EUROOPAN YHTEISÖJEN KOMISSIO

Bryssel 26.1.2001
KOM(2000) 890 lopullinen

**KOMISSION TIEDONANTO**
**NEUVOSTOLLE, EUROOPAN PARLAMENTILLE,**
**TALOUS- JA SOSIAALIKOMITEALLE JA**
**ALUEIDEN KOMITEALLE**

# Turvallisempaan tietoyhteiskuntaan tietojärjestelmien turvallisuutta parantamalla ja tietokonerikollisuutta ehkäisemällä

**Tiivistelmä**

Euroopan unionin muuntuminen tietoyhteiskunnaksi näkyy selvästi elämän kaikilla osa-alueilla: niin työssä, koulutuksessa ja vapaa-ajassa kuin julkisessa hallinnossa, elinkeinoelämässä ja kaupan alalla. Uudet tieto- ja viestintätekniikat mullistavat talouselämän ja yhteiskunnan toiminnan. Toimivan tietoyhteiskunnan luominen on tärkeää EU:n talouskasvun, kilpailukyvyn ja työllisyysnäkymien kannalta ja sillä on kauaskantoisia taloudellisia, yhteiskunnallisia ja oikeudellisia vaikutuksia.

Komissio käynnisti joulukuussa 1999 *e*Europe-aloitteen varmistaakseen, että Euroopan unioni voi hyödyntää digitaalitekniikan edut ja että syntyvä tietoyhteiskunta on kaikkien kansalaisten käytettävissä. Kesäkuussa 2000 Feirassa kokoontunut Eurooppa-neuvosto hyväksyi laajan *e*Europe-toimintasuunnitelman, jonka se määräsi pantavaksi täytäntöön vuoden 2002 loppuun mennessä. Toimintasuunnitelmassa korostetaan verkkoturvallisuuden merkitystä sekä tietoverkkorikollisuuden torjuntaa.

Tieto- ja viestintäverkoista on tullut yksi talouden keskeinen tekijä. Valitettavasti näissä rakenteissa on omat heikkoutensa, joiden vuoksi niitä on mahdollista käyttää uudentyyppiseen rikolliseen toimintaan. Rikollista toimintaa voidaan harjoittaa monin eri tavoin ja monien rajojen yli. Vaikka luotettavia tilastotietoja ei monestakaan syystä ole käytettävissä, nämä rikokset epäilemättä muodostavat uhkan teollisuuden investoinneille ja omaisuudelle sekä tietoyhteiskunnan turvallisuudelle ja uskottavuudelle. Äskettäisten ruuhkauttamis- ja virushyökkäysten on todettu aiheuttaneen suuria taloudellisia vahinkoja.

Rikollista toimintaa voidaan ehkäistä toisaalta tehostamalla tietojärjestelmien tietoturvaa ja toisaalta varmistamalla, että lainvalvontaviranomaisilla on käytössään tarkoituksenmukaiset keinot. Samalla on kuitenkin tiukasti pidettävä kiinni kansalaisten perusoikeuksista.

Euroopan unioni on jo toteuttanut toimenpiteitä Internetissä esiintyvän haitallisen ja laittoman sisällön torjumiseksi, teollis- ja tekijänoikeuksien sekä henkilötietojen suojaamiseksi, sähköisen kaupankäynnin ja sähköisten allekirjoitusten käytön edistämiseksi sekä tapahtumankäsittelyn tietoturvan parantamiseksi. Huhtikuussa 1998 komissio esitti neuvostolle tietokonerikollisuutta koskevan tutkimuksen (ns. COMCRIME-tutkimuksen) tulokset. Lokakuussa 1999 Tampereella pidetyssä Eurooppa-neuvoston kokouksessa päätettiin, että myös huipputekniikkaan liittyvälle rikollisuudelle olisi kehitettävä yhteiset tunnusmerkistöt ja seuraamukset. Myös Euroopan parlamentti on esittänyt, että tietokonerikoksille olisi löydettävä yhteiset määritelmät ja kansallisia lakeja olisi lähennettävä tehokkaasti varsinkin aineellisen rikosoikeuden alalla. Euroopan unionin neuvosto on vahvistanut yhteisen kannan tietoverkkorikollisuutta koskevasta Euroopan neuvoston yleissopimuksesta käytäviin neuvotteluihin ja lisäksi vahvistanut joitakin alustavia toimenpiteitä osana unionin strategiaa huipputekniikkaan liittyvän rikollisuuden torjumiseksi. Eräät EU:n jäsenvaltiot ovat myös olleet näkyvästi mukana alaan liittyvässä G8-maiden toiminnassa.

Tässä tiedonannossa tarkastellaan laaja-alaisen poliittisen aloitteen tarvetta ja mahdollisia toteutustapoja. EU:n laajempien *tietoyhteiskuntaan* sekä *vapauteen, turvallisuuteen ja oikeudenmukaisuuteen* liittyvien tavoitteiden osana pyritään lisäämään tietojärjestelmien tietoturvaa ja ehkäisemään tietoverkkorikollisuutta kunnioittaen samalla unionin tunnustamia kansalaisten perusoikeuksia.

Komission mielestä lyhyellä aikavälillä on tarpeen laatia EU-säädös sen varmistamiseksi, että jäsenvaltioilla on käytössään tehokkaat keinot Internetissä välitettävän lapsipornografian vähentämiseksi. Komissio esittää myöhemmin tänä vuonna ehdotuksen puitepäätökseksi, joka on osa laajempaa toimenpidekokonaisuutta lasten seksuaalisen hyväksikäytön ja ihmiskaupan torjumiseksi. Puitepäätöksessä annetaan muun muassa lakien ja seuraamusten lähentämistä koskevia säännöksiä.

Pitkällä aikavälillä komissio tekee säädösehdotuksia, joiden tarkoituksena on edelleen lähentää rikoslainsäädäntöä huipputekniikkaan liittyvän rikollisuuden osalta. Lokakuussa 1999 Tampereella kokoontuneen Eurooppa-neuvoston päätelmien mukaisesti komissio tutkii myös, miten voitaisiin toteuttaa tietoverkkorikosten tutkinnan yhteydessä ennen oikeudenkäyntiä annettujen määräysten vastavuoroinen tunnustaminen.

Samanaikaisesti komissio aikoo edistää kansallisten tietokonerikoksiin erikoistuneiden poliisiyksikköjen perustamista siellä missä tällaisia yksikköjä ei vielä ole, tukea lainvalvontaviranomaisten tarkoituksenmukaista teknistä koulutusta ja kannustaa Euroopassa harjoitettavaa tietoturvaan liittyvää toimintaa.

Teknisellä puolella komission tarkoituksena on asiaa koskevien säännösten puitteissa edistää tutkimus- ja kehitystoimintaa, jonka avulla voidaan paremmin ymmärtää ja korjata järjestelmän heikkouksia sekä levittää tietämystä.

Lisäksi komissio aikoo perustaa EU:lle oman keskustelufoorumin, jolla lainvalvontaviranomaiset, Internet-palveluntarjoajat, kansalaisoikeusjärjestöt, kuluttajien edustajat, tietosuojaviranomaiset ja muut osapuolet voivat vaihtaa ajatuksia ja tehostaa yhteistoimintaansa EU:n tasolla. Näin pyritään tuomaan yleiseen tietoisuuteen Internetiä käyttävien rikollisten aiheuttamia riskejä, edistämään turvallisuuden kannalta parhaita käytäntöjä, kehittämään tehokkaita rikostentorjuntavälineitä ja -keinoja tietokonerikollisuuden kitkemiseksi sekä kehittämään ennakkovaroitus- ja kriisinhallintajärjestelmiä edelleen.

## TIEDONANTOA KOSKEVAT KOMMENTIT

**Euroopan komissio pyytää kaikkia kiinnostuneita esittämään kommenttinsa tässä tiedonannossa käsitellyistä asioista. Kommentteja voidaan lähettää 23.3.2001 asti sähköpostitse osoitteeseen**

Infso-jai-cybercrime-comments@cec.eu.int.

**Yleensä kommentit julkaistaan komission www-sivuilla, ellei lähettäjä sitä erikseen kiellä. Nimettömiä kommentteja ei julkaista. Komissio pidättää itselleen oikeuden jättää saamansa kommentit julkaisematta (esimerkiksi jos ne sisältävät loukkaavaa kielenkäyttöä). Julkaistut kommentit ovat luettavissa seuraavan osoitteen kautta:**

http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/crime1.html**.**

**Kommenttien laatimista koskevat tekniset ohjeet ja julkaisukäytäntöä koskevat tiedot julkaistaan samoilla www-sivuilla lähiaikoina. Kommentoijia pyydetään tutustumaan ohjeisiin ennen kommenttiensa lähettämistä.**

## JULKINEN KUULEMISTILAISUUS

**Euroopan komissio järjestää asianomaisten julkisen kuulemistilaisuuden tiedonannossa käsitellyistä asioista. Tilaisuus pidetään 7.3.2001. Niitä, jotka haluavat esittää tilaisuudessa puheenvuoron, pyydetään ilmoittautumaan 20.2.2001 mennessä sähköpostilla seuraavaan osoitteeseen:**

Infso-jai-cybercrime-hearing@cec.eu.int

**tai postitse seuraavaan osoitteeseen:**

**Euroopan komissio**
**BU33-5/9**
**200 Wetstraat/Rue de la Loi**
**B-1049 Brussel/Bruxelles**
**Belgia**

**Jos ilmoittautumisia on paljon, komissio pitää itsellään oikeuden valita kuultaviksi kutsuttavat osapuolet siten, että mahdollisimman monet eturyhmät ovat edustettuina.**

# SISÄLLYSLUETTELO

## 1 TIETOYHTEISKUNNAN MAHDOLLISUUDET JA UHKAKUVAT

Ajallemme on ominaista talouselämän globalisaatio ja se, että yhä useammilla on varaa hankkia ja mahdollisuus käyttää tietoyhteiskunnan tekniikkaa. Internetin kaltaisten avointen verkkojen tekninen kehitys ja käytön lisääntyminen tulevina vuosina luo uusia mahdollisuuksia ja myös uusia haasteita.

Maaliskuussa 2000 Lissabonissa kokoontunut Eurooppa-neuvosto ilmaisi pitävänsä tärkeänä siirtymistä kilpailukykyiseen, dynaamiseen ja osaamiselle rakentuvaan talouteen ja pyysi neuvostoa ja komissiota laatimaan *e*Europe-toimintasuunnitelman, jonka avulla nämä mahdollisuudet voidaan hyödyntää mahdollisimman hyvin.[1] Komission ja neuvoston laatimaan toimintasuunnitelmaan, jonka Feirassa kokoontunut Eurooppa-neuvosto hyväksyi kesäkuussa 2000, sisältyy toimenpiteitä verkkoturvallisuuden parantamiseksi sekä tietoverkkorikollisuutta koskevan koordinoidun ja johdonmukaisen toimintamallin luomiseksi vuoden 2002 loppuun mennessä.[2]

Tietojärjestelmistä on tullut tärkeä talouselämän tukipilari. Käyttäjien on voitava luottaa tietopalvelujen saatavuuteen ja siihen, että kukaan ulkopuolinen ei pääse luvatta lukemaan tai muuttamaan heidän viestejään ja tietojaan. Näistä seikoista riippuu, yleistyykö sähköinen kaupankäynti ja toteutuuko tietoyhteiskunta kokonaisvaltaisesti.

Uudet digitaalitekniikat ja langattomat tekniikat ulottuvat jo kaikkialle. Niiden ansiosta voimme liikkua vapaasti ja olla silti aina tavoitettavissa sekä käyttää lukemattomia palveluja, jotka perustuvat useista verkoista koostuviin verkostoihin. Niiden avulla voimme osallistua, opettaa ja opiskella, voimme harrastaa ja työskennellä yhdessä ja voimme olla mukana poliittisessa päätöksenteossa. Kun yhteiskunta tulee entistä riippuvaisemmaksi uusista tekniikoista, on kuitenkin otettava käyttöön tehokkaita käytännöllisiä ja oikeudellisia keinoja riskien hallitsemiseksi.

Tietoyhteiskunnan tekniikkaa voidaan käyttää erilaisten rikosten tekemiseen ja sillä voidaan helpottaa rikosten tekemistä. Vilpillisessä mielessä toimivien, pahantahtoisten tai välinpitämättömien henkilöiden käsissä tekniikkaa voidaan käyttää apuvälineenä toiminnassa, joka uhkaa tai vahingoittaa yksilöiden henkeä, omaisuutta tai ihmisarvoa taikka loukkaa yleistä etua.

Perinteisesti tietoturvasta on huolehdittu luokittelemalla tiedot organisatorisesti, maantieteellisesti ja rakenteellisesti niiden arkaluonteisuuden ja aihepiirin mukaan. Digitaaliympäristössä tämä toimintamalli ei ole enää käyttökelpoinen, sillä kun tietojenkäsittely on hajautettua, palvelut kulkevat liikkuvien käyttäjien mukana ja järjestelmien on oltava yhteensopivia. Uuteen tekniikkaan perustuvat innovatiiviset ratkaisut korvaavat perinteiset suojauskeinot. Innovatiivisia ratkaisuja ovat salausmenetelmät, digitaaliset allekirjoitukset, käyttöoikeuksien tarkistamisessa ja todentamisessa käytettävät uudet välineet ja erilaiset suodattimet[3]. Tietojärjestelmien turvallisuuden ja luotettavuuden takaamiseksi tarvitaan erilaisia tekniikoita, joita on myös osattava käyttää asianmukaisella ja

---

1 Lissabonin Eurooppa-neuvosto, 23.-24. maaliskuuta 2000, puheenjohtajan päätelmät, katso http://ue.eu.int/fi/Info/eurocouncil/index.htm.

2 http://europa.eu.int/comm/information_society/eeurope/pdf/actionplan_fi.pdf.

3 Tietovirtoja suodatetaan ja valvotaan kaikilla tasoilla: palomuuri tarkastaa datapaketit, ohjelmasuodatin etsii vahingolliset ohjelmat, sähköpostisuodatin poistaa roskapostin huomaamattomasti ja selailusuodatin estää pääsyn haitalliseen aineistoon.

tehokkaalla tavalla. Osa näistä tekniikoista on jo olemassa, mutta käyttäjät eivät useinkaan ole tietoisia niistä eivätkä siitä, kuinka niitä käytetään tai miksi niitä olisi peräti välttämätöntä käyttää.

