kopiointia ei pykälän 3 momentin mukaan vielä pidetä datan takavarikkona.

Tosiasialliselta luonteeltaan momentissa tarkoitettu kopiointi on siten lähinnä etsintätoimenpide, joka tähtää sen selvittämiseen, onko tallennusallustalla, esimerkiksi tietokoneen kiintolevyllä, rikostutkinnan kannalta merkityksellistä aineistoa. Koska kopiointi liittyy kiinteästi sitä mahdollisesti seuraavaan datan takavarikkoon, siitä on tarkoituksenmukaista säätää tässä pykälässä eikä etsintää koskevassa 5 luvussa.

Toimenpiteelle ei laissa aseteta samoja rikoksen törkeyttä ja toimenpiteen tuloksellisuutta koskevia edellytyksiä kuin etsinnälle, vaikka kysymyksessä on etsintää muistuttava toimenpide. Käytännön merkitystä tällä ei kuitenkaan ole, koska tietokoneen kiintolevyn kopiointi käytännössä edellyttää yleensä kotietsinnän toimittamista, jonka jälkeen vasta kopiointi voidaan suorittaa. Kotietsintää koskevat 5 luvun säännökset esimerkiksi päätökseen oikeutetusta virkamiehestä (3 §), läsnäolo-oikeudesta (4 §), toimitustavasta (5 §) ja pöytäkirjasta (7 §) koskevat käytännössä välillisesti myös datan takavarikkoa. Vaikka datan kopioinnista ei esimerkiksi tarvitse laatia takavarikkopöytäkirjaa, toimenpide on kuitenkin kirjattava kotietsintäpöytäkirjaan. Lisäksi on huomattava, että ehdotettu sääntely saattaa tulla sovellettavaksi myös henkilöön kohdistuvan etsinnän yhteydessä sekä tilanteessa, jossa tietokone on 4 luvun 1 §:n nojalla takavarikoitu esineenä. Silloin kopiointi kohdistuu takavarikoidun esineen sisältämään dataan.

Rikostutkinnassa on erityisen tärkeää se, että data voidaan kopioida ennen kuin sen sisältö aletaan tutkia. Tämä johtuu siitä, että kiintolevyn sisältö muuttuu joka kerta kun siinä olevia tietoja luetaan. Poliisin käytössä on laitteita, joiden avulla kiintolevyn sisällöstä voidaan tehdä alkuperäisen kanssa täysin identtinen kopio siten, että esimerkiksi alkuperäisen tallennusallustan sisältämät tiedostoja koskevat aikaleimat ja muut rekisteritiedot säilyvät muuttumattomina. Jos kopiointi tapahtuisi vasta sen jälkeen kun tiedoston sisältöä on ensin tutkittu, saatettaisiin menettää rikostutkinnan kannalta merkityksellistä tietoa. Kun datan sisällön tutkinta tapahtuu tutkintakopiota hyväksikäyttäen tätä

vaaraa ei ole. Vasta kopioinnin ja tutkinnan jälkeen on edellytykset harkita mahdollista datan takavarikkoa.

Datalla tarkoitetaan 4 luvun 1 §:n 2 momentissa olevan määritelmän mukaan tietoa, joka on tietokoneessa tai muussa vastaavassa tietojärjestelmässä taikka sen tallennusalustalla. Datan määritelmää on tarkemmin selostettu kyseisen säännöksen yksityiskohtaisissa perusteluissa. Määritelmä rajaa käsillä olevan säännöksen koskemaan vain tietojärjestelmiä ja niiden erillisiä tallennusalustoja. Varsinaisen kopioinnin kohteen eli datan osalta määritelmä on laaja ja kattaa kaiken mitä tietojärjestelmästä käytännössä voidaan kopioida.

Kopioinnin edellytyksenä on datan oletettu rikostutkinnallinen merkitys. Edellytys on sama kuin esineen takavarikkoa koskevassa 1 §:ssä. Edellytys täyttyy, jos on perusteita olettaa, että data sisältää todistusaineistoa. Sillä, kuinka suuri tai pieni osa datasta on rikostutkinnan kannalta merkityksellistä, ei ole merkitystä. Esitutkintaviranomainen voi siten kopioida koko kiintolevyn vaikka etsinnässä tavoiteltaisiin vain esimerkiksi yhtä datan muodossa olevaa asiakirjaa. Datan poistaminen ja sen käytön estäminen arvioidaan erikseen jäljempänä selostetun 2 momentin perusteella.

Jos kopioinnin kohteena on datan muodossa oleva asiakirja, kopiointiin sovelletaan 4 luvun 1 §:n 3 momentin mukaan samoja rajoitussäännöksiä kuin paperimuodossa olevaan asiakirjaan.

Pelkkä epäillyn väite siitä, että tallennusalustalla on takavarikkokiellon alaista aineistoa ei kuitenkaan vielä estä kopiointia. Esitutkintaviranomainen voi siten tällaisesta väitteestä huolimatta kopioida datan tai tilanteesta riippuen myös takavarikoida koko tietokoneen tai tallennusalustan. Jos väite osoittautuu myöhemmin todeksi tai esitutkintaviranomainen havaitsee itse takavarikkokiellon alaista aineistoa, toimenpide on peruutettava kyseisten datamuodossa olevien asiakirjojen osalta. Se, miten toimenpiteen peruuttamisesta teknisesti huolehditaan, on ratkaistava tapauskohtaisesti harkiten tarkoituksenmukaisella tavalla. Vaihtoehtoina tulevat kysymykseen esimerkiksi datamuotoisen asiakirjan tuhoaminen tai palauttaminen sen alkuperäiselle haltijalle. Oleellista on se, että peruuttamisen jälkeen esitutkintaviranomaisen hallussa ei saa olla takavarikkokiellon alaista asiakirjaa eikä minkäänlaista kopiota siitä.

Käytännössä ongelmallinen tilanne syntyy silloin, jos edellä kuvatun tutkintakopion havaitaan sisältävän takavarikkokiellon alaista aineistoa. Tällainen aineisto tulee takavarikkokiellon tarkoitus huomioon ottaen poistaa tallenteesta. Tutkintakopio tehdään kuitenkin tietojen oikeellisuuden ja eheyden varmistamiseksi tarkoituksellisesti siten, että siinä olevia tietoja ei voida muuttaa eikä poistaa. Tämän vuoksi myöskään takavarikkokiellon alaisen aineiston poistaminen tai tuhoaminen siitä ei ole mahdollista. Jos koko tutkintakopio tuhotaan, esitutkintaviranomainen menettää tärkeää todistusaineistoa. Jos tutkintakopiosta tehdään uusi kopio siten, että takavarikkokiellon alainen aineisto jätetään kopioimatta uudelle kopiolle, uusi kopio ei vastaa eheydeltään alkuperäistä tutkintakopiota. Takavarikkokiellon alaiset asiakirjat ja muut asiakirjat eivät aina ole sellaisina itsenäisinä tiedostoina tai muutoinkaan sellaisessa muodossa, että niitä voisi erikseen poistaa tai kopioida. Silloin kopioinnin kohdistaminen haluttuihin tietoihin saattaa olla mahdotonta tai ainakin teknisesti vaikeaa ja erittäin työlästä. Takavarikon toteuttamiseen liittyvät tekniset syyt ja käytännön tarpeet eivät kuitenkaan voi oikeuttaa poikkeamaan lakiin perustuvasta takavarikkokiellosta. Jos muuta keinoa edellä kuvatun tilanteen ratkaisemiseksi ei ole, koko tutkintakopio on tuhottava tai palautettava.

Pykälän 2 momentti koskee datan poistamista. Ehdotetun säännöksen mukaan data voidaan kopioinnin lisäksi poistaa alkuperäisestä tallennusalustasta tai muutoin estää sen käyttö, jos on syytä

olettaa, että se on rikoksella joltakulta viety tai että tuomioistuimien julistaa sen menetetyksi taikka jos se on rikoksen selvittämiseksi tarpeen.

Poistamisen edellytyksenä on rikosoikeudellisen menettämisseuraamuksen tai oikean omistajan aseman turvaaminen. Edellytykset ovat tältä osin samat kuin esineen takavarikkoa koskevassa 1 §:ssä. Näiden perusteiden lisäksi data voidaan poistaa jos datan poistaminen on rikostutkinnallisista syistä tarpeellista. Tämäkin edellytys vastaa 1 §:ssä olevaa sääntelyä.

Menettämisseuraamuksista säädetään rikoslain 10 luvussa. Mainitun luvun 4 §:n mukaan esine tai muu omaisuus voidaan tuomita valtiolle menetetyksi muun ohessa jos sen hallussapito on rangaistavaa tai jos sitä on käytetty tahallisen rikoksen tekemisessä.

Muulla omaisuudella tarkoitetaan lain esitöiden (HE 80/2000) mukaan sellaista objektia, jota ei voida luontevasti pitää esineenä. Esimerkkinä mainitaan tietokoneohjelma.

Esimerkkinä datasta, jonka hallussapito on rangaistavaa voidaan mainita datan muodossa oleva lapsipornografinen aineisto. Rikoksen tekovälineenä voitaisiin taas poistaa esimerkiksi tietoverkkorikoksessa käytetty murto-ohjelma tai tietokonevirus.

Myös data voi olla rikoksella toiselta viety. Tätä edellytystä sovelletaan käytännössä todennäköisesti harvoin. Edellytys on kuitenkin tärkeä sisällyttää säännökseen sääntelyn johdonmukaisuuden takia.

Datan poistaminen voi olla rikostutkinnallista syistä tarpeellista esimerkiksi tilanteessa, jossa on tärkeää huolehtia siitä, etteivät muut kuin esitutkintaviranomaiset pääse esimerkiksi todisteiden hävittämistarkoituksessa tutustumaan datan sisältöön sen jälkeen kun esitutkintaviranomainen on kopioinut sen.

Käytön estäminen on datan poistamiselle vaihtoehtoinen keino. Sääntelyn tarkoitus ja edellytykset ovat samat kuin datan poistamisen osalta. Se, kumpi keino valitaan, on ratkaistava tapauskohtaisesti sen mukaan, kumpi keinoista on esimerkiksi sen tekninen toteuttamistapa huomioon ottaen tarkoituksenmukaisempi.

Dataa koskevan takavarikon peruuttamisesta säädetään jäljempänä selostetussa uudessa 17 a §:ssä. Jos esitutkintaviranomaisen todennäköisyysarvio osoittautuu vääräksi eikä dataa tuomita valtiolle menetetyksi, data on palautettava sen haltijan käyttöön. Mahdollisen palautusvelvollisuuden turvaamiseksi data on tämän vuoksi aina kopioitava poistamisen yhteydessä. Tätä tarkoitetaan kun säännöksen mukaan poistaminen tulee tehdä kopioinnin lisäksi.

Myös telekuuntelussa ja televalvonnassa kopioidaan ja tallennetaan tietoja, jotka ovat datan muodossa. Esimerkiksi sähköpostiviestin sisällön tallentaminen tai puheluita koskevien liikennetietojen selvittäminen tapahtuvat käytännössä tietojärjestelmässä olevaa dataa tallentamalla. Silloin, kun tietojärjestelmä on 5 a luvussa tarkoitettu viestintäverkko ja datan sisältönä on samassa luvussa tarkoitettu viesti tai siihen liittyvä liikennetieto, sovelletaan luonnollisesti asiaa sääntelevän 5 a luvun säännöksiä eikä ehdotettua 4 a §:ää.

Pykälän 3 momentissa säädetään takavarikkoa koskevien säännösten soveltamisesta datan kopiointiin ja poistamiseen. Säännöksen mukaan pelkkä datan kopiointi ei ole vielä takavarikko. Sen sijaan jos data kopioinnin yhteydessä samalla poistetaan tai sen käyttö estetään, toimenpide on

takavarikko. Erottelun perusteena on edellä kerrotulla tavalla toimenpiteen erilainen merkitys datan haltijalle.

Sääntely vastaa tältä osin paperimuodossa olevan asiakirjan takavarikossa noudatettua käytäntöä. Jos asiakirjan takavarikossa asiakirja kopioidaan jo esimerkiksi tutkintapaikalla ja välittömästi sen jälkeen palautetaan omistajalleen, takavarikko katsotaan samalla päättyneeksi. Asiassa laaditaan takavarikkopöytäkirja, mutta takavarikon ei katsota ulottuvan alkuperäisestä asiakirjasta tehtyyn kopioon. Jos sen sijaan alkuperäinen asiakirja takavarikoidaan, takavarikko on sen osalta voimassa siihen asti, kun se palautetaan omistajalle. Tästä seuraa muun ohessa se, että esitutkintaviranomaisen ei tarvitse pelkän asiakirjakopion hallussapidon perusteella huolehtia 4 luvun 11 §:n mukaisten takavarikkoa koskevien määräaikojen noudattamisesta. Nyt ehdotettua säännöstä ei sovelleta paperimuodossa olevan asiakirjan kopioimiseen ja takavarikkoon vaan ainoastaan dataan.

Korkein oikeus on ratkaisussa KKO:2002:85 käsitellyt datan muodossa olevan tiedon kopioimisen oikeudellista luonnetta. Tapauksessa poliisi oli kopioinut asianajaja A:n tietokoneen kovalevyn kokonaisuudessaan. Tämän vuoksi kopioon sisältyi myös sellaisia tietoja, joiden osalta A oli vaitiolovelvollinen ja jotka eivät liittyneet takavarikon perusteena olleeseen rikosepäilyyn. Kun takavarikko riidattomasti kohdistui tietoihin, joita ei pakkokeinolain mukaan saanut takavarikoida, takavarikko oli kumottava. Korkein oikeus katsoi ratkaisussaan, että datan kopiointi oli takavarikkotoimenpide vaikka kopioinnin kohteena ollut kiintolevy oli jo palautettu asianajajalle.

Korkein oikeus totesi perusteluissaan, että vaikka mainittuihin tietoihin ei olekaan tarkoitettu kohdistaa takavarikkoa, ne ovat tulleet takavarikon kohteeksi siitä syystä, että takavarikossa käytetyn teknisen menetelmän vuoksi tietokoneen kovalevy on jouduttu kopioimaan kokonaisuudessaan. Takavarikko on siten tosiasiallisesti kohdistunut sellaisiin tietoihin, joihin sitä ei olisi pakkokeinolain 4 luvun 2 §:n 2 momentin mukaan saanut kohdistaa. Poliisilla on pakkokeinolain 4 luvun 1 §:n nojalla sinänsä ollut oikeus ottaa asianajajaan kohdistuneiden rikosepäilyjen perusteella puheena oleva kovalevy takavarikkoon sekä teknisistä syistä myös kopioida kovalevyllä olevat tiedot ja tutkia niitä takavarikoitavan aineiston löytämiseksi. Takavarikon toteuttamiseen liittyvät tekniset syyt ja käytännön tarpeet eivät kuitenkaan oikeuta poikkeamaan lakiin perustuvasta takavarikkokiellosta. Siksi poliisin olisi tullut todettuaan takavarikkokiellon alaiset tiedostot välittömästi palauttaa ne A:lle tai tuhota ne.

Korkein oikeus on tietokoneen kiintolevyllä olevan tiedon osalta tulkinnut pakkokeinolain takavarikkoa koskevia säännöksiä siten, että kiintolevyn kopiointia on oikeudellisesti pidettävä takavarikkona. Poliisilla on kuitenkin ollut oikeus ottaa kovalevy haltuun ja kopioida kiintolevy kokonaisuudessaan takavarikoitavan aineiston löytämiseksi. Vasta kopiota tarkistettaessa poliisi on ollut velvollinen tutkimaan, onko kiintolevyllä takavarikkokiellon alaista tietoa, ei siis vielä siinä vaiheessa, kun kiintolevyä ryhdyttiin kopioimaan.

Ehdotettu säännös poikkeaa korkeimman oikeuden ratkaisusta siten, että pelkkää kopiointia ei vielä säännöksen mukaan pidettäisi takavarikkona. Ehdotettu sääntely vastaa korkeimman oikeuden ratkaisua siltä osin, että kopiointivaiheessa ei vielä tarvitse selvittää, onko kiintolevyllä takavarikkokiellon alaista aineistoa. Tämä selvitetään vasta kopiota tutkimalla.

Se, ettei pelkkä datan kopiointi ehdotuksen mukaan ole vielä takavarikko, ei tarkoita sitä, etteikö sellaisessa tilanteessa, jossa datan muotoinen asiakirja on takavarikkokiellon alainen, takavarikkokiello ulottaisi vaikutuksia myös datasta tehtyyn kopioon. Niin kuin edellä on tarkemmin selostettu, esitutkintaviranomainen on velvollinen tuhoamaan tai palauttamaan myös

hallussaan olevan kopion, joko kokonaan tai osittain, jos kopioimisen jälkeen ilmenee, että aineisto sisältää takavarikkokiellon alaista materiaalia. Selvää on myös se, että henkilöllä, jonka oikeutta asia koskee, on tällaisessa tapauksessa 4 luvun 13 §:n nojalla oikeus saattaa asia tuomioistuimen käsiteltäväksi.

Jos data kopioimisen yhteydessä poistetaan tai sen käyttö estetään, toimenpide katsotaan takavarikkoksi. Tämän johdosta datan poistamisen osalta on, niin kauan kuin tilanne kestää, voimassa kaikki ne säännökset, jotka laissa sääntelevät takavarikkoo. Tällaisia säännöksiä ovat muun muassa 4 luvun 5 § takavarikoimisesta päättävästä viranomaisesta, 7 § ilmoitusvelvollisuudesta, 9 § pöytäkirjasta ja todistuksesta, 13 § takavarikon saattamisesta tuomioistuimen tutkittavaksi ja erityisesti jo edellä viitattu 11 § takavarikon kumoamisesta ja noudatettavista määräajoista.

Rikoslain 10 luvun 4 §:n mukaan tietokone voidaan tahallisen rikoksen tekovälineenä tuomita valtiolle menetetyksi. Jos esimerkiksi tietomurrosta epäillyn tietokone takavarikoidaan tällaisen esineellisen menettämisseuraamuksen turvaamiseksi, tietokoneen sisältämä data tulee esineen mukana samalla takavarikoiduksi. Erillisellä dataa koskevalla sääntelyllä ei ole silloin käytännössä itsenäistä merkitystä.

*4 b § Tietojärjestelmän haltijan tietojenantovelvollisuus.* Ehdotettu uusi pykälä sisältää datan kopiointiin ja takavarikkoon liittyvät tietojärjestelmän haltijan tietojenantovelvollisuutta koskevat säännökset. Sääntelyn tarkoituksena on huolehtia siitä, että esitutkintaviranomainen saa tarvittaessa apua tutkittavana olevan tietojärjestelmän suojauksen tai salauksen murtamisessa ja mahdollisissa muissa teknisissä ongelmissa.

Pykälän 1 momentin mukaan tietojärjestelmän haltija, ylläpitäjä tai muu henkilö on velvollinen antamaan esitutkintaviranomaiselle tämän pyynnöstä tiedossaan olevat 4 a §:ssä tarkoitetun toimenpiteen suorittamiseksi tarpeelliset salasanat ja muut vastaavat tiedot.

Tietojenantovelvollisten piiriä ei ole säännöksessä rajoitettu tietyssä asemassa oleviin henkilöihin. Tietojärjestelmän haltija ja ylläpitäjä mainitaan ainoastaan esimerkkeinä säännöksen tyypillisestä soveltamistilanteesta. Tietojenantovelvollisuus voi pykälän sanamuodon mukaan siten kohdistua keneen hyvänsä, jolla on säännöksessä tarkoitettuja datan kopioimiseksi tai takavarikoimiseksi tarpeellisia tietoja hallussaan. Säännöksen soveltamisala on tältä osin laaja. Pakkokeinolain 7 luvun 1 a §:stä ilmenevä suhteellisuusperiaate rajoittaa myös tietojenantovelvollisuutta koskevan pyynnön käyttöä. Pyyntöä ei saa esittää, jos odotettavissa oleva rikostutkinnallinen hyöty ei ole järkevässä suhteessa pyynnön kohteena olevalle henkilölle aiheutuvaan haittaan. Käytännössä aiheutuva haitta on yleensä vähäinen, koska säännös tulee yleisimmin sovellettavaksi juuri esimerkiksi epäillyn kanssa samassa yrityksessä työskentelevään tietotekniikkahenkilöstöön eikä se edellytä näiltä muuta kuin velvollisuuden kertoa määrättyjä tietoja. Säännöksen tarkoituksena on helpottaa esitutkintaviranomaisen työtä vähentämällä datan kopiointiin ja takavarikkoon kuluvaa aikaa. Tästä saattaa olla välillisesti hyötyä myös epäilylle ja hänen työnantajalleen.

Sääntely vastaa tältä osin yleissopimuksen 15 artiklan vaatimuksia toimenpiteen kohtuullisuudesta ja suhteellisuusperiaatteen noudattamisesta.

Tietojenantovelvollisuuden kohteena tulevat salasanojen lisäksi kyseeseen myös kaikki muut toimenpiteen suorittamiseksi tarpeelliset tiedot. Tällaisia tietoja voivat olla esimerkiksi salauksen purkamiseen tarvittavat tiedot sekä järjestelmän ominaisuuksia koskevat tekniset tiedot. Tiedot eivät

siten liity suoraan tutkittavana olevaan rikokseen vaan ainoastaan varsinaisen todistusaineiston esille hakuun.

Tietojenantopyynnön voi säännöksen mukaan esittää kyseistä rikosta tutkiva esitutkintaviranomainen ja se voidaan esittää myös suullisesti.

Pykälän 2 momentin mukaan tietojenantovelvollisuus ei koske epäiltyä eikä henkilöä, joka esitutkintalain 27 §:n nojalla on oikeutettu tai velvollinen esitutkinnassa kieltäytymään todistamasta. Henkilö, joka ei ole velvollinen todistamaan asiassa, ei ole siten säännöksen mukaan velvollinen myöskään välillisesti myötävaikuttamaan asian selvittämiseen antamalla 1 momentissa tarkoitettuja tietoja. Vastaavasti, jos henkilö kieltäytyy antamasta tietoja, häntä voidaan pykälän 3 momentin mukaan kuulustella tuomioistuimessa, jolloin käytettävissä ovat oikeudenkäymiskaaren 17 luvun 37 §:ssä säädetyt painostuskeinot, uhkasakko ja vankeus.

Sääntely vastaa tältä osin yleissopimuksen 15 artiklan vaatimuksia toimenpiteen kohtuullisuudesta ja tuomioistuinkontrollista.

Ehdotetulla pykälällä saatetaan lainsäädäntö vastaamaan yleissopimuksen 19 artiklan 4 kohdan vaatimuksia.

*4 c § Datan säilyttämismääräys.* Lukuun ehdotetaan lisättäväksi datan säilyttämismääräystä koskevat säännökset (4 c § ja 4 d §). Datan säilyttämismääräys on uusi pakkokeino, jota voidaan tarvittaessa käyttää esitoimenpiteenä ennen muita dataan kohdistuvia pakkokeinoja. Sen tarkoituksena on estää rikostutkinnallisesti merkityksellisen datan häviäminen tai muuttaminen ennen kuin datan haltuunotto on muiden pakkokeinojen nojalla mahdollista.

Pykälän 1 momentin mukaan rikostutkinnan kannalta merkityksellisen datan haltijalle voidaan antaa säilyttämismääräys, jos on syytä olettaa, että data muutoin häviää tai sitä muutetaan.

Rikostutkinnan kannalta merkityksellinen data voidaan heti takavarikoida kun tallennusalusta on löydetty. Yleensä tilanteessa, jossa säilyttämismääräyksen edellytykset täyttyvät, esitutkintaviranomainen voi samalla jo toteuttaa itse takavarikon. Tämän vuoksi säilytysmääräys tulee käytännössä todennäköisesti vain harvoin sovellettavaksi datan takavarikkoa edeltävänä toimenpiteenä.

Myös televalvonta ja esimerkiksi sähköpostiviestien telekuuntelu kohdistuvat niiden teknisen toteuttamistavan vuoksi datan muodossa olevaan tietoon. Näiden pakkokeinojen käyttö edellyttää pääsääntöisesti tuomioistuimen luvan. Ennen kuin dataan päästään käsiksi tuomioistuimen luvan nojalla data saattaa hävitä. Säilyttämismääräyksen avulla datan häviäminen voidaan estää.

Sen varmistamiseksi, että säilyttämismääräys on tarvittaessa käytettävissä minkä hyvänsä datamuotoisen tiedon osalta, sääntely on ehdotuksen mukaan soveltamisalaltaan laaja.

Datalla tarkoitetaan 4 luvun 1 §:n 2 momentin mukaan tietoa, joka on tietokoneessa tai muussa vastaavassa tietojärjestelmässä taikka sen tallennusalustalla. Datan määritelmää on tarkemmin selostettu kyseisen säännöksen yksityiskohtaisissa perusteluissa.