## 1.1 Kansalliset ja kansainväliset reaktiot

Tietokonerikoksia tehdään kaikkialla tietoverkoissa yli valtioiden rajojen. Periaatteessa niitä voidaan tehdä mistä päin maailmaa tahansa ja ne voivat kohdistua kehen hyvänsä tietokoneen käyttäjään. Yleisesti ollaan yksimielisiä siitä, että tehokkaita tietokonerikollisuutta ehkäiseviä toimenpiteitä tarvitaan sekä kansallisella että kansainvälisellä tasolla.[4]

Kansallisella tasolla voidaan todeta, että monissa maissa verkkoturvallisuuden ja tietokonerikollisuuden uusiin haasteisiin ei ole vastattu laaja-alaisella ja kansainvälisesti suuntautuneella tavalla. Useimmissa maissa tietokonerikollisuutta pyritään hillitsemään kansallisen (pääasiassa rikosoikeudellisen) lainsäädännön avulla, mutta samalla laiminlyödään vaihtoehtoiset ennaltaehkäisevät toimenpiteet.

Huolimatta kansainvälisten ja ylikansallisten järjestöjen ponnisteluista kansallisissa laeissa on maailmanlaajuisesti huomattavia eroavuuksia mm. rikosoikeudellisissa säännöksissä, jotka koskevat tietojärjestelmiin murtautumista, liikesalaisuuksien suojaa ja laitonta sisältöä. Merkittäviä eroja on myös säännöksissä, joita on annettu tutkintaelinten pakkokeinovaltuuksista (varsinkin salattujen tietojen ja kansainvälisissä verkostoissa suoritettavien tutkimusten osalta), lainkäyttövallasta rikosasioissa sekä toisaalta välittäjinä toimivien palveluntarjoajien ja toisaalta sisällöntuottajien vastuusta. Välityspalvelujen tarjoajien vastuuta koskevia säännöksiä on muutettu sähköisestä kaupankäynnistä annetulla direktiivillä 2000/31/EY[5]. Lisäksi direktiivissä kielletään jäsenvaltioita asettamasta välityspalvelujen tarjoajille yleistä velvoitetta valvoa siirtämiään ja tallentamiaan tietoja.

Kansainvälisellä ja ylikansallisella tasolla on laajalti tunnustettu, että tietokonerikollisuuden torjumiseksi tarvitaan tehokkaita keinoja, ja monet järjestöt koordinoivat tai pyrkivät yhdenmukaistamaan toimiaan. Joulukuussa 1997 G8-maiden oikeus- ja sisäasioista vastaavat ministerit hyväksyivät periaateluettelon ja kymmenkohtaisen toimintasuunnitelman, joka vahvistettiin G8-maiden huippukokouksessa Birminghamissa kesäkuussa 1998 ja jota nyt toteutetaan.[6] Helmikuussa 1997 Euroopan neuvosto ryhtyi valmistelemaan tietoverkkorikollisuutta koskevaa kansainvälistä yleissopimusta, joka valmistunee vuoden 2001 aikana.[7] Tietoverkkorikollisuuden torjumista käsitellään myös Euroopan komission ja eräiden EU:n ulkopuolisten maiden välisissä neuvotteluissa. Tämä on johtanut

---

4 Ks. esim. *e*Europe-toimintasuunnitelma sivulla http://europa.eu.int/comm/information_society/eeurope/pdf/actionplan_fi.pdf, komissaari António Vitorinon puheenvuoro sivulla http://europa.eu.int/comm/commissioners/vitorino/speeches/2000/septembre/2000-19-09-en_brussels.pdf ja Ranskan pääministeri Lionel Jospinin puheenvuoro sivulla http://www.france.diplomatie.fr/actual/evenements/cybercrim/jospin.gb.html.

5 Tietoyhteiskunnan palveluja, erityisesti sähköistä kaupankäyntiä, sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista 8. kesäkuuta 2000 annettu direktiivi 2000/31/EY ("direktiivi sähköisestä kaupankäynnistä").

6 EU:n oikeus- ja sisäasioiden neuvosto hyväksyi 19. maaliskuuta 1998 G8-maiden huipputekniikkaan liittyvää rikollisuutta koskevat 10 periaatetta ja kehotti sellaisia EU:n jäsenvaltioita, jotka eivät kuulu G8-maihin, valmistelemaan verkostoon liittymistä (http://ue.eu.int/ejn/index.htm).

7 Sopimusluonnos ja lehdistötiedote (jotka julkaistiin 27. huhtikuuta 2000) "Crime in Cyberspace – First Draft of International Convention Released for Public Discussion" ovat saatavana Internetistä kahtena kieliversiona, englanniksi (http://conventions.coe.int/treaty/en/projets/cybercrime.htm) ja ranskaksi (http://conventions.coe.int/treaty/fr/projets/cybercrime.htm).

kriittisten järjestelmien suojaa käsittelevän EY:n ja USA:n yhteisen työryhmän perustamiseen.[8]

Myös YK ja OECD ovat toimineet aktiivisesti tällä alalla, jota käsitellään myös sellaisilla kansainvälisillä foorumeilla kuin Global Business Dialogue ja Trans-Atlantic Business Dialogue.[9]

Euroopan unionin lainsäädäntö on viime aikoihin asti koskenut pääasiassa tekijänoikeutta, perusoikeuksiin kuuluvaa yksityisyyden ja henkilötietojen suojaa, ehdollisen pääsyn järjestelmiä, sähköistä kaupankäyntiä, sähköisiä allekirjoituksia ja erityisesti tietokonerikollisuuteen välillisesti liittyvien salaustuotteiden kaupan vapauttamista.

Lainsäädännön lisäksi kolmen–neljän viime vuoden aikana on toteutettu myös muita merkittäviä toimenpiteitä. Näihin kuuluvat Internetin laitonta ja haitallista sisältöä koskeva toimintasuunnitelma, josta myönnetään rahoitusta valistustoimintaan, sisällön luokittelua ja suodattamista koskeviin kokeiluihin ja ns. vihjelinjojen toimintaan, sekä aloitteet, jotka koskevat alaikäisten ja ihmisarvon suojelua tietoyhteiskunnassa, lapsipornografiaa ja lainvalvontaviranomaisten harjoittamaa telekuuntelua.[10] EU on jo kauan tukenut tutkimus- ja kehityshankkeita, joilla pyritään edistämään tietojärjestelmien ja sähköisten liiketoimien turvallisuutta ja luotettavuutta, ja on äskettäin myöntänyt lisämäärärahoja IST-ohjelman niitä koskevalle osuudelle. Tutkimus- ja toimintahankkeita, joilla edistetään lainvalvontaviranomaisten erityiskoulutusta sekä lainvalvontaviranomaisten ja atk-alan välistä yhteistyötä, on tuettu myös kolmanteen pilariin kuuluvien ohjelmien (STOP, Falcone, Oisin, Grotius ym.) avulla.[11]

Järjestäytyneen rikollisuuden vastaisessa toimintasuunnitelmassa, jonka oikeus- ja sisäasioiden neuvosto hyväksyi toukokuussa 1997 ja jonka Amsterdamissa kokoontunut Eurooppa-neuvosto vahvisti, pyydettiin komissiota tekemään tutkimus tietokonerikollisuudesta vuoden 1998 loppuun mennessä. Komissio esittikin niin sanotun COMCRIME-tutkimuksen neuvoston alaiselle järjestäytyneen rikollisuuden vastaiselle

---

8 Työryhmä toimii EY:n ja USA:n tiede- ja teknologiayhteistyösopimukseen perustuvan yhteisen neuvoa-antavan ryhmän alaisena.

9 YK on julkaissut laajan tietokonerikollisuuden ehkäisemistä ja valvontaa koskevan käsikirjan (”Manual on the prevention and control of computer-related crime”), jonka tiedot on äskettäin saatettu ajan tasalle. Vuonna 1983 OECD tutki rikoslakien kansainvälisen soveltamisen ja yhdenmukaistamisen mahdollisuutta tietokonerikollisuudesta tai atk:n väärinkäytöstä aiheutuvien ongelmien ratkaisemiseksi. Vuonna 1986 se julkaisi kertomuksen ”Computer-Related Crime: Analysis of Legal Policy”, jossa tarkasteltiin silloisia lakeja ja muutosehdotuksia eräissä jäsenvaltioissa ja suositeltiin otettavaksi käyttöön luettelo väärinkäytöksistä, joiden kieltämistä ja rikosoikeudellista rangaistavuutta näiden maiden olisi syytä harkita. Vuonna 1992 OECD antoi tietojärjestelmien turvallisuutta koskevat suuntaviivat, jotka on tarkoitettu valtioiden ja yksityisen sektorin tietojärjestelmien turvallisuusrakenteiden perustaksi.

10 Euroopan audiovisuaalisia ja tietopalveluja tuottavien yritysten kilpailukyvyn parantamisesta edistämällä kansallisia järjestelmiä, joiden tarkoituksena on saattaa alaikäisten ja ihmisarvon suojelu vertailukelpoiselle ja tehokkaalle tasolle, 24. syyskuuta 1998 annettu neuvoston suositus 98/560/EY. Vihreä kirja alaikäisten ja ihmisarvon suojelusta audiovisuaalisissa ja tietopalveluissa, KOM(96)483, lokakuu 1996, http://europa.eu.int/en/record/green/gp9610/protec.htm.
Komission tiedonanto neuvostolle, Euroopan parlamentille, talous- ja sosiaalikomitealle ja alueiden komitealle – Internetin laiton ja haitallinen sisältö (KOM(96) 487 lopullinen).
Päätöslauselma Internetin laitonta ja haitallista sisältöä koskevasta komission tiedonannosta (KOM(96)487 - C4-0592/96).
Laillisen telekuuntelun kansainvälisistä edellytyksistä 17. tammikuuta 1995 annettu neuvoston päätöslauselma (EYVL C 329, 4.11.1996, s. 1).

11 http://europa.eu.int/comm/justice_home/jai/prog_fi.htm.

monitieteiselle työryhmälle huhtikuussa 1998.[12] Myös käsillä olevaa tiedonantoa voidaan pitää jatkovastauksena oikeus- ja sisäasioiden neuvoston pyyntöön.

Ennen tiedonannon laatimista komissio kävi epävirallisia keskusteluja jäsenvaltioiden lainvalvontaviranomaisten ja tietosuojaviranomaisten[13] sekä alan eurooppalaisten toimijoiden (lähinnä Internet-palveluntarjoajien ja teleoperaattoreiden) kanssa.[14]

Tiedonannossa tarkastellaan erilaisia toimenpidevaihtoehtoja, joiden avulla EU voi torjua tietokonerikollisuutta. Lähtökohtana ovat olleet edellä mainitussa tutkimuksessa esitetyt analyysit ja suositukset, kuulemisprosessin perusteella tehdyt johtopäätökset, Amsterdamin sopimuksen tarjoamat uudet mahdollisuudet sekä EU:ssa, G8-maissa ja Euroopan neuvostossa jo tehty työ. Valitut ratkaisumallit eivät saa haitata tai pirstoa Euroopan unionin sisämarkkinoita eivätkä johtaa perusoikeuksien suojaa heikentäviin toimenpiteisiin.[15]

## 2 TIETOJÄRJESTELMIEN TIETOTURVA

Tietoyhteiskunnassa käyttäjien ohjaamat maailmanlaajuiset verkot korvaavat vähitellen vanhat kansalliset viestintäverkot. Internetin menestys perustuu muun muassa siihen, että sen käyttäjät voivat hyödyntää uusinta tekniikkaa. Mooren lain[16] mukaan tietokoneiden teho kaksinkertaistuu puolessatoista vuodessa. Viestintätekniikka kehittyy tätäkin nopeammin.[17] Esimerkiksi Internetin kautta siirrettävän tiedon määrä on viime aikoina kaksinkertaistunut alle vuodessa.

Perinteiset puhelinverkot ovat olleet kansallisten organisaatioiden rakentamia ja hoitamia. Niiden käyttäjillä ei ole ollut juurikaan valinnanvaraa palvelujen suhteen eikä valtaa vaikuttaa toimintaympäristöön. Ensimmäiset tietoverkot rakennettiin saman keskitetyn valvonnan periaatteen pohjalta, mikä vaikutti myös niiden tietoturvaan.

Internet ja muut uudet verkot ovat aivan erilaisia, mikä on otettava huomioon niiden tietoturvan hallinnassa. Näissä verkoissa äly ja valvonta sijaitsevat etäällä ytimestä eli siellä missä käyttäjät ja palvelut ovat. Verkon runko on yksinkertainen ja tehokas, ja sen tehtävänä on lähinnä tiedon siirtäminen. Sisällön tarkastus ja valvonta on vähäistä. Vasta määränpäässä bitit muuttuvat ääneksi, röntgenkuvaksi tai tilitapahtuman vahvistukseksi. Näin ollen

---

12 ”Legal Aspects of Computer-related Crime in the Information Society – COMCRIME”. Würzburgin yliopistossa työskentelevä professori U. Sieber teki tutkimuksen Euroopan komission toimeksiannosta. Loppuraportti on saatavana verkko-osoitteesta http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html.

13 Tietosuojaa valvovat viranomaiset muodostavat direktiivin 95/46/EY 29 artiklan mukaisen tietosuojatyöryhmän, joka on itsenäisesti toimiva neuvoa-antava EU:n elin, ks. myös direktiivin 30 artikla.

14 Lainvalvontaviranomaisten kanssa pidettiin kaksi kokousta, 10. joulukuuta 1999 ja 1. maaliskuuta 2000. Internet-yritysten edustajien kanssa pidettiin kokous 13. maaliskuuta 2000, ja henkilötietojen suojaan erikoistuneiden asiantuntijoiden kanssa pienimuotoinen kokous 31. maaliskuuta 2000. Kaikkien edellä mainittujen tahojen kanssa pidettiin loppukokous 17. huhtikuuta 2000. Kokouspöytäkirjoja voi tilata kirjallisesti osoitteesta Euroopan komissio, yksikkö INFSO/A5 tai Euroopan komissio, yksikkö JAI/B2, Wetstraat/Rue de la Loi 2000, B-1049 Brussel/Bruxelles, Belgia.

15 EU:n perusoikeuskirja (ks. http://db.consilium.eu.int/df/default.asp?lang=fi), Euroopan unionista tehdyn sopimuksen 6 artikla ja Euroopan yhteisöjen tuomioistuimen oikeuskäytäntö.

16 Vuonna 1965 Gordon Moore, yksi Intelin perustajista, havaitsi, että integroitujen piirien transistoritiheys kasvaa koko ajan. Nykyään transistoritiheys kaksinkertaistuu suurin piirtein puolessatoista vuodessa, mikä on vaikuttanut suoraan tietokoneen mikrosirujen hintaan ja ominaisuuksiin. Monet asiantuntijat uskovat, että kehitys jatkuu tällaisena vielä ainakin vuosikymmenen ajan.

17 Uusimman tekniikan ansiosta yhdellä ainoalla valokaapelilla voidaan siirtää samanaikaisesti sataa miljoonaa äänipuhelua vastaava tietomäärä.

tietoturva on ennen muuta käyttäjien vastuulla, sillä ainoastaan käyttäjät voivat määritellä lähetettyjen tai vastaanotettujen bittien arvon ja päättää tarvittavasta suojan tasosta.

Käyttäjä on siten tietojärjestelmän keskeinen osa. Turvamenetelmien käyttöönotto edellyttää käyttäjän suostumusta ja osallistumista sekä hänen tarpeidensa huomioon ottamista. Tämä on erityisen tärkeää silloin, kun otetaan huomioon, miten monenlaisiin tarkoituksiin ihmiset käyttävät samaa päätettä. eri henkilöt käyttävät samaa päätettä yhä useampiin toimintoihin. He työskentelevät, pelaavat pelejä, katsovat televisiota ja maksavat laskuja saman laitteen avulla.

Käytössä on jo runsaasti tietoturvatekniikkaa, ja uutta kehitetään koko ajan lisää. Avoimen lähdekoodin ohjelmistojen kehittämisen edut tietoturvan kannalta ovat entistä ilmeisempiä. Muodollisten menetelmien ja tietoturvan arviointiperusteiden kehittämiseen on panostettu paljon. Salaustekniikasta ja sähköisistä allekirjoituksista tulee välttämättömiä varsinkin langattoman viestinnän lisääntyessä. Käyttöoikeuksien todentamiseen tarvitaan yhä uusia keinoja, sillä käyttäjillä on erilaisissa käyttötilanteissa eri tarpeet. On tilanteita, joissa käyttäjällä on tarve tai halu esiintyä nimettömänä. Joskus taas käyttäjän on kenties voitava henkilöllisyyttään paljastamatta todistaa olevansa täysi-ikäinen, jonkin yrityksen työntekijä tai asiakas tms. On myös tilanteita, joissa käyttäjän on voitava todistaa henkilöllisyytensä. Kaiken aikaa kehitetään myös ohjelmistosuodattimia, joiden avulla käyttäjät voivat suojata itseään tai huollettaviaan epätoivottavalta aineistolta, roskapostilta, vahingollisilta ohjelmilta tai muunlaisilta hyökkäyksiltä. Internetin ja uusien verkkojen turvavaatimusten täyttäminen ja turvajärjestelmien hallinnointi merkitsee melkoista kustannuserää sekä valmistajille että käyttäjille. Siksi on tärkeää kannustaa innovaatiota ja edistää tietoturvatekniikan ja -palveluiden kaupallista käyttöä.

Turvallisuusnäkökohdat ovat tietenkin tärkeitä myös yhteiskäyttöiselle siirtoyhteyksistä ja nimipalvelimista koostuvalle runkojärjestelmälle. Tiedonsiirto riippuu konkreettisista yhteyksistä, joiden kautta tieto reititetään tietokoneesta toiseen. Nämä yhteydet on sijoitettava ja suojattava niin että tiedon siirtäminen onnistuu mahdollisista onnettomuuksista ja hyökkäyksistä sekä viestiliikenteen jatkuvasta kasvusta huolimatta. Viestiliikenteen toiminnan kannalta olennaisia ovat keskeiset palvelut, esimerkiksi nimipalvelimet ja varsinkin lukumäärältään harvat juuripalvelimet, jotka vastaavat Internet-osoitteista. Kaikkia näitä osatekijöitä on suojattava asianmukaisella tavalla, joka riippuu siitä, mistä nimistön osasta on kyse ja mitä käyttäjäkuntaa kulloinkin palvellaan.

Tietotekniikan perusrakenteita kehitettäessä päätavoitteena on ollut joustavuuden lisääminen ja käyttäjien tarpeiden tyydyttäminen. Näin tekniikka on kehittynyt yhä monimutkaisemmaksi, kun taas tietoturvaan on monesti kiinnitetty liian vähän huomiota. Kun ohjelmat ovat yhä monisäikeisempiä ja riippuvaisempia toisistaan, niissä saattaa olla heikkoja kohtia, joita vahingontekijät voivat helposti käyttää hyväksi. Tietoverkkojen monimutkaistumisen ja niiden osasten teknisen kehityksen myötä niihin voi ilmaantua uusia, odottamattomia heikkouksia.

Tietoverkkojen turvallisuuden parantamiseksi on jo toteutettu useita teknisiä toimenpiteitä, ja uusia kehitetään koko ajan. Toimenpiteiden tavoitteena on

- varmistaa järjestelmien kriittisten osien tietoturva käyttämällä julkisen avaimen järjestelmiä, kehittämällä tietoturvaa tukevia yhteyskäytäntöjä jne.

- turvata yksityiset ja julkiset käyttöympäristöt kehittämällä laadukkaita ohjelmistoja, palomuureja, viruksentorjuntaohjelmia, oikeuksien hallinnointijärjestelmiä, salaustekniikoita jne.

- turvata valtuutettujen käyttäjien sähköinen tunnistus, älykorttien käyttö, biometrinen tunnistus, sähköiset allekirjoitukset, rooliperustaiset tekniikat jne.

Tätä varten on panostettava entistä enemmän tietoturvatekniikan kehittämiseen ja yhteistyöhön tavoitteena päästä sopimukseen kansainvälisistä standardeista, joiden avulla erilaiset ratkaisut saadaan toimimaan yhteen.

On myös tärkeää, että turvallisuussuunnittelu on järjestelmän yleisen arkkitehtuurin erottamaton osa ja että uhat ja heikkoudet ovat selvillä suunnitteluprosessin alusta lähtien. Tämä poikkeaa perinteisestä toimintamallista, jossa yritetään vain tilkitä järjestelmän aukkoja, joita rikolliset pystyvät käyttämään hyväkseen yhä kehittyneemmillä menetelmillä.

Käyttäjäystävällistä tietoyhteiskuntaa koskeva EU:n IST-ohjelma[18] tietotekniikkaa, verkkoturvallisuutta ja muita luottamusta lisääviä tekniikoita koskevine toimintoineen[19] luo puitteet, joiden pohjalta voidaan kehittää keinoja vastata tietokonerikollisuuteen liittyviin haasteisiin. Tällaisia keinoja ovat esimerkiksi tekniset välineet, joiden avulla suojellaan yksityisyyden ja henkilötietojen suojaa sekä muita henkilökohtaisia oikeuksia ja torjutaan tietokonerikollisuutta. IST-ohjelman osana on lisäksi käynnistetty käyttövarmuusaloite, jolla pyritään parantamaan käyttäjien luottamusta tiiviisti verkottuneisiin tietojärjestelmiin ja sulautettuihin järjestelmiin kiinnittämällä käyttäjien huomiota aiempaa enemmän käyttövarmuuteen ja edistämällä käyttövarmuutta. Aloitteeseen kuuluu kiinteänä osana myös kansainvälistä yhteistoimintaa. IST-ohjelma toimii joiltain osin yhteistyössä Yhdysvaltojen puolustusteollisuuden huippututkimushankkeita koordinoivan viraston (DARPA) ja kansallisen tiedesäätiön (NSF) kanssa ja on perustanut yhdessä Yhdysvaltojen ulkoasiainministeriön kanssa kriittisten järjestelmien suojelua käsittelevän EY:n ja USA:n yhteisen työryhmän.[20]

Muun muassa EU:n tietosuojadirektiiveissä säädettyjen tietoturvavaatimusten[21] käyttöönotto lisää myös osaltaan tietoverkkojen ja tietojenkäsittelyn turvallisuutta.

## 3 TIETOKONERIKOLLISUUS

Nykyaikaisten tieto- ja viestintäjärjestelmien avulla on mahdollista harjoittaa laitonta toimintaa missä ja milloin tahansa ja kohdistaa toiminta minne tahansa. Tietokonerikollisuudesta ei ole saatavana luotettavia, kattavia tilastotietoja. Todettujen ja ilmoitettujen tunkeutumistapausten lukumäärä on todennäköisesti toistaiseksi pienempi kuin ongelman todellinen laajuus edellyttäisi. Monet tapaukset jäävät järjestelmävastaavien ja käyttäjien tietämyksen ja kokemuksen rajallisuuden vuoksi huomaamatta. Lisäksi yritykset eivät ole useinkaan halukkaita kertomaan tietotekniikan väärinkäytöksistä, koska ne eivät

---

18 IST-ohjelmaa hallinnoi Euroopan komissio. Ohjelma on osa tutkimuksen ja teknologisen kehittämisen viidettä puiteohjelmaa (1998—2002). Lisätietoja saa verkko-osoitteesta http://www.cordis.lu/ist.

19 Avaintoiminto 2 – Uudet työtavat ja sähköinen kaupankäynti.

20 Työryhmä toimii EY:n ja USA:n tiede- ja teknologiayhteistyösopimukseen perustuvan yhteisen neuvoa-antavan ryhmän alaisena.

21 Ks. direktiivin 97/66/EY 4 artikla (jossa säädetään myös velvollisuudesta tiedottaa turvallisuusriskeistä) ja direktiivin 95/46/EY 17 artikla.

halua saada kielteistä julkisuutta eivätkä altistua uusille hyökkäyksille. Toistaiseksi vain harvat poliisiviranomaiset tilastoivat tietokoneiden ja viestintäjärjestelmien käyttöä näissä ja muissa rikoksissa. Voidaan kuitenkin olettaa, että laiton toiminta lisääntyy tietokoneiden ja verkkojen käytön kasvaessa. On selvää, että tarvitaan luotettavaa tietoa tietokonerikollisuuden laajuudesta.

Tässä tiedonannossa ’tietokonerikollisuus’ on määritelty hyvin laajasti: sillä tarkoitetaan kaikkea rikollisuutta, jossa tavalla tai toisella käytetään apuna tietotekniikkaa. Tietokonerikollisuuden olemuksesta on kuitenkin olemassa erilaisia käsityksiä. Ilmaisuja ’tietokonerikollisuus’, ’atk-rikollisuus’, ’huipputekniikkaan liittyvä rikollisuus’ ja ’tietoverkkorikollisuus’ käytetään usein synonyymeina. Toisistaan voidaan erottaa varsinainen tietokonerikollisuus ja perinteinen rikollisuus, jossa käytetään apuna tietotekniikkaa. Ajankohtainen esimerkki tästä on tyypillisten tullirikosten (salakuljetus, väärentäminen jne.) tekeminen Internetin avulla. Varsinaisten tietokonerikosten osalta on tarpeen saattaa kansallisten rikoslakien tunnusmerkistöt ajan tasalle, kun taas tietokoneen avulla tehtyjen perinteisten rikosten torjumiseksi on syytä parantaa yhteistyötä ja menettelytapoja.

Kaikki mainitut rikollisuuden muodot hyötyvät rajattomista tieto- ja viestintäverkoista sekä aineettomasta ja erittäin nopeasti muuttuvasta tiedonsiirrosta. Näiden ominaisuuksien vuoksi nykyisiä toimia on tarkistettava, jotta voidaan puuttua myös näiden verkkojen ja järjestelmien avulla harjoitettavaan laittomaan toimintaan.

Useat maat ovat antaneet tietokonerikollisuutta koskevaa lainsäädäntöä. Myös Euroopan unionin jäsenvaltioissa on annettu joitakin säädöksiä. Lukuun ottamatta lapsipornografiasta tehtyä neuvoston päätöstä suoranaisia tietokonerikollisuutta koskevia EU-säädöksiä ei ole toistaiseksi annettu, mutta joillakin säädöksillä on kuitenkin asian kannalta välillistä merkitystä.

EU:n tai jäsenvaltioiden lainsäädännössä huomioidut tärkeimmät tietokonerikollisuuden osa-alueet ovat:

*Yksityisyyden loukkaukset*: Useat maat ovat antaneet rikosoikeudellisia säännöksiä, jotka koskevat henkilötietojen laitonta keruuta, tallentamista, muuttamista, luovuttamista tai levittämistä. Euroopan unionissa on annettu kaksi direktiiviä, joilla lähennetään kansallista lainsäädäntöä yksityisyyden suojasta henkilötietojen käsittelyssä.[22] Direktiivin 95/46/EY 24 artiklan mukaan jäsenvaltioiden on toteutettava tarvittavat toimenpiteet direktiivin säännösten täydellisen soveltamisen varmistamiseksi ja määriteltävä seuraamukset direktiivin mukaisesti säädettyjen säännösten rikkomistapauksissa. Myös Euroopan unionin perusoikeuskirjaan sisältyy määräyksiä yksityisyyden suojasta ja tietosuojasta.

[22] Yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24. lokakuuta 1995 annettu Euroopan parlamentin ja neuvoston direktiivi 95/46/EY sekä henkilötietojen käsittelystä ja yksityisyyden suojasta televiestinnän alalla 15. joulukuuta 1997 annettu Euroopan parlamentin ja neuvoston direktiivi 97/66/EY. Direktiivin 95/46/EY 24 artiklan mukaan jäsenvaltioiden on määriteltävä seuraamukset, joita sovelletaan tietosuojasäännösten rikkomistapauksissa.

*Sisältöön liittyvät rikokset:* Internetin avulla tapahtuva lapsi- ym. pornografian, rasististen lausuntojen ja väkivaltaa lietsovien tietojen levittäminen on nostanut esiin kysymyksen, kuinka tällaista toimintaa voitaisiin torjua rikoslainsäädännöllä. Komissio tukee näkemystä, jonka mukaan se mikä on laitonta verkon ulkopuolella, on laitonta myös verkossa. Tekijä tai sisällöntuottaja[23] voidaan saattaa rikosoikeudelliseen vastuuseen. Internetissä välitettävän lapsipornografian torjumiseksi on tehty neuvoston päätös.[24]

Välittäjinä toimivien palveluntarjoajien vastuuvelvollisuutta silloin, kun niiden verkkoja tai palvelimia käytetään kolmannen osapuolen tietojen siirtämiseen tai tallentamiseen, säännellään sähköisestä kaupankäynnistä annetussa direktiivissä.

*Talousrikokset, luvaton käyttö ja vahingonteko:* Useat maat ovat säätäneet tietokoneisiin liittyvää talousrikollisuutta koskevia lakeja, joissa määritellään tietokonejärjestelmien luvattomaan käyttöön liittyviä uudentyyppisiä rikoksia (esimerkiksi tietojärjestelmiin murtautumista ja niiden vahingoittamista, tietokonevirusten levittämistä sekä tietokonevakoilua, -väärennöksiä ja -petoksia[25]) ja uudenlaisia rikoksentekotapoja (esimerkiksi tietokoneen harhauttaminen ihmiseen kohdistuvan petoksen asemesta). Rikoksen kohteet ovat usein aineettomia, esimerkiksi pankkitalletuksia tai tietokoneohjelmia. Tällä hetkellä tämäntyyppiseen laittomaan toimintaan ei puututa missään EU-säädöksessä. Kaksikäyttötuotteista äskettäin annettu asetus on kuitenkin huomattavasti vapauttanut salaustuotteiden kauppaa.