Määräyksen kohteena on tietty yksilöity data. Tämä ei tarkoita sitä, että esitutkintaviranomaisen pitäisi jo säilytysmääräyksen antaessaan kyetä yksilöimään data täydellisesti. Yksilöinniltä vaadittava tarkkuus riippuu tapauksen erityispiirteistä. Esimerkiksi televalvonnan turvaamiseksi

annettavassa säilytysmääräyksessä määräyksen kohteena oleva data voidaan rajata koskemaan tietyn teleosoitteen liikennetietoja. Selvää on, että määräys ei voi koskea esimerkiksi tietyn teleoperaattorin kaikkia liikennetietoja.

Säännöksessä edellytetyn häviämiskaavan osalta riittää esitutkintaviranomaisen oma arvio häviämisen todennäköisyydestä. Vähäinenkin todennäköisyys riittää määräyksen antamiseen. Teleoperaattori on velvollinen hävittämään puhelujen liikennetiedot sen jälkeen kun niitä ei enää tarvita laskutukseen. Se, koska tämä tapahtuu, ei ole ulkopuolisen arvioitavissa. Tämän vuoksi liikennetietoa voidaan aina pitää säännöksessä tarkoitettuna häviämiskaavassa olevana datana.

Datan rikostutkinnallisen merkittävyyden osalta edellytys on sama kuin datan tai esineen takavarikossa.

Datan osalta on käytännössä monesti vaikea osoittaa, kuka on datan varsinainen omistaja, eikä omistussuhteilla ole ehdotetun säännöksen kannalta myöskään merkitystä. Oleellista on sen sijaan henkilön tosiasiallinen mahdollisuus toteuttaa säilyttämismääräyksessä tarkoitettu velvoite. Tämän vuoksi säilyttämismääräyksen kohteena kyseeseen tuleva henkilö on yksilöity datan tosiasiallisen hallinnan perusteella.

Toimivalta säilyttämismääräyksen antamiseen on pidättämiseen oikeutetulla virkamiehellä. Pykälän 2 momentin mukaan säilyttämismääräyksen voi kuitenkin antaa muukin esitutkintaa suorittava virkamies, jos asia ei siedä viivytystä. Asia on silloin välittömästi saatettava pidättämiseen oikeutetun virkamiehen päätettäväksi. Sääntely vastaa tältä osin asiallisesti 4 luvun 6 §:ssä olevaa säännöstä, jonka mukaan poliisi saa ilman pidättämiseen oikeutetun virkamiehen määräystäkin ottaa haltuunsa takavarikoimista varten esineen.

Säilyttämismääräys on annettava pääsääntöisesti kirjallisena. Kiireellisessä tapauksessa voidaan käytännössä menetellä myös niin, että säilytysmääräys annetaan esimerkiksi puhelimitse suullisena ja vahvistetaan myöhemmin kirjallisesti.

Pykälän 3 momentissa todetaan selvyyden vuoksi, että datan säilytysmääräys voi koskea myös datan muodossa olevaa viestiä ja sen liikennetietoja. Momentti sisältää samalla liikennetiedon määritelmän, jota käytetään jäljempänä 4 momentissa. Määritelmän mukaan liikennetiedolla tarkoitetaan viestiin liittyvää tietoa viestin alkuperästä, määränpäästä, reitistä ja koosta sekä viestinnän ajankohdasta, kestosta, laadusta ja muista vastaavista seikoista. Esimerkkeinä liikennetiedoista voidaan mainita soittajan tai vastaanottajan puhelinnumero, puhelun kesto tai sähköpostiviestin alkuperä, määränpää, lähetysajankohta ja koko. Myös matkapuhelimen paikkatieto on liikennetieto.

Pykälän 4 momentissa todetaan selvyyden vuoksi pääsääntö, jonka mukaan esitutkintaviranomaisella ei ole säilyttämismääräyksen nojalla oikeutta saada tietoonsa viestin, liikennetiedon tai muun tallennetun tiedon sisältöä. Momentin toisessa virkkeessä on poikkeus pääsäännöstä. Sen mukaan esitutkintaviranomaisella on oikeus saada tietoonsa palveluntarjoajien tunnistamiseksi tarvittavat liikennetiedot, jos viestin välittämiseen on osallistunut useampi palveluntarjoaja.

Poikkeussäännös koskee ainoastaan viestiin liittyviä liikennetietoja ja niidenkin osalta ainoastaan sellaisia tietoja, jotka ovat välttämättömiä viestin reitin selvittämiseksi.

Tietojärjestelmässä kulkeva viesti saattaa kulkea useiden teleoperaattorien verkkojen kautta. Silloin yhdelle siirtoketjuun osallistuneelle operaattorille osoitettu säilyttämismääräys ei välttämättä riitä viestin tai sen liikennetietojen häviämisen estämiseen. Jotta säilyttämismääräys voitaisiin kohdistaa kaikkiin siirtoketjuun osallistuneisiin tahoihin, tarvitaan tieto siitä, mitkä kaikki operaattorit ovat siirtämiseen osallistuneet. Jokaisella operaattorilla on tieto siitä, miltä operaattorilta viesti on sille tullut ja tieto siitä, mille operaattorille viesti on siltä lähtenyt. Nämä liikennetiedot ovat säännöksessä tarkoitettuja palveluntarjoajan tunnistamiseksi tarvittavia tietoja ja vain näiden osalta säilyttämismääräys oikeuttaa esitutkintaviranomaisen saamaan tiedon liikennetiedon sisällöstä.

Käytännössä säilyttämismääräys voidaan edellä kuvattu tilanne huomioon ottaen antaa siten, että esitutkintaviranomaisen tiedon saantioikeus ja säilyttämismääräys kohdistuu kaikkiin siirtoketjussa oleviin operaattoreihin, vaikkei niitä määräystä annettaessa voida vielä yksilöidä.

Säilyttämismääräyksen teho perustuu siihen, että sen velvoittama henkilö noudattaa sitä. Jos säilyttämismääräyksen saanut kieltäytyy noudattamasta määräystä, hänet voidaan tuomita rikoslain 16 luvun 4 §:n nojalla niskoittelusta poliisia vastaan. Jos säilyttämismääräyksen kohteena on teleoperaattori tai muu oikeushenkilö, rangaistusuhka kohdistuu siihen luonnolliseen henkilöön, jonka katsotaan olevan vastuussa säilyttämismääräyksen toteuttamisesta.

Jos säilyttämismääräystä ei voida noudattaa esimerkiksi sen vuoksi, että se on teknisesti mahdotonta, on selvää että rangaistusta ei voida tuomita. Teleoperaattorilla ei ole tämän säännöksen nojalla myöskään velvollisuutta muuttaa järjestelmän teknisiä ominaisuuksia.

Ehdotetulla säännöksellä yhdessä jäljempänä selostetun 4 d §:n kanssa saatetaan lainsäädäntö vastaamaan yleissopimuksen 16 ja 17 artiklan vaatimuksia.

*4 d § Datan säilyttämismääräyksen kesto ja salassapitovelvollisuus.* Ehdotetussa pykälässä on 4 c §:ää täydentävät säännökset säilyttämismääräyksen määräaikaisuudesta, enimmäiskestosta ja määräyksen saaneen henkilön salassapitovelvollisuudesta.

Pykälän 1 momentin mukaan datan säilyttämismääräys annetaan määräajaksi ja enintään kolmeksi kuukaudeksi. Määräaikaa voidaan pidentää enintään kolmella kuukaudella kerralla, jos rikoksen tutkinta sitä edellyttää. Säilyttämismääräyksen edellytykset on siten otettava uudelleen harkittavaksi vähintään kolmen kuukauden välein. Säilyttämismääräyksen kokonaiskestolle ei ole sen sijaan asetettu enimmäisrajaa. Pakkokeinojen käyttöä yleisesti rajoittava 7 luvun 1 a §:ssä säädetty suhteellisuusperiaate rajoittaa kuitenkin myös tämän pakkokeinon käyttöä. Säilytysmääräys on heti kumottava, kun se ei ole enää tarpeen tai jos odotettavissa oleva rikostutkinnallinen hyöty ei ole järkevässä suhteessa määräyksen saaneelle aiheutuvaan haittaan. Tarpeettomana säilytysmääräys on kumottava esimerkiksi silloin kun se on annettu esitoimenpiteenä televalvonnalle ja esitutkintaviranomainen saa pyytämänsä televalvontaluvan tuomioistuimelta ja saa säilytysmääräyksellä jäädytetyn datan haltuunsa. Vastaavasti toimenpide on peruutettava edellä kuvatussa tilanteessa myös silloin, jos tuomioistuin hylkää lainvoimaisella päätöksellä televalvontahakemuksen eikä esitutkintaviranomaisella ole enää tämän vuoksi perusteita ylläpitää säilytysmääräystä.

Pykälän 2 momentin mukaan säilyttämismääräyksen saanut on velvollinen pitämään salassa saamansa määräyksen. Säännöksen tarkoituksena on yhtäältä turvata rikostutkinnan häiriötön kulku, mutta toisaalta myös suojata epäillyn henkilön yksityisyyttä. Pykälän 3 momentissa on selventävä viittaussäännös, jonka mukaan rangaistus 2 momentissa säädetyn salassapitovelvollisuuden rikkomisesta tuomitaan rikoslain salassapitorikosta koskevan 38 luvun 1 §:n tai saman luvun



salassapitorikkomusta koskevan 2 §:n mukaan, jollei teosta muualla laissa säädetä ankarampaa rangaistusta.

Ehdotetulla pykälällä saatetaan lainsäädäntö vastaamaan yleissopimuksen 16 artiklan 2 ja 3 kohdan vaatimuksia.

*15 a § Takavarikosta päättäminen vieraan valtion oikeusapupyynnön johdosta.* Koska lakiin ehdotetaan lisättäväksi datan takavarikointia koskevat erityiset säännökset, pykälän ensimmäiseen virkkeeseen ehdotetaan johdonmukaisuuden vuoksi lisättäväksi myös data takavarikoitavissa olevien objektien luetteloon.

*17 a § Takavarikoidun datan palauttaminen.* Pykälässä on selventävä säännös, jonka mukaan data on palautettava sen omistajan tai haltijan käytettäväksi, jos 4 a §:n 2 momentissa tarkoitettu datan takavarikko kumotaan. Jos data on takavarikossa poistettu tallennusalustasta, se on palautettava sille, jonka hallusta se takavarikoitiin. Jos datan käyttö on estetty, käytön estämiseksi toteutettu tekninen suojajärjestelmä on purettava.

## **2.4 Esitutkintalaki**

27 §. Pykälään ehdotetaan lisättäväksi uusi 2 momentti, jolloin nykyinen 2 momentti muuttuu 3 momentiksi. Ehdotetun 2 momentin mukaan todistaja olisi 1 momentin mukaisen ilmaisuvollisuuden lisäksi velvollinen myös esittämään hallussaan olevan rikostutkinnan kannalta merkityksellisen asiakirjan tai muun todistusaineiston. Datan muodossa oleva aineisto on epäillyn hallussa, jos tietokone, tietojärjestelmä tai erillinen tallennusalusta, jolla data sijaitsee on epäillyn hallussa, tai jos data on sen fyysisestä sijainnista riippumatta epäillyn hallinnassa ja käytettävissä.

Nykyisen lain nojalla asiakirja tai muu aineisto kuten esimerkiksi datan muodossa oleva tallenne voidaan takavarikoida. Jos aineiston säilytyspaikka ei ole tiedossa, aineiston haltija on todistajana velvollinen kertomaan sen. Ehdotetun säännöksen tarkoituksena on selkiyttää sääntelyä siten, että mainitussa tilanteessa todistaja on velvollinen esittämään aineiston itse. Todistajan esittämä aineisto voidaan sitten tarvittaessa myös takavarikoida. Todistajan esittämisvelvollisuutta rajoittaa kuitenkin suhteellisuusperiaate. Jos aineiston omatoiminen esittäminen on aineiston laajuuden tai muun vastaavan syyn vuoksi poikkeuksellisen työlästä, on selvää, että esitutkintaviranomainen on velvollinen mahdollisuuksiensa mukaan avustamaan todistajaa esimerkiksi noutamalla aineiston todistajan ilmoittamasta paikasta.

Nykyinen todistajan kieltäytymisoikeutta ja -velvollisuutta koskeva 2 momentti muuttuu ehdotuksen myötä 3 momentiksi. Tätä säännöstä sovelletaan myös todistajan esittämisvelvollisuuteen.

Jos todistaja kieltäytyy noudattamasta esittämisvelvollisuutta todistaja voidaan jäljempänä selostetun ehdotetun uuden 28 §:n 2 momentin nojalla velvoittaa siihen tuomioistuimessa.

Säännöksellä yhdessä 28 §:n 2 momentin kanssa muutetaan lainsäädäntö vastaamaan yleissopimuksen esittämismääräystä koskevia 18 artiklan määräyksiä.

Yleissopimus edellyttää esittämisvelvollisuutta ainoastaan datan osalta. Ehdotuksen mukaan esittämisvelvollisuus koskee myös paperimuodossa olevaa asiakirjaa ja muuta todistusaineistoa.

Ehdotus menee siten pidemmälle kuin mitä yleissopimus välttämättä edellyttää. Tämä on kuitenkin sääntelyn johdonmukaisuus ja tarkoituksenmukaisuusperusteet huomioon ottaen välttämätöntä. Datan ja esimerkiksi paperimuodossa olevan todistusaineiston erilaiselle sääntelylle tässä suhteessa ei ole järkeviä perusteita. Yleissopimusta on tältä osin selostettu myös 18 artiklan yksityiskohtaisissa perusteluissa.

28 §. Pykälään ehdotetaan lisättäväksi uusi 2 momentti, jolloin nykyinen 2 momentti muuttuu 3 momentiksi. Ehdotetun 2 momentin mukaan 1 momentin mukainen tuomioistuinkäsittely olisi käytettävissä myös silloin, kun todistaja kieltäytyy noudattamasta ehdotetun uuden 27 §:n 2 momentin mukaista esittämisvelvollisuutta. Silloin käytettävissä on oikeudenkäymiskaaren 17 luvun 15 §:ssä säädetty painostuskeino, uhkasakko ja lisäksi mahdollisuus määrätä ulosottomies noutamaan aineisto.

Esittämisvelvollisuuden osalta on huomattava, että oikeudenkäymiskaaren 17 luvun 37 §:ssä säädettyä painostusvankeutta ei voida sen osalta käyttää, koska mainitun säännöksen soveltamisala rajoittuu ainoastaan todistajan suulliseen kuulusteluun. Tällä ei ole kuitenkaan käytännössä merkitystä, koska todistajaa voidaan aineiston sijaintipaikan osalta kuulustella myös suullisesti.

Käytännössä säännös voi tulla sovellettavaksi vain tilanteessa, jossa todistajalla jollain perusteella tiedetään olevan hallussaan rikostutkinnan kannalta merkityksellistä aineistoa. Tieto voi perustua esimerkiksi todistajan omaan ilmoitukseen tai toisen todistajan kertomukseen. Tyypillisenä esimerkkinä voidaan mainita tilanne, jossa todistaja myöntää, että hänellä on hallussaan aineistoa, mutta kieltäytyy esittämästä sitä, vedoten johonkin asiakirjan takavarikkoa koskevaan takavarikkokieltöön.

Nykyiset 2 ja 3 momentin menettelyä ja todistajan palkkiota koskevat säännökset muuttuvat ehdotuksen myötä 3 ja 4 momentiksi. Näitä säännöksiä sovelletaan myös esittämisvelvollisuutta koskevaan tuomioistuinkäsittelyyn.

Säännöksellä yhdessä 27 §:n 2 momentin kanssa muutetaan lainsäädäntö vastaamaan yleissopimuksen esittämismääräystä koskevia 18 artiklan määräyksiä. Sääntely vastaa myös 15 artiklan vaatimuksia toimenpiteen kohtuullisuudesta, suhteellisuusperiaatteen noudattamisesta ja tuomioistuinkontrollista.

## **2.5 Laki kansainvälisestä oikeusavusta rikosasioissa**

*15 § Pakkokeinojen käytön rajoitukset.* Pykälään ehdotetaan lisättäväksi uusi 2 momentti, jolloin nykyiset 2 ja 3 momentti muuttuvat 3 ja 4 momentiksi. Ehdotetun 2 momentin mukaan 1 momentissa oleva kaksoisrangaistavuuden vaatimus ei koske tässä esityksessä ehdotettua uutta pakkokeinolain 4 luvun 4 b §:ssä tarkoitettua datan säilyttämismääräystä.

Datan säilyttämismääräys on uusi pakkokeino, jota voidaan tarvittaessa käyttää esitoimenpiteenä ennen muita dataan kohdistuvia pakkokeinoja. Sen tarkoituksena on estää rikostutkinnallisesti merkityksellisen datan häviäminen tai muuttaminen ennen kuin datan haltuunotto ja sen sisällön tutkiminen on muiden pakkokeinojen nojalla mahdollista. Asiaa on tarkemmin selostettu mainitun pykälän perusteluissa.

Ehdotettu poikkeus kaksoisrangaistavuuden vaatimuksesta koskee ainoastaan datan säilyttämismääräystä, ei sitä käytännössä säännönmukaisesti seuraavia varsinaisia dataan

kohdistuvia pakkokeinoja. Säätelyn tarkoituksena on menettelyä nopeuttamalla estää datan häviäminen. Kaksoisrangaistavuuden vaatimuksen täyttymistä koskeva ratkaisu edellyttää selvitystä tutkittavana olevasta rikoksesta ja asiaan vaikuttavien seikkojen harkitsemista. Jos oikeusapupyynnön tutkiminen kestää kauan, säilytettäväksi pyydetty data saattaa hävitä menettelyn aikana. Datan säilyttämismääräyksellä on kuitenkin vain vähäisiä vaikutuksia datan haltijan oikeuksiin. Tämän vuoksi on tarkoituksenmukaista, ettei tällaisen varmistavan esitoimenpiteen osalta kaksoisrangaistavuuden vaatimusta tarvitse tutkia lainkaan. Jos myöhemmin varsinaista pakkokeinoa koskevaa pyyntöä käsiteltäessä havaitaan, että kaksoisrangaistavuuden vaatimus ei täyty, pyyntö hylätään ja säilytysmääräys perutaan.

Säännöksellä saatetaan lainsäädäntö vastaamaan yleissopimuksen 29 artiklan 3 kappaleen vaatimuksia. Yleissopimusta on tältä osin selostettu 29 artiklan yksityiskohtaisissa perusteluissa.

*23 § Pakkokeinojen käyttäminen todisteiden hankkimiseksi ja menettämisseuraamuksen täytäntöönpanon turvaamiseksi.* Pykälän 1 momenttia ehdotetaan muutettavaksi siten, että siinä olevaan oikeusapupyynnön perusteella toimeenpantavissa olevien pakkokeinojen luetteloon lisätään tässä esityksessä ehdotettu uusi pakkokeinolain 4 luvun 4 c §:n mukainen datan säilyttämismääräys.

### 3. Voimaantulo

Yleissopimus tulee voimaan, kun viisi valtiota, joista vähintään kolme on Euroopan neuvoston jäseniä, on ratifioinut sopimuksen. Sopimus ei ole vielä voimassa ja sen voimaantulopäivää on vaikea arvioida.

Esityksen mukaan yleissopimuksen voimaansaattamista koskevan lain voimaantulosta säädetään tasavallan presidentin asetuksella. Lain on tarkoitus tulla voimaan samanaikaisesti kun yleissopimus tulee voimaan Suomen osalta.

Lait rikoslain, pakkokeinolain, esitutkintalain ja rikosoikeusapulain muuttamisesta ehdotetaan tulevaksi voimaan mahdollisimman pian sen jälkeen kun ne on hyväksytyt.

### 4. Eduskunnan suostumuksen tarpeellisuus

Perustuslain 94 §:n 1 momentin mukaan eduskunta hyväksyy muun ohessa sellaiset valtiosopimukset ja muut kansainväliset velvoitteet, jotka sisältävät lainsäädännön alaan kuuluvia määräyksiä. Perustuslakivaliokunnan tulkintakäytännön mukaan eduskunnan hyväksymistoimivalta kattaa kaikki aineelliselta luonteeltaan lain alaan kuuluvat kansainvälisen veloitteen määräykset siihen katsomatta, onko määräys ristiriidassa tai sopusoinnussa Suomessa lailla annetun säännöksen kanssa. Perustuslakivaliokunta on tulkintakäytännössään pitänyt asianmukaisena, että eduskunta antaa nimenomaisella päätöksellä suostumuksensa myös eduskunnan toimivallan alaan kuuluvia sopimusmääräyksiä koskevien selitysten ja varaumien antamiseen.

Yleissopimus sisältää sen luonteen vuoksi pääasiassa lainsäädännön alaan kuuluvia määräyksiä. Kaikki yleissopimuksen rikoksia, pakkokeinoja, rikoslain alueellista soveltamista, rikoksen tekijän luovuttamista ja kansainvälistä oikeusapua koskevat määräykset kuuluvat lainsäädännön alaan. Poikkeuksena on 35 artikla, jossa on kyse ainoastaan artiklassa tarkoitettun ympärivuorokautisen päivystyksen järjestämisestä.

Ehdotuksen mukaan eduskunta hyväksyy sopimuksen siten, että hyväksymispäätös kattaa sopimuksen kokonaisuudessaan.

Lainsäädännön alaan kuuluvat myös kaikki esityksessä ehdotetut selitykset ja varaukset.

Eduskunnan suostumus tarvitaan siten 2 artiklan mukaiseen selitykseen, jonka mukaan Suomi asettaa artiklassa tarkoitetun luvattoman tunkeutumisen rangaistavuuden edellytykseksi sen, että rikos on tehty turvajärjestelyt murtamalla.

Eduskunnan suostumus tarvitaan myös:

1) yleissopimuksen 11 artiklan 3 kappaleen mukaiseen varaukseen, jonka mukaan Suomi ei sovelle mainitun artiklan yrityksen kriminalisointiin velvoittavaa 2 kappaletta lievään vahingontekoon eikä lievään väärennykseen;

2) yleissopimuksen 14 artiklan 3 kappaleen a) kohdan mukaiseen varaukseen, jonka mukaan Suomi soveltaa 20 artiklaa ainoastaan automaattiseen tietojenkäsittelyjärjestelmään kohdistuneeseen rikokseen, joka on tehty telepäätelaitetta käyttäen, paritukseen, oikeudenkäytössä kuultavan uhkaamiseen, laittomaan uhkaukseen, huumausainerikokseen ja näiden yritykseen sekä terroristisessa tarkoituksessa tehtävän rikoksen valmisteluun ja rikoksiin, joista säädetty ankarin rangaistus on vähintään 4 vuotta vankeutta;

3) yleissopimuksen 14 artiklan 3 kappaleen b) kohdan mukaiseen varaukseen, jonka mukaan Suomi ei sovelle 20 ja 21 artiklassa tarkoitettuja pakkokeinoja tietojärjestelmän sisäiseen viestintään, jos tietojärjestelmällä on rajattu käyttäjäryhmä ja tietojärjestelmää ei käytetä julkisten tietoverkkojen avulla eikä sitä ole kytketty toiseen julkiseen tai yksityiseen tietojärjestelmään.

## 5. Säättämisyjärjestys

Esityksessä ehdotetaan, että yleissopimuksen lainsäädännön alaan kuuluvat määräykset saatetaan valtion sisäisesti voimaan niin sanotulla blankettimuotoisella lailla. Yleissopimuksessa on määräyksiä jotka koskevat rangaistavaksi säädettäviä tekoja, rikosoikeudellisia pakkokeinoja ja kansainvälistä oikeusapua. Eräät pakkokeinoja ja oikeusapua koskevat yleissopimuksen määräykset saattavat olla säättämisyjärjestuksen kannalta merkityksellisiä. Nämä ovat yleissopimuksen 19 artiklan 3 kohta datan takavarikosta ja kopioinnista, 16 artikla tallennetun datan nopeasta varmistamisesta, 17 artikla liikennetietojen säilyttämisen nopeasta varmistamisesta ja osittaisesta luovutuksesta sekä kaksoisrangaistavuutta koskeva 29 artiklan 3 kohta.

Yleissopimuksen 19 artiklan 3 kohta sisältää dataan kohdistuvaa takavarikkoa ja kopiointia koskevat määräykset. Koska takavarikon kohteena on datan muodossa oleva omaisuus, määräys liittyy perustuslain 15 §:n mukaiseen omaisuuden suojaan. Määräys vastaa pääosin Suomessa nykyisin noudatettua käytäntöä eikä se laajenna viranomaisten takavarikko-oikeutta. Tämän vuoksi määräys ei ole omaisuuden suojan kannalta ongelmallinen.

Yleissopimuksen 16 artiklassa määräykset tallennetun datan säilyttämisen nopeasta varmistamisesta. Kyseessä on uusi pakkokeino, jota voidaan tarvittaessa käyttää esitoimenpiteenä ennen muita dataan kohdistuvia pakkokeinoja. Sen tarkoituksena on estää rikostutkinnallisesti merkityksellisen datan häviäminen tai muuttaminen ennen kuin datan haltuunotto on muiden pakkokeinojen nojalla mahdollista. Säännöksen nojalla datan haltijaa voidaan tilapäisesti kieltää hävittämästä hallussaan oleva dataa. Koska toimenpiteen kohteena on datan muodossa oleva omaisuus, pykälä liittyy perustuslain 15 §:n mukaiseen omaisuuden suojaan. Säännös kajoaa

omaisuuden suojaan kuitenkin vain vähäisessä määrin. Tämän vuoksi ehdotettu uusi säännös ei ole omaisuuden suojan kannalta ongelmallinen.

Yleissopimuksen 17 artiklassa on määräykset liikennetietojen säilyttämisen nopeasta varmistamisesta ja osittaisesta luovutuksesta. Artiklan mukaan 16 artiklassa tarkoitettun toimenpiteen kohteena voi olla myös tietojärjestelmän välityksellä siirretty viesti ja siihen liittyvä liikennetieto. Viranomaisella ei ole kuitenkaan pääsääntöisesti oikeutta saada tietoonsa viestin, liikennetiedon tai muun tallennetun tiedon sisältöä. Tästä pääsäännöstä on kuitenkin yksi poikkeus. Jos viestin välittämiseen on osallistunut useampi palveluntarjoaja, viranomaisella on oltava oikeus saada tietoonsa palveluntarjoajien tunnistamiseksi tarvittavat liikennetiedot. Tältä osin artikla liittyy myös perustuslain 10 §:n mukaiseen luottamuksellisen viestin suojaan. Perustuslakivaliokunnan tulkintakäytännön mukaan luottamuksellisen viestin liikennetiedot kuuluvat 10 §:n mukaisen suojan piiriin vaikka ne ovatkin perusoikeuden reuna-alueella.

Mainittu poikkeus koskee ainoastaan viestiin liittyviä liikennetietoja ja niidenkin osalta ainoastaan sellaisia tietoja, jotka ovat välttämättömiä viestin reitittämiseksi. Käytännössä tämä tarkoittaa ainoastaan tietoa siitä, mitkä operaattorit ovat osallistuneet viestin välittämiseen. Näiden tietojen luovuttaminen viranomaiselle ei loukkaa käytännössä kohteena olevan henkilön yksityisyyttä lainkaan tai loukkaa sitä erittäin vähän. Tietojen luovuttaminen on kuitenkin välttämätöntä, jotta säilyttämismääräys voitaisiin nopeasti kohdistaa kaikkiin viestin siirtoketjuun osallistuneisiin tahoihin. Tämän vuoksi ehdotettu säännös ei ole perustuslain 10 §:n kannalta ongelmallinen.

Yleissopimuksen 29 artiklan 3 kohdan mukaan 16 artiklassa tarkoitettua datan varmistamista koskevan oikeusapupyynnön toimeenpanon osalta ei saa edellyttää kaksoisrangaistavuutta. Käytännössä tämä merkitsee muun ohessa sitä, että Suomen viranomaisella on ulkomaisen viranomaisen pyynnöstä velvollinen käyttämään mainittua pakkokeinoa vaikka pakkokeinon perusteena oleva teko ei olisikaan Suomen lain mukaan rangaistava. Koska pakkokeino edellyttää myös tiettyjen liikennetietojen luovuttamista, pykälä liittyy ainakin jossain määrin perustuslain 1 §:n mukaiseen Suomen täysivaltaisuuteen.

Perustuslain 1 §:n 3 momentin mukaan Suomi osallistuu kansainväliseen yhteistyöhön rauhan ja ihmisoikeuksien turvaamiseksi sekä yhteiskunnan kehittämiseksi. Tällä säännöksellä on perustuslain esitöiden mukaan tulkinnallista merkitystä arvioitaessa sitä, milloin kansainvälinen velvoite on ristiriidassa perustuslain täysivaltaisuutta koskevien säännösten kanssa. Uuden tulkintakäytännön lähtökohtana on, että sellaiset kansainväliset velvoitteet, jotka ovat tavanomaisia nykyaikaisessa kansainvälisessä yhteistoiminnassa ja jotka vain vähäisessä määrin vaikuttavat valtion täysivaltaisuuteen, eivät sellaisenaan ole ristiriidassa perustuslain täysivaltaisuutta koskevien säännösten kanssa.

Artiklan edellyttämä poikkeus kaksoisrangaistavuuden vaatimuksesta koskee ainoastaan 16 artiklassa tarkoitettua datan varmistamista, ei sitä käytännössä säännönmukaisesti seuraavia varsinaisia dataan kohdistuvia pakkokeinoja. Artiklan yksinomaisena tarkoituksena on menettelyä nopeuttamalla estää rikostutkinnallisesti merkityksellisen datan häviäminen. Sääntelyn vaikutukset sen kohteena oleviin henkilöihin tai esimerkiksi teleoperaattoreihin ovat edellä kuvatulla tavalla vähäiset. Kansainvälinen yhteistoiminta tietoverkkorikosten tutkinnassa ja selvittämisessä on omiaan myötävaikuttamaan yhteiskunnan kehittämiseen juuri siinä merkityksessä kuin perustuslain 1 §:n 3 momentissa tarkoitetaan.

Näiden syiden vuoksi artiklan määräyksen ei voida katsoa olevan ristiriidassa perustuslain 1 §:n kanssa.

Ehdotus voimaansaattamislainsäädännön voimaansaattamiseksi voidaan siten käsitellä tavallisen lain säätämisympäristössä.

Edellä olevan perusteella ja perustuslain 94 §:n mukaisesti esitetään,

*että Eduskunta hyväksyy Budapestissä 23 päivänä marraskuuta 2001 tehdyn Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen;*

*että Eduskunta antaa suostumuksensa siihen, että Suomi antaa 2 artiklan mukaiseen selityksen, jonka mukaan Suomi asettaa artiklassa tarkoitetun luvattoman tunkeutumisen rangaistavuuden edellytykseksi sen, että rikos on tehty turvajärjestelyt murtamalla;*

*että Eduskunta antaa suostumuksensa siihen, että Suomi tekee 11 artiklan 3 kappaleen mukaisen varauman, jonka mukaan Suomi ei sovelle mainitun artiklan yrityksen kriminalisointiin velvoittavaa 2 kappaletta lievään vahingontekoon eikä lievään väärennykseen;*

*että Eduskunta antaa suostumuksensa siihen, että Suomi tekee 14 artiklan 3 kappaleen a) kohdan mukaisen varauman, jonka mukaan Suomi soveltaa 20 artiklaa ainoastaan automaattiseen tietojenkäsittelyjärjestelmään kohdistuneeseen rikokseen, joka on tehty telepäätelaitetta käyttäen, paritukseen, oikeudenkäytössä kuultavan uhkaamiseen, laittomaan uhkaukseen, huumausainerikokseen ja näiden yritykseen sekä terroristisessa tarkoituksessa tehtävän rikoksen valmisteluun ja rikoksiin, joista säädetty ankaran rangaistus on vähintään neljä vuotta vankeutta;*

*että Eduskunta antaa suostumuksensa siihen, että Suomi tekee 14 artiklan 3 kappaleen b) kohdan mukaisen varauman, jonka mukaan Suomi ei sovelle 20 ja 21 artiklassa tarkoitettuja pakkokeinoja tietojärjestelmän sisäiseen viestintään, jos tietojärjestelmällä on rajattu käyttäjäryhmä ja tietojärjestelmää ei käytetä julkisten tietoverkkojen avulla eikä sitä ole kytketty toiseen julkiseen tai yksityiseen tietojärjestelmään.*

Samalla annetaan Eduskunnan hyväksyttäväksi seuraavat lakiehdotukset:

## LAKIEHDOTUKSET

### 1. Laki Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta

Eduskunnan päätöksen mukaan säädetään:

#### 1 §

##### *Yleissopimuksen voimaansaattaminen*

Budapestissä 23 päivänä marraskuuta 2001 tehdyn Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

#### 2 §

##### *Asetuksenantovaltuus*

Tarkempia säännöksiä tämän lain täytäntöönpanosta voidaan antaa valtioneuvoston asetuksella.

#### 3 §

##### *Voimaantulo*

Tämän lain voimaantulosta säädetään tasavallan presidentin asetuksella.

-----

### 2. Laki rikoslain muuttamisesta

Eduskunnan päätöksen mukaisesti:

*muutetaan* 19 päivänä joulukuuta 1889 annetun rikoslain (39/1889) 34 luvun 9 a § ja 38 luvun 10 §:n 2 momentti sellaisena kuin ne ovat 34 luvun 9 a § laissa 951/1999 ja 38 luvun 10 §:n 2 momentti laissa 578/1995, sekä

*lisätään* 34 lukuun uusi 9 b § ja 13 §, 35 luvun 1 §:ään sellaisena kuin se on laissa 769/1990 uusi 3 momentti, lukuun uusi 8 §, 38 luvun 5 §:ään sellaisena kuin se on laissa 578/1995 uusi 2 momentti, luvun 6 §:ään sellaisena kuin se on mainitussa laissa uusi 2 momentti, luvun 7 §:ään sellaisena kuin se on mainitussa laissa uusi 2 momentti, lukuun uusi 7 a, 7 b ja 12 § sekä 49 lukuun uusi 4 § seuraavasti:

## 34 luku

**Yleisvaarallisista rikoksista**

## 9 a §

*Vaaran aiheuttaminen tietojenkäsittelylle*

Joka aiheuttaakseen haittaa tai vahinkoa tietojenkäsittelylle taikka tieto- tai viestintäjärjestelmän toiminnalle tai turvallisuudelle

- 1) tuo maahan, valmistaa, myy tai muuten levittää taikka asettaa saataville
  - a) sellaisen laitteen, tai tietokoneohjelman tai ohjelmakäskyjen sarjan, joka on suunniteltu tai muunnettu ensisijaisesti vaarantamaan tai vahingoittamaan tietojenkäsittelyä taikka tieto- tai viestintäjärjestelmän toimintaa taikka tietojärjestelmän suojauksen murtamiseen tai
  - b) tietojärjestelmän salasanan tai käyttäjätunnuksen tai muun vastaavan tiedon taikka;
- 2) levittää tai asettaa saataville 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskyjen sarjan valmistusohjeen,  
on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, *vaaran aiheuttamisesta tietojenkäsittelylle* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

## 9 b §

*Tietoverkkorikosvälineen hallussapito*

Joka ilman hyväksyttävää syytä pitää hallussaan 9 a §:n 1) kohdassa tarkoitettua laitetta, tietokoneohjelmaa, ohjelmakäskyjen sarjaa tai tietoa, on tuomittava *tietoverkkorikosvälineen hallussapidosta* sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

## 13 §

*Oikeushenkilön rangaistusvastuu*

Vaaran aiheuttamiseen tietojenkäsittelylle ja tietoverkkorikosvälineen hallussapitoon sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään.

## 35 luku

**Vahingonteosta**

## 1 §

*Vahingonteko*

-----  
Edellä 2 momentissa tarkoitetun rikoksen yritys on rangaistava.



## 8 §

*Oikeushenkilön rangaistusvastuu*

Luvun 1 §:n 2 momentissa tarkoitettuun vahingontekoon ja 3 §:ssä tarkoitettuun törkeään vahingontekoon, siltä osin kuin pykälää sovelletaan 2 momentissa tarkoitettuihin tekoihin, sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään.

## 38 luku

**Tieto- ja viestintärikoksista**

## 5 §

*Tietoliikenteen häirintä*

-----

Yritys on rangaistava.

## 6 §

*Törkeä tietoliikenteen häirintä*

-----

Yritys on rangaistava.

## 7 §

*Lievä tietoliikenteen häirintä*

-----

Yritys on rangaistava.

## 7 a §

*Tietojärjestelmän häirintä*

Joka toista vahingoittaakseen oikeudettomasti dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla näihin verrattavalla tavalla, estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä on tuomittava jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, *tietojärjestelmän häirinnästä* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Yritys on rangaistava.

## 7 b §

*Törkeä tietojärjestelmän häirintä*

Jos tietojärjestelmän häirinnässä

- 1) aiheutetaan erityisen tuntuva haittaa tai taloudellista vahinkoa taikka
  - 2) rikos tehdään erityisen suunnitelmallisesti
- ja rikos on myös kokonaisuutena arvostellen törkeä, rikoksen tekijä on tuomittava *törkeästi tietojärjestelmän häirinnästä* vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.

Yritys on rangaistava.

## 10 §

*Syyteoikeus*

-----

Virallinen syyttäjä ei saa nostaa syytettä viestintäsalaisuuden loukkauksesta, törkeästä viestintäsalaisuuden loukkauksesta, tietojärjestelmän häirinnästä, törkeästä tietojärjestelmän häirinnästä, tietomurrosta tai suojauksen purkujärjestelmärikoksesta, ellei asianomistaja ilmoita rikosta syytteeseen pantavaksi tai ellei rikosentekijä rikosta tehdessään ole ollut yleistä posti- tai teletoimintaa harjoittavan laitoksen palveluksessa taikka ellei erittäin tärkeä yleinen etu vaadi syytteen nostamista.

-----

## 12 §

*Oikeushenkilön rangaistusvastuu*

Viestintäsalaisuuden loukkaukseen, törkeään viestintäsalaisuuden loukkaukseen, tietoliikenteen häirintään, törkeään tietoliikenteen häirintään, tietomurtoon, tietojärjestelmän häirintään ja törkeään tietojärjestelmän häirintään sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään.

## 49 luku

**Eräiden aineettomien oikeuksien loukkaamisesta**

## 4 §

*Oikeushenkilön rangaistusvastuu*

Tekijänoikeusrikokseen sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään.

----

Tämä laki tulee voimaan päivänä kuuta 20 .

-----

### 3. Laki pakkokeinolain muuttamisesta

Eduskunnan päätöksen mukaisesti:

*muutetaan* 30 päivänä huhtikuuta 1987 annetun pakkokeinolain (450/1987) 4 luvun 1 ja 15 a §:n 1 momentti, sellaisena kuin niistä 15 a §:n 1 momentti on laissa 10/1994 sekä *lisätään* 4 lukuun uusi 4 a - 4 c ja 17 a § seuraavasti:

#### 4 luku

#### **Takavarikko**

##### 1 §

##### *Takavarikon edellytykset.*

Esine tai asiakirja voidaan takavarikoida, jos on syytä olettaa, että se voi olla todisteena rikosasiassa tai on rikoksella joltakulta viety taikka että tuomioistuim julistaa sen menetetyksi.

Mitä 1 momentissa säädetään koskee myös tietoa, joka on tietokoneessa tai muussa vastaavassa tietojärjestelmässä taikka sen tallennusalustalla (*data*).

Mitä luvun 2 ja 8 §:ssä säädetään asiakirjasta sovelletaan myös datan muodossa olevaan asiakirjaan.

##### 4 a §

##### *Datan kopiointi ja takavarikointi*

Data voidaan kopioida ja tallentaa se toiselle tallennusalustalle, jos on syytä olettaa, että se voi olla todisteena rikosasiassa.

Data voidaan kopioinnin lisäksi poistaa alkuperäisestä tallennusalustasta tai muutoin estää sen käyttö, jos on syytä olettaa, että se on rikoksella joltakulta viety tai että tuomioistuim julistaa sen menetetyksi taikka jos se on rikoksen selvittämiseksi tarpeen.

Edellä 2 momentissa tarkoitetun toimenpiteen osalta on voimassa mitä takavarikosta säädetään.

## 4 b §

*Tietojärjestelmän haltijan tietojenantovelvollisuus*

Tietojärjestelmän haltija, ylläpitäjä tai muu henkilö on velvollinen antamaan esitutkintaviranomaiselle tämän pyynnöstä tiedossaan olevat 4 a §:ssä tarkoitetun toimenpiteen suorittamiseksi tarpeelliset salasanat ja muut vastaavat tiedot.

Mitä 1 momentissa säädetään ei kuitenkaan koske epäiltyä eikä henkilöä, joka esitutkintalain 27 §:n nojalla on oikeutettu tai velvollinen esitutkinnassa kieltäytymään todistamasta.

Jos henkilö kieltäytyy antamasta tietoja, häntä voidaan kuulustella tuomioistuimessa, siten kuin esitutkintalain 28 §:ssä säädetään.

## 4 c §

*Datan säilyttämismääräys*

Jos on syytä olettaa, että tietty data, jolla on merkitystä tutkittavana olevan rikoksen selvittämiseksi, häviää tai sitä muutetaan, pidättämiseen oikeutettu virkamies voi määrätä sen, jonka hallussa tai määräysvallassa data on, säilyttämään sen muuttumattomana.

Jos asia ei siedä viivytystä, 1 momentissa tarkoitetun säilyttämismääräyksen voi antaa muukin esitutkintaa suorittava virkamies. Asia on silloin välittömästi saatettava pidättämiseen oikeutetun virkamiehen päätettäväksi.

Mitä 1 momentissa säädetään, koskee myös tietojärjestelmän välityksellä siirrettyä viestiä ja siihen liittyvää tietoa viestin alkuperästä, määränpäästä, reitistä ja koosta sekä viestinnän ajankohdasta, kestosta, laadusta ja muista vastaavista seikoista (*liikennetieto*).

Esitutkintaviranomaisella ei ole 1 momentissa tarkoitetun säilyttämismääräyksen nojalla oikeutta saada tietoonsa viestin, liikennetiedon tai muun tallennetun tiedon sisältöä. Jos 3 momentissa tarkoitetun viestin välittämiseen on osallistunut useampi palveluntarjoaja, esitutkintaviranomaisella on kuitenkin oikeus saada tietoonsa palveluntarjoajien tunnistamiseksi tarvittavat liikennetiedot.

## 4 d §

*Datan säilyttämismääräyksen kesto ja salassapitovelvollisuus*

Datan säilyttämismääräys annetaan määräajaksi, enintään kolmeksi kuukaudeksi. Määräaika voidaan pidentää enintään kolmella kuukaudella kerralla, jos rikoksen tutkinta sitä edellyttää.

Säilyttämismääräyksen saanut on velvollinen pitämään salassa saamansa määräyksen.

Rangaistus 2 momentissa säädetyn salassapitovelvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teosta muualla laissa säädetä ankarampaa rangaistusta.

## 15 a §

*Takavarikosta päättäminen vieraan valtion oikeusapupyynnön johdosta*

Esine, asiakirja tai data voidaan vieraan valtion viranomaisen pyynnöstä takavarikoida, jos se voi olla todisteena pyynnön esittäneen vieraan valtion viranomaisen käsiteltävänä olevassa rikosasiassa taikka se on rikoksella joltakulta viety. Esine voidaan takavarikoida, jos se on vieraan valtion tuomioistuimen antamalla päätöksellä julistettu rikoksen johdosta menetetyksi taikka jos voidaan aiheellisesti olettaa, että esine tullaan julistamaan rikoksen johdosta menetetyksi vieraan valtion viranomaisen käsiteltävänä olevassa asiassa.

## 17 a §

*Takavarikoidun datan palauttaminen*

Jos 4 a §:n 2 momentissa tarkoitettu datan takavarikko kumotaan, data on palautettava sen omistajan tai haltijan käytettäväksi.

Tämä laki tulee voimaan päivänä kuuta 20 .

**4. Laki esitutkintalain muuttamisesta**

Eduskunnan päätöksen mukaisesti:

*lisätään* 30 päivänä huhtikuuta 1987 annetun esitutkintalain (449/1987) 27 §:ään uusi 2 momentti, jolloin nykyinen 2 momentti siirtyy 3 momentiksi ja 28 §:ään sellaisena kuin se on laissa 692/1997 uusi 2 momentti, jolloin nykyinen 2 momentti siirtyy 3 momentiksi seuraavasti:

## 27 §

Todistaja, jolla on 1 momentissa tarkoitettu ilmaisovelvollisuus, on velvollinen myös esittämään hallussaan olevan rikostutkinnan kannalta merkityksellisen asiakirjan tai muun todistusaineiston.

## 28 §

Mitä 1 momentissa säädetään sovelletaan myös todistajaan, joka kieltäytyy esittämästä asiakirjaa tai muuta todistusaineistoa.

----

Tämä laki tulee voimaan päivänä kuuta 20 .

-----

## 5. Laki kansainvälisestä oikeusavusta rikosasioissa annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti:

*muutetaan* 5 päivänä tammikuuta 1994 annetun kansainvälisestä oikeusavusta rikosasioissa annetun lain 23 §:n 1 momentti sellaisena kuin se on laissa 406/1995 sekä *lisätään* 15 §:ään uusi 2 momentti, jolloin nykyinen 2 ja 3 momentti siirtyvät 3 ja 4 momentiksi seuraavasti:

### 15 §

#### *Pakkokeinojen käytön rajoitukset*

-----

Mitä edellä 1 momentissa säädetään ei kuitenkaan koske pakkokeinolain 4 luvun 4 c §:ssä tarkoitettua datan säilyttämismääräystä.

-----

### 23 §

#### *Pakkokeinojen käyttäminen todisteiden hankkimiseksi ja menettämisseuraamuksen täytäntöönpanon turvaamiseksi*

Vieraan valtion viranomaisen tekemän oikeusapupyynnön perusteella voidaan todisteiden hankkimiseksi panna toimeen etsintä, takavarikko ja datan säilyttämismääräys, suorittaa telekuuntelua, televalvontaa ja teknistä tarkkailua sekä ottaa henkilötuntemerkit, jos tätä on pyydetty oikeusapupyynnössä taikka se on tarpeen oikeusapupyynnön toimeenpanemiseksi.

-----

----

Tämä laki tulee voimaan päivänä kuuta 20 .

-----

Helsingissä päivänä kuuta 20 .

Tasavallan Presidentti

Oikeusministeri

## LIITTEET

### Rinnakkaistekstit

#### 2. Laki rikoslain muuttamisesta

Eduskunnan päätöksen mukaisesti:

*muutetaan* 19 päivänä joulukuuta 1889 annetun rikoslain (39/1889) 34 luvun 9 a § ja 38 luvun 10 §:n 2 momentti sellaisena kuin ne ovat 34 luvun 9 a § laissa 951/1999 ja 38 luvun 10 §:n 2 momentti laissa 578/1995, sekä

*lisätään* 34 lukuun uusi 9 b § ja 13 §, 35 luvun 1 §:ään sellaisena kuin se on laissa 769/1990 uusi 3 momentti, lukuun uusi 8 §, 38 luvun 5 §:ään sellaisena kuin se on laissa 578/1995 uusi 2 momentti, luvun 6 §:ään sellaisena kuin se on mainitussa laissa uusi 2 momentti, luvun 7 §:ään sellaisena kuin se on mainitussa laissa uusi 2 momentti, lukuun uusi 7 a, 7 b ja 12 § sekä 49 lukuun uusi 4 § seuraavasti:

*Voimassaoleva laki*

*Ehdotus*

34 luku

34 luku

#### **Yleisvaarallisista rikoksista**

#### **Yleisvaarallisista rikoksista**

9 a §

9 a §

*Vaaran aiheuttaminen tietojenkäsittelylle*

*Vaaran aiheuttaminen tietojenkäsittelylle*

Joka, aiheuttaakseen haittaa tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle,

- 1) valmistaa tai asettaa saataville sellaisen tietokoneohjelman tai ohjelmakäskeyjen sarjan, joka on suunniteltu vaarantamaan tietojenkäsittelyä tai tieto- tai telejärjestelmän toimintaa taikka vahingoittamaan sellaisen järjestelmän sisältämiä tietoja tai ohjelmistoja, tai levittää sellaista tietokoneohjelmaa tai ohjelmakäskeyjen sarjaa taikka
- 2) asettaa saataville ohjeen 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskeyjen sarjan valmistamiseen tai levittää sellaista ohjetta,

on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa

Joka aiheuttaakseen haittaa *tai vahinkoa* tietojenkäsittelylle taikka tieto- tai viestintäjärjestelmän toiminnalle *tai turvallisuudelle*

- 1) *tuo maahan*, valmistaa, *myy* tai muuten levittää taikka asettaa saataville
  - a) sellaisen *laitteen*, tai tietokoneohjelman tai ohjelmakäskeyjen sarjan, joka on suunniteltu *tai muunnettu* ensisijaisesti vaarantamaan tai vahingoittamaan tietojenkäsittelyä taikka tieto- tai viestintäjärjestelmän toimintaa *taikka tietojärjestelmän suojauksen murtamiseen* tai
  - b) *tietojärjestelmän salasanan tai käyttäjätunnuksen tai muun vastaavan tiedon taikka*;
- 2) levittää tai asettaa saataville 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskeyjen sarjan valmistusohjeen,

rangaistusta, vaaran aiheuttamisesta tietojenkäsittelylle sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, vaaran aiheuttamisesta tietojenkäsittelylle sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

### 9 b §

#### *Tietoverkkorikosvälineen hallussapito*

(uusi)

*Joka ilman hyväksyttävää syytä pitää hallussaan 9 a §:n 1) kohdassa tarkoitettua laitetta, tietokoneohjelmaa, ohjelmakäskyjen sarjaa tai tietoa, on tuomittava tietoverkkorikosvälineen hallussapidosta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.*

### 13 §

#### *Oikeushenkilön rangaistusvastuu*

(uusi)

*Vaaran aiheuttamiseen tietojenkäsittelylle ja tietoverkkorikosvälineen hallussapitoon sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään.*

### 35 luku

#### **Vahingonteosta**

#### 1 §

#### *Vahingonteko*

Joka oikeudettomasti hävittää tai vahingoittaa toisen omaisuutta, on tuomittava vahingonteosta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Vahingonteosta tuomitaan myös se, joka toista vahingoittaakseen oikeudettomasti hävittää, turmelee, kätkee tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen.