*Teollis- ja tekijänoikeuksiin kohdistuvat rikokset:* Tietokoneohjelmien ja tietokantojen oikeudellisesta suojasta on annettu kaksi direktiiviä[26], jotka koskevat suoranaisesti tietoyhteiskuntaa ja joissa säädetään seuraamuksista. Neuvosto on vahvistanut yhteisen kannan ehdotuksesta direktiiviksi tekijänoikeudesta ja lähioikeuksista tietoyhteiskunnassa.[27] Direktiivi annettaneen vuoden 2001 alkupuolella. Siinä on tarkoitus säätää seuraamuksista, joita voidaan määrätä tekijänoikeuteen ja lähioikeuksiin kohdistuvista rikoksista sekä näiden oikeuksien suojaamiseksi tarkoitettujen teknisten järjestelmien kiertämisestä. Komissio antaa vuoden 2000 loppuun mennessä väärentämistä ja luvatonta jäljentämistä käsittelevän tiedonannon, jossa se esittää tiivistelmän vuonna 1998 vihreän kirjan julkaisemisella aloittamansa kuulemisprosessin tuloksista ja julkaisee asiaa koskevan toimintasuunnitelman. Internetin kaupallisen merkityksen kasvaessa jatkuvasti esiin tulee uusia kiistoja, jotka koskevat Internet-osoitteiden rekisteröintiin liittyvää monenlaista spekulatiivista

---

23 Sisällöntuottajaa ei pidä sekoittaa palveluntarjoajaan.

24 Internetissä välitettävän lapsipornografian vastaisista toimenpiteistä 29. toukokuuta 2000 tehty neuvoston päätös (EYVL L 138, 9.6.2000, s. 1).

25 Tiedotusvälineissä on kerrottu laajasti äskettäisistä suuriin www-sivustoihin kohdistuneista ruuhkauttamishyökkäyksistä ja niin sanotusta LoveLetter-viruksesta. Näitä tapauksia tarkasteltaessa olisi kuitenkin syytä pitää mielessä oikeat mittasuhteet. Ruuhkauttamishyökkäyksiä – tahallisia tai tahattomia – ja sähköpostin kautta leviäviä viruksia on ollut olemassa jo useiden vuosien ajan. Aiempia esimerkkejä ovat Morrisin mato ja IBM:n joulukuusi. Näiden häiriötekijöiden ehkäisemiseksi on olemassa erilaisia tuotteita ja toimintatapoja. Lisäksi Internet-käyttäjien kesken harjoitetaan jo paljon hyödyllistä yhteistoimintaa ilmenevien ongelmien aiheuttamien vahinkojen rajoittamiseksi. Myös roskapostin levittämistä pyritään ehkäisemään vastaavantyyppisellä yhteistoiminnalla.

26 Tietokoneohjelmien oikeudellisesta suojasta 14. toukokuuta 1991 annettu neuvoston direktiivi 91/250/ETY (EYVL L 122, 17.5.1991, s. 42).
Tietokantojen oikeudellisesta suojasta 11. maaliskuuta 1996 annettu Euroopan parlamentin ja neuvoston direktiivi 96/9/EY (EYVL L 77, 27.3.1996, s. 20).

27 Neuvoston vahvistama yhteinen kanta (EY) N:o 48/2000 Euroopan parlamentin ja neuvoston direktiivin antamiseksi tekijänoikeuden ja lähioikeuksien tiettyjen piirteiden yhdenmukaistamisesta tietoyhteiskunnassa (CS/2000/9512).

väärinkäyttöä (*cybersquatting*, *warehousing*, *reverse hijacking*), ja luonnollisesti alalla kaivataan sääntöjä ja menettelyjä näiden ongelmien ratkaisemiseksi.[28]

On huolehdittava myös siitä, että verotukseen liittyviä velvoitteita noudatetaan. Jos online-palvelujen saaja on sijoittautunut EU:n alueelle, palveluja koskevista liiketoimista syntyy yleensä verovelvoite siinä verotuspaikassa, jossa palvelut katsotaan kulutetuiksi.[29] Verovelvoitteen laiminlyöminen voi johtaa yksityisoikeudellisiin (tai jopa rikosoikeudellisiin) seuraamuksiin, kuten pankkitalletusten ja muun omaisuuden takavarikointiin. Vaikka velvoitteiden vapaaehtoinen noudattaminen on aina toivottavaa, viime kädessä velvoitteet on voitava panna juridisesti täytäntöön. Tämän tavoitteen toteutumisen kannalta ratkaisevan tärkeää on veroviranomaisten yhteistyö.

Aina kun kehitetään keino laillisen toiminnan suojaamiseksi, samalla rikolliset saavat keinon laittoman toimintansa suojaamiseen. Turvalliseen sähköiseen kaupankäyntiin tarkoitettuja välineitä voidaan käyttää myös huumekaupan edistämiseen. On siis asetettava asiat tärkeysjärjestykseen ja tehtävä valintoja.

Tietokonerikollisuuden uhrien suojaamiseen kuuluu myös rikoksiin liittyvien vastuu- ja korvauskysymysten ratkaiseminen. Luottamus edellyttää tarkoituksenmukaisen teknologian lisäksi myös siihen liittyviä oikeudellisia ja taloudellisia takeita. Näitä kysymyksiä on tarkasteltava tietokonerikollisuuden koko laajan kirjon kannalta.

Tietokonerikollisuuden uhrien suojelemiseksi ja rikoksentekijöiden vastuuseen saattamiseksi tarvitaan tehokkaita aineellisia ja prosessioikeudellisia välineitä, joita on lähennettävä toisiinsa maailmanlaajuisesti tai ainakin EU:n tasolla. Toisaalta henkilökohtainen viestintä, yksityisyyden ja henkilötietojen suoja, tiedon saatavuus ja tiedon levittäminen ovat nykyaikaisen demokratian perusoikeuksia. Tämän vuoksi käytettävissä olisi oltava tehokkaita ennalta ehkäiseviä toimenpiteitä, jotta oikeudellisiin pakkokeinoihin ei tarvitsisi ryhtyä. Tietokonerikollisuutta koskevassa lainsäädännössä on saatettava nämä tärkeät edut tasapainoon.

## 4 AINEELLISEEN OIKEUTEEN LIITTYVIÄ NÄKÖKOHTIA

Huipputekniikkaan liittyviä rikoksia koskevan aineellisen oikeuden lähentäminen varmistaa suojelun vähimmäistason tietoverkkorikollisuuden (mm. lapsipornografian) uhreille, täyttää vaatimuksen, jonka mukaan edellytyksenä keskinäisen oikeusavun antamiselle rikostutkinnassa on se, että toiminta katsotaan rikolliseksi molemmissa maissa (kaksoisrangaistavuuden vaatimus), ja selkeyttää alan pelisääntöjä (esimerkiksi sen osalta, mikä on katsottava laittomaksi sisällöksi).

---

[28] Komission tiedonanto neuvostolle ja Euroopan parlamentille – Internetin organisaatio ja hallinto – Kansainväliset ja eurooppalaiset poliittiset näkökohdat 1998–2000, huhtikuu 2000, KOM(2000) 202.

[29] Komissio on ehdottanut useita muutoksia EU:n alv-järjestelmään verotuspaikan määrittämisen helpottamiseksi (Ehdotus neuvoston direktiiviksi direktiivin 77/388/ETY muuttamisesta tiettyihin sähköisessä muodossa toimitettaviin palveluihin sovellettavien arvonlisäverojärjestelyjen osalta, KOM(2000) 349). Muutokset ovat parhaillaan neuvoston ja Euroopan parlamentin käsiteltävinä. Joissain tilanteissa veron voi joutua maksamaan palveluntarjoaja, vaikka tällä ei olisikaan toimipaikkaa verotuspaikan alueella.

Lokakuussa 1999 pidetystä Tampereen Eurooppa-neuvostosta[30] lähtien EU on suunnitellut säädöksen antamista tietokonerikollisuutta koskevan jäsenvaltioiden aineellisen rikosoikeuden lähentämiseksi. Mainitussa kokouksessa sisällytettiin huipputekniikkaan liittyvä rikollisuus niihin aloihin, joilla olisi pyrittävä laatimaan yhteiset rikostunnusmerkistöt ja määrittelemään syytteeseen asettamisen edellytykset sekä seuraamukset. Luettelo näistä aloista sisältyy oikeus- ja sisäasioiden neuvoston maaliskuussa 2000 hyväksymään järjestäytyneen rikollisuuden ehkäisemistä ja valvontaa koskevaan strategiaan (suositus 7).[31] Tämä tavoite on sisällytetty myös komission työohjelmaan vuodelle 2000 ja komission laatimaan vapauteen, turvallisuuteen ja oikeuteen perustuvan alueen perustamista koskevaan tulostauluun, jonka oikeus- ja sisäasioiden neuvosto hyväksyi 27. maaliskuuta 2000.[32]

Komissio on seurannut Euroopan neuvoston työtä tietoverkkorikollisuutta koskevan yleissopimuksen aikaan saamiseksi. Yleissopimusluonnoksessa luetellaan neljä rikosten luokkaa: 1) tietojärjestelmien luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuvat rikokset, 2) tietokonerikokset, 3) sisältöön liittyvät rikokset ja 4) tekijänoikeuden ja lähioikeuksien rikkomiseen liittyvät rikokset.

EU:n jäsenvaltioiden lainsäädännön lähentäminen voitaisiin toteuttaa nopeammin[33] ja siinä voitaisiin mennä pitemmälle kuin Euroopan neuvoston yleissopimuksessa, jossa määritellään kansainvälisen lähentämisen vähimmäistaso. Näin tuotaisiin tietokonerikollisuus EU-lainsäädännön piiriin ja saataisiin käyttöön EU:n laajuiset lainvalvontajärjestelyt.

Komission mielestä on hyvin tärkeää varmistaa, että EU:lla on käytössään tehokkaat keinot torjua erityisesti Internetissä välitettävää lapsipornografiaa. Komissio suhtautuu myönteisesti Internetissä välitettävän lapsipornografian torjumisesta tehtyyn neuvoston päätökseen mutta on Euroopan parlamentin kanssa samaa mieltä siitä, että kansallisia lakeja on edelleen lähennettävä toisiinsa. Komissio aikoo vielä vuoden 2000 aikana esittää ehdotuksen neuvoston puitepäätökseksi, johon sisältyy Internetissä välitettävää lapsipornografiaa koskevien lakien ja seuraamusten lähentämistä koskevia määräyksiä.[34]

Komissio esittää lähiaikoina Tampereen Eurooppa-neuvoston päätelmien mukaisesti Euroopan unionista tehdyn sopimuksen VI osaston mukaisen säädösehdotuksen huipputekniikkaan liittyvää rikollisuutta koskevan lainsäädännön lähentämisestä. Ehdotuksessa kehitellään edelleen Euroopan neuvostossa tehdyn työn tuloksia ja käsitellään jäsenvaltioiden lakien lähentämistä muun muassa tietojärjestelmiin murtautumisen ja ruuhkauttamishyökkäysten osalta. Ehdotuksessa esitetään myös EU:n vakiomääritelmät alan käsitteille. Siinä saatetaan mennä Euroopan neuvoston yleissopimusta pidemmälle myös siten, että vakavista rikoksista säädettäisiin kaikissa jäsenvaltioissa noudatettava vähimmäisrangaistus.

---

30 http://db.consilium.eu.int/fi/Info/eurocouncil/index.htm.

31 Järjestäytyneen rikollisuuden ehkäiseminen ja valvonta: Euroopan unionin strategia uuden vuosituhannen alkaessa (EYVL C 124, 3.5.2000).

32 http://europa.eu.int/comm/dgs/justice_home/index_fi.htm.

33 Euroopan neuvoston yleissopimus tulee voimaan vasta sitten kun se on ratifioitu.

34 Tämä aloite kuuluu ehdotuskokonaisuuteen, joka käsittää myös lasten seksuaaliseen hyväksikäyttöön ja ihmiskauppaan liittyviä laajempia aihepiirejä, kuten todetaan joulukuussa 1998 annetussa ihmiskauppaa käsittelevässä komission tiedonannossa. Ehdotus neuvoston puitepäätökseksi on liitteenä komission tiedonannossa neuvostolle ja Euroopan parlamentille ihmiskaupan ja lasten seksuaalisen hyväksikäytön torjumisesta. Lisäksi tämän tiedonannon yhteydessä julkaistaan kaksi puitepäätösehdotusta.

Komissio tarkastelee myös erilaisia vaihtoehtoja Internetissä esiintyvän rasismin ja muukalaisvihan torjumiseksi ja pyrkii laatimaan ehdotuksen Euroopan unionista tehdyn sopimuksen VI osaston mukaisesti tehtäväksi neuvoston puitepäätökseksi, joka kattaisi rasistisen ja muukalaisvastaisen toiminnan (sekä verkossa että sen ulkopuolella). Siinä otetaan huomioon 15. heinäkuuta 1996 hyväksytystä rasismin ja muukalaisvihan vastaista toimintaa koskevasta yhteisestä toiminnasta[35] lähiaikoina tehtävän arvioinnin tulokset. Asian merkityksellisyyttä ja arkaluonteisuutta kuvaa ranskalaisen tuomioistuimen 20. marraskuuta 2000 antama tuomio, jossa määrättiin Yahoo estämään ranskalaisten käyttäjien pääsy verkkosivuille, joilla myydään natsirihkamaa.[36]

Lisäksi komissio selvittää, kuinka voitaisiin tehostaa Internetissä käytävän huumekaupan vastaisia toimia, joiden tärkeys tunnustetaan Helsingissä kokoontuneen Eurooppa-neuvoston vahvistamassa huumausaineiden torjuntaa koskevassa Euroopan unionin toimintasuunnitelmassa (2000–2004).[37]

## 5 PROSESSIOIKEUTEEN LIITTYVIÄ NÄKÖKOHTIA

Tietokonerikoksissa prosessioikeudelliset näkökohdat saavat luonnostaan osakseen kansallista ja kansainvälistä huomiota, sillä näitä asioita käsitellään usein eri valtioiden tuomioistuimissa ja niihin joudutaan soveltamaan useamman kuin yhden valtion lakia. Tietokonerikokset muodostavat kaikkia muita valtioiden rajat ylittäviä rikoksia suuremman haasteen nykyisille rikosprosessioikeuden säännöille.

Prosessioikeudellista toimivaltaa koskevan lainsäädännön lähentäminen parantaa rikoksen uhrien suojaa varmistamalla, että lainvalvontaviranomaisilla on oman maansa alueella tehtyjen rikosten tutkimiseen tarvittavat valtuudet ja että ne pystyvät vastaamaan ripeästi ja tehokkaasti muiden maiden yhteistyöpyyntöihin.

On myös tärkeää varmistaa, että rikoslainsäädännön perusteella toteutettavat toimenpiteet, jotka kuuluvat yleensä jäsenvaltioiden toimivaltaan ja Euroopan unionista tehdyn sopimuksen VI osaston piiriin, ovat yhteisön lainsäädännön vaatimusten mukaisia. Yhteisöjen tuomioistuin on johdonmukaisesti korostanut, että säännöissä ei voida syrjiä henkilöitä, joilla yhteisön oikeuden mukaan on oikeus yhdenvertaiseen kohteluun, eikä rajoittaa yhteisön oikeudessa taattuja perusvapauksia.[38] Uusien lainvalvontavaltuuksien myöntämistä on arvioitava suhteessa yhteisön oikeuteen ja sen vaikutuksen kannalta, joka niillä on yksityisyyden suojaan.