### 35 luku

#### **Vahingonteosta**

#### 1 §

#### *Vahingonteko*

-----  
*Edellä 2 momentissa tarkoitettun rikoksen yritys on rangaistava.*



## 8 §

*Oikeushenkilön rangaistusvastuu*

(uusi)

*Luvun 1 §:n 2 momentissa tarkoitettuun vahingontekoon ja 3 §:ssä tarkoitettuun törkeään vahingontekoon, siltä osin kuin pykälää sovelletaan 2 momentissa tarkoitettuihin tekoihin, sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään.*

## 38 luku

**Tieto- ja viestintärikoksista**

## 5 §

*Tietoliikenteen häirintä*

Joka puuttamalla postiliikenteessä taikka tele- tai radioviestinnässä käytettävän laitteen toimintaan, lähettämällä ilkeävaltaisessa tarkoituksessa radiolaitteella tai televerkossa häiritseviä viestejä tai muulla vastaavalla tavalla oikeudettomasti estää tai häiritsee postiliikennettä taikka tele- tai radioviestintää, on tuomittava *tietoliikenteen häirinnästä* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

## 6 §

*Törkeä tietoliikenteen häirintä*

Jos tietoliikenteen häirinnässä  
1) rikoksentehtyjä käyttää rikoksen tekemisessä hyväksi asemaansa teletoimintalaissa tarkoitetun yleistä teletoimintaa, [kaapelilähetystoiminnasta annetun lain (307/87)] mukaista kaapelilähetystoimintaa tai yleisradiotoimintaa harjoittavan laitoksen palveluksessa tai muuta

## 38 luku

**Tieto- ja viestintärikoksista**

## 5 §

*Tietoliikenteen häirintä*

-----  
*Yritys on rangaistava.*

## 6 §

*Törkeä tietoliikenteen häirintä*

erityistä luottamusasemaansa taikka  
2) rikoksella estetään tai häiritään hätäkutsujen radioviestintää tai muuta sellaista tele- tai radioviestintää, jota harjoitetaan ihmishengen turvaamiseksi,  
ja tietoliikenteen häirintä on myös kokonaisuutena arvostellen törkeä, rikoksentehtäjä on tuomittava *törkeästä tietoliikenteen häirinnästä* vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.

-----  
*Yritys on rangaistava.*

7 §

*Lievä tietoliikenteen häirintä*

Jos tietoliikenteen häirintä, huomioon ottaen aiheutetun häiriön laatu tai määrä taikka muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentehtäjä on tuomittava lievästä tietoliikenteen häirinnästä sakkoon.

7 §

*Lievä tietoliikenteen häirintä*

-----  
*Yritys on rangaistava.*

7 a §

*Tietojärjestelmän häirintä*

(uusi)

*Joka toista vahingoittaakseen oikeudettomasti dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla näihin verrattavalla tavalla estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä, on tuomittava jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, tietojärjestelmän häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.*

*Yritys on rangaistava.*

7 b §

*Törkeä tietojärjestelmän häirintä*

(uusi)

*Jos tietojärjestelmän häirinnässä*

- 1) aiheutetaan erityisen tuntuva haittaa tai taloudellista vahinkoa taikka  
 2) rikos tehdään erityisen suunnitelmallisesti ja rikos on myös kokonaisuutena arvostellen törkeä, rikoksen tekijä on tuomittava törkeästä tietojärjestelmän häirinnästä vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.

*Yritys on rangaistava.*

10 §

*Syyteoikeus*

-----  
 Virallinen syyttäjä ei saa nostaa syytettä viestintäsalaisuuden loukkauksesta, törkeästä viestintäsalaisuuden loukkauksesta, tietomurrosta tai suojauksen purkujärjestelmär rikoksesta, ellei asianomistaja ilmoita rikosta syytteeseen pantavaksi tai ellei rikosentekijä rikosta tehdessään ole ollut yleistä posti- tai teletoimintaa harjoittavan laitoksen palveluksessa taikka ellei erittäin tärkeä yleinen etu vaadi syytteen nostamista.  
 -----

10 §

*Syyteoikeus*

-----  
 Virallinen syyttäjä ei saa nostaa syytettä viestintäsalaisuuden loukkauksesta, törkeästä viestintäsalaisuuden loukkauksesta, tietojärjestelmän häirinnästä, törkeästä tietojärjestelmän häirinnästä, tietomurrosta tai suojauksen purkujärjestelmär rikoksesta, ellei asianomistaja ilmoita rikosta syytteeseen pantavaksi tai ellei rikosentekijä rikosta tehdessään ole ollut yleistä posti- tai teletoimintaa harjoittavan laitoksen palveluksessa taikka ellei erittäin tärkeä yleinen etu vaadi syytteen nostamista.  
 -----

12 §

*Oikeushenkilön rangaistusvastuu*

(uusi)

*Viestintäsalaisuuden loukkaukseen, törkeään viestintäsalaisuuden loukkaukseen, tietoliikenteen häirintään, törkeään tietoliikenteen häirintään, lievään tietoliikenteen häirintään, tietomurtoon, tietojärjestelmän häirintään ja törkeään tietojärjestelmän häirintään sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään.*

49 luku

**Eräiden aineettomien oikeuksien loukkaamisesta**

49 luku

**Eräiden aineettomien oikeuksien loukkaamisesta**

## 4 §

*Oikeushenkilön rangaistusvastuu*

(uusi)

*Tekijänoikeusrikokseen sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään.*

**3. Laki pakkokeinolain muuttamisesta**

Eduskunnan päätöksen mukaisesti:

*muutetaan 30 päivänä huhtikuuta 1987 annetun pakkokeinolain (450/1987) 4 luvun 1 ja 15 a §:n 1 momentti, sellaisena kuin niistä 15 a §:n 1 momentti on laissa 10/1994 sekä lisätään 4 lukuun uusi 4 a - 4 c ja 17 a § seuraavasti:*

*Voimassaoleva laki**Ehdotus*

4 luku

4 luku

**Takavarikko****Takavarikko**

1 §

1 §

*Takavarikon edellytykset.**Takavarikon edellytykset.*

Esine voidaan takavarikoida, jos on syytä olettaa, että se voi olla todisteena rikosasiassa tai on rikoksella joltakulta viety taikka että tuomioistuin julistaa sen menetetyksi.

Mitä luvun 2 ja 8 §:ssä säädetään asiakirjasta sovelletaan myös datan muodossa olevaan asiakirjaan.

Esine *tai asiakirja* voidaan takavarikoida, jos on syytä olettaa, että se voi olla todisteena rikosasiassa tai on rikoksella joltakulta viety taikka että tuomioistuin julistaa sen menetetyksi.

*Mitä 1 momentissa säädetään koskee myös tietoa, joka on tietokoneessa tai muussa vastaavassa tietojärjestelmässä taikka sen tallennusalustalla (data).*

*Mitä luvun 2 ja 8 §:ssä säädetään asiakirjasta sovelletaan myös datan muodossa olevaan asiakirjaan.*

4 a §

*Datan kopiointi ja takavarikointi*

(uusi)

*Data voidaan kopioida ja tallentaa se toiselle tallennusalustalle, jos on syytä olettaa, että se voi olla todisteena rikosasiassa.*

*Data voidaan kopiointiin lisäksi poistaa alkuperäisestä tallennusalustasta tai muutoin estää sen käyttö, jos on syytä olettaa,*

*että se on rikoksella joltakulta viety tai että tuomioistuimien julistaa sen menetetyksi taikka jos se on rikoksen selvittämiseksi tarpeen.*

*Edellä 2 momentissa tarkoitetun toimenpiteen osalta on voimassa mitä takavarikosta säädetään.*

#### 4 b §

##### *Tietojärjestelmän haltijan tietojenantovelvollisuus*

(uusi)

*Tietojärjestelmän haltija, ylläpitäjä tai muu henkilö on velvollinen antamaan esitutkintaviranomaiselle tämän pyynnöstä tiedossaan olevat 4 a §:ssä tarkoitetun toimenpiteen suorittamiseksi tarpeelliset salasanat ja muut vastaavat tiedot.*

*Mitä 1 momentissa säädetään ei kuitenkaan koske epäiltyä eikä henkilöä, joka esitutkintalain 27 §:n nojalla on oikeutettu tai velvollinen esitutkinnassa kieltäytymään todistamasta.*

*Jos henkilö kieltäytyy antamasta tietoja, häntä voidaan kuulustella tuomioistuimessa, siten kuin esitutkintalain 28 §:ssä säädetään.*

#### 4 c §

##### *Datan säilyttämismääräys*

(uusi)

*Jos on syytä olettaa, että tietty data, jolla on merkitystä tutkittavana olevan rikoksen selvittämiseksi, häviää tai sitä muutetaan, pidättämiseen oikeutettu virkamies voi määrätä sen, jonka hallussa tai määräysvallassa data on, säilyttämään sen muuttumattomana.*

*Jos asia ei siedä viivytystä, 1 momentissa tarkoitetun säilyttämismääräyksen voi antaa muukin esitutkintaa suorittava virkamies. Asia on silloin välittömästi saatettava pidättämiseen oikeutetun virkamiehen päätettäväksi.*

*Mitä 1 momentissa säädetään, koskee myös tietojärjestelmän välityksellä*

*siirrettyä viestiä ja siihen liittyvää tietoa viestin alkuperästä, määränpäästä, reitistä ja koosta sekä viestinnän ajankohdasta, kestosta, laadusta ja muista vastaavista seikoista (liikennetieto).*

*Esitutkintaviranomaisella ei ole 1 momentissa tarkoitetun säilyttämismääräyksen nojalla oikeutta saada tietoonsa viestin, liikennetiedon tai muun tallennetun tiedon sisältöä. Jos 3 momentissa tarkoitetun viestin välittämiseen on osallistunut useampi palveluntarjoaja, esitutkintaviranomaisella on kuitenkin oikeus saada tietoonsa palveluntarjoajien tunnistamiseksi tarvittavat liikennetiedot.*

#### 4 d §

*Datan säilyttämismääräyksen kesto ja salassapitovelvollisuus*

(uusi)

*Datan säilyttämismääräys annetaan määräajaksi, enintään kolmeksi kuukaudeksi. Määräaika voidaan pidentää enintään kolmella kuukaudella kerralla, jos rikoksen tutkinta sitä edellyttää.*

*Säilyttämismääräyksen saanut on velvollinen pitämään salassa saamansa määräyksen.*

*Rangaistus 2 momentissa säädetyn salassapitovelvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teosta muualla laissa säädetä ankarampaa rangaistusta.*

#### 15 a §

*Takavarikosta päättäminen vieraan valtion oikeusapupyynnön johdosta*

Esine tai asiakirja voidaan vieraan valtion viranomaisen pyynnöstä takavarikoida, jos se voi olla todisteena pyynnön esittäneen vieraan valtion viranomaisen käsiteltävänä olevassa rikosasiassa taikka se on rikoksella joltakulta viety. Esine voidaan takavarikoida, jos se on vieraan valtion tuomioistuimen antamalla päätöksellä julistettu rikoksen johdosta menetetyksi taikka jos voidaan aiheellisesti

#### 15 a §

*Takavarikosta päättäminen vieraan valtion oikeusapupyynnön johdosta*

Esine, asiakirja tai data voidaan vieraan valtion viranomaisen pyynnöstä takavarikoida, jos se voi olla todisteena pyynnön esittäneen vieraan valtion viranomaisen käsiteltävänä olevassa rikosasiassa taikka se on rikoksella joltakulta viety. Esine voidaan takavarikoida, jos se on vieraan valtion tuomioistuimen antamalla päätöksellä julistettu rikoksen johdosta menetetyksi taikka jos

olettaa, että esine tullaan julistamaan rikoksen johdosta menetetyksi vieraan valtion viranomaisen käsiteltävänä olevassa asiassa.

-----

voidaan aiheellisesti olettaa, että esine tullaan julistamaan rikoksen johdosta menetetyksi vieraan valtion viranomaisen käsiteltävänä olevassa asiassa.

-----

## 17 a §

*Takavarikoidun datan palauttaminen*

(uusi)

Jos 4 a §:n 2 momentissa tarkoitettu datan takavarikko kumotaan, data on palautettava sen omistajan tai haltijan käytettäväksi.

**4. Laki esitutkintalain muuttamisesta**

Eduskunnan päätöksen mukaisesti:

*lisätään* 30 päivänä huhtikuuta 1987 annetun esitutkintalain (449/1987) 27 §:ään uusi 2 momentti, jolloin nykyinen 2 momentti siirtyy 3 momentiksi ja 28 §:ään sellaisena kuin se on laissa 692/1997 uusi 2 momentti, jolloin nykyinen 2 momentti siirtyy 3 momentiksi seuraavasti:

*Voimassaoleva oikeus*

## 27 §

Todistajan on totuudenmukaisesti ja mitään salaamatta ilmaistava, mitä hän tietää tutkittavasta asiasta. Jos hän kuitenkin olisi oikeudenkäynnissä oikeutettu tai velvollinen kieltäytymään todistamasta, ilmaisemasta seikkaa tai vastaamasta kysymykseen, jos tutkittavana olevasta rikoksesta nostettaisiin syyte, hän on oikeutettu tai velvollinen siihen myös esitutkinnassa.

Oikeudenkäymiskaaren 17 luvun 23 §:n 1 momentissa tarkoitettu henkilö, joka saman pykälän 3 momentin nojalla voidaan velvoittaa todistamaan salassa pidettävästä asiasta, on oikeutettu todistamaan tästä esitutkinnassa, jos tutkittavana on rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta. Oikeudenkäymiskaaren 17 luvun 24 §:n 2 tai 3 momentissa tarkoitettu henkilö, joka saman pykälän 4 momentin nojalla voidaan velvoittaa vastaamaan pykälän 2 momentissa tarkoitettuun kysymykseen, on velvollinen vastaamaan tällaiseen kysymykseen

*Ehdotus*

## 27 §

Todistajan on totuudenmukaisesti ja mitään salaamatta ilmaistava, mitä hän tietää tutkittavasta asiasta. Jos hän kuitenkin olisi oikeudenkäynnissä oikeutettu tai velvollinen kieltäytymään todistamasta, ilmaisemasta seikkaa tai vastaamasta kysymykseen, jos tutkittavana olevasta rikoksesta nostettaisiin syyte, hän on oikeutettu tai velvollinen siihen myös esitutkinnassa.

*Todistaja, jolla on 1 momentissa tarkoitettu ilmaisovelvollisuus, on velvollinen myös esittämään hallussaan olevan rikostutkinnan kannalta merkityksellisen asiakirjan tai muun todistusaineiston.*

Oikeudenkäymiskaaren 17 luvun 23 §:n 1 momentissa tarkoitettu henkilö, joka saman pykälän 3 momentin nojalla voidaan velvoittaa todistamaan salassa pidettävästä asiasta, on oikeutettu todistamaan tästä esitutkinnassa, jos tutkittavana on rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta. Oikeudenkäymiskaaren 17

myös esitutkinnassa, jos tutkittavana on edellä tässä momentissa tarkoitettu rikos.

luvun 24 §:n 2 tai 3 momentissa tarkoitettu henkilö, joka saman pykälän 4 momentin nojalla voidaan velvoittaa vastaamaan pykälän 2 momentissa tarkoitettuun kysymykseen, on velvollinen vastaamaan tällaiseen kysymykseen myös esitutkinnassa, jos tutkittavana on edellä tässä momentissa tarkoitettu rikos.

## 28 §

Jos todistajalla ilmeisesti on tiedossaan seikka, joka on tärkeä syyllisyyden selvittämiseksi tai rikoksella saadun hyödyn jäljittämiseksi ja pois ottamiseksi ja hän kieltäytyy sitä ilmaisemasta, vaikka hän olisi siihen velvollinen tai 27 §:n 2 momentin mukaan oikeutettu, todistajan kuulustelu toimitetaan tutkinnanjohtajan pyynnöstä tuomioistuimessa.

Todistajan kuulustelu voidaan toimittaa siinä käräjäoikeudessa, jossa se käy sopivasti päinsä. Todistajan kuulustelussa on soveltuvin osin voimassa, mitä todistelun vastaanottamisesta pääkäsittelyn ulkopuolella oikeudenkäymiskaassa säädetään. Epäillyn ja hänen avustajansa tai asiamiehensä oikeudesta olla läsnä todistajaa kuulusteltaessa on voimassa, mitä 32 ja 35 §:ssä säädetään. Läsnäolo-oikeudesta päättää tuomioistuin tutkinnanjohtajaa kuultuaan.

Todistajalla on oikeus saada korvausta taloudellisesta menetyksestä sekä matka- ja toimeentulokustannuksista niiden perusteiden mukaan, joista säädetään valtion varoista maksettavista todistelukustannuksista annetussa laissa (666/72). Oikeutta korvaukseen ei kuitenkaan ole, jos tuomioistuin katsoo, että todistajan kieltäytyminen on ollut ilmeisen aiheeton.

## 28 §

Jos todistajalla ilmeisesti on tiedossaan seikka, joka on tärkeä syyllisyyden selvittämiseksi tai rikoksella saadun hyödyn jäljittämiseksi ja pois ottamiseksi ja hän kieltäytyy sitä ilmaisemasta, vaikka hän olisi siihen velvollinen tai 27 §:n 2 momentin mukaan oikeutettu, todistajan kuulustelu toimitetaan tutkinnanjohtajan pyynnöstä tuomioistuimessa.

*Mitä 1 momentissa säädetään sovelletaan myös todistajaan, joka kieltäytyy esittämästä asiakirjaa tai muuta todistusaineistoa.*

Todistajan kuulustelu voidaan toimittaa siinä käräjäoikeudessa, jossa se käy sopivasti päinsä. Todistajan kuulustelussa on soveltuvin osin voimassa, mitä todistelun vastaanottamisesta pääkäsittelyn ulkopuolella oikeudenkäymiskaassa säädetään. Epäillyn ja hänen avustajansa tai asiamiehensä oikeudesta olla läsnä todistajaa kuulusteltaessa on voimassa, mitä 32 ja 35 §:ssä säädetään. Läsnäolo-oikeudesta päättää tuomioistuin tutkinnanjohtajaa kuultuaan.

Todistajalla on oikeus saada korvausta taloudellisesta menetyksestä sekä matka- ja toimeentulokustannuksista niiden perusteiden mukaan, joista säädetään valtion varoista maksettavista todistelukustannuksista annetussa laissa (666/72). Oikeutta korvaukseen ei kuitenkaan ole, jos tuomioistuin katsoo, että todistajan kieltäytyminen on ollut ilmeisen aiheeton.



## 5. Laki kansainvälisestä oikeusavusta rikosasioissa annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti:

*muutetaan* 5 päivänä tammikuuta 1994 annetun kansainvälisestä oikeusavusta rikosasioissa annetun lain 23 §:n 1 momentti sellaisena kuin se on laissa 406/1995 sekä *lisätään* 15 §:ään uusi 2 momentti, jolloin nykyinen 2 ja 3 momentti siirtyvät 3 ja 4 momentiksi seuraavasti:

*Voimassaoleva oikeus*

15 §

*Pakkokeinojen käytön rajoitukset*

Jos oikeusapupyynnö tarkoittaa tai sen täyttäminen edellyttää pakkokeinolaissa (450/87) tarkoitettujen pakkokeinojen käyttämistä, ei pakkokeinoja saa käyttää, jos tämä ei Suomen lain mukaan olisi sallittua, jos pyynnön perusteena oleva teko olisi tehty Suomessa vastaavissa olosuhteissa.

Jos oikeusapupyynnö koskee rikoksesta epäillyn tai vieraassa valtiossa vireillä olevan rikosoikeudenkäynnin vastaajan kuulemista oikeusapupyynnön mukaisesti esitutkinnassa tai tuomioistuimessa, ei kuultavaa saa pyynnön perusteena olevan teon johdosta pidättää, vangita tai määrätä matkustuskieltoon.

Jos oikeusapupyynnö sisältää kutsun saapua kuultavaksi vieraan valtion viranomaisen eteen, ei Suomen viranomainen saa velvoittaa kuultavaksi kutsuttua noudattamaan kutsua taikka käyttää kuultavaksi kutsuttua vastaan pakkokeinoja kutsun noudattamatta jättämisen johdosta. Todistajan ja asianomistajan velvollisuudesta noudattaa toisen pohjoismaan tuomioistuimen antamaa kutsua säädetään velvollisuudesta saapua toisen pohjoismaan tuomioistuimeen eräissä tapauksissa annetussa laissa (349/75).

*Ehdotus*

15 §

*Pakkokeinojen käytön rajoitukset*

Jos oikeusapupyynnö tarkoittaa tai sen täyttäminen edellyttää pakkokeinolaissa (450/87) tarkoitettujen pakkokeinojen käyttämistä, ei pakkokeinoja saa käyttää, jos tämä ei Suomen lain mukaan olisi sallittua, jos pyynnön perusteena oleva teko olisi tehty Suomessa vastaavissa olosuhteissa.

*Mitä edellä 1 momentissa säädetään ei kuitenkaan koske pakkokeinolain 4 luvun 4 c §:ssä tarkoitettua datan säilyttämismääräystä.*

Jos oikeusapupyynnö koskee rikoksesta epäillyn tai vieraassa valtiossa vireillä olevan rikosoikeudenkäynnin vastaajan kuulemista oikeusapupyynnön mukaisesti esitutkinnassa tai tuomioistuimessa, ei kuultavaa saa pyynnön perusteena olevan teon johdosta pidättää, vangita tai määrätä matkustuskieltoon.

Jos oikeusapupyynnö sisältää kutsun saapua kuultavaksi vieraan valtion viranomaisen eteen, ei Suomen viranomainen saa velvoittaa kuultavaksi kutsuttua noudattamaan kutsua taikka käyttää kuultavaksi kutsuttua vastaan pakkokeinoja kutsun noudattamatta jättämisen johdosta. Todistajan ja asianomistajan velvollisuudesta noudattaa toisen pohjoismaan tuomioistuimen antamaa kutsua säädetään velvollisuudesta saapua toisen pohjoismaan tuomioistuimeen eräissä tapauksissa annetussa laissa (349/75).

## 23 §

*Pakkokeinojen käyttäminen todisteiden hankkimiseksi ja menettämisseuraamuksen täytäntöönpanon turvaamiseksi*

Vieraan valtion viranomaisen tekemän oikeusapupyynnön perusteella voidaan todisteiden hankkimiseksi panna toimeen *etsintä ja takavarikko*, suorittaa telekuuntelua, televalvontaa ja teknistä tarkkailua sekä ottaa henkilötuntemerkit, jos tätä on pyydetty oikeusapupyynnössä taikka se on tarpeen oikeusapupyynnön toimeenpanemiseksi.

-----

## 23 §

*Pakkokeinojen käyttäminen todisteiden hankkimiseksi ja menettämisseuraamuksen täytäntöönpanon turvaamiseksi*

Vieraan valtion viranomaisen tekemän oikeusapupyynnön perusteella voidaan todisteiden hankkimiseksi panna toimeen *etsintä, takavarikko ja datan säilyttämismääräys*, suorittaa telekuuntelua, televalvontaa ja teknistä tarkkailua sekä ottaa henkilötuntemerkit, jos tätä on pyydetty oikeusapupyynnössä taikka se on tarpeen oikeusapupyynnön toimeenpanemiseksi.

-----

## Sopimusteksti

### Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus

#### Johdanto

Euroopan neuvoston jäsenvaltiot ja muut tämän yleissopimuksen allekirjoittajavaltiot, jotka

ottavat huomioon, että Euroopan neuvoston päämääränä on sen jäsenten välisen yhtenäisyyden lisääminen;

ovat tietoisia muiden tämän yleissopimuksen allekirjoittajavaltioiden kanssa harjoitettavan yhteistyön edistämisen merkityksestä;

ovat vakuuttuneita siitä, että valtioille on ensisijaisen tärkeää harjoittaa yhteistä rikospolitiikkaa, jonka päämääränä on suojella yhteiskuntaa tietoverkkorikollisuudelta muun muassa asiaan liittyvän lainsäädännön ja tehokkaamman kansainvälisen yhteistyön avulla;

ovat tietoisia suurista muutoksista, joita tietoverkkojen digitalisointi, konvergenssi ja jatkuva globalisoituminen ovat aiheuttaneet;

ovat tietoisia siitä vaarasta, että tietoverkkoja ja sähköistä tietoa voidaan käyttää myös rikosten tekemiseen, sekä siitä, että tällaisiin rikoksiin liittyvää todistusaineistoa voidaan tallentaa tietoverkkoihin ja siirtää tietoverkkojen avulla;

ovat tietoisia yhteistyön tarpeesta valtioiden ja yksityisten yritysten välillä tietoverkkorikollisuuden torjumiseksi, sekä tarpeesta suojella tietotekniikan käyttöön ja kehittämiseen liittyviä oikeuksia;

uskovat, että tehokas tietoverkkorikollisuuden vastainen toiminta edellyttää laajempaa, nopeaa ja hyvin toimivaa kansainvälistä yhteistyötä rikosoikeuden alalla;

ovat vakuuttuneita siitä, että tämä yleissopimus

### 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

on tarpeen tietojärjestelmien, tietoverkkojen ja datan luottamuksellisuuden, eheyden ja käytettävyyden loukkausten sekä niiden väärinkäytön ennalta ehkäisemiseksi, koska sen avulla voidaan varmistaa, että kyseisenlainen toiminta säädetään rangaistavaksi tämän yleissopimuksen määräysten mukaisesti ja että viranomaisille annetaan näiden rikosten tehokasta torjuntaa varten riittävät toimivaltuudet, helpottaa näiden rikosten havaitsemista ja tutkintaa ja niihin liittyviä syytetoimia sekä kansallisella että kansainvälisellä tasolla, sekä mahdollistaa nopea ja luotettava kansainvälinen yhteistyö;

pitävät mielessä tarpeen varmistaa, että lainvalvonnan tarpeet ja ihmisoikeuksien suoja, joka taataan vuonna 1950 ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyssä Euroopan neuvoston yleissopimuksessa, vuonna 1966 tehdyssä Yhdistyneiden Kansakuntien kansalaisoikeuksia ja poliittisia oikeuksia koskevassa kansainvälisessä yleissopimuksessa ja muissa sovellettavissa kansainvälisissä ihmisoikeussopimuksissa, ovat sopivassa tasapainossa. Nämä sopimukset vahvistavat jokaisen mielipiteen vapauden, sananvapauden, johon sisältyy oikeus etsiä, vastaanottaa ja levittää kaikenlaisia tietoja ja ajatuksia alueellisista rajoista riippumatta, sekä yksityiselämän kunnioitukseen liittyvät oikeudet;

pitävät mielessä myös oikeuden henkilötietojen suojaan muun muassa vuonna 1981 yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä tehdyn Euroopan neuvoston yleissopimuksen mukaisesti;

ottavat huomioon vuonna 1989 tehdyn Yhdistyneiden Kansakuntien yleissopimuksen lapsen oikeuksista sekä vuonna 1999 tehdyn kansainvälisen työjärjestön yleissopimuksen pahimpien lapsityön muotojen kieltämisestä;

ottavat huomioon olemassa olevat Euroopan neuvoston yleissopimukset yhteistyöstä rikosoikeuden alalla, sekä vastaavat Euroopan neuvoston jäsenvaltioiden ja muiden valtioiden

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

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

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

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

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and

väliset sopimukset, ja korostavat, että tämän yleissopimuksen tarkoituksena on täydentää kyseisiä yleissopimuksia tehostamalla tietojärjestelmiin ja datasiirtoon liittyvien rikosten tutkintaa ja niihin liittyviä oikeudenkäyntejä ja mahdollistamalla rikoksiin liittyvän sähköisessä muodossa olevan todistusaineiston keräämisen;

suhtautuvat myönteisesti viimeaikaiseen kehitykseen, joka lisää edelleen tietoverkkorikollisuuden torjuntaan liittyvää kansainvälistä osaamista ja yhteistyötä, mukaan luettuna Yhdistyneiden Kansakuntien, OECD:n, Euroopan Unionin ja G8-ryhmän puitteissa toteutetut toimenpiteet;

palauttavat mieleen ministerineuvoston suosituksen R(85)10, joka koskee keskinäistä oikeusapua rikosasioissa koskevan eurooppalaisen yleissopimuksen soveltamista telekuunteluun liittyviin oikeusapupyyntöihin, suosituksen R(88)2, joka koskee piraattikopioita tekijänoikeuksien ja lähioikeuksien alalla, suosituksen R(87)15, joka koskee henkilötietojen käsittelyä poliisitoiminnassa, suosituksen R (95)4 henkilötietojen suojasta televiestintäpalveluiden alalla ja erityisesti puhelinpalveluiden alalla, sekä suosituksen R(89)9, joka koskee tietokoneavusteisia rikoksia ja jossa annetaan suuntaviivat kansallista lainsäätäjää varten tiettyjen tietotekniikkarikosten määrittelyn osalta, ja suosituksen R(95)13, joka koskee tietotekniikkaan liittyviä rikosprosessioikeuden ongelmia;

ottavat huomioon Euroopan oikeusministerien 21. konferenssissaan (Prahassa 10 ja 11 päivänä kesäkuuta 1997 hyväksymän päätöslauselman nro 1, jossa suositellaan, että ministerineuvosto tukee Euroopan neuvoston rikosasiain yhteistyökomitean (CDPC) tietoverkkorikollisuutta koskevaa työtä, jonka päämääränä on yhtenäistää kansallisia rikosoikeuden säännöksiä ja mahdollistaa tehokkaiden keinojen käyttö tietoverkkorikosten tutkinnassa, sekä Euroopan oikeusministerien 23. konferenssissaan (Lontoossa 8 ja 9 päivänä kesäkuuta 2000) hyväksymän päätöslauselman

other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

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

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

nro 3, jossa neuvottelujen osapuolia kannustetaan etsimään sellaisia tarkoituksenmukaisia ratkaisuja, joiden avulla mahdollisimman moni valtio voi tulla yleissopimuksen sopimuspuoleksi, ja jossa tiedostetaan tarve luoda nopea ja tehokas kansainvälinen yhteistyöjärjestelmä siten, että tietoverkkorikollisuuden torjunnan erityisvaatimukset otetaan asianmukaisesti huomioon;

ottavat myös huomioon toimintasuunnitelman, jonka Euroopan neuvoston valtion- ja hallitustenpäämiehet hyväksyivät toisessa huippukokouksessaan (Strasbourgissa 10 ja 11 päivänä lokakuuta 1997), ja jonka tarkoituksena on etsiä yhteisiä, Euroopan neuvoston vaatimuksiin ja arvoihin perustuvia keinoja vastata uuden informaatiotekniikan kehitykseen;

ovat sopineet seuraavasta:

## I LUKU KÄSITTEIDEN KÄYTTÖ

### 1 artikla Määritelmät

Tässä yleissopimuksessa:

- a) ”tietojärjestelmä” tarkoittaa laitetta tai toisiinsa kytkettyjä tai liitettyjä laitteita, joista yksi tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten;
- b) ”data” tarkoittaa sellaisessa muodossa olevien tosiseikkojen, tietojen tai käsitteiden esitystä, että se soveltuu käsiteltäväksi tietojärjestelmässä, mukaan lukien ohjelmat, joiden avulla tietojärjestelmä pystyy suorittamaan jonkin toiminnon;
- c) ”palveluntarjoaja” tarkoittaa:
  - i) julkista tai yksityistä yksikköä, joka tarjoaa palveluidensa käyttäjille mahdollisuuden tietojärjestelmän välityksellä tapahtuvaan viestintään, ja
  - ii) muuta yksikköä, joka käsittelee tai tallentaa dataa edellä mainitun palveluntarjoajan tai

negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

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

Have agreed as follows:

## CHAPTER I USE OF TERMS

### Article 1 Definitions

For the purposes of this Convention:

- a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
- b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
- c) "service provider" means:
  - i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
  - ii) any other entity that processes or stores computer data on behalf of such communication

palveluiden käyttäjien puolesta;

d) ”liikennetiedot” tarkoittaa tietojärjestelmän välityksellä siirrettyyn viestiin liittyvää dataa, jonka viestinsiirtoketjuun kuuluva tietoverkko on tuottanut, ja josta ilmenee viestin alkuperä, määränpää, reitti, kellonaika, päivämäärä, koko, kesto, tai siihen liittyvän palvelun tyyppi.

service or users of such service;

d) “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

## **II LUKU KANSALLISET TOIMENPITEET**

## **CHAPTER II MEASURES TO BE TAKEN AT THE NATIONAL LEVEL**

### **1 jakso Rikosoikeuden aineelliset säännökset**

### **Section 1 Substantive criminal law**

#### **1 osasto Datasiirron ja tietojärjestelmien luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat rikokset**

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

#### **2 artikla Luvaton tunkeutuminen**

#### **Article 2 Illegal access**

Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen tahallisen tietojärjestelmään tai sen osaan tunkeutumisen kansallisen lainsäädäntönsä mukaisesti rangaistavaksi teoksi. Sopimuspuoli voi asettaa rangaistavuuden edellytykseksi sen, että rikos on tehty turvajärjestelyt murtamalla, tarkoituksin päästä käsiksi dataan, tai muuta epärehellistä tarkoitusta varten, tai että se liittyy sellaiseen tietojärjestelmään, joka on kytketty toiseen tietojärjestelmään.

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.

#### **3 artikla Viestintäsalaisuuden loukkaaminen**

#### **Article 3 Illegal interception**

Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi tahallisen ja oikeudettoman teknisin keinoin tapahtuvan tiedon hankkimisen tietojärjestelmän sisäisestä tai tietojärjestelmien välisestä luottamuksellisesta datasta ja sen siirrosta, sekä tällaista dataa sisältävästä tietojärjestelmästä lähtevästä sähkömagneettisesta säteilystä. Sopimuspuoli voi asettaa rangaistavuuden edellytykseksi sen, että rikos on tehty epärehellisin tarkoituksin, tai että se liittyy sellaiseen tietojärjestelmään, joka

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

on kytketty toiseen tietojärjestelmään.

#### **4 artikla Datan vahingoittaminen**

1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi tahallisen ja oikeudettoman datan vahingoittamisen, tuhoamisen, turmelemisen, muuttamisen tai poistamisen.

2. Sopimuspuoli voi tehdä varauman, jonka mukaan rangaistavuuden edellytyksenä on, että 1 kappaleessa tarkoitettu teko aiheuttaa huomattavaa vahinkoa.

#### **5 artikla Tietojärjestelmän häirintä**

Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi tahallisen ja oikeudettoman tietojärjestelmän toiminnan vakavan estämisen dataa syöttämällä, siirtämällä, vahingoittamalla, tuhoamalla, turmelemalla, muuttamalla tai poistamalla.

#### **6 artikla Laitteiden väärinkäyttö**

1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen kansallisen lainsäädäntönsä mukaisesti rangaistaviksi seuraavat tahalliset ja oikeudettomat teot:

a) seuraavien tuottaminen, myynti, hankkiminen, tuonti, levittäminen tai muu saataville asettaminen:

i) väline, mukaan luettuna tietokoneohjelma, joka on suunniteltu tai muutettu ensisijaisesti tämän yleissopimuksen 2-5 artiklan mukaisesti rangaistaviksi säädettyjen rikosten tekemistä varten;

ii) tietojärjestelmän salasana tai käyttäjätunnus tai muu vastaava tieto, joka mahdollistaa pääsyn tietojärjestelmään tai sen osaan,

tarkoituksin, että sitä käytetään tämän

#### **Article 4 Data interference**

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

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

#### **Article 5 System interference**

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

#### **Article 6 Misuse of devices**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a) the production, sale, procurement for use, import, distribution or otherwise making available of:

i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of



yleissopimuksen 2-5 artiklan mukaisesti rangaistaviksi säädettyjen rikosten tekemiseen.

b) tämän kappaleen a kohdan i tai ii alakohdassa tarkoitettujen tuotteiden hallussapito, tarkoituksin käyttää sitä 2-5 artiklan mukaisesti rangaistaviksi säädettyjen rikosten tekemiseen. Sopimuspuoli voi asettaa rikosvastuun syntymisen edellytykseksi sen, että tekijän hallussa on useita tällaisia tuotteita.

2. Tämän artiklan määräysten ei katsota perustavan rikosvastuuta muun muassa silloin kun tämän artiklan 1 kappaleessa tarkoitettujen tuotteiden, myynnin, hankkimisen, tuonnin, levittämisen tai muun saataville asettamisen tarkoituksena ei ole tehdä tämän yleissopimuksen 2-5 artiklan mukaisesti rangaistavaksi säädettyä rikosta, vaan tietojärjestelmän luvallinen testaus tai suojeleminen.

3. Kukin sopimuspuoli voi tehdä varauksen, jonka mukaan se ei sovelle tämän artiklan 1 kappaletta, edellyttäen kuitenkin, että varaus ei koske tämän artiklan 1 kappaleen a kohdan ii alakohdassa tarkoitettujen tuotteiden myyntiä, levittämistä tai muuta saataville asettamista.

## **2 osasto Tietokoneavusteiset rikokset**

### **7 artikla Tietokoneavusteinen väärennös**

Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi sellaisen tahallisen ja oikeudettoman datan syöttämisen, muuttamisen, tuhoamisen tai poistamisen, jonka tuloksena syntyvä väärä data on tarkoitettu käytettäväksi oikeudellisissa tarkoituksissa harhauttavana todisteena, riippumatta siitä onko data sellaisenaan luettavissa tai ymmärrettävissä. Sopimuspuoli voi asettaa rikosvastuun syntymisen edellytykseksi sen, teko on toteutettu petostarkoituksin tai muuta epärehellistä tarkoitusta varten.

committing any of the offences established in Articles 2 through 5; and

b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

## **Title 2 Computer-related offences**

### **Article 7 Computer-related forgery**

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

### **8 artikla Tietokoneavusteinen petos**

Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi tahallisen ja oikeudettoman taloudellisen vahingon aiheuttamisen toiselle, kun teko on tehty:

- a) dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla;
- b) tietojärjestelmän toimintaa häiritsemällä,

tarkoituksin saada itselle tai toiselle taloudellista hyötyä petoksella tai muulla epärehellisellä keinolla.

### **3 osasto Viestin sisältöön liittyvät rikokset**

#### **9 artikla Lapsipornografiaan liittyvät rikokset**

1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi tahallisen ja oikeudettoman:

- a) lapsipornografian tuottamisen tietojärjestelmän välityksellä tapahtuvaa levittämistä varten;
- b) lapsipornografian tarjoamisen tai saataville asettamisen tietojärjestelmän välityksellä;
- c) lapsipornografian levittämisen tai siirtämisen tietojärjestelmän välityksellä;
- d) lapsipornografian hankkimisen omaan tai toisen käyttöön tietojärjestelmän välityksellä;
- e) lapsipornografian hallussapidon tietojärjestelmässä tai tietovälineellä.

2. Tämän artiklan 1 kappaletta sovellettaessa ”lapsipornografialla” tarkoitetaan myös pornografista kuvatallennetta, jossa esitetään:

### **Article 8 Computer-related fraud**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

- a) any input, alteration, deletion or suppression of computer data;
- b) any interference with the functioning of a computer system,

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

### **Title 3 Content-related offences**

#### **Article 9 Offences related to child pornography**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

- a) producing child pornography for the purpose of its distribution through a computer system;
- b) offering or making available child pornography through a computer system;
- c) distributing or transmitting child pornography through a computer system;
- d) procuring child pornography through a computer system for oneself or for another person;
- e) possessing child pornography in a 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) alaikäistä seksuaalisessa kanssakäymisessä;
- b) alaikäiseltä näyttävää henkilöä seksuaalisessa kanssakäymisessä;
- c) todellisuudenmukaisia kuvia alaikäisestä seksuaalisessa kanssakäymisessä.

3. Tämän artiklan 2 kappaletta sovellettaessa ”alaikäisellä” tarkoitetaan jokaista alle 18-vuotiasta henkilöä. Sopimuspuoli voi soveltaa myös alemmaa ikärajaa, joka ei kuitenkaan saa olla alempi kuin 16 vuotta.

4. Kukin sopimuspuoli voi tehdä varauman, jonka mukaan se ei sovelta kokonaan tai osittain 1 kappaletta d ja e kohtaa ja 2 kappaletta b ja c kohtaa.

#### **4 osasto Tekijänoikeusrikokset ja tekijänoikeuden lähioikeuksia koskevat rikokset**

#### **10 artikla Tekijänoikeusrikokset ja tekijänoikeuden lähioikeuksia koskevat rikokset**

1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi siinä määriteltävän tahallisen tekijänoikeuden loukkauksen, niiden velvoitteidensa mukaisesti, joihin se on sitoutunut kirjallisten ja taiteellisten teosten suojaamisesta tehtyä Bernin yleissopimusta muuttavassa, 24 päivänä heinäkuuta 1971 tehdyssä Pariisin asiakirjassa, teollis- ja tekijänoikeuksien kauppaan liittyviä näkökohtia koskevassa sopimuksessa ja WIPO:n tekijänoikeussopimuksessa, silloin kun teko on tehty kaupallista tarkoitusta varten tietojärjestelmän avulla, ei kuitenkaan näiden yleissopimusten takaamien moraalisten oikeuksien osalta.

2. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin

- a) a minor engaged in sexually explicit conduct;
- b) a person appearing to be a minor engaged in sexually explicit conduct;
- c) realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

#### **Title 4 Offences related to infringements of copyright and related rights**

#### **Article 10 Offences related to infringements of copyright and related rights**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish

säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi siinä määriteltävän tahallisen tekijänoikeuden lähioikeuden loukkauksen, niiden velvoitteidensa mukaisesti, joihin se on sitoutunut esittävien taiteilijoiden, äänitteiden valmistajien sekä radioyriyten suojaamisesta Roomassa tehdyssä kansainvälisessä yleissopimuksessa (Rooman yleissopimus), teollis- ja tekijänoikeuksien kauppaan liittyviä näkökohtia koskevassa sopimuksessa ja WIPO:n esitys- ja äänitesopimuksessa, silloin kun teko on tehty kaupallista tarkoitusta varten tietojärjestelmän avulla, ei kuitenkaan näiden yleissopimusten takaamien moraalisten oikeuksien osalta.

3. Sopimuspuoli voi tehdä varauman, jonka mukaan se ei sovelle tämän artiklan 1 ja 2 kappaleen mukaista rikosvastuuta rajoitetuissa tapauksissa, edellyttäen kuitenkin, että niillä, joiden oikeuksia on loukattu, on käytettävissään muita tehokkaita oikeussuojakeinoja, eikä varauma merkitse poikkeusta sopimuspuolen kansainvälisistä velvoitteista, jotka perustuvat tämän artiklan 1 ja 2 kappaleessa mainittuihin kansainvälisiin asiakirjoihin.

## **5 osasto Osallisuus, yhteisövastuu ja sanktiot**

### **11 artikla Rikoksen yritys sekä avunanto tai yllytys rikokseen**

1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen tahallisen avunannon ja yllytyksen tämän yleissopimuksen 2-10 artiklan mukaisiin rikoksiin kansallisen lainsäädäntönsä mukaisesti rangaistaviksi teoiksi silloin kun teon tarkoituksena on aikaansaada rikoksen täyttyminen.

2. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen tämän yleissopimuksen 3-5, 7 ja 8 artiklan sekä 9 artiklan 1 kappaleen a ja c kohdan mukaisten rikosten tahallisen yrityksen kansallisen lainsäädäntönsä mukaisesti rangaistavaksi teoksi.

3. Kukin valtio voi tehdä varauman, jonka

as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

## **Title 5 Ancillary liability and sanctions**

### **Article 11 Attempt and aiding or abetting**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3. Each Party may reserve the right not to apply,

mukaan se ei sovelleta kokonaan tai osittain tämän artiklan 2 kappaletta.

## 12 artikla Yhteisövastuu

1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin varmistaa vastuuseen tämän yleissopimuksen mukaisesti rangaistavaksi säädetystä teosta, jonka luonnollinen henkilö on tehnyt oikeushenkilön hyväksi joko itsenäisesti tai oikeushenkilön nimissä, silloin kun asianomainen henkilö on oikeushenkilössä johtavassa asemassa, joka perustuu:

- a) valtuutukseen edustaa kyseistä oikeushenkilöä;
- b) valtuutukseen tehdä päätöksiä kyseisen oikeushenkilön puolesta;
- c) valtuutukseen harjoittaa oikeushenkilön sisäistä valvontaa.

2. Sen lisäksi mitä tämän artiklan 1 kappaleessa määrätään, sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin varmistaa vastuuseen myös silloin kun 1 kappaleessa tarkoitettu luonnollinen henkilö on laiminlyönyt valvonnan, ja kyseisen oikeushenkilön valtuuttaman luonnollisen henkilön on sen vuoksi ollut mahdollista tehdä tämän yleissopimuksen mukaisesti rangaistavaksi säädetty rikos kyseisen oikeushenkilön hyödyksi.

3. Jollei sopimuspuolen soveltamista oikeusperiaatteista muuta johdu, oikeushenkilön vastuu voi olla rikos-, yksityis- tai hallinto-oikeudellista.

4. Oikeushenkilön vastuu ei vaikuta rikoksen tehneen luonnollisen henkilön rikosvastuuseen.

## 13 artikla Sanktiot ja muut seuraamukset

1. Kukin sopimuspuoli ryhtyy tarvittaviin

in whole or in part, paragraph 2 of this article.

## Article 12 Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

- a) a power of representation of the legal person;
- b) an authority to take decisions on behalf of the legal person;
- c) an authority to exercise control within the legal person.

2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

## Article 13 Sanctions and measures

1. Each Party shall adopt such legislative and

lainsäädännöllisiin ja muihin toimenpiteisiin varmistaa, että 2-11 artiklan mukaisesti rangaistaviksi säädettyihin tekoihin syyllistyneille voidaan määrätä tehokkaat, tekoon nähden oikeassa suhteessa olevat ja riittävät rangaistukset, mukaan luettuna vankeusrangaistus.

2. Kukin sopimuspuoli varmistaa, että 12 artiklan mukaisesti vastuuseen saatetuille oikeushenkilöille voidaan määrätä tehokas, tekoon nähden oikeassa suhteessa oleva ja riittävä rangaistus tai muu sanktio tai seuraamus, mukaan luettuna sakkorangaistus.

## **2 jakso Prosessioikeus**

### **1 osasto Yhteiset määräykset**

#### **14 artikla Oikeudenkäyntimenettelyä koskevien määräysten soveltamisala**

1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen tämän jakson määräysten mukaisten toimivaltuuksien ja menettelytapojen soveltamisesta yksittäiseen rikostutkintaan tai rikosoikeudenkäyntiin.

2. Jollei 21 artiklassa nimenomaisesti toisin määrätä, kukin sopimuspuoli soveltaa tämän artiklan 1 kappaleessa tarkoitettuja toimivaltuuksia ja menettelytapoja:

- a) tämän yleissopimuksen 2-11 artiklan mukaisesti rangaistaviksi teoiksi säädettyihin rikoksiin;
- b) muihin tietojärjestelmän avulla tehtyihin rikoksiin; ja
- c) rikokseen liittyvän sähköisessä muodossa olevan todistusaineiston keräämiseen.

3. a) Kukin sopimuspuoli voi tehdä varauman, jonka mukaan se soveltaa 20 artiklassa tarkoitettuja toimenpiteitä ainoastaan varaumassa yksilöityihin rikoksiin tai rikostyyppeihin, edellyttäen kuitenkin, että näiden rikosten tai rikostyyppien valikoima ei

other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

## **Section 2 Procedural law**

### **Title 1 Common provisions**

#### **Article 14 Scope of procedural provisions**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

- a) the criminal offences established in accordance with Articles 2 through 11 of this Convention;
- b) other criminal offences committed by means of a computer system; and
- c) the collection of evidence in electronic form of a criminal offence.

3. a) Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it

ole suppeampi kuin niiden rikosten valikoima, joihin se soveltaa 21 artiklassa tarkoitettuja toimenpiteitä. Kukin sopimuspuoli harkitsee tällaisen varauman rajoittamista siten, että 20 artiklassa tarkoitettuja toimenpiteitä voidaan soveltaa mahdollisimman laajalti.

b) Mikäli sopimuspuoli ei tämän yleissopimuksen hyväksymisajankohtana voimassa olevien lainsäädäntönsä asettamien rajoitusten vuoksi pysty soveltamaan 20-21 artiklassa tarkoitettuja toimenpiteitä palveluntarjoajan tietojärjestelmän sisäisesti siirrettyihin viesteihin silloin kun

i) tietojärjestelmällä on rajattu käyttäjäryhmä, ja

ii) tietojärjestelmää ei käytetä julkisten tietoverkkojen avulla eikä sitä ole kytketty toiseen julkiseen tai yksityiseen tietojärjestelmään,

kyseinen sopimuspuoli voi tehdä varauman, jonka mukaan se ei sovelta näitä toimenpiteitä kyseisenlaisiin viesteihin. Kukin sopimuspuoli harkitsee tällaisen varauman rajoittamista siten, että 20 ja 21 artiklassa tarkoitettuja toimenpiteitä voidaan soveltaa mahdollisimman laajalti.