---

35 EYVL L 185, 24.7.1996, s. 5. Englanniksi ja ranskaksi myös Euroopan oikeudellisen verkoston www-sivuilla http://ue.eu.int/ejn/index.htm.

36 Pariisin ensimmäisen asteen tuomioistuimen välipäätös nro RG 00/05308, 20.11.2000.

37 Huumausaineiden torjuntaa koskeva EU:n toimintasuunnitelma (2000–2004), KOM(1999) 239 lopullinen, http://europa.eu.int/comm/justice_home/pdf/action_fi.pdf.

38 Asia C-274/96, Bickel ja Franz, tuomio 24.11.1998, 17 kohta (Kok. 1996, s. I-7637) ja asia C-186/87, Cowan, tuomio 2.2.1989, 19 kohta (Kok. 1987, s. 195). Hallinnolliset ja rikosoikeudelliset toimenpiteet eivät saa olla ankarampia kuin on välttämättä tarpeen, valvontamuodollisuuksia ei saa järjestää siten, että niillä rajoitettaisiin perustamissopimuksessa tarkoitettua vapautta eikä rikkomuksesta saa määrätä sellaista seuraamusta, joka olisi rikkomuksen vakavuuteen nähden niin suhteeton, että siitä tulisi este tälle vapaudelle (asia C-203/80, Casati, tuomio 11.11.1981, 27 kohta (Kok. 1981, s. 2595)).

## 5.1 Telekuuntelu

Euroopan unionissa noudatetaan yleistä viestintäsalaisuuden periaatetta (joka kattaa myös teleliikennetiedot). Viestintäsalaisuuden rikkominen on laitonta, ellei laissa anneta siihen erityistapauksissa tarvittavia rajoitettuja valtuuksia. Tämä on seurausta Euroopan ihmisoikeussopimuksen 8 artiklasta, johon viitataan Euroopan unionista tehdyn sopimuksen 6 artiklassa. Asiasta säädetään yksityiskohtaisemmin direktiiveissä 95/46/EY ja 97/66/EY.

Kaikissa jäsenvaltioissa on annettu säädöksiä, joiden nojalla lainvalvontaviranomaiset voivat hankkia tuomioistuimen määräyksen (kahdessa jäsenvaltiossa johtavan ministerin henkilökohtaisesti hyväksymän luvan) telekuuntelua varten yleisissä televerkoissa.[39] Säädösten on oltava yhteisön lainsäädännön mukaisia. Niihin sisältyy yleensä yksityisyyden suojaa koskevia takeita, kuten telekuuntelun käytön rajoittaminen vakavien rikosten tutkimiseen, vaatimus, jonka mukaan yksittäisiin tutkimuksiin liittyvän telekuuntelun on oltava välttämätöntä ja oikeasuhteista, ja että telekuuntelun kohteelle on ilmoitettava kuuntelusta heti, kun tästä ei enää ole haittaa tutkinnan kannalta. Monien jäsenvaltioiden lainsäädännössä velvoitetaan (yleiset) teleoperaattorit järjestämään telekuuntelumahdollisuus. Vuonna 1995 annetulla neuvoston päätöslauselmalla pyrittiin sovittamaan yhteen telekuuntelua koskevat vaatimukset.[40]

Perinteiset verkko-operaattorit, varsinkin puheensiirtopalveluja tarjoavat, ovat luoneet toimivat suhteet lainvalvontaviranomaisten kanssa viestintäsalaisuuden laillisen murtamisen helpottamiseksi. Televiestinnän vapautuminen ja Internetin käytön räjähdysmäinen kasvu ovat houkutelleet markkinoille paljon uusia yrittäjiä, jotka ovat joutuneet tekemisiin telekuunteluvalmiuden vaatimuksen kanssa. Julkisen sektorin, alan edustajien ja muiden asianomaisten (mm. tietosuojaviranomaisten) onkin nyt keskusteltava sääntelystä, teknisestä toteutettavuudesta, kustannusten kohdentamisesta ja kaupallisista vaikutuksista.

Uusien tekniikkojen vuoksi jäsenvaltioiden on toimittava yhdessä voidakseen säilyttää laillisen telekuuntelun valmiudet. Kun jäsenvaltioissa asetetaan teleoperaattoreille ja Internet-palveluntarjoajille telekuuntelua koskevia uusia teknisiä vaatimuksia, ne on komission mielestä sovitettava yhteen kansainvälisesti, jotta voidaan estää yhtenäismarkkinoiden vääristyminen ja minimoida operaattoreille aiheutuvat kustannukset sekä samalla turvata yksityisyyden suoja ja tietosuoja. Vaatimusten on oltava mahdollisimman julkisia ja selkeitä eikä niissä saa olla viestintärakenteita heikentäviä osatekijöitä.

---

39 Kahdessa jäsenvaltiossa ei hyväksytä telekuuntelun avulla saatua aineistoa todisteeksi rikosoikeudenkäynneissä.

40 Laillisen telekuuntelun kansainvälisistä edellytyksistä 17. tammikuuta 1995 annettu neuvoston päätöslauselma (EYVL C 329, 4.11.1996, s. 1). Liitteessä luetellaan laillista telekuuntelua koskevat viranomaisedellytykset, jotka jäsenvaltioiden olisi otettava huomioon määritellessään ja toteuttaessaan asian kannalta merkityksellisiä kansallisia periaatteita ja toimenpiteitä. Puheenjohtajuuskaudellaan vuonna 1998 Itävalta ehdotti, että neuvosto antaisi päätöslauselman, jossa vuoden 1995 päätöslauselman soveltamisalaa laajennettaisiin käsittämään Internetin ja satelliittiviestinnän kaltaiset uudet tekniikat. Ehdotusta on käsitelty kahdessa Euroopan parlamentin valiokunnassa (kansalaisvapauksien ja -oikeuksien valiokunta, oikeudellisten asioiden valiokunta), joiden omaksumat kannat poikkesivat toisistaan. Edellinen katsoi uuden päätöslauselman selventävän ja ajantasaistavan vanhaa päätöslauselmaa ja piti sitä sen vuoksi hyväksyttävänä. Jälkimmäinen sen sijaan suhtautui hyvin kriittisesti sekä ihmisoikeusloukkausten mahdollisuuteen että operaattoreille aiheutuviin kustannuksiin, hylkäsi neuvoston ehdotuksen ja kehotti komissiota laatimaan uuden ehdotuksen Amsterdamin sopimuksen tultua voimaan. Päätöslauselmaluonnosta ei ole viime kuukausina aktiivisesti käsitelty neuvostossa eikä sen työryhmissä.

Yleissopimuksessa keskinäisestä oikeusavusta rikosasioissa Euroopan unionin jäsenvaltioiden välillä[41] on sovittu toimintamallista, joka helpottaa lailliseen telekuunteluun liittyvää yhteistyötä.[42] Yleissopimukseen sisältyy määräyksiä satelliittipuhelujen telekuuntelusta[43] ja toisen jäsenvaltion alueella olevaan henkilöön kohdistuvasta telekuuntelusta[44]. Komission mielestä tässä vaiheessa ei voida mennä keskinäistä oikeusapua koskevaa yleissopimusta pitemmälle. Yleissopimuksen tekstissä ei puututa teknisiin yksityiskohtiin; sopimuksen toimivuus on testattava käytännössä ennen kuin mitään parannuksia voidaan harkita. Komissio tarkastelee sopimuksen täytäntöönpanoa jäsenvaltioiden, alan yritysten, käyttäjien ja tietosuojaviranomaisten kanssa ja pyrkii siten varmistamaan, että sen tekemät aloitteet ovat tehokkaita, avoimia ja tasapainoisia.

Viestintäsalaisuuden vääränlainen ja mielivaltainen murtaminen nostaa esiin ihmisoikeuskysymykset varsinkin kansainvälisellä tasolla ja kalvaa kansalaisten luottamusta tietoyhteiskuntaan. Komissio pitää sille esitettyjä väitteitä telekuunteluvalmiuksien väärinkäytöstä erittäin huolestuttavina.[45]

## 5.2 Teleliikennetietojen säilyttäminen

Internetin ja muiden viestintäverkkojen käyttöön liittyvien rikosten tutkinnassa ja rikosoikeudenkäynneissä käytetään usein todisteina teleliikennetietoja, joita palveluntarjoajat säilyttävät laskutusta varten. Kun viestintäkulut riippuvat yhä vähemmän etäisyydestä ja vastaanottajan sijaintipaikasta ja kun palveluntarjoajat siirtyvät kiinteähintaiseen laskutukseen, tietoja ei enää tarvitse säilyttää. Lainvalvontaviranomaiset pelkäävät, että tällöin rikostutkimuksiin on käytettävissä aiempaa vähemmän aineistoa, ja toivovatkin palveluntarjoajien säilyttävän tietyt liikennetiedot vähintään tietyn ajan, jotta ne ovat lainvalvontaviranomaisten käytettävissä.[46]

---

41 EYVL C 197, 12.7.2000, s. 1. Yleissopimus hyväksyttiin 29. toukokuuta 2000. Sen määräyksiä telekuuntelusta sovelletaan ainoastaan Euroopan unionin jäsenvaltioihin, ei yhteisön ulkopuolisiin maihin.

42 Yleissopimus sisältää vähimmäistakeet yksityisyyden ja henkilötietojen suojan turvaamiseksi.

43 Neuvottelujen alkuperäinen tarkoitus oli antaa jäsenvaltioille mahdollisuus harjoittaa telekuuntelua, joka kohdistuu niiden alueella satelliittipuhelimia käyttäviin henkilöihin. Teknisesti ratkaisevassa asemassa telekuuntelun kannalta ovat satelliittiviestinnän maa-asemat. Tämän vuoksi oli pyydettävä teknistä apua jäsenvaltiolta, jossa maa-asema sijaitsi. Yleissopimukseen sisältyy kaksi vaihtoehtoista toimintamallia: nopeutettu keskinäinen oikeusapumenettely, jonka mukaan on pyydettävä erikseen apua jäsenvaltiolta jossa satelliittiviestinnän maa-asema sijaitsee, ja tekninen ratkaisumalli, jossa jäsenvaltio harjoittaa telekuuntelua etätoimintana maa-asemalta, mihin ei tarvita eri pyyntöä.

44 Yleissopimuksessa esitetään myös oikeudelliset puitteet toisen jäsenvaltion (pyynnön vastaanottaneen jäsenvaltion) alueella olevan henkilön telekuuntelua koskeville pyynnöille. Tällöin sekä telekuuntelua suorittavalla jäsenvaltiolla että pyynnön vastaanottaneella jäsenvaltiolla on oltava kansallisten lakien mukainen kuuntelulupa. Lisäksi yleissopimuksessa määritellään säännöt, joiden mukaisesti telekuuntelua suorittava jäsenvaltio voi suorittaa toisen jäsenvaltion alueella olevan henkilön telekuuntelua ilman kyseisen jäsenvaltion teknistä apua.

45 Echelon-telekuunteluverkkoa koskevaa laajaa, runsaasti dokumentoitua Campbell-raporttia (http://www.gn.apc.org/duncan/stoa_cover.htm) käsiteltiin Euroopan parlamentin järjestämässä julkisessa kuulemistilaisuudessa. Raportissa todetaan, että Echelon kehitettiin kansallisiin turvallisuustarpeisiin mutta sitä on käytetty myös teollisuusvakoiluun. Euroopan parlamentti on perustanut väliaikaisen valiokunnan, jonka tehtävänä on tutkia asiaa ja raportoida siitä täysistunnolle vuoden kuluessa.

46 Tämä koskee myös rikostutkimuksia asioissa, joissa ei ole kysymys tietokone- tai verkkorikoksista, mutta joissa kyseiset tiedot voivat auttaa rikoksen selvittämisessä.

Henkilötietojen suojaa koskevien EU-direktiivien eli direktiivin 95/46/EY yleisten käyttötarkoitusrajoitusten ja direktiivin 97/66/EY yksityiskohtaisempien säännösten mukaisesti liikennetiedot on poistettava tai tehtävä nimettömiksi heti telepalvelun käytön jälkeen, ellei niiden säilyttäminen ole laskutuksen vuoksi välttämätöntä. Kiinteähintaisten tai ilmaisten palvelujen tarjoajat eivät periaatteessa saa säilyttää liikennetietoja.

EU:n tietosuojadirektiivien mukaan jäsenvaltiot voivat lakisääteisesti rajoittaa liikennetietojen poistamisvelvoitetta, jos tällaiset rajoitukset ovat välttämättömiä telejärjestelmien luvattoman käytön tai rikosten torjunnan, tutkinnan, selvittämisen sekä syytetutkinnan turvaamiseksi.[47]

Jotta kansallisessa lainsäädännössä voitaisiin säätää teleliikennetietojen säilyttämisestä lainvalvontaviranomaisten käyttöön, ehdotettujen toimenpiteiden on oltava tarkoituksenmukaisia, tarpeellisia ja oikeasuhteisia yhteisön oikeudessa ja kansainvälisessä oikeudessa tarkoitetulla tavalla. Niiden on noudatettava muun muassa direktiivien 97/66/EY ja 95/46/EY säännöksiä, 4. marraskuuta 1950 tehtyä Euroopan yleissopimusta ihmisoikeuksien ja perusvapauksien suojaamiseksi ja 28. tammikuuta 1981 tehtyä Euroopan neuvoston yleissopimusta yksilöiden suojelusta henkilötietojen automaattisessa käsittelyssä. Tämä pätee erityisesti toimenpiteisiin, joihin sisältyy suurta väestönosaa koskevien tietojen rutiiniluonteista säilyttämistä.

Joissakin jäsenvaltioissa valmistellaan lakialoitteita, joiden mukaan palveluntarjoajien on säilytettävä tai ne voivat säilyttää tietyntyyppisiä teleliikennetietoja, joita ei tarvita laskutukseen palvelun antamisen jälkeen, mutta joita pidetään hyödyllisinä rikostutkinnassa.

Lakialoitteiden soveltamisala ja muoto vaihtelee huomattavasti, mutta niiden kaikkien lähtökohtana on se, että lainvalvontaviranomaisten on saatava enemmän tietoja kuin jos palveluntarjoajat käsittelisivät ainoastaan palvelun tarjoamisen edellyttämät vähimmäistiedot. Komissio tutkii näiden aloitteiden suhdetta voimassa olevaan yhteisön oikeuteen.

Euroopan parlamentti valvoo tarkasti kansalaisten yksityisyyden suojaa ja on yleensä ilmaissut kannattavansa vahvaa henkilötietojen suojaa. Internetissä välitettävän lapsipornografian torjuntaa koskevissa keskusteluissa parlamentti on kuitenkin ehdottanut yleistä velvoitetta säilyttää teleliikennetiedot kolmen kuukauden ajan.[48]

Tämä osoittaa, kuinka tärkeä on arkaluontoinen kysymys teleliikennetietojen säilyttämisestä, jossa päätöksentekijöiden haasteena on tasapainoisen ratkaisun löytäminen.