### **15 artikla Soveltamiseen liittyvät rajoitukset ja takeet**

1. Kukin sopimuspuoli varmistaa, että tämän jakson määräysten mukaisten toimivaltuuksien ja menettelytapojen käyttöönottoa, täytäntöönpanoa ja soveltamista koskevat sen kansalliseen lainsäädäntöön perustuvat rajoitukset ja takeet, joihin sisältyy suhteellisuusperiaate, varmistuen riittävän ihmisoikeuksien ja perusvapauksien suojan, mukaan luettuna oikeudet, joihin sopimuspuoli on sitoutunut vuonna 1950 ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyssä Euroopan neuvoston yleissopimuksessa, vuonna 1966 tehdyssä Yhdistyneiden Kansakuntien kansalaisoikeuksia ja poliittisia oikeuksia koskevassa kansainvälisessä yleissopimuksessa ja muissa sovellettavissa kansainvälisissä ihmisoikeussopimuksissa.

applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b) Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i) is being operated for the benefit of a closed group of users, and

ii) does not employ public communications networks and is not connected with another computer system, whether public or private,

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

### **Article 15 Conditions and safeguards**

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Edellä mainittuihin rajoituksiin ja takeisiin sisältyy, sen mukaan kuin se on tarkoituksenmukaista kyseisen toimivaltuuden tai menettelytavan luonteen huomioon ottaen, muun muassa tuomioistuimen tai muun riippumattoman tahon suorittamaa valvontaa, toimivaltuuden tai menettelytavan soveltamiseen oikeuttavat perusteet sekä sen soveltamisen asiallinen ja ajallinen rajaus.

3. Sopimuspuoli ottaa huomioon tämän jakson mukaisten toimivaltuuksien ja menettelytapojen vaikutuksen kolmansien osapuolten oikeuksiin, velvollisuuksiin ja oikeutettuihin etuihin siinä määrin kuin tämä on yleisen edun mukaista ja erityisesti järkevän lainkäytön mukaista.

## **2 osasto Tallennetun datan säilyttämisen nopea varmistaminen**

### **16 artikla Tallennetun datan säilyttämisen nopea varmistaminen**

1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin antaakseen toimivaltaisille viranomaisilleen valtuudet määrätä tai muutoin varmistaa nopeasti sellaisen yksilöidyn datan säilyttäminen, mukaan luettuna liikennetiedot, joka on tallennettu tietojärjestelmän avulla, erityisesti silloin kun viranomaisilla on syytä uskoa, että datan häviäminen tai muuttaminen on erityisen todennäköistä.

2. Mikäli sopimuspuoli panee tämän artiklan 1 kappaleen täytäntöön mahdollistamalla määräyksen antamisen henkilölle hänen hallussaan tai hallinnassaan olevan yksilöidyn datan säilyttämisestä, kyseinen sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin, joiden avulla kyseinen henkilö voidaan velvoittaa turvaamaan mainitun datan eheys riittävän pituiseksi määräajaksi, joka on enintään 90 päivää, jotta sen toimivaltaiset viranomaiset voivat saada datan sisällön selvitettyksi. Sopimuspuoli voi myös säätää tämän määräajan pidentämisen

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

## **Title 2 Expedited preservation of stored computer data**

### **Article 16 Expedited preservation of stored computer data**

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.



mahdollisuudesta.

3. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin velvoittaakseen datan haltijan tai muun datan säilyttämisen varmistamiseen velvoitetun henkilön pitämään edellä mainitun menettelyn salassa sen lainsäädännön mukaiseksi määräajaksi.

4. Tässä artiklassa tarkoitettuihin toimivaltuuksiin ja menettelytapoihin sovelletaan 14 ja 15 artiklan määräyksiä.

### **17 artikla Liikennetietojen säilyttämisen nopea varmistaminen ja osittainen luovutus**

1. Kukin sopimuspuoli ryhtyy 16 artiklan mukaisesti säilytettäviä liikennetietoja koskeviin tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin:

a) varmistaakseen, että nämä liikennetiedot voidaan määrätä nopeasti säilytettäväksi riippumatta siitä, onko viestin siirrossa ollut mukana yksi tai useampi palveluntarjoaja; ja

b) varmistaakseen riittävien liikennetietojen nopean luovutuksen toimivaltaisille viranomaisilleen tai kyseisten viranomaisten nimeämälle henkilölle, jotta sopimuspuoli voi tunnistaa palveluntarjoajat ja polun, jota pitkin viesti on siirretty.

2. Tässä artiklassa tarkoitettuihin toimivaltuuksiin ja menettelytapoihin sovelletaan 14 ja 15 artiklan määräyksiä.

### **3 osasto Esittämismääräys**

#### **18 artikla Esittämismääräys**

1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin antaakseen toimivaltaisille viranomaisilleen valtuudet määrätä:

a) kyseisen sopimusvaltion alueella oleva henkilö esittämään hallussaan tai hallinnassaan

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

### **Article 17 Expedited preservation and partial disclosure of traffic data**

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

### **Title 3 Production order**

#### **Article 18 Production order**

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a) a person in its territory to submit specified computer data in that person's possession or

oleva yksilöity data, joka on tallennettu tietojärjestelmään tai tietovälineeseen; ja

b) kyseisen sopimusvaltion alueella palveluita tarjoava palveluntarjoaja esittämään palveluiden tilaajia koskevia tietoja, jotka ovat kyseisen palveluntarjoajan hallussa tai hallinnassa.

2. Tässä artiklassa tarkoitettuihin toimivaltuuksiin ja menettelytapoihin sovelletaan 14 ja 15 artiklan määräyksiä.

3. Tätä artiklaa sovellettaessa ”tilaajia koskevilla tiedoilla” tarkoitetaan kaikkia palveluntarjoajan tarjoamien palveluiden tilaajia koskevia tietoja, jotka eivät ole liikennetietoja tai viestin sisältöä koskevia tietoja, ja joita palveluntarjoaja säilyttää tietojärjestelmään tallennettuina tai missä tahansa muussa muodossa, ja joista ilmenevät:

a) käytetyn viestintäpalvelun tyyppi, sitä koskevat tekniset järjestelyt ja palvelun kesto;

b) tilaajan henkilöllisyys, posti- tai käyntiosoite, puhelinnumero ja muut yhteystiedot sekä laskutus- ja maksutiedot, jotka perustuvat palvelusopimukseen tai –järjestelyyn;

c) muut viestintälaitteiden sijaintipaikkaa koskevat tiedot, jotka perustuvat palvelusopimukseen tai –järjestelyyn.

#### **4 osasto Tallennettuun dataan kohdistuva etsintä ja takavarikko**

##### **19 artikla Tallennettuun dataan kohdistuva etsintä ja takavarikko**

1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin antaakseen toimivaltaisille viranomaisilleen omalla alueellaan valtuudet suorittaa etsintä, joka kohdistuu:

a) tietojärjestelmään tai sen osaan ja niihin tallennettuun dataan; ja

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

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

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3. For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a) the type of communication service used, the technical provisions taken thereto and the period of service;

b) the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

#### **Title 4 Search and seizure of stored computer data**

##### **Article 19 Search and seizure of stored computer data**

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a) a computer system or part of it and computer data stored therein; and

b) datan tallentamiseen soveltuvaan tietovälineeseen,

tai muulla vastaavalla tavalla hankkia pääsy mainittuihin järjestelmään, järjestelmän osaan, dataan ja tietovälineeseen.

2. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin varmistaakseen, että sen viranomaiset, jotka ovat suorittaneet tiettyyn tietojärjestelmään tai sen osaan kohdistuvan etsinnän tai muulla vastaavalla tavalla hankkineet pääsyn niihin 1 kappaleen a kohdan mukaisesti, voivat nopeasti laajentaa etsinnän tai muulla tavoin tapahtuvan pääsyn hankinnan myös toiseen tietojärjestelmään, silloin kun kyseisillä viranomaisilla on syytä uskoa, että etsinnän kohteena oleva data on tallennettu toiseen kyseisen sopimuspuolen alueella olevaan tietojärjestelmään tai sen osaan, ja tämä data on laillisesti saatavilla ensin mainitun järjestelmän avulla.

3. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin antaakseen toimivaltaisille viranomaisilleen valtuudet takavarikoida tai muulla vastaavalla tavalla turvata 1 ja 2 kappaleen mukaisen etsinnän kohteena oleva data. Näihin toimenpiteisiin sisältyy valtuus:

a) takavarikoida tai muulla vastaavalla tavalla turvata tietojärjestelmä tai sen osa tai tietoväline;

b) tehdä ja säilyttää kopio takavarikoidusta datasta;

c) turvata merkityksellisen tallennetun datan eheys;

d) estää pääsy tietojärjestelmästä etsinnän kohteena olevaan dataan tai poistaa se järjestelmästä.

4. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin antaakseen toimivaltaisille viranomaisilleen valtuudet määrätä henkilö, jolla on tietoa

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

tietojärjestelmän toiminnasta tai siihen sisältyvän datan suojaamiseen sovelletuista menetelmistä, esittämään tarvittavat tiedot, siinä määrin kuin se katsotaan kohtuulliseksi, jotta ne voivat ryhtyä tämän artiklan 1 ja 2 kappaleessa tarkoitettuihin toimenpiteisiin.

5. Tässä artiklassa tarkoitettuihin toimivaltuuksiin ja menettelytapoihin sovelletaan 14 ja 15 artiklan määräyksiä.

## **5 osasto Tiedon hankkiminen datasta reaaliajassa**

### **20 artikla Tiedon hankkiminen liikennetiedoista reaaliajassa**

1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin antaakseen toimivaltaisille viranomaisilleen valtuudet:

a) hankkia tai tallentaa kyseisen sopimuspuolen alueella teknisin keinoin, ja

b) velvoittaa palveluntarjoaja sen olemassa olevan teknisen valmiuden puitteissa:

i) hankkimaan tai tallentamaan kyseisen sopimuspuolen alueella teknisin keinoin; tai

ii) toimimaan yhteistyössä toimivaltaisten viranomaisten kanssa ja avustamaan niitä, kun nämä hankkivat tai tallentavat,

reaaliajassa tietoja liikennetiedoista, jotka liittyvät yksilöityjen viestien siirtämiseen tietojärjestelmän avulla kyseisen sopimusvaltion alueella.

2. Mikäli sopimuspuoli ei voi kansallisen oikeusjärjestelmänsä vakiintuneiden periaatteiden johdosta ryhtyä 1 kappaleen a kohdassa tarkoitettuihin toimenpiteisiin, se voi ryhtyä tarvittaviin vaihtoehtoihin lainsäädännöllisiin ja muihin toimenpiteisiin varmistaakseen alueellaan lähetettyihin yksilöityihin viesteihin liittyvien tietojen hankkimisen tai tallentamisen reaaliajassa

computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

## **Title 5 Real-time collection of computer data**

### **Article 20 Real-time collection of traffic data**

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and

b) compel a service provider, within its existing technical capability:

i) to collect or record through the application of technical means on the territory of that Party; or

ii) to co-operate and assist the competent authorities in the collection or recording of,

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

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

kyseisen sopimuspuolen alueella teknisin keinoin.

3. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin velvoittaakseen palveluntarjoajan pitämään salassa tämän artiklan mukaisten toimivaltuuksien käytön ja niihin liittyvät tiedot.

4. Tässä artiklassa tarkoitettuihin toimivaltuuksiin ja menettelytapoihin sovelletaan 14 ja 15 artiklan määräyksiä.

## **21 artikla Tiedon hankkiminen viestin sisällöstä**

1. Kukin sopimuspuoli ryhtyy tiettyjen kansallisen lainsäädäntönsä määrittämien törkeiden rikosten osalta tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin antaakseen toimivaltaisille viranomaisilleen valtuudet:

a) hankkia tai tallentaa kyseisen sopimuspuolen alueella teknisin keinoin, ja

b) velvoittaa palveluntarjoaja sen olemassa olevan teknisen valmiuden puitteissa:

i) hankkimaan tai tallentamaan kyseisen sopimuspuolen alueella teknisin keinoin; tai

ii) toimimaan yhteistyössä toimivaltaisten viranomaisten kanssa ja avustamaan niitä, kun nämä hankkivat tai tallentavat,

reaaliajassa tietoja sopimusvaltion alueella tietojärjestelmän avulla siirrettyjen yksilöityjen viestien sisällöstä.

2. Mikäli sopimuspuoli ei voi kansallisen oikeusjärjestelmänsä vakiintuneiden periaatteiden johdosta ryhtyä 1 kappaleen a kohdassa tarkoitettuihin toimenpiteisiin, se voi ryhtyä tarvittaviin vaihtoehtoihin lainsäädännöllisiin ja muihin toimenpiteisiin varmistaakseen alueellaan teknisin keinoin siirrettyjen yksilöityjen viestien sisältöä koskevien tietojen reaaliaikaisen hankkimisen

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

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

## **Article 21 Interception of content data**

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and

b) compel a service provider, within its existing technical capability:

i) to collect or record through the application of technical means on the territory of that Party, or

ii) to co-operate and assist the competent authorities in the collection or recording of,

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

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

tai tallentamisen.

3. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin velvoittaakseen palveluntarjoajan pitämään salassa tämän artiklan mukaisten toimivaltuuksien käytön ja niihin liittyvät tiedot.

4. Tässä artiklassa tarkoitettuihin toimivaltuuksiin ja menettelytapoihin sovelletaan 14 ja 15 artiklan määräyksiä.

### **3 jakso Lainkäyttövalta**

#### **22 artikla Lainkäyttövalta**

1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin ulottaakseen lainkäyttövaltansa tämän yleissopimuksen 2-11 artiklan mukaisesti rangaistaviksi säädettyihin tekoihin silloin kun:

- a) rikos on tehty sen alueella; tai
- b) rikos on tehty sen lippua käyttävässä aluksessa; tai
- c) sen lakien mukaisesti rekisteröidyssä ilma-aluksessa; tai
- d) rikoksentekijä on sen kansalainen, jos rikos on rangaistava myös tekopaikan lain mukaan, tai kun rikos on tehty millekään valtiolle kuulumattomalla alueella.

2. Kukin sopimuspuoli voi tehdä varauman, jonka mukaan se ei sovelle tai soveltaa ainoastaan tiettyihin tapauksiin tai tietyin edellytyksin tämän artiklan 1 kappaleen b-d kohtaan tai johonkin niistä sisältyviä lainkäyttövaltaa koskevia määräyksiä.

3. Kukin sopimuspuoli ryhtyy tarvittaviin toimenpiteisiin ulottaakseen lainkäyttövaltansa tämän yleissopimuksen 24 artiklan 1 kappaleessa tarkoitettuihin rikoksiin silloin kun epäilty rikoksentekijä tavataan sen alueella eikä se rikoksen johdosta tapahtuvaa luovuttamista koskevan pyynnön saatuaan luovuta häntä toiselle sopimuspuolelle pelkästään hänen

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

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

### **Section 3 Jurisdiction**

#### **Article 22 Jurisdiction**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

- a) in its territory; or
- b) on board a ship flying the flag of that Party; or
- c) on board an aircraft registered under the laws of that Party; or
- d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

kansalaisuutensa perusteella.

4. Tämä yleissopimus ei sulje pois kansallisen lainsäädännön mukaisesti harjoitettua rikosoikeudellista lainkäyttövaltaa.

5. Jos useampi sopimuspuoli ilmoittaa aikomuksestaan käyttää lainkäyttövaltaansa tämän yleissopimuksen mukaisesti rangaistavaksi teoksi säädetyn väitetyn rikoksen osalta, asianomaiset sopimuspuolet neuvottelevat keskenään, jos se on tarkoituksenmukaista, ratkaistakseen mikä lainkäyttöpaikka soveltuu parhaiten syytetoimia varten.

### **III LUKU KANSAINVÄLINEN YHTEISTYÖ**

#### **1 jakso Yleiset periaatteet**

##### **1 osasto Kansainvälistä yhteistyötä koskevat yleiset periaatteet**

##### **23 artikla Kansainvälistä yhteistyötä koskevat yleiset periaatteet**

Sopimuspuolet toimivat keskenään yhteistyössä tämän luvun määräysten mukaisesti sekä soveltamalla asiaan liittyviä kansainvälistä rikosoikeudellista yhteistyötä koskevia kansainvälisiä asiakirjoja, yhtenäisiä tai vastavuoroisia lainsäädäntöjärjestelyjä ja kansallista lainsäädäntöä mahdollisimman laajasti tietojärjestelmiin ja dataan liittyviä rikoksia koskevaan tutkintaan ja oikeudenkäyntiin tai rikokseen liittyvän sähköisessä muodossa olevan todistusaineiston keräämiseen.

##### **2 osasto Rikoksen johdosta tapahtuvaa luovuttamista koskevat periaatteet**

##### **24 artikla Rikoksen johdosta tapahtuva luovuttaminen**

1. a) Tätä artiklaa sovelletaan sopimuspuolten väliseen tämän yleissopimuksen 2-11 artiklan mukaisesti rangaistavaksi säädetyn rikoksen johdosta tapahtuvaan luovuttamiseen,

4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

### **CHAPTER III INTERNATIONAL CO-OPERATION**

#### **Section 1 General principles**

##### **Title 1 General principles relating to international co-operation**

##### **Article 23 General principles relating to international co-operation**

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

##### **Title 2 Principles relating to extradition**

##### **Article 24 Extradition**

1. a) This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable

edellyttäen, että nämä rikokset ovat molempien sopimuspuolten lainsäädännön mukaisesti rangaistavia tekoja, joista säädetty enimmäisrangaistus on vähintään yksi vuosi vankeutta taikka ankarampi rangaistus.

b) Mikäli kahden tai useamman sopimuspuolen välisen yhtenäisen tai vastavuoroisen lainsäädäntöjärjestelyn tai rikoksen johdosta tapahtuvaa luovuttamista koskevan sopimuksen perusteella, myös rikoksen johdosta tapahtuvaa luovuttamista koskevan eurooppalaisen yleissopimuksen (ETS 24) perusteella sovellettava enimmäisrangaistus poikkeaa edellä mainitusta, sovelletaan kyseisen järjestelyn tai sopimuksen mukaista enimmäisrangaistusta.

2. Tämän artiklan 1 kappaleessa tarkoitettujen rikosten katsotaan sisältyvän sopimuspuolten välillä voimassa oleviin rikoksen johdosta tapahtuvaa luovuttamista koskeviin sopimuksiin rikoksina, joiden johdosta rikoksenteijä voidaan luovuttaa. Sopimuspuolet sitoutuvat sisällyttämään nämä rikokset niiden välillä myöhemmin tehtäviin rikoksen johdosta tapahtuvaa luovuttamista koskeviin sopimuksiin rikoksina, joiden johdosta rikoksenteijä voidaan luovuttaa.

3. Jos sopimuspuoli, joka asettaa rikoksen johdosta tapahtuvan luovuttamisen ehdoksi sitä koskevan sopimuksen olemassaolon, saa luovutuspyynnön sellaiselta sopimuspuolelta, jonka kanssa sillä ei ole rikoksen johdosta tapahtuvaa luovuttamista koskevaa sopimusta, se voi pitää tätä yleissopimusta luovuttamisen oikeusperustana tämän artiklan 1 kappaleessa tarkoitettujen rikosten osalta.

4. Sopimuspuolet, jotka eivät aseta rikoksen johdosta tapahtuvan luovuttamisen ehdoksi sitä koskevan sopimuksen olemassaoloa, katsovat tämän artiklan 1 kappaleessa tarkoitettut rikokset keskinäisissä suhteissaan rikoksiksi, joiden johdosta rikoksenteijä voidaan luovuttaa.

5. Rikoksen johdosta tapahtuvaan luovuttamiseen sovelletaan luovutuspyynnön vastaanottavan sopimuspuolen lainsäädännön tai sovellettavan rikoksen johdosta tapahtuvaa

under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b) Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may



luovuttamista koskevan sopimuksen asettamia ehtoja, mukaan luettuna perusteet, joilla pyynnön vastaanottava sopimuspuoli voi kieltäytyä luovuttamisesta.

6. Jos tämän artiklan 1 kappaleessa tarkoitettun rikoksen johdosta tapahtuvasta luovuttamisesta kieltäydytään pelkästään pyynnön kohteena olevan henkilön kansalaisuuden perusteella, tai koska pyynnön vastaanottanut sopimuspuoli katsoo, että sillä on rikokseen nähden lainkäyttövalta, pyynnön vastaanottanut sopimuspuoli saattaa tapauksen pyynnön esittäneen sopimuspuolen pyynnöstä toimivaltaisten viranomaistensa käsiteltäväksi syytetoimia varten, ja ilmoittaa käsittelyn lopputuloksesta pyynnön esittäneelle sopimuspuolelle kohtuullisessa ajassa. Kyseiset viranomaiset antavat päätöksensä ja suorittavat rikostutkinnan ja oikeudenkäynnin samalla tavalla kuin minkä tahansa vastaavan rikoksen osalta asianomaisen sopimuspuolen lainsäädännön mukaisesti.

7. a) Allekirjoittaessaan tämän yleissopimuksen tai tallettaessaan ratifioimis-, hyväksymis- tai liittymiskirjansa kukin sopimuspuoli toimittaa Euroopan neuvoston pääsihteerille kunkin sellaisen viranomaisen nimen ja osoitteen, joka on vastuussa rikoksen johdosta tapahtuvaa luovuttamista koskevien pyyntöjen vastaanottamisesta tai rikoksentekijän väliaikaisesta pidätyksestä silloin kun sopimuspuolten välillä ei ole sovellettavaa sopimusta.

b) Euroopan neuvoston pääsihteerin laatii ja päivittää rekisterin sopimuspuolten nimeämistä viranomaisista. Kunkin sopimuspuoli varmistaa, että rekisterin sisältämät tiedot ovat aina ajan tasalla.

### **3 osasto Keskinäistä oikeusapua koskevat yleiset periaatteet**

#### **25 artikla Keskinäistä oikeusapua koskevat yleiset periaatteet**

1. Sopimuspuolet antavat toisilleen mahdollisimman laajaa oikeusapua

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

tietojärjestelmiin ja dataan liittyvien rikosten tutkintaa ja niitä koskevia oikeudenkäyntejä varten, tai rikokseen liittyvän sähköisessä muodossa olevan todistusaineiston keräämiseen.

2. Kukin sopimuspuoli ryhtyy myös tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin noudattaakseen 27-35 artiklan mukaisia velvoitteitaan.

3. Kukin sopimuspuoli voi kiireellisissä tapauksissa esittää keskinäistä oikeusapua tai siihen liittyviä viestejä koskevan pyynnön nopeutettua viestintäkeinoa käyttäen, mukaan luettuna telefax tai sähköposti, siinä määrin kuin tällaiset keinot mahdollistavat turvallisen viestinnän ja viestin oikeaperäisyyden varmistamisen (mukaan luettuna tarvittaessa salauksen käyttö), ja lähettää sen jälkeen muodollisen vahvistuksen, jos pyynnön vastaanottanut sopimuspuoli sitä edellyttää. Pyyntöön vastaanottanut sopimuspuoli hyväksyy tällaisen pyynnön ja vastaa siihen jotakin nopeutettua viestintäkeinoa käyttäen.

4. Jollei tämän osan artikloissa nimenomaisesti toisin määrätä, keskinäiseen oikeusapuun sovelletaan pyynnön vastaanottaneen sopimuspuolen lainsäädännön tai sovellettavan keskinäistä oikeusapua koskevan sopimuksen asettamia ehtoja, mukaan luettuna perusteet, joilla pyynnön vastaanottanut sopimuspuoli voi kieltäytyä yhteistyöstä. Pyyntöön vastaanottanut sopimuspuoli ei käytä oikeuttaan kieltäytyä antamasta 2-11 artiklassa tarkoitettuihin rikoksiin liittyvää keskinäistä oikeusapua pelkästään sillä perusteella, että pyyntö koskee rikosta, jota se pitää verorikoksena.

5. Mikäli pyynnön vastaanottaneella sopimuspuolella on tämän osan määräysten mukaisesti oikeus asettaa keskinäisen oikeusavun ehdoksi kaksoisrangaistavuus, tämän ehdon katsotaan täyttyvän, jos pyynnön kohteena olevan rikoksen perustana oleva toiminta on sen lainsäädännön mukaisesti rikos, riippumatta siitä, luokitellaanko kyseinen rikos sen lainsäädännössä samalla tavalla tai onko siinä käytetty rikosnimike sama kuin pyynnön

purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under

esittäneen sopimuspuolen lainsäädännössä.

its laws.

## **26 artikla Tietojen antaminen omasta aloitteesta**

1. Sopimuspuoli voi välittää lainsäädäntönsä asettamissa rajoissa ja ilman ennakkopyyntöä toiselle sopimuspuolelle tietoja, jotka se on saanut suorittamansa rikostutkinnan puitteissa, jos se katsoo, että näiden tietojen luovuttaminen voisi auttaa vastaanottavaa sopimuspuolta tämän yleissopimuksen mukaisesti rangaistavaksi säädettyä tekoa koskevan rikostutkinnan tai oikeudenkäynnin aloittamisessa tai suorittamisessa, tai voisi johtaa kyseisen sopimuspuolen esittämään tämän osan määräysten mukaisen yhteistyöpyynnön.

2. Ennen edellä tarkoitettujen tietojen antamista tiedot antava sopimuspuoli voi pyytää, että tiedot pidetään salassa tai että niitä käytetään tiettyjen ehtojen mukaisesti. Jos tiedot vastaanottava sopimuspuoli ei voi noudattaa pyyntöä, se ilmoittaa tästä tiedot antavalle sopimuspuolelle, joka sitten päättää antaako se tiedot siitä huolimatta. Jos tiedot vastaanottava sopimuspuoli hyväksyy tiedot annettujen ehtojen mukaisesti, ne sitovat sitä.

## **4 osasto Keskinäistä oikeusapua koskeviin pyyntöihin sovellettavat menettelytavat silloin kun niihin ei ole sovellettavissa kansainvälistä sopimusta**

### **27 artikla Keskinäistä oikeusapua koskeviin pyyntöihin sovellettavat menettelytavat silloin kun niihin ei ole sovellettavissa kansainvälistä sopimusta**

1. Tämän artiklan 2-9 kappaleen määräyksiä sovelletaan, jos pyynnön esittäneen sopimuspuolen ja pyynnön vastaanottaneiden sopimuspuolten välillä ei ole voimassa keskinäistä oikeusapua koskevaa sopimusta tai yhtenäistä tai vastavuoroista lainsäädäntöjärjestelyä. Tämän artiklan määräyksiä ei sovelleta, jos sellainen sopimus tai järjestely on olemassa, jolleivät sopimuspuolet sovi joidenkin tai kaikkien tämän

## **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.

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

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

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

artiklan määräysten soveltamisesta kyseisen sopimuksen tai järjestelyn sijaan.

2. a) Kukin sopimuspuoli nimeää keskusviranomaisen tai useamman keskusviranomaisen, jotka ovat vastuussa keskinäistä oikeusapua koskevien pyyntöjen lähettämisestä ja niihin vastaamisesta, pyyntöjen täytäntöönpanosta tai niiden välittämisestä täytäntöönpanosta vastaaville toimivaltaisille viranomaisille;

b) Keskusviranomaiset ovat suoraan yhteydessä toisiinsa;

c) Allekirjoittaessaan tämän yleissopimuksen tai tallettaessaan ratifioimis-, hyväksymis- tai liittymiskirjansa, kukin sopimuspuoli toimittaa Euroopan neuvoston pääsihteerille tämän kappaleen mukaisesti nimettyjen viranomaisten nimet ja osoitteet;

d) Euroopan neuvoston pääsihteeri laatii ja päivittää rekisterin sopimuspuolten nimeämistä keskusviranomaisista. Kukin sopimuspuoli varmistaa, että rekisterin sisältämät tiedot ovat aina ajan tasalla.

3. Tämän artiklan mukaiset keskinäistä oikeusapua koskevat pyynnöt pannaan täytäntöön pyynnön esittäneen sopimuspuolen täsmentämien menettelytapojen mukaisesti, jolleivät ne ole pyynnön vastaanottaneen sopimuspuolen lainsäädännön vastaisia.

4. Pyyntöön vastaanottanut sopimuspuoli voi kieltäytyä antamasta oikeusapua 25 artiklan 4 kappaleessa määrättyjen perusteiden lisäksi seuraavien perusteiden:

a) jos pyyntö koskee rikosta, jota pyynnön vastaanottanut sopimuspuoli pitää poliittisena rikoksena tai poliittiseen rikokseen liittyvänä rikoksena;

b) jos se katsoo, että pyynnön täytäntöönpano todennäköisesti vaarantaisi sen suvereniteetin, turvallisuuden, oikeusjärjestyksen perusteet tai muita merkittäviä etuja.

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. Pyynnön vastaanottanut sopimuspuoli voi lykätä pyynnön johdosta toteutettavia toimenpiteitä, jos näistä toimenpiteistä olisi haittaa kyseisen sopimuspuolen viranomaisten suorittamalle rikostutkinnalle tai rikosoikeudenkäynnille.

6. Ennen kuin pyynnön vastaanottanut sopimuspuoli kieltäytyy antamasta apua tai lykkää sitä, se harkitsee tarvittaessa, neuvoteltuaan pyynnön esittäneen sopimuspuolen kanssa, voidaanko pyyntöön suostua osittain tai tarpeellisiksi katsotuin ehdoin.

7. Pyynnön vastaanottanut sopimuspuoli ilmoittaa viipymättä pyynnön esittäneelle sopimuspuolelle oikeusapua koskevan pyynnön täytäntöönpanon lopputuloksesta. Oikeusavun antamisesta kieltäytyminen tai sen lykkääminen on perusteltava. Sopimuspuoli on velvollinen myös ilmoittamaan perusteista, joiden vuoksi oikeusavun antaminen on mahdotonta tai joiden johdosta se saattaa viivästyä olennaisesti.

8. Pyynnön esittänyt sopimuspuoli voi pyytää, että pyynnön vastaanottanut sopimuspuoli pitää salassa tämän luvun määräysten mukaisesti esitetyn pyynnön sekä sen kohteen, paitsi siinä määrin kuin se on tarpeen pyynnön täytäntöönpanoa varten. Jos pyynnön vastaanottanut sopimuspuoli ei voi noudattaa salassapitopyyntöä, se ilmoittaa tästä viipymättä pyynnön esittäneelle sopimuspuolelle, joka sitten päättää tulisiko pyyntö siitä huolimatta panna täytäntöön.

9. a) Kiireellisissä tapauksissa keskinäistä oikeusapua koskevan pyynnön esittävän sopimuspuolen oikeusviranomaiset voivat toimittaa pyynnön tai siihen liittyvän viestin suoraan pyynnön vastaanottavan sopimuspuolen vastaaville viranomaisille. Tällaisessa tapauksessa pyynnöstä lähetetään samalla jäljennös pyynnön vastaanottavan sopimuspuolen keskusviranomaiselle pyynnön esittävän sopimuspuolen keskusviranomaisen välityksellä.

5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9. a) In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b) Tämän kappaleen mukainen pyyntö tai viesti voidaan lähettää Kansainvälisen rikospoliisijärjestön (Interpol) välityksellä.

c) Jos pyyntö tehdään tämän artiklan a kohdan mukaisesti, eikä viranomaisen ole toimivaltainen käsittelemään pyyntöä, se saattaa pyynnön toimivaltaisen kansallisen viranomaisen käsiteltäväksi ja ilmoittaa tästä suoraan pyynnön esittäneelle sopimuspuolelle.

d) Pynnön esittävän sopimuspuolen toimivaltaiset viranomaiset voivat toimittaa tämän kappaleen mukaisesti lähetetyn pyynnön tai viestin, joka ei edellytä pakkotoimia, suoraan pyynnön vastaanottavan sopimuspuolen toimivaltaisille viranomaisille.

e) Allekirjoittaessaan tämän yleissopimuksen tai tallettaessaan ratifioimis-, hyväksymis- tai liittymiskirjansa kukin sopimuspuoli voi ilmoittaa Euroopan neuvoston pääsihteerille, että tehokkuussyistä tämän kappaleen mukaiset pyynnöt tulee osoittaa sen keskusviranomaiselle.

## **28 artikla Tietojen salassapito ja käyttörajoitukset**

1. Tämän artiklan määräyksiä sovelletaan, jos pyynnön esittäneen sopimuspuolen ja pyynnön vastaanottaneiden sopimuspuolten välillä ei ole voimassa keskinäistä oikeusapua koskevaa sopimusta tai yhtenäistä tai vastavuoroista lainsäädäntöjärjestelyä. Tämän artiklan määräyksiä ei sovelleta, jos sellainen sopimus tai järjestely on olemassa, jolleivät sopimuspuolet sovi joidenkin tai kaikkien tämän artiklan määräysten soveltamisesta kyseisen sopimuksen tai järjestelyn sijaan.

2. Pynnön vastaanottanut sopimuspuoli voi asettaa pyydettyjen tietojen tai aineiston antamisen ehdoksi, että:

a) tiedot pidetään salassa, jos keskinäistä oikeusapua koskevaan pyyntöön ei voitaisi vastata ilman tällaisen ehdon soveltamista, tai että

b) Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c) Where a request is made pursuant to subparagraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d) Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

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

## **Article 28 Confidentiality and limitation on use**

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a) kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b) tietoja ei käytetä muuhun kuin pyynnössä mainittuun rikostutkintaan tai rikosoikeudenkäyntiin.

3. Jos pyynnön esittänyt sopimuspuoli ei voi noudattaa 2 kappaleessa tarkoitettua ehtoa, se ilmoittaa tästä viipymättä toiselle sopimuspuolelle, joka sitten päättää tulisiko tiedot kuitenkin antaa. Jos pyynnön esittänyt sopimuspuoli hyväksyy ehdon, tämä ehto sitoo sitä.

4. Sopimuspuoli, joka toimittaa tietoja tai aineistoa 2 kappaleessa tarkoitettulla ehdolla, voi pyytää toista sopimuspuolta selittämään tietojen tai aineiston käyttötarkoituksen tämän ehdon kannalta.

## **2 jakso Erityiset määräykset**

### **1 osasto Väliaikaisia toimenpiteitä koskeva keskinäinen oikeusapu**

#### **29 artikla Tallennetun datan säilyttämisen nopea varmistaminen**

1. Sopimuspuoli voi pyytää toista sopimuspuolta määräämään tai muutoin varmistamaan nopeasti sellaisen tietojärjestelmän avulla tallennetun datan säilyttämisen, joka on jälkimmäisen sopimuspuolen alueella ja jonka osalta pyynnön esittänyt sopimuspuoli aikoo esittää keskinäistä oikeusapua koskevan pyynnön dataan kohdistuvaa etsintää tai muulla tavoin tapahtuvaa pääsyn hankkimista, takavarikkoa tai muuta turvaamistoimea taikka datan luovutusta varten.

2. Tämän artiklan 1 kappaleen mukaisesti tehdyssä varmistamista koskevassa pyynnössä on mainittava:

- a) varmistamista pyytävä viranomainen;
- b) rikos, joka on tutkinnan tai oikeudenkäynnin kohteena, sekä lyhyt tiivistelmä asiaan liittyvistä tosiseikoista;
- c) säilytettävä tallennettu data ja sen yhteys

b) not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4. Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

## **Section 2 Specific provisions**

### **Title 1 Mutual assistance regarding provisional measures**

#### **Article 29 Expedited preservation of stored computer data**

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2. A request for preservation made under paragraph 1 shall specify:

- a) the authority seeking the preservation;
- b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
- c) the stored computer data to be preserved and

rikokseen;

d) saatavilla olevat tiedot tallennetun datan haltijasta tai tietojärjestelmän sijainnista;

e) säilyttämisen tarpeellisuus; ja

f) maininta siitä, että sopimuspuoli aikoo esittää keskinäistä oikeusapua koskevan pyynnön tallennettuun dataan kohdistuvaa etsintää tai muulla tavoin tapahtuvaa pääsyn hankkimista, takavarikkoa tai muuta turvaamistoimea taikka datan luovutusta varten.

3. Sopimuspuoli, joka vastaanottaa pyynnön toiselta sopimuspuolelta, ryhtyy kaikkiin tarvittaviin toimenpiteisiin varmistaakseen nopeasti yksilöidyn datan säilyttämisen kansallisen lainsäädäntönsä mukaisesti. Pyyntöön vastattaessa kaksoisrangaistavuutta ei pidetä tällaisen datan säilyttämisen varmistamisen ehtona.

4. Sopimuspuoli, joka pitää kaksoisrangaistavuutta tallennettuun dataan kohdistuvaa etsintää tai muulla tavoin tapahtuvaa pääsyn hankkimista, takavarikkoa tai muuta turvaamistoimea taikka datan luovutusta varten esitettyyn keskinäistä oikeusapua koskevaan pyyntöön vastaamisen ehtona, voi muiden kuin tämän yleissopimuksen 2-11 artiklan mukaisesti rangaistaviksi teoiksi säädettyjen rikosten osalta tehdä varauksen, jonka mukaan se voi kieltäytyä vastaamasta tämän artiklan mukaiseen datan säilyttämisen varmistamista koskevaan pyyntöön silloin kun sillä on syytä uskoa, että datan luovutuksen ajankohtana kaksoisrangaistavuuden ehto ei täyty.

5. Muutoin datan säilyttämisen varmistamista koskevaan pyyntöön vastaamisesta voidaan kieltäytyä ainoastaan, jos:

a) pyyntö koskee rikosta, jota pyynnön vastaanottanut sopimuspuoli pitää poliittisena rikoksena tai poliittiseen rikokseen liittyvänä rikoksena;

its relationship to the offence;

d) any available information identifying the custodian of the stored computer data or the location of the computer system;

e) the necessity of the preservation; and

f) that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5. In addition, a request for preservation may only be refused if:

a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or



b) pyynnön vastaanottanut sopimuspuoli katsoo, että pyynnön täytäntöönpano todennäköisesti vaarantaisi sen suvereniteetin, turvallisuuden, oikeusjärjestyksen perusteet tai muita oleellisia etuja.

b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

6. Jos pyynnön vastaanottanut sopimuspuoli uskoo, että datan säilyttämisen varmistamistoimi ei varmista sitä, että data on myöhemmin saatavilla, tai vaarantaa pyynnön esittäneen sopimuspuolen suorittaman rikostutkinnan salassapidon tai muutoin haittaa sitä, se ilmoittaa tästä viipymättä pyynnön esittäneelle sopimuspuolelle, joka sitten päättää tulisiko pyyntö siitä huolimatta panna täytäntöön.

6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7. Sellaisen varmistamisen, joka toteutetaan vastauksena artiklan 1 kappaleessa tarkoitettuun pyyntöön, tulee kestää vähintään kuusikymmentä päivää, jotta pyynnön esittänyt sopimuspuolella on mahdollisuus esittää tallennettuun dataan kohdistuvaa etsintää tai muulla tavoin tapahtuvaa pääsyn hankkimista, takavarikkoa tai muuta turvaamistoimea taikka datan luovutusta koskeva pyyntö. Tällaisen pyynnön vastaanottamisen jälkeen datan säilyttäminen varmistetaan edelleen, kunnes pyyntöä koskeva päätös on tehty.

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.

### **30 artikla Varmistettujen liikennetietojen nopea luovutus**

### **Article 30 Expedited disclosure of preserved traffic data**

1. Mikäli pyynnön vastaanottanut sopimuspuoli havaitsee, pannessaan 29 artiklan mukaisesti esitetyn yksilöityä viestiä koskevien liikennetietojen säilyttämisen varmistamista koskevaa pyyntöä täytäntöön, että viestin siirtoon on ollut osallisena toisessa valtiossa oleva palveluntarjoaja, pyynnön vastaanottanut sopimuspuoli luovuttaa pyynnön esittäneelle sopimuspuolelle nopeasti riittävän määrän tietoja, joiden avulla palveluntarjoaja ja viestin siirtoon käytetty polku ovat tunnistettavissa.

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. Tämän artiklan mukaisesta liikennetietojen luovutuksesta voidaan pidättäytyä ainoastaan, jos:

2. Disclosure of traffic data under paragraph 1 may only be withheld if:

a) pyyntö koskee rikosta, jota pyynnön

a) the request concerns an offence which the

vastaanottanut sopimuspuoli pitää poliittisena rikoksena tai poliittiseen rikokseen liittyvänä rikoksena; tai

b) pyynnön vastaanottanut sopimuspuoli katsoo, että pyynnön täytäntöönpano todennäköisesti vaarantaisi sen suvereniteetin, turvallisuuden, oikeusjärjestyksen perusteet tai muita oleellisia etuja.

## **2 osasto Tutkintaan liittyviä toimivaltuuksia koskeva keskinäinen oikeusapu**

### **31 artikla Keskinäinen oikeusapu pääsyn hankkimisessa tallennettuun dataan**

1. Sopimuspuoli voi pyytää toiselta sopimuspuolelta tämän alueella olevan tietojärjestelmän avulla tallennettuun dataan kohdistuvaa etsintää tai muulla tavoin tapahtuvaa pääsyn hankkimista, takavarikkoa tai muuta turvaamistoimea ja datan luovutusta, mukaan luettuna data, jonka säilyttäminen on varmistettu 29 artiklan mukaisesti.

2. Pyyntöön vastaanottanut sopimuspuoli vastaa pyyntöön soveltamalla 23 artiklassa tarkoitettuja kansainvälisiä asiakirjoja, järjestelyjä ja lainsäädäntöä, sekä muiden tämän luvun asiaan liittyvien määräysten mukaisesti.

3. Pyyntöön vastataan nopeutettua menettelyä noudattaen, jos:

a) on syytä uskoa, että asiaan liittyvän datan häviäminen tai muuttaminen on erityisen todennäköistä; tai

b) tämän artiklan 2 kappaleessa tarkoitetuissa sopimuksissa, järjestelyissä tai lainsäädännössä muutoin määrätään nopeutetusta yhteistyöstä.

### **32 artikla Pääsyn hankkiminen tallennettuun dataan valtion rajojen yli suostumuksesta tai silloin kun data on julkista**

Sopimuspuoli voi ilman toisen sopimuspuolen lupaa:

a) hankkia pääsyn julkisesti saatavilla olevaan

requested Party considers a political offence or an offence connected with a political offence; or

b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

## **Title 2 Mutual assistance regarding investigative powers**

### **Article 31 Mutual assistance regarding accessing of stored computer data**

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2. The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3. The request shall be responded to on an expedited basis where:

a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

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

A Party may, without the authorisation of another Party:

a) access publicly available (open source) stored

(avoin lähde) tallennettuun dataan riippumatta siitä missä data maantieteellisesti sijaitsee; tai

b) hankkia pääsyn omalla alueellaan olevan tietojärjestelmän avulla toisen sopimuspuolen alueella sijaitsevaan tallennettuun dataan tai vastaanottaa tällaista dataa, jos ensin mainittu sopimuspuoli saa siihen sellaisen henkilön laillisesti ja vapaaehtoisesti annetun suostumuksen, jolla on laillinen oikeus luovuttaa data sopimuspuolelle tietojärjestelmän avulla.

### **33 artikla Keskinäinen oikeusapu tiedon hankkimisessa liikennetiedoista reaaliajassa**

1. Sopimuspuolet antavat toisilleen keskinäistä oikeusapua reaaliaikaiseksi tiedon hankkimiseksi sellaisista liikennetiedoista, jotka liittyvät niiden alueella tietojärjestelmän avulla siirrettyyn yksilöityyn viestiin. Jollei 2 kappaleen määräyksistä muuta johdu, tähän oikeusapuun sovelletaan kansallisen lainsäädännön mukaisia ehtoja ja menettelytapoja.

2. Kukin sopimuspuoli antaa edellä mainittua oikeusapua ainakin sellaisten rikosten osalta, joihin liittyen tietoa voitaisiin hankkia liikennetiedoista reaaliajassa vastaavassa kansallisessa tapauksessa.

### **34 artikla Keskinäinen oikeusapu tiedon hankkimisessa viestin sisällöstä**

Sopimuspuolet antavat toisilleen keskinäistä oikeusapua reaaliaikaiseksi tiedon hankkimiseksi tietojärjestelmän välityksellä siirrettyjen yksilöityjen viestien sisällöstä siinä määrin kuin se on niiden soveltamien sopimusten ja kansallisen lainsäädännön mukaan sallittua.

### **3 osasto 24-tuntinen jokapäiväinen verkosto**

### **35 artikla 24-tuntinen jokapäiväinen verkosto**

1. Kukin sopimuspuoli nimeää yhteyspisteen, joka on käytettävissä joka päivä 24 tuntia vuorokaudessa, sen varmistamiseksi, että

computer data, regardless of where the data is located geographically; or

b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

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

1. The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

### **Article 34 Mutual assistance regarding the interception of content data**

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

### **Title 3 24/7 Network**

### **Article 35 24/7 Network**

1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of

oikeusapua voidaan antaa välittömästi tietojärjestelmiin ja datasiirtoon liittyvien rikosten tutkinnassa tai niitä koskevassa oikeudenkäynnissä tai rikokseen liittyvän sähköisessä muodossa olevan todistusaineiston keräämisessä. Tällaiseen oikeusapuun sisältyy seuraavissa toimenpiteissä avustaminen tai, jos se on sopimuspuolen lainsäädännön ja käytäntöjen mukaista, niiden suorittaminen:

- a) teknisen avun antaminen;
- b) datan säilyttämisen varmistaminen 29 ja 30 artiklan mukaisesti;
- c) todisteiden kerääminen, oikeudellisten tietojen antaminen ja epäiltyjen paikantaminen.

2. a) Sopimuspuolen yhteyspisteellä tulee olla valmiudet viestintään toisen sopimuspuolen yhteyspisteen kanssa nopeutettua menettelyä noudattaen.

b) Jos sopimuspuolen nimeämä yhteyspiste ei ole kyseisen sopimuspuolen kansainvälisestä oikeusavusta tai rikoksen johdosta tapahtuvasta luovuttamisesta vastaavan viranomaisen tai viranomaisten osa, yhteyspisteen tulee varmistaa, että se pystyy koordinoimaan toimintaansa kyseisen viranomaisen tai viranomaisten kanssa nopeutettua menettelyä noudattaen.

3. Verkoston toiminnan helpottamiseksi kukin sopimuspuoli varmistaa, että sillä on käytettävissään koulutettua ja toimintavalmista henkilökuntaa.

#### **IV LUKU LOPPUMÄÄRÄYKSET**

##### **36 artikla Allekirjoittaminen ja voimaantulo**

1. Tämä yleissopimus on avoinna allekirjoittamista varten Euroopan neuvoston jäsenvaltioille ja sen ulkopuolisille valtioille, jotka ovat osallistuneet yleissopimuksen valmisteluun.

2. Tämä yleissopimus on ratifioitava tai hyväksyttävä. Ratifioimis- ja hyväksymiskirjat

immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

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

2. a) A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b) If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

#### **CHAPTER IV FINAL PROVISIONS**

##### **Article 36 Signature and entry into force**

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2. This Convention is subject to ratification, acceptance or approval. Instruments of

talletetaan Euroopan neuvoston pääsihteerin huostaan.

3. Tämä yleissopimus tulee voimaan seuraavan kuukauden ensimmäisenä päivänä, kun on kulunut kolme kuukautta siitä päivästä, jona viisi valtiota, mukaan lukien kolme Euroopan neuvoston jäsenvaltiota, on ilmaissut suostumuksensa tulla yleissopimuksen sitomaksi 1 ja 2 kappaleen määräysten mukaisesti.

4. Sellaisen allekirjoittajavaltion osalta, joka myöhemmin ilmaisee suostumuksensa tulla yleissopimuksen sitomaksi, se tulee voimaan seuraavan kuukauden ensimmäisenä päivänä, kun on kulunut kolme kuukautta siitä päivästä, jona se on ilmaissut suostumuksensa tulla yleissopimuksen sitomaksi 1 ja 2 kappaleen mukaisesti.

### **37 artikla Yleissopimukseen liittyminen**

1. Tämän yleissopimuksen voimaantulon jälkeen Euroopan neuvoston ministerikomitea, neuvoteltuaan yleissopimuksen sopimuspuolten kanssa ja saatuaan niiden yksimielisen suostumuksen, voi kutsua minkä tahansa Euroopan neuvoston ulkopuolisen valtion, joka ei ole osallistunut yleissopimuksen valmisteluun, liittymään yleissopimukseen. Tätä koskeva päätös tehdään Euroopan neuvoston perussäännön 20 artiklan d kohdan määräysten mukaisella äänten enemmistöllä sekä niiden sopimuspuolten edustajien yksimielisellä päätöksellä, joilla on oikeus kuulua ministerikomiteaan.

2. Yleissopimus tulee siihen tämän artiklan 1 kappaleen mukaisesti liittyvän valtion osalta voimaan seuraavan kuukauden ensimmäisenä päivänä, kun on kulunut kolme kuukautta siitä päivästä, jona se on tallettanut liittymiskirjansa Euroopan neuvoston pääsihteerin huostaan.

### **38 artikla Alueellinen soveltaminen**

1. Valtio voi allekirjoittaessaan tämän

ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

### **Article 37 Accession to the Convention**

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

### **Article 38 Territorial application**

1. Any State may, at the time of signature or

yleissopimuksen tai tallettaessaan ratifioimis-, hyväksymis- tai liittymiskirjansa mainita alueen tai alueet, joihin yleissopimusta sovelletaan.

2. Sopimuspuoli voi milloin tahansa myöhemmin Euroopan neuvoston pääsihteerille osoitetulla selityksellä laajentaa tämän yleissopimuksen soveltamisen koskemaan muuta selityksessä mainittua aluetta.

Yleissopimus tulee tällaisen alueen osalta voimaan seuraavan kuukauden ensimmäisenä päivänä, kun on kulunut kolme kuukautta siitä päivästä, jona pääsihteeri on vastaanottanut selityksen.