Komissio katsoo, että teleliikennetietojen säilyttäminen on monimutkainen kysymys, johon olisi löydettävä perusteltu ja oikeasuhteinen ratkaisu, joka saattaa erilaiset edut oikeudenmukaiseen tasapainoon. Tavoite voidaan saavuttaa ainoastaan yhdistämällä julkisen hallinnon, alan yritysten, tietosuojaviranomaisten ja käyttäjien asiantuntemus ja kyvyt. On selvää, että kaikissa jäsenvaltioissa sovellettava johdonmukainen ratkaisumalli olisi erittäin suotava, jotta saavutettaisiin tehokkuus- ja suhteellisuustavoitteet ja vältettäisiin tilanne, jossa sekä lainvalvontaviranomaiset että Internet-yhteisö joutuisivat toimimaan sekalaisten teknisten ja oikeudellisten määräysten viidakossa.

---

47 Direktiivin 97/66/EY 14 artikla ja direktiivin 95/46/EY 13 artikla.

48 Lainsäädäntöpäätöslauselma, johon sisältyy Euroopan parlamentin lausunto ehdotuksesta yhteiseksi toiminnaksi, jonka neuvosto on hyväksynyt Euroopan unionista tehdyn sopimuksen K.3 artiklan perusteella, Internetissä välitettävän lapsipornografian vastaisista toimenpiteistä (EYVL C 219, 30.7.1999, s. 68; kyseinen kohta on sivulla 71).

On otettava huomioon useita varsin erilaisia näkökohtia. Toisaalta tietosuojaviranomaiset ovat katsoneet, että yksityisyyteen kohdistuvia vältettäviä riskejä voidaan tehokkaimmin vähentää huomioiden samalla lainvalvontaviranomaisten tarpeet, kun teleliikennetietoja ei säilytetä ainoastaan lainvalvontatarkoituksia varten.[49] Toisaalta lainvalvontaviranomaiset ovat todenneet, että vähimmäisvaatimukset täyttäviä teleliikennetietoja on säilytettävä jonkin aikaa rikostutkimusten helpottamiseksi.

On alan yritysten etujen mukaista osallistua tietojärjestelmiin murtautumisen, tietokonepetosten ym. rikosten vastaiseen yhteistyöhön, mutta niitä ei voida vaatia toteuttamaan kohtuuttoman kalliita toimenpiteitä. Toimenpiteiden taloudellisia vaikutuksia on arvioitava huolellisesti ja ne on suhteutettava toimenpiteen tehokkuuteen tietoverkkorikollisuuden torjumisessa, jotta vältetään Internet-palvelujen hintojen nousu ja saatavuuden heikkeneminen. Samalla on taattava säilytettävien teleliikennetietojen riittävä tietoturva.

Yritykset ovat joka tapauksessa ratkaisevassa asemassa kehitettäessä tietoyhteiskuntaa turvallisemmaksi. Käyttäjien on voitava luottaa tietoyhteiskunnan turvallisuuteen ja tuntea olevansa suojassa rikollisuudelta ja yksityisyyden loukkauksilta.

Komissio tukee varauksettomasti lainvalvontaviranomaisten, alan yritysten, tietosuojaviranomaisten, kuluttajajärjestöjen ja muiden asianomaisten välistä rakentavaa vuoropuhelua. Se kehottaa kaikkia osapuolia osallistumaan perusteelliseen keskusteluun tätä varten perustettavalla EU:n foorumilla (ks. tämän tiedonannon 6.4 kohta). Keskustelun ensisijaisena aiheena ovat teleliikennetietojen säilyttämiseen liittyvät monimutkaiset kysymykset, ja niissä pyritään yhdessä löytämään tarkoituksenmukaisia, tasapainoisia ja oikeasuhteisia ratkaisuja, jotka ovat sopusoinnussa yksityisyyden ja henkilötietojen suojaan liittyvien perusoikeuksien[50] kanssa. Keskustelujen perusteella komissio voi arvioida, tarvitaanko koko EU:ta koskevia säädöksiä tai muita toimenpiteitä.

### 5.3 Anonyymi käyttö

Lainvalvonnan asiantuntijat ovat ilmaisseet olevansa huolissaan siitä, että anonymiteetti voi johtaa vastuukysymysten hämärtymiseen ja hankaloittaa suuresti rikollisten kiinni saamista. Joissakin maissa (ei kaikissa) on mahdollista käyttää matkaviestimiä nimettömänä maksukorttien avulla. Internetiä on mahdollista käyttää nimettömänä muun muassa uudelleenlähetyspalvelujen tarjoajien ja Internet-kahviloiden kautta. Anonymiteettiä edistetään myös dynaamisella Internet-osoitejärjestelmällä, jossa käyttäjille annetaan osoite yhtä käyttökertaa varten eikä pysyvästi.

Jotkut alan edustajista ovat komission kanssa käymissään keskusteluissa vastustaneet täydellistä anonymiteettiä, mihin osasyynä ovat niiden omaan turvallisuuteen, petostentorjuntaan ja verkon eheyteen liittyvät seikat. London Internet Exchange on laatinut hyvää toimintatapaa koskevat suuntaviivat, jotka ovat osoittautuneet Yhdistyneessä

---

[49] "Laajamittainen tietojen tunnusteleva ja yleinen tarkkailu on kiellettävä... tehokkain tapa vähentää yksityisyyteen kohdistuvia epäsuotavia uhkia ja samalla ottaa huomioon tehokkaan lainvalvonnan tarpeet on omaksua periaate, jonka mukaan teleliikennetietoja ei tulisi säilyttää pelkästään lainvalvontatarkoituksia varten, ja kansallisen lainsäädännön ei tulisi velvoittaa teletoiminnan harjoittajia, telepalveluiden tarjoajia ja Internet-palveluntarjoajia säilyttämään liikennetietoja pidempään kuin on tarpeellista laskutuksen vuoksi." 29 artiklan nojalla perustetun tietosuojatyöryhmän suositus 3/99, annettu 7. syyskuuta 1999, http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

[50] Sellaisina kuin ne on määritelty Euroopan ihmisoikeussopimuksessa (8 artikla, yksityisyyden suoja), EU:n perusoikeuskirjassa, Euroopan unionista tehdystä sopimuksessa ja EY:n tietosuojadirektiiveissä.

kuningaskunnassa hyvin käyttökelpoisiksi.[51] Sen sijaan eräät muut alan edustajat ja tietosuoja-asiantuntijat ovat katsoneet, että perusoikeuksia ei voida turvata ilman anonymiteettiä.

Direktiivin 95/46/EY 29 artiklalla perustettu tietosuojatyöryhmä on antanut Internetin anonyymiä käyttöä koskevan suosituksen.[52] Siinä todetaan, että anonymiteetti Internetissä on selvästikin ongelmallinen aihe hallituksille ja kansainvälisille järjestöille. Mahdollisuus pysyä anonyyminä on tärkeää, jos verkossa halutaan noudattaa yksityiselämän kunnioittamisen ja sananvapauden perusperiaatteita. Mahdollisuus toimia ja kommunikoida verkossa henkilöllisyyttään paljastamatta vaikeuttaa kuitenkin kehitteillä olevia aloitteita, jotka liittyvät yhteiskuntapolitiikan muihin tärkeisiin aloihin. Näitä ovat esimerkiksi laittoman ja haitallisen sisällön, talouspetosten ja tekijänoikeuden loukkausten torjunta. Tällainen selkeä ristiriita erilaisten poliittisten tavoitteiden välillä ei ole tietenkään mitään uutta. Perinteisemmissä viestintätavoissa, kuten kirje- ja pakettilähetyksissä, puhelinliikenteessä, sanomalehdissä tai radio- ja televisiotoiminnassa on saavutettu tasapaino eri tavoitteiden välillä. Päätöksentekijöiden haasteena on tällä hetkellä varmistaa, että myös verkossa säilytetään tämä tasapainoinen lähestymistapa, joka takaa perusoikeudet mutta sallii toisaalta mittasuhteiltaan kohtuulliset rajoitukset näihin oikeuksiin erityisolosuhteissa. Olennaista tässä tasapainossa on se, missä määrin ja missä rajoissa henkilö voi osallistua verkossa tapahtuvaan toimintaan anonyyminä.

Kuten Bonnissa 6.—8. heinäkuuta 1997 maailmanlaajuisia tietoverkkoja käsitelleen ministerikokouksen loppujulistuksessa aivan oikein todettiin, periaatteena pitäisi olla se, että kun käyttäjä voi valita nimettömänä pysymisen verkon ulkopuolella, hänen tulisi pystyä siihen myös verkossa. Vallitsee selkeä yksimielisyys siitä, että verkossa tapahtuvaa toimintaa ei voida jättää muutoin sovellettavien oikeudellisten perusperiaatteiden ulkopuolelle. Internet ei ole mikään anarkistinen tyhjiö, jossa yhteiskunnan säännöt eivät päde. Vastaavasti hallituksilla ja viranomaisilla ei pitäisi olla suurempaa mahdollisuutta rajoittaa yksittäisten henkilöiden oikeuksia ja valvoa potentiaalisesti laitonta toimintaa yleisissä verkoissa kuin niiden ulkopuolella. Myös verkossa on noudatettava vaatimusta, jonka mukaan perusoikeuksien ja -vapauksien rajoitusten on oltava perusteltuja, tarpeellisia ja suhteutettuja muihin yhteiskuntapolitiikan tavoitteisiin.

Tietosuojatyöryhmän suosituksessa esitetään seikkaperäisesti, kuinka tämä voidaan toteuttaa tietyissä erityistapauksissa (esimerkiksi sähköpostin, keskusteluryhmien ym. osalta).[53] Komissio yhtyy työryhmän esittämiin näkemyksiin.

### 5.4 Kansainvälinen käytännön yhteistyö

Viime aikoina on toteutettu maailmanlaajuisia lainvalvontaviranomaisten yhteisoperaatioita, esimerkiksi pedofiilirenkaiden vastaiset operaatiot Starburst ja Cathedral, jotka ovat osoitus siitä, mitä rikollisuuden torjunnan ja lainkäytön kansainvälisellä koordinoimisella voidaan saavuttaa, kun vaihdetaan tietoja jo alkuvaiheessa ja estetään renkaan muiden jäsenten varoittaminen pidätysten ja takavarikkojen yhteydessä. Internet on osoittautunut arvokkaaksi ja tehokkaaksi apuvälineeksi myös poliisin ja tullin tutkiessa perinteisiä rikoksia, jotka on tehty Internetin avulla. Toisaalta rikollisuuden torjunnasta ja lainkäytöstä vastaavat viranomaiset ovat törmänneet operaatioiden yhteydessä huomattaviin oikeudellisiin ja toiminnallisiin hankaluuksiin, jotka liittyvät esimerkiksi todistusaineiston toimittamiseen

---

51 http://www.linx.net/noncore/bcp/.

52 Tietosuojatyöryhmän suositus 3/97. Anonymiteetti Internetissä. Annettu 3.12.1997. http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

53 http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

rajojen yli, virka-avun pyytämiseen, uhrien tunnistamiseen ja poliisiasioista vastaavien hallitustenvälisten järjestöjen (lähinnä Interpolin ja Europolin) asemaan.

Kansainväliset tietojenvaihtoverkostot ovat yhä tärkeämpiä käytännön poliisi- ja tulliyhteistyössä.

G8-maat ovat perustaneet ympärivuorokautisen lainvalvonnan yhteyspisteiden verkoston, joka on jo toiminnassa. Sen tärkein tehtävä on vastaanottaa yhteistyöpyyntöjä ja vastata niihin asioissa, jotka koskevat sähköisessä muodossa olevaa todistusaineistoa. Tämän verkoston avulla on saatu hyviä tuloksia useissa tapauksissa. EU:n oikeus- ja sisäasioiden neuvosto vahvisti 19. maaliskuuta 1998 G8-maiden hyväksymät huipputekniikkaan liittyvän rikollisuuden torjunnan kymmenen periaatetta ja kehotti myös niitä jäsenvaltioita, jotka eivät kuulu G8-maihin, liittymään verkostoon.[54] Yhteyspisteiden on määrä harjoittaa suoraa yhteistoimintaa sekä täydentää nykyisiä keskinäisen oikeusavun rakenteita ja viestintäkanavia.[55]

Tällaisen verkoston luominen mainitaan myös Euroopan neuvoston yleissopimusluonnoksessa. Ympärivuorokautisiin yhteyspisteisiin viitataan myös Internetissä välitettävän lapsipornografian vastaisista toimenpiteistä tehdyssä neuvoston päätöksessä ja tietoverkkorikollisuutta koskevasta yleissopimusehdotuksesta hyväksytyssä EU:n yhteisessä kannassa[56] sekä G8-maiden toimintasuunnitelman vahvistavassa neuvoston päätöksessä[57], mutta nimenomaan EU:ta koskevia konkreettisia aloitteita ei ole vielä tehty.

Komission mielestä neuvoston suunnitelmat on toteutettava viipymättä, koska alalla tarvitaan asiantuntemusta ja pikaisia toimia. Jotta verkosto onnistuisi tehtävässään, sitä varten on koulutettava sekä oikeustieteeseen että tekniikkaan perehtyneitä asiantuntijoita.

Myös tulliviranomaisten yhteistyötä ja tietojenvaihtoa on tehostettava. On kehitettävä sekä nykyisiä yhteistyömuotoja että uusia tapoja hoitaa yhteisiä operaatioita ja tietojenvaihtoa. Tulliviranomaiset ovat yhä yksimielisempiä siitä, että on muodostettava kansainvälisiä verkostoja tietojenvaihdon tehostamiseksi. Samalla on kuitenkin otettava riittävästi huomioon tietosuojavaatimukset. Lisäksi on panostettava sekä atk-järjestelmien kehittämiseen että henkilöstön koulutukseen, jotta tulliviranomaiset voisivat hoitaa tehtävänsä entistä tehokkaammin.

---

54 Toistaiseksi tähän ns. 24/7-verkostoon on liittynyt viisi G8-maihin kuulumatonta EU:n jäsenvaltiota.

55 Lasten kaupallisen seksuaalisen hyväksikäytön vastaisessa maailmankonferenssissa Tukholmassa 28. elokuuta 1996 ehdotettiin, että Interpolin olisi kuuluttava kyseisiin verkostoihin. Internetissä välitettävän lapsipornografian vastaisista toimenpiteistä tehdyn neuvoston päätöksen mukaan myös Europolin on määrä osallistua tähän toimintaan.

56 Yhteisen kannan 1 artiklan 4 kohta: "Jäsenvaltioiden olisi kannatettava sellaisten määräysten laatimista, keskinäistä oikeusapua koskevat määräykset mukaan lukien, jotka helpottavat mahdollisimman paljon kansainvälistä yhteistyötä. Yleissopimuksen olisi helpotettava nopeaa yhteistyötä atk- ja tietokoneavusteisten rikosten osalta. Tällaiseen yhteistyöhön voi kuulua rikollisuuden torjunnasta ja lainkäytöstä vastaavien ympärivuorokautisten yhteyspisteiden perustaminen, jotka täydentävät olemassa olevia keskinäisen oikeusavun menettelyjä."

57 Katso http:/ue.eu.int/ejn/index.htm.

## 5.5 Lainvalvontaviranomaisten prosessioikeudelliset toimivaltuudet ja lainkäyttövalta

Kun kansallisessa lainsäädännössä määritellyt välttämättömät edellytykset täyttyvät, lainvalvontaviranomaisten on voitava tutkia ja takavarikoida tietokoneella olevat tiedot riittävän nopeasti estääkseen rikostutkimuksen kannalta ratkaisevan todistusaineiston tuhoamisen. Lainvalvontaviranomaiset katsovat tarvitsevansa toimialueellaan riittävät pakkokeinovaltuudet tutkia tietokonejärjestelmiä ja takavarikoida tietoja, määrätä kansalaiset toimittamaan vaaditut sähköisessä muodossa olevat tiedot ja määrätä ne säilytettäviksi tavanomaisia oikeudellisia suojatoimenpiteitä ja menettelyjä noudattaen. Toistaiseksi näitä toimenpiteitä ja menettelyjä koskevat jäsenvaltioiden säännökset eivät kuitenkaan ole yhdenmukaiset.

Ongelmia voi ilmaantua, jos viranomaiset huomaavat, että järjestelmään kuuluu useita tietokoneita ja verkkoja, jotka sijaitsevat eri puolilla maata. Asian käsittely mutkistuu huomattavasti, jos viranomainen tietokoneelta tietoja hakiessaan tai rikostutkinnan yhteydessä toteaa pääsevänsä käsiksi tai tarvitsevansa päästä käsiksi yhdessä tai useammassa maassa sijaitseviin tietoihin. Kysymys on keskeisistä suvereniteettiin, ihmisoikeuksiin ja lainvalvontaan liittyvistä eduista, jotka on tasapainotettava.

Nykyiset kansainvälisen yhteistyön rikosoikeudelliset keinot eivät ehkä ole tarkoituksenmukaisia tai riittäviä, koska niiden käyttöönotto voi viedä useita päiviä tai jopa viikkoja tai kuukausia. Tarvitaan järjestelmä, jonka avulla maat voivat tutkia rikoksia ja saada todistusaineistoa nopeasti ja tehokkaasti ja jonka avulla varmistetaan ainakin se, että rajat ylittävässä lainvalvonnassa ei menetetä tärkeitä todisteita, mutta samalla kunnioitetaan kansallisen suvereniteetin, perustuslaillisten oikeuksien ja ihmisoikeuksien periaatteita sekä yksityisyyden ja henkilötietojen suojaa.

Tietoverkkorikollisuutta käsittelevän Euroopan neuvoston yleissopimusluonnoksen yhteydessä on esitetty uusia ehdotuksia näiden ongelmien ratkaisemiseksi esimerkiksi siten, että tiedot voitaisiin määrätä säilytettäviksi rikostutkintaa varten. Sen sijaan muihin vielä ratkaisematta oleviin asioihin, kuten tietojen rajatylittävään hakuun ja takavarikointiin, liittyy vaikeita poliittisia kysymyksiä. Tarvitaan vielä neuvotteluja kaikkien asiaan liittyvien tahojen kesken ennen kuin voidaan esittää konkreettisia aloitteita.

Huipputekniikkaan liittyvää rikollisuutta käsittelevä G8-maiden työryhmä on keskustellut valtioiden rajat ylittävään hakuun ja takavarikointiin liittyvistä kysymyksistä ja päättänyt yksimielisesti periaatteista[58], joita sovelletaan toistaiseksi, kunnes saadaan aikaan pysyvä sopimus. Keskeiset ongelmat ovat liittyneet erityisesti siihen, milloin nopea haku tai takavarikko on mahdollista toteuttaa ennen kuin asiasta ilmoitetaan valtiolle, jossa toimi suoritetaan. Lisäksi on annettava riittävät takeet perusoikeuksien suojaamisesta. Tietoverkkorikollisuutta koskevasta yleissopimusehdotuksesta hyväksymässään yhteisessä kannassa EU:n ministerit ovat päätyneet väljään sanamuotoon.[59]

---

[58] Moskovassa 19.–20. lokakuuta kansainvälisen järjestäytyneen rikollisuuden torjumisesta pidetyn G8-maiden ministerikokouksen tiedonanto (ks. http://www.usdoj.gov/criminal/cybercrime/action.htm ja http://www.usdoj.gov/criminal/cybercrime/principles.htm).

[59] EYVL L 142/2: "Jollei perustuslaista ilmenevistä periaatteista ja muiden valtioiden suvereniteetin, turvallisuuden, yleisen järjestyksen ja muiden ensisijaisten etujen asianmukaiseksi kunnioittamiseksi vahvistettavista erityisistä suojatoimenpiteistä muuta johdu, yleissopimuksessa tarkemmin määriteltävien vakavien rikosten tutkimiseksi suoritettavia rajat ylittäviä hakuja voidaan harkita poikkeustapauksissa ja erityisesti kiireellisissä tapauksissa esim. vakavan rikoksen todisteiden tuhoamisen tai muuttamisen

Käsiteltäessä rajat ylittäviä atk-rikoksia tarvitaan selkeät säännöt, joissa määritellään, millä valtiolla on lainkäyttövalta syytetutkinnassa. Erityisesti on vältettävä tilannetta, jossa millään valtiolla ei ole lainkäyttövaltaa. Euroopan neuvoston yleissopimusluonnoksen keskeisten sääntöjen mukaan lainkäyttövalta kuuluu sille valtiolle, jonka alueella rikos on tehty tai jonka kansalainen on tehnyt rikoksen. Jos useampi kuin yksi valtio katsoo lainkäyttövallan kuuluvan itselleen, kyseisten valtioiden on neuvoteltava määritelläkseen, minkä valtion on tarkoituksenmukaisinta käyttää lainkäyttövaltaa. Lopputulos riippuu kuitenkin paljolti kahden- tai monenvälisistä käytännön neuvotteluista. Komissio tarkastelee tilannetta selvittääkseen, tarvitaanko EU:n tasolla uusia toimenpiteitä.

Komissio on osallistunut sekä Euroopan neuvostossa että G8-maiden kesken käytyihin keskusteluihin ja on hyvin selvillä siitä, että prosessioikeudelliset kysymykset ovat hankalia ja monitahoisia. EU:n sisällä harjoitettava tehokas tietoverkkorikollisuuden torjunta on kuitenkin olennainen osa turvallisempaa tietoyhteiskuntaa sekä vapauteen, turvallisuuteen ja oikeuteen perustuvaa aluetta.

Komissio aikoo jatkaa keskusteluja kaikkien asiaan liittyvien tahojen kanssa tulevina kuukausina tähänastisen työn pohjalta. Lisäksi tätä kysymystä tarkastellaan osana laajempaa kokonaisuutta eli lokakuussa 1999 Tampereella kokoontuneen Eurooppa-neuvoston päätelmien täytäntöönpanon kannalta. Tampereen Eurooppa-neuvostohan kehotti neuvostoa ja komissiota hyväksymään joulukuuhun 2000 mennessä toimenpideohjelman vastavuoroisen tunnustamisen periaatteen täytäntöönpanemiseksi. Komissio on jo julkaissut tiedonannon rikosasioita koskevien lopullisten päätösten vastavuoroisesta tunnustamisesta.[60] Lisäksi komissio aikoo tutkia toimenpideohjelman yhteydessä mahdollisuuksia tietoverkkorikollisuuden tutkintaan liittyvien, ennen oikeudenkäyntiä annettujen määräysten vastavuoroiseen tunnustamiseen. Tarkoituksena on esittää Euroopan unionista tehdyn sopimuksen VI osaston mukainen lainsäädäntöehdotus.

### 5.6 Sähköisessä muodossa olevien tietojen käyttö todistusaineistona

Silloinkin kun viranomaiset ovat saaneet käyttöönsä sähköisessä muodossa olevia tietoja, jotka vaikuttavat rikostutkimuksen kannalta ratkaisevalta todistusaineistolta, niiden on voitava päästä käsiksi tietoihin ja todistaa ne oikeiksi käyttääkseen niitä rikos- ja syytetutkinnassa. Tehtävä ei ole helppo, kun otetaan huomioon sähköisten tietojen muuttuva luonne ja niiden manipuloinnin, väärentämisen, teknisen suojelun ja poistamisen helppous. Tietokonerikosten jälkien tutkiminen (*computer forensics*) onkin erikoistunut tutkimusala**,** jossa kehitetään ja sovelletaan tieteellisiä menetelmiä tietojärjestelmien sisällön selvittämiseen, aitousanalyysiin ja säilyttämiseen.

Tietokoneelle tallennettujen tietojen käyttöä todistusaineistona käsittelevä kansainvälinen järjestö (International Organisation on Computer Evidence, IOCE) on G8-maiden asiantuntijoiden pyynnöstä luvannut laatia suosituksia standardeiksi, joissa on tarkoitus määritellä yhteinen termistö, käytettävät tunnistusmenetelmät sekä rikostutkimuspyyntöjen yhteinen muoto. EU:n on suotavaa osallistua tähän toimintaan sekä jäsenvaltioiden tasolla tietokonerikollisuuteen erikoistuneiden tutkimusyksikköjen välityksellä että viidennen puiteohjelman tukeman tutkimus- ja kehitystoiminnan (IST-ohjelman) kautta.

---

estämiseksi tai sellaisen rikoksen tekemisen estämiseksi, joka todennäköisesti johtaa kuolemaan tai aiheuttaa henkilölle vakavan ruumiinvamman."

60 KOM(2000) 495, Bryssel 26.7.2000.

# 6 MUUT KUIN OIKEUDELLISET TOIMENPITEET

Tietokonerikollisuuden ja verkkojen väärinkäytön torjumiseen tarvitaan sekä kansallista että kansainvälistä lainsäädäntöä, mutta se ei yksin riitä. Tehokas torjunta edellyttää myös oikeudellisia toimenpiteitä täydentäviä toimia. Useimmat niistä sisältyvät COMCRIME-tutkimuksessa esitettyihin suosituksiin ja G8-maiden kymmenen kohdan toimintasuunnitelmaan, ja niitä ovat yleensä kannattaneet myös tahot, jotka osallistuivat tämän tiedonannon laatimista edeltäneeseen epäviralliseen lausuntokierrokseen. Täydentäviä toimenpiteitä ovat:

- kansallisten tietokonerikollisuuteen erikoistuneiden poliisiyksikköjen perustaminen, ellei sellaisia ole vielä perustettu

- lainvalvontaviranomaisten, alan yritysten, kuluttajajärjestöjen ja tietosuojaviranomaisten välisen yhteistyön parantaminen

- alan yritysten tai yhteisön johdolla toteutettavien (mm. turvallisuustuotteita koskevien) aloitteiden edistäminen.

Tältä osin salaus on todennäköisesti vastedeskin tärkeä tekijä. Salaus on olennainen uusien palvelujen käyttöönottoa helpottava apuväline, jolla voidaan merkittävästi tehostaa Internetissä esiintyvän rikollisuuden torjumista. Komissio on linjannut kantansa salaukseen tiedonannossaan turvallisuuden ja luottamuksen varmistamisesta sähköisessä viestinnässä[61]. Tiedonannossa todetaan, että komissio pyrkii poistamaan kaikki salaustuotteiden vapaan liikkuvuuden esteet Euroopan yhteisössä. Lisäksi salaustuotteiden vapaalle liikkuvuudelle jäsenvaltioissa asetettujen rajoitusten on oltava yhteisön oikeuden mukaisia. Komissio tutkii, ovatko kyseiset kansalliset rajoitukset perusteltuja ja oikeasuhteisia, kun otetaan huomioon muun muassa vapaata liikkuvuutta koskevat perustamissopimuksen määräykset, Euroopan yhteisöjen tuomioistuimen oikeuskäytäntö ja tietosuojadirektiiveissä asetetut vaatimukset. On kuitenkin selvää, että salaus luo myös uusia, vaikeita haasteita lainvalvontaviranomaisille.

Tämän vuoksi komissio suhtautuu myönteisesti äskettäin annettuun tarkistettuun kaksikäyttötuotteita koskevaan asetukseen, jonka myötä salaustuotteiden saatavuus parani huomattavassa määrin. Tästä huolimatta käyttäjien, yritysten ja viranomaisten välistä vuorovaikutusta on lisättävä. Komissio pyrkii omalta osaltaan edistämään vuorovaikutusta unionin tasolla kaavailemansa huipputekniikkaan liittyvää rikollisuutta käsittelevän EU:n keskustelufoorumin avulla. Kaikkialla EU:n alueella saatavana olevat tehokkaat salaustuotteet ja muut turvallisuustuotteet, jotka on tarvittaessa sertifioitava sovittujen arviointiperusteiden mukaisesti, parantaisivat mahdollisuuksia rikosten torjuntaan ja lisäisivät käyttäjien luottamusta tietoyhteiskunnan toimintoihin.

## 6.1 Kansalliset erikoisyksiköt

Koska osa tietokonerikollisuudesta on teknisesti ja oikeudellisesti erittäin monimutkaista, on välttämätöntä perustaa kansallisia erikoisyksikköjä. Erikoisyksikköihin on saatava eri alojen (rikollisuuden torjunnan ja lainkäytön) asiantuntijoita, ja niiden käyttöön on annettava riittävät tekniset välineet. Erikoisyksiköt toimisivat yhteyspisteinä, joiden tehtävänä on:

[61] KOM(1997) 503.

- reagoida nopeasti epäiltyjä rikoksia koskeviin tietopyyntöihin. On määriteltävä tietojenvaihdon yhteiset muodot, vaikka G8-maiden asiantuntijoiden kanssa käydyt keskustelut ovatkin osoittaneet, että tämä ei ole kansallisten oikeusjärjestelmien erojen vuoksi mikään helppo tehtävä.

- toimia ns. vihjelinjojen[62] kansallisina ja kansainvälisinä lainvalvonnan yhteyspisteinä, jotka vastaanottavat Internetin käyttäjien valituksia laittomasta sisällöstä

- parantaa ja kehittää erityisiä atk-tutkimusmenetelmiä tietokonerikosten havaitsemiseksi, tutkimiseksi ja syyllisten löytämiseksi

- toimia tietoverkkorikollisuuteen keskittyvinä osaamiskeskuksina, jotka edistävät parhaiden käytäntöjen leviämistä ja kokemusten vaihtoa.