3. Tämän artiklan kahden edeltävän kappaleen mukaisesti annettu selitys voidaan peruuttaa minkä tahansa selityksessä mainitun alueen osalta ilmoittamalla siitä Euroopan neuvoston pääsihteerille. Peruuttaminen tulee voimaan seuraavan kuukauden ensimmäisenä päivänä, kun on kulunut kolme kuukautta siitä päivästä, jona pääsihteeri on vastaanottanut ilmoituksen.

### **39 artikla Yleissopimuksen vaikutukset**

1. Tämän yleissopimuksen tarkoituksena on täydentää sopimuspuolten välillä sovellettavia monen- tai kahdenvälisiä sopimuksia tai järjestelyitä, mukaan luettuna:

- Rikoksen johdosta tapahtuvaa luovuttamista koskeva eurooppalainen yleissopimus, joka avattiin allekirjoittamista varten Strasbourgissa 13 päivänä joulukuuta 1957 (ETS No. 24);

- Keskinäistä oikeusapua rikosasioissa koskeva eurooppalainen yleissopimus, joka avattiin allekirjoittamista varten Strasbourgissa 20 päivänä huhtikuuta 1959 (ETS No. 30);

- Keskinäistä oikeusapua rikosasioissa koskevan eurooppalaisen yleissopimuksen lisäpöytäkirja, joka avattiin allekirjoittamista varten Strasbourgissa 17 päivänä maaliskuuta 1978 (ETS No. 99).

2. Jos kaksi sopimuspuolta tai useampi

when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

### **Article 39 Effects of the Convention**

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

- the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

- the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

- the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2. If two or more Parties have already concluded

sopimuspuoli on jo tehnyt sopimuksen tähän yleissopimukseen sisältyvistä asioista tai on muutoin järjestänyt suhteensa näiden asioiden osalta, tai tekevät niin myöhemmin, niillä on oikeus soveltaa myös kyseistä sopimusta tai noudattaa suhteitaan koskevaa järjestelyä. Mikäli sopimuspuolet kuitenkin järjestävät suhteensa tähän yleissopimukseen sisältyvien asioiden osalta sen määräyksistä poikkeavalla tavalla, niiden on tehtävä järjestely siten, että se ei ole yleissopimuksen tavoitteiden ja periaatteiden vastainen.

3. Tämän yleissopimuksen määräykset eivät vaikuta sopimuspuolen muihin oikeuksiin, rajoituksiin, velvoitteisiin ja vastuuseen.

#### **40 artikla Selitykset**

Valtio voi allekirjoittaessaan tämän yleissopimuksen tai tallettaessaan ratifioimis-, hyväksymis- tai liittymiskirjansa antaa Euroopan neuvoston pääsihteerille selityksen, jonka mukaan se käyttää hyväkseen oikeuttaan asettaa lisäehtoja 2 ja 3 artiklan, 6 artiklan 1 kappaleen b kohdan, 9 artiklan 3 kappaleen ja 27 artiklan 9 kappaleen e kohdan määräysten mukaisesti.

#### **41 artikla Liittovaltioita koskeva lauseke**

1. Liittovaltio voi tehdä varauman, jonka mukaan se noudattaa II lukuun perustuvia velvoitteitaan niiden peruseriaatteiden mukaisesti, jotka koskevat kyseisen liittovaltion keskushallinnon ja osavaltioiden tai muiden vastaavien alueiden välisiä suhteita, edellyttäen kuitenkin, että kyseinen liittovaltio voi varaumasta huolimatta tehdä III luvun mukaista yhteistyötä.

2. Tehdessään tämän artiklan 1 kappaleen mukaisen varauman, liittovaltio ei saa soveltaa varaumansa ehtoja siten, että se jättää noudattamatta tai merkittävästi vähentää velvoitteitaan ryhtyä II luvun mukaisiin toimenpiteisiin. Liittovaltio yleensäkin varmistaa valmiuden laajaan ja tehokkaaseen lainvalvontaan II luvun mukaisten toimenpiteiden osalta.

an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

#### **Article 40 Declarations**

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

#### **Article 41 Federal clause**

1. A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2. When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3. Liittovaltion hallitus ilmoittaa osavaltioidensa tai muiden vastaavien alueidensa toimivaltaisille viranomaisille niistä tämän yleissopimuksen määräyksistä, joiden soveltaminen kuuluu kyseisten osavaltioiden tai alueiden toimivaltaan, sekä määräykset hyväksyvistä mielipiteestään, kannustaen niitä ryhtymään tarvittaviin toimenpiteisiin määräysten täytäntöönpanoa varten.

#### **42 artikla Varaumat**

Valtio voi allekirjoittaessaan tämän yleissopimuksen tai tallettaessaan ratifioimis-, hyväksymis- tai liittymiskirjansa antaa Euroopan neuvoston pääsihteerille kirjallisen selityksen, jonka mukaan se käyttää hyväkseen oikeuttaan tehdä 4 artiklan 2 kappaleen, 6 artiklan 3 kappaleen, 9 artiklan 4 kappaleen, 10 artiklan 3 kappaleen, 11 artiklan 3 kappaleen, 14 artiklan 3 kappaleen, 22 artiklan 2 kappaleen, 29 artiklan 4 kappaleen ja 41 artiklan 1 kappaleen mukaisia varauksia. Tähän yleissopimukseen ei saa tehdä muita varauksia.

#### **43 artikla Varauksien voimassaolo ja peruuttaminen**

1. Sopimuspuoli, joka on tehnyt varauksen 42 artiklan mukaisesti, voi peruuttaa sen kokonaan tai osittain Euroopan neuvoston pääsihteerille osoitetulla ilmoituksella. Peruuttaminen tulee voimaan sinä päivänä, jona pääsihteerin vastaanottanut ilmoituksen. Jos ilmoituksessa mainitaan, että varauksen peruuttaminen tulee voimaan ilmoituksessa mainittuna päivänä, ja kyseinen päivä on myöhempi kuin ilmoituksen vastaanottopäivä, peruuttaminen tulee voimaan ilmoituksessa mainittuna myöhempänä päivänä.

2. Sopimuspuoli, joka on tehnyt 42 artiklassa tarkoitetun varauksen, peruuttaa varauksen kokonaan tai osittain heti kun olosuhteet sen sallivat.

3. Pääsihteerin voi ajoittain tiedustella yhden tai

3. With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

#### **Article 42 Reservations**

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

#### **Article 43 Status and withdrawal of reservations**

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3. The Secretary General of the Council of



useamman 42 artiklassa tarkoitetun varauman tehneiltä sopimuspuoilta mahdollisuuksista peruuttaa nämä varauumat.

#### **44 artikla Muutokset**

1. Sopimuspuoli voi ehdottaa tähän yleissopimukseen muutoksia, ja Euroopan neuvoston pääsihteeri toimittaa muutosehdotukset Euroopan neuvoston jäsenvaltioille, Euroopan neuvoston ulkopuolisille valtioille, jotka ovat osallistuneet tämän yleissopimuksen valmisteluun, sekä sellaisille valtioille, jotka ovat liittyneet tai jotka on kutsuttu liittymään tähän yleissopimukseen 37 artiklan määräysten mukaisesti.

2. Sopimuspuolen tekemä muutosehdotus annetaan tiedoksi Euroopan neuvoston rikosasiain yhteistyökomitealle (CDPC), joka antaa mielipiteensä muutosehdotuksesta ministerikomitealle.

3. Ministerikomitea käsittelee muutosehdotuksen ja CDPC:n mielipiteen ja voi hyväksyä muutoksen neuvoteltuaan ensin tämän yleissopimuksen sopimuspuolina olevien Euroopan neuvoston ulkopuolisten valtioiden kanssa.

4. Ministerikomitean tämän artiklan 3 kappaleen mukaisesti hyväksymän muutoksen teksti toimitetaan sopimuspuolille hyväksyttäväksi.

5. Tämän artiklan 3 kappaleen mukaisesti hyväksytty muutos tulee voimaan kolmantenakymmenentenä päivänä sen jälkeen, kun kaikki sopimuspuolet ovat ilmoittaneet pääsihteerille hyväksyneensä sen.

#### **45 artikla Riitojen ratkaisu**

1. Euroopan neuvoston rikosasiain yhteistyökomitealle (CDPC) annetaan tietoa tämän yleissopimuksen tulkintaan ja soveltamiseen liittyvistä asioista.

2. Mikäli sopimuspuolten välille syntyy riita

Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

#### **Article 44 Amendments**

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

#### **Article 45 Settlement of disputes**

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2. In case of a dispute between Parties as to the

tämän yleissopimuksen tulkinnasta tai soveltamisesta, ne pyrkivät ratkaisemaan sen neuvotteluihin tai muulla valitsemallaan rauhanomaisella keinolla, mukaan lukien riidan saattaminen CDPC:n, sopimuspuolia sitovan ratkaisun antavan välimiesoikeuden tai Kansainvälisen tuomioistuimen ratkaistavaksi riidan osapuolina olevien sopimuspuolten välisen sopimuksen mukaisesti.

#### **46 artikla Sopimuspuolten väliset neuvottelut**

1. Sopimuspuolet neuvottelevat ajoittain ja tarpeen mukaan helpottaakseen:

a) tämän yleissopimuksetehokasta soveltamista ja täytäntöönpanoa, mukaan luettuna siihen liittyvien ongelmien toteaminen, sekä lieventääkseen tämän yleissopimuksen mukaisten selitysten ja varaumien vaikutuksia;

b) tietojenvaihtoa merkittävästä oikeudellisesta, poliittisesta tai teknologisesta kehityksestä, joka liittyy tietoverkkorikollisuuteen ja rikoksiin liittyvän sähköisessä muodossa olevan todistusaineiston keräämiseen;

c) yleissopimuksen mahdollisen täydentämisen tai muuttamisen käsittelyä.

2. Euroopan neuvoston rikosasiain yhteistyökomitealle (CDPC) annetaan ajoittain tietoa tämän artiklan 1 kappaleessa tarkoitettujen neuvottelujen tuloksista.

3. CDPC helpottaa tarvittaessa 1 kappaleessa tarkoitettuja neuvotteluja ja ryhtyy tarvittaviin toimenpiteisiin auttaakseen sopimuspuolia niiden pyrkimyksissä täydentää tai muuttaa yleissopimusta. Viimeistään kolmen vuoden kuluttua tämän yleissopimuksen voimaantulosta Euroopan neuvoston rikosasiain yhteistyökomitea (CDPC) tarkistaa yhteistyössä sopimuspuolten kanssa kaikki tämän yleissopimuksen määräykset ja suosittaa tarvittaessa niiden muuttamista.

4. Jollei Euroopan neuvosto vastaa 1 kappaleen määräysten täytäntöönpanon aiheuttamista kustannuksista, sopimuspuolet vastaavat niistä

interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

#### **Article 46 Consultations of the Parties**

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

a) the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b) the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c) consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the

keskenään sopimallaan tavalla.

5. Euroopan neuvoston sihteeristö avustaa sopimuspuolia täyttämään tämän artiklan mukaiset velvoitteensa.

#### **47 artikla Irtisanominen**

1. Sopimuspuoli voi milloin tahansa irtisanoa tämän yleissopimuksen Euroopan neuvoston pääsihteerille osoitetulla ilmoituksella.

2. Irtisanominen tulee voimaan seuraavan kuukauden ensimmäisenä päivänä, kun on kulunut kolme kuukautta siitä päivästä, jona pääsihteeri on vastaanottanut ilmoituksen.

#### **48 artikla Ilmoitukset**

Euroopan neuvoston pääsihteeri ilmoittaa Euroopan neuvoston jäsenvaltioille, Euroopan neuvoston ulkopuolisille valtioille, jotka ovat osallistuneet tämän yleissopimuksen valmisteluun, sekä sellaisille valtioille, jotka ovat liittyneet tai jotka on kutsuttu liittymään tähän yleissopimukseen:

- a) jokaisesta allekirjoituksesta;
- b) jokaisen ratifioimis-, hyväksymis- tai liittymiskirjan tallettamisesta;
- c) jokaisesta tämän yleissopimuksen 36 ja 37 artiklan mukaisesta voimaantulopäivästä;
- d) jokaisesta 40 mukaisesta selityksestä, tai [41 tai] 42 artiklan mukaisesta varaumasta;
- e) jokaisesta muusta tähän yleissopimukseen liittyvästä toimesta, ilmoituksesta tai tiedonannosta.

Tämän vakuudeksi allekirjoittaneet, siihen asianmukaisesti valtuutettuina, ovat allekirjoittaneet tämän yleissopimuksen.

Tehty Budapestissä 23 päivänä marraskuuta 2001 yhtenä englannin- ja ranskankielisenä

Parties in the manner to be determined by them.

5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

#### **Article 47 Denunciation**

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

#### **Article 48 Notification**

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

- a) any signature;
- b) the deposit of any instrument of ratification, acceptance, approval or accession;
- c) any date of entry into force of this Convention in accordance with Articles 36 and 37;
- d) any declaration made under Article 40 or reservation made in accordance with Article 42;
- e) any other act, notification or communication relating to this Convention.

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

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being

alkuperäiskappaleena, jonka molemmat tekstit ovat yhtä todistusvoimaiset, ja joka talletetaan Euroopan neuvoston arkistoon. Euroopan neuvoston pääsihteeri toimittaa sen oikeaksi todistetun jäljennöksen kullekin Euroopan neuvoston jäsenvaltiolle, Euroopan neuvoston ulkopuoliselle valtiolle, joka on osallistunut tämän yleissopimuksen valmisteluun, sekä sellaisille valtioille, jotka on kutsuttu liittymään siihen.

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.

# TIETOVERKKORIKOSTYÖRYHMÄN MIETINTÖ

Asianajaja Satu Tiirikan eriävä mielipide 16.6.2003

## 1 Myös datan kopioinnin tulee olla takavarikko

### 1.1 Ehdotettua pakkokeinolain 4 luvun 4 a §:n 3 momenttia ei tule hyväksyä

Työryhmän ehdotukseen sisältyvän pakkokeinolain 4 luvun 4 a §:n 3 momentin mukaan datan kopiointi ja tallentaminen toiselle tallennusalustalle ei ole takavarikointia.

Työryhmän ehdottamaa kantaa ei tule hyväksyä, vaan myös datan kopiointiin tulee soveltaa takavarikkoa koskevia säännöksiä seuraavilla perusteilla.

### 1.2 Asianosaiselle vain datan sisältämän informaation haltuun saamisella on merkitystä

Työryhmä esittää perusteluna datan kopioinnin erilaiseen kohteluun verrattuna datan poistamiseen tai sen käytön estämiseen, että ”...toimenpiteiden merkitys on niiden kohteena olevan henkilön kannalta erilainen. Datan poistaminen merkitsee tuntuvampaa kajoamista epäillyn oikeuksiin kuin pelkkä datan kopioiminen.”

Lähes poikkeuksetta asianosaiselle ei kuitenkaan ole mitään merkitystä sillä, onko esitutkintaviranomaisen hallussa alkuperäinen data vai sen kopio. Pääsääntöisesti tärkeätä on vain datan sisällön, informaation, haltuun saaminen eikä sen konkreettinen ”hallussapito”. Nykyaikana myöskään esitutkintaviranomaiselle ei itse tutkinnan suorittamisen kannalta ole yleensä mitään merkitystä sillä, onko sen hallussa alkuperäinen data vai sen kopio.

Kun tutkintaviranomainen voi myös käyttää dataa muun muassa tutkinnan ohjaamiseen ns. vihjetietona aivan samalla tavoin olipa sen hallussa alkuperäinen data tai sen kopio, ei tältäkkään kannalta ole syytä tehdä eroa alkuperäisen datan ja kopion suhteen.

### 1.3 Poikkeamiseen korkeimman oikeuden kannasta ei ole perustetta

Esityksessä on viitattu korkeimman oikeuden ratkaisuun 2002:85, jossa on todettu, että ”kiintolevyn kopiointia on oikeudellisesti pidettävä takavarikkona”. Esityksen perusteluissa myös todetaan, että ”Ehdotettu säännös poikkeaa korkeimman oikeuden ratkaisusta siten, että pelkkää kopiointia ei vielä säännöksen mukaan pidettäisi takavarikkona.”

Perustetta sille, miksi korkeimman oikeuden ratkaisusta tulisi nimenomaan poiketa ei ole, kun perusteena ei voi olla datan kopioinnin erilainen merkitys haltijalle verrattuna sen poistamiseen tai sen käytön estämiseen.

Korkeimman oikeuden kannasta ei myöskään voi olla epäselvyyttä, sillä korkein oikeus on em. ratkaisunsa 2002:85 perusteluissa vielä viitannut samassa asiassa aikaisemmin antamaansa ratkaisuun 2001:39, jossa se oli jo todennut, että datan kopiointiin tulee soveltaa takavarikkoa koskevia säännöksiä.

### 1.4 Takavarikon kohteen suojaksi säädettyjä lainsäännöksiä tulee noudattaa myös kopion osalta

On myös muistettava, että ellei datan kopiointi olisi takavarikko, ei kopion osalta tarvitsisi noudattaa muun muassa pakkokeinolain 4 luvun seuraavia säännöksiä:

- 5 § takavarikoimisesta päättävä viranomainen,
- 7 § ilmoitusvelvollisuus,
- 9 § pöytäkirja ja todistus,
- 11 § takavarikon kumoaminen ja noudatettavat määräajat sekä
- 13 § takavarikon saattaminen tuomioistuimen tutkittavaksi.

Kun nämä lainkohdat on säädetty nimenomaan takavarikon kohteen oikeusturvan varmistamiseksi, ei säännöksillä ole juuri merkitystä, jos ehdotus hyväksytään.

#### 1.5 Myös asiakirjan osalta tulee noudattaa samaa käytäntöä

Perusteena sille, ettei kopiointi ole takavarikko, on esityksessä viitattu myös paperimuodossa olevan asiakirjan takavarikossa noudatettuun käytäntöön.

Tältä osin on todettava, että takavarikkosäännösten soveltaminen myös asiakirjan kopioon tulee nykytekniikan aikana olla itsestään selvyys.

## **2 Takavarikkokiellon alaisen materiaalin salassapito on turvattava**

### 2.1 Takavarikkokiellon alainen materiaali tulee erottaa jo kopiointivaiheessa

Työryhmän perusteluiden mukaan esitutkintaviranomainen voi kopioida esimerkiksi koko kovalevyn, vaikka tutkinnan kohteena oleva henkilö väittäisi, että materiaalissa on takavarikkokiellon eli pakkokeinolain 4 luvun 2 §:n 2 momentin alaista materiaalia. Perusteluna työryhmä on viitannut korkeimman oikeuden ratkaisuun 2002:85, jonka mukaan poliisi oli voinut ottaa kovalevyn haltuunsa ja kopioida kiintolevyn kokonaisuudessaan takavarikoitavan aineiston löytämiseksi ja vasta kopiota tarkastettaessa ollut velvollinen tutkimaan, onko kiintolevyllä takavarikkokiellon alaista tietoa.

Jotta pakkokeinolain mukainen takavarikkokiello toteutuisi, tulee esitutkintaviranomaisen kuitenkin jo kopiointivaiheessa eikä vasta myöhemmin kopiota tutkimalla selvittää, onko kovalevyllä takavarikkokiellon alaista aineistoa. Takavarikkokiellon alainen materiaali tulee myös välittömästi poistaa.

Takavarikon toteuttamiseen liittyvät tekniset syyt ja esitutkintaviranomaisen käytännön tarpeet eivät siten voi oikeuttaa poikkeamaan sen selvittämisestä, onko kovalevyllä takavarikkokiellon alaista materiaalia. Esitutkinnassa tulee noudattaa pakkokeinolaissa säädettyä takavarikkokielloa.

## 2.2 Salassapidon toteutuminen takavarikkotilanteessa tulee varmistaa

Jotta salassapito toteutuisi takavarikkotilanteessa pakkokeinolain 4 luvun 2 §:n 2 momentissa edellytetyllä tavalla, tulee oikeusturvaa takavarikkotilanteessa nimenomaan parantaa. Siten takavarikossa on käytettävä virka-apuna toista salassapitovelvollista, jotta salassapidolla suojeltava taho (potilaat ja asiakkaat) eivät joutuisi uhrautuksi.

Oikeusturvan parantaminen voidaan toteuttaa esimerkiksi siten, että lääkärin potilas- tai asianajajan asianajosalaisuudet erottelisi samassa asemassa oleva ulkopuolinen lääkäri/asianajaja tai siten, että esitutkintaviranomainen joutuisi lisäksi hakemaan tuomioistuimelta etukäteen kotietsintä- ja takavarikkoluvan silloin, kun etsintä toteutetaan lääkärin tai asianajajan luona tai esimerkiksi lehden toimituksessa (lähdesuoja). Tuomioistuin voisi tällöin antaa luvan esimerkiksi sillä ehdolla, että sen nimeämä asianajaja/lääkäri on paikalla ja varmistaa sen, ettei muihin kuin etsittyihin asiakirjoihin puututa.



## 2.2.1 Euroopan ihmisoikeustuomioistuimen kanta

Syyskuun 19 päivänä 2002 annetussa englantilaisessa ihmisoikeustapauksessa *Tamosius v. UK*, jossa oli kyse talousrikostutkinnasta asianajajan luona, katsottiin valitus ilmeisen perusteettomaksi, kun käytössä oli olleet riittävät oikeussuojakeinot eli

- etukäteinen tuomioistuimen lupa,
- epäilyllä oli tehokas muutoksenhakekeino, jonka ajan takavarikoitu aiheisto oli sinetöitynä ja
- etsinnässä oli ollut paikalla oikeuskanslerin määräämä riippumaton asianajaja.

Tapaus löytyy osoitteesta [http://www.finlex.fi/oikeus/ey/feit/feit\\_1450.html](http://www.finlex.fi/oikeus/ey/feit/feit_1450.html)

Seuraavassa on referoituna tapauksen Finlex-seloste:

Kysymys siitä, liittyikö asianajajan toimistossa toimitettuun etsintään ja asiakirjojen takavarikkoon riittäviä prosessuaalisia takeita.

TOSISEIKAT: Valittaja on asianajaja. Vuodesta 1996 lähtien veroviranomaiset ovat tehneet tarkastuksia hänen yhden asiakkaansa kohdalta. Vuonna 1998 verottaja pyysi kotietsinnän toimittamista valittajan toimistossa. Hän vetosi asianajajan salassapitovelvollisuuteen eräiden asiakirjojen kohdalta. Vuonna 1999 em. asiakasta vastaan nostettiin rikosjuttu veropetoksen johdosta. Samana vuonna verottaja sai **oikeudelta** vastapuolta kuulematta annetun **päätöksen, jolla verottaja oikeutettiin toimituttamaan valittajan toimitiloissa etsintä** hänen päämiestensä tekemiksi epäiltyjä törkeitä veropetoksia osoittavien asiakirjojen löytämiseksi. Verottaja epäili valittajan itsensäkin syyllistyneen sellaisiin rikoksiin olemalla mukana järjestelyissä ja salaamalla järjestelyjä verottajalta.

---

**Takavarikoida ei kuitenkaan saanut asianajajan salassapitovel-**

### **vollisuuden käsittämiä asiakirjoja.**

Valittaja sai päätöksen osalta valitusluvan. Samalla määrättiin, että **toimitiloista otettava aineisto oli sinetöitävä eikä sitä saanut tarkastaa ennen valituksen käsittelyä.**

- - -

...uusi päätös pantiin täytäntöön vuonna 1999. Tällöin takavarikoitiin vajaat 70 asiakirjaa. Menettely oli seuraava: Takavarikon toimittajat hakivat asiaan liittyvää aineistoa. Kun sellaista katsottiin löytyneen, **aineiston tarkasti oikeuskanslerin määräämä asianajaja lausuakseen siitä, oliko se salassapitovelvollisuuden alais- ta.** Kaikki salassa pidettävät asiakirjat annettiin takaisin valittajan asianajajalle.

EIT lausui, että kun

- etsintä oli toimitettu tuomarin antaman päätöksen nojalla,
- etsintää oli lisäksi valvonut asianajaja, jonka oli tullut osoittaa ne salassa pidettävät asiakirjat, joita ei saanut takavarikoida, ja kun
- oikeuskanslerin määräämä asianajaja oli toiminut itsenäisesti ja hän oli antanut riippumattoman lausunnon,

etsintä ei toimitetun kaltaisena ollut suhteetonta tavoitteisiinsa nähden ja etsintään oli liittynyt riittäviä prosessuaalisia takeita. Siten EIT totesi, että valitus oli ilmeisen perusteeton.

#### 2.2.2 Pakkokeinolain takavarikkokieltosäännös tulee yhdenmukaistaa EIT:n kannan kanssa

Pakkokeinolain 4 luvun 2 §:n 2 momentti tulee muuttaa vastaamaan edellä selostettua Euroopan ihmisoikeustuomioistuimen päätöstä.

Helsingissä kesäkuun 16 päivänä 2003

Satu Tiirikka

Asianajaja