Joissakin EU:n jäsenvaltioissa on jo perustettu tietokonerikollisuuteen keskittyviä erikoisyksikköjä. Komissio kannustaakin jäsenvaltioita tähän, koska se katsoo erikoisyksikköjen perustamisen olevan jäsenvaltioiden tehtävä. Uusimpien laitteiden ja ohjelmien hankkiminen näille yksiköille ja yksikköjen henkilöstön kouluttaminen on kuitenkin kallista ja edellyttää painopistealueiden määrittelyä ja poliittisten päätösten tekoa asianmukaisella tasolla.[63] Jäsenvaltioissa jo toiminnassa olevien yksikköjen kokemukset voivat olla erityisen arvokkaita. Komissio tukee näiden kokemusten vaihtoa.

Komissio uskoo myös, että Europol voi tuoda oman panoksensa toimintaan EU:n tasolla toimintojen koordinoinnin ja analysoinnin sekä muun kansallisille erikoisyksiköille annettavan avun muodossa. Tämän vuoksi komissio kannattaa tietoverkkorikollisuuden sisällyttämistä Europolin toimialaan.

## 6.2 Erityiskoulutus

Täydentävän erityiskoulutuksen järjestäminen oikeus- ja poliisiviranomaisille vaatii paljon työtä, sillä tietokonerikollisuudessa käytettävät tekniikat ja mahdollisuudet muuttuvat nopeammin kuin perinteisemmillä rikollisuuden aloilla.

Joissakin jäsenvaltioissa on toteutettu lainvalvontahenkilöstön huipputekniikkakoulutusta koskevia aloitteita. Nämä aloitteet voivat olla hyödyllisiä ja suuntaa-antavia jäsenvaltioille, joissa ei ole vielä toteutettu tällaisia toimenpiteitä.

---

62 Toistaiseksi vihjelinjoja on vain muutamissa maissa. Esimerkkeinä mainittakoon Yhdysvalloissa toimiva Cybertipline ja Yhdistyneessä kuningaskunnassa toimiva Internet Watch Foundation (IWF), jonka puhelin- ja sähköpostipalveluun kansalaiset ovat joulukuusta 1996 lähtien voineet ilmoittaa laittomana pitämästään Internet-aineistosta. IWF arvioi, onko aineisto laitonta, ja ilmoittaa asiasta palveluntarjoajille ja poliisille. Valvontaelimiä on myös Norjassa (Redd Barna), Alankomaissa (Meldpunt), Saksassa (Newswatch, FSM ja Jugendschutz), Itävallassa (ISPAA) ja Irlannissa (ISPAI). Childnet International on vastikään käynnistänyt EU:n Daphne-ohjelman alaisen hankkeen ("International Hotline Providers in Europe Forum"). Tammikuussa 1999 Pariisissa järjestetyssä Unescon asiantuntijakokouksessa kannatettiin kansallisia vihjelinjoja sekä vihjelinjojen verkostojen tai kansainvälisen "sähköisen viestinnän valvontaviraston" perustamista.

63 Alan kokemuksista Yhdysvalloissa kerrotaan Michael A. Sussmannin kirjoituksessa "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium", Duke Journal of Comparative and International Law, Vol. 9 Spring 1999, s. 464.

Tähän tähtääviä yksittäisiä hankkeita – kokemusten vaihtoa, seminaareja tiettyjen ammattiryhmien yhteisistä haasteista – on käynnistetty komission hallinnoimien ohjelmien tuella (erityisesti STOP-, Falcone- ja Grotius-ohjelmien avulla). Komissio aikoo tehdä ehdotuksia alan uusista toimintamuodoista kuten tietokone- ja verkkoavusteisesta koulutuksesta.

Europolin aloitteesta järjestetään jäsenvaltioiden viranomaisille marraskuussa 2000 viikon kestävä koulutusjakso, jossa käsitellään erityisesti lapsipornografian torjuntaa. Tällaisen koulutusjakson sisältöä voitaisiin laajentaa siten, että se käsittäisi tietokonerikollisuuden yleensä. Interpol on toiminut alalla aktiivisesti jo joitakin vuosia. Sen aloitteisiin voisi osallistua nykyistä enemmän harjoittelijoita.

G8-maat ovat kehitelleet aloitteita, joiden puitteissa viranomaiset voivat vaihtaa kokemuksia ja luoda konkreettisten tapausten perusteella yhteisiä tutkimusmenetelmiä. Niiden on tarkoitus tehdä uusi koulutusaloite vuoden 2001 jälkipuoliskolla. G8-maihin kuuluvat EU:n jäsenvaltiot voisivat raportoida kokemuksistaan muille jäsenvaltioille.

Internetissä välitettävän lapsipornografian torjunnan yhteydessä voitaisiin perustaa kansainvälinen digitaalinen lapsipornografisten kuvien keskusarkisto. Kansalliset erikoisyksiköt voisivat käyttää arkistoa Internetin kautta, ja arkistoon pääsyä ja yksityisyyden suojaa säänneltäisiin tarvittavin vaatimuksin ja rajoituksin. Näin helpotettaisiin uhrien ja rikoksentekijöiden löytämistä sekä rikosten luonteen määrittämistä ja poliisin erityiskoulutuksen järjestämistä.[64]

## 6.3 Tietämyksen lisääntyminen ja tietojen tallentamista koskevat yhteiset säännöt

Poliisi- ja oikeusviranomaisten tietojen tallentamista koskevat yhdenmukaiset säännöt ja tietokonerikollisuuden analysoinnin apuna käytettävät tilastot auttaisivat viranomaisia säilyttämään, analysoimaan ja arvioimaan keräämiään virallisia tietoja nykyistä paremmin tällä jatkuvasti muuttuvalla alalla.

Myös yksityisellä sektorilla tarvitaan tällaisia tilastoja, jotta yritykset voivat arvioida riskejä ja tehdä riskinhallintaan liittyvän kustannus–hyötyanalyysin. Tilastoja tarvitaan sekä toimintaan liittyvistä syistä (esim. päätettäessä toteutettavista turvatoimista) että vakuuttamista varten.

COMCRIME-tutkimuksen tuloksena syntyi tietokonerikollisuuteen liittyvien säädösten tietokanta, jota saatetaan parhaillaan ajan tasalle ja jonka komissio saa käyttöönsä. Komissio tutkii, miten tietokannan sisältöä (säädökset, oikeusasiat ja kirjallisuus) ja käyttökelpoisuutta voitaisiin parantaa.

---

64 Ruotsin kansallisen tietotekniikkarikoksia tutkivan yksikön kehittämä ja STOP-ohjelman osana yhdessä Euroopan komission kanssa rahoitettu Excalibur-hanke on onnistunut erinomaisesti. Hanke käynnistettiin yhteistyössä Saksan, Yhdistyneen kuningaskunnan, Alankomaiden ja Belgian poliisin sekä Europolin ja Interpolin kanssa. On myös syytä mainita Saksan Bundeskriminalamtin Perkeo-hanke ja Ranskan sisäasiainministeriön Surfimage-hanke, joka rahoitettiin osaksi STOP-ohjelmasta.

## 6.4 Eri toimijoiden yhteistyö: EU:n keskustelufoorumi

Viranomaisten ja alan yritysten välistä tehokasta oikeudellista yhteistoimintaa pidetään keskeisenä tekijänä kaikessa tietokonerikosten torjuntaan tähtäävässä julkisessa toiminnassa.[65] Viranomaiset ovat myöntäneet, että aina ei ole ollut selvää, mitä vaatimuksia olisi asetettava palveluntarjoajille. Alan edustajat ovat ilmaisseet suhtautuvansa yleensä myönteisesti lainvalvojien kanssa tehtävän yhteistyön tehostamiseen, korostaen samalla, että on saavutettava tasapaino kansalaisten perusoikeuksien ja vapauksien – erityisesti yksityisyyden suojan[66] –, rikollisuuden torjunnan ja palveluntarjoajille aiheutuvien taloudellisten rasitteiden välillä.

Alan yritykset ja lainvalvontaviranomaiset voivat yhdessä tuoda yleiseen tietoisuuteen Internetiä käyttävien rikollisten aiheuttamia riskejä, edistää turvallisuuden kannalta parhaita käytäntöjä ja kehittää tehokkaita rikostentorjuntavälineitä ja -keinoja. Joissakin jäsenvaltioissa on jo toteutettu tällaisia aloitteita, joista Yhdistyneessä kuningaskunnassa toimiva *Internet Crime Forum* lienee pitkäikäisin ja kattavin.[67]

Komissio suhtautuu myönteisesti näihin aloitteisiin ja katsoo, että niitä on edistettävä kaikissa jäsenvaltioissa. Komissio aikoo perustaa EU:lle oman keskustelufoorumin, jolla lainvalvontaviranomaiset, Internet-palveluntarjoajat, teleoperaattorit, kansalaisvapausjärjestöt, kuluttajien edustajat, tietosuojaviranomaiset ja muut asianomaiset voivat kohdata ja tehostaa yhteistyötään EU:n tasolla. Aluksi yhteistyöhön osallistuvat jäsenvaltioiden nimeämät virkamiehet, tekniset asiantuntijat, tietosuojatyöryhmän nimeämät yksityisyyden suojelun asiantuntijat sekä atk-alan järjestöjen ja kuluttajajärjestöjen suositusten perusteella nimettävät yritysten ja kuluttajien edustajat. Myöhemmin toimintaan voi osallistua myös kansallisten aloitteiden edustajia.

EU:n keskustelufoorumi, johon liittyvät asiakirjat julkaistaan www-sivuilla, on avoin kanava kaikkien asiasta kiinnostuneiden tahojen kommenteille.

EU:n keskustelufoorumin tarkoituksena on:

- kehittää julkishallinnon ja alan yritysten välisiä ympärivuorokautisia yhteyspisteitä
- kehittää vakiomallinen tietopyyntö, jolla viranomaiset pyytävät tietoja alan yrityksiltä, ja näin lisätä Internetin käyttöä viranomaisten ja palveluntarjoajien välisessä yhteydenpidossa

---

65 G8-maiden oikeus- ja sisäasioista vastaavat ministerit julistivat huipputekniikkaan liittyvän rikollisuuden torjunnan periaatteista ja kymmenkohtaisesta toimintasuunnitelmasta Washingtonissa 9.-10. joulukuuta 1997 antamassaan tiedonannossa, että maailmanlaajuisia verkostoja suunnittelevat, käyttävät ja ylläpitävät nimenomaan atk-alan yritykset, jotka vastaavat siten ensisijaisesti teknisten standardien kehittämisestä. Näin ollen alan on osallistuttava turvallisten järjestelmien kehittämiseen ja levittämiseen, jotta voidaan havaita tietokoneiden väärinkäyttö, säilyttää sähköisessä muodossa oleva todistusaineisto ja selvittää rikollisten sijaintipaikka ja henkilöllisyys. Internetissä välitettävän lapsipornografian vastaisista toimenpiteistä tehdyssä neuvoston päätöksessä korostetaan, että jäsenvaltiot aloittavat rakentavan vuoropuhelun atk-alan kanssa ja tekevät yhteistyötä vaihtamalla keskenään kokemuksia.

66 Sellaisena kuin se on määritelty EU:n tietosuojadirektiiveissä, Euroopan neuvoston ihmisoikeussopimuksessa, Euroopan neuvoston yleissopimuksessa N:o 108 yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä ja jäsenvaltioiden laissa.

67 Vuonna 1997 perustettuun Internet Crime Forumiin kuuluu poliiseja, sisäasiainministeriön virkamiehiä, tietosuojaviranomaisia ja Internet-yritysten edustajia. Se kokoontuu 3–4 kertaa vuodessa ja lisäksi sillä on pysyviä työryhmiä.

- kannustaa alan yrityksiä ja viranomaisia kehittämään ja ottamaan käyttöön toimintasääntöjä ja parhaita käytäntöjä ja soveltamaan näitä yhdessä[68]

- kannustaa eri osapuolia, erityisesti alan yrityksiä ja viranomaisia, vaihtamaan tietoja huipputekniikkaan liittyvän rikollisuuden suuntauksista

- selvittää lainvalvonnan kannalta merkityksellisen uuden tekniikan kehittämistä

- edistää ennakkovaroitus- ja kriisinhallintajärjestelmien jatkokehittelyä tietojärjestelmiin kohdistuvien uhkien ja häiriötekijöiden torjumiseksi, tunnistamiseksi ja selvittämiseksi

- järjestää pätevää asiantuntija-apua työhön, jota tehdään neuvostossa ja muissa kansainvälisissä yhteyksissä, esimerkiksi Euroopan neuvostossa ja G8-maiden kesken

- kannustaa osapuolia tekemään yhteistyötä mm. esittämällä yhteiset periaatteet (esim. yhteistyöasiakirjan tai käytännesääntöjen muodossa), joita viranomaisten, alan yritysten ja käyttäjien on noudatettava.

## 6.5 Alan edustajien suora toiminta

Tietokonerikollisuuden torjuminen on selkeästi koko yhteiskunnan edun mukaista. Jotta kuluttajat luottaisivat sähköiseen kaupankäyntiin, tietokonerikosten torjumiseksi toteutettavat toimenpiteet on hyväksyttävä hyvän liiketavan olennaiseksi osaksi. Tietokonerikollisuuden potentiaalisia uhreja ovat muun muassa pankkiala, viestintäala, luottokorttiyritykset ja tekijänoikeusjärjestöt sekä niiden asiakkaat. Yritykset osallistuvat luonnostaan petosten torjuntaan suojelemalla toiminimiään ja tavaramerkkejään. Ohjelmisto- ja ääniteteollisuutta edustavilla järjestöillä (esim. British Phonographic Industry, BPI) on työryhmiä, jotka tutkivat (mm. Internetiin liittyvää) luvatonta jäljentämistä. Joissakin maissa Internet-palveluntarjoajat ovat perustaneet vihjelinjoja, joihin käyttäjät voivat ilmoittaa laittomasta ja haitallisesta sisällöstä.

Komissio on tukenut joitakin näistä aloitteista osana EU:n tutkimuksen ja teknologisen kehittämisen viidettä puiteohjelmaa, Internet-toimintasuunnitelmaa[69] ja Euroopan unionista tehdyn sopimuksen VI osaston mukaisia ohjelmia, kuten STOP- ja Daphne-ohjelmat.

Tietoja näiden osa-alueiden parhaista käytännöistä vaihdetaan EU:n keskustelufoorumilla.

## 6.6 EU:n tukemat TTK-hankkeet

Käyttäjäystävällistä tietoyhteiskuntaa koskevassa IST-ohjelmassa, joka on osa tutkimuksen ja teknologisen kehittämisen viidettä puiteohjelmaa (1998–2002), painopiste on luottamusta lisäävien tekniikkojen kehittämisessä ja käytössä. Luottamusta lisääviin tekniikkoihin kuuluvat sekä tieto- ja verkkoturvallisuustekniikat että yksityisyyden suojaan, tietosuojaan ja muihin henkilökohtaisiin oikeuksiin kohdistuvien loukkausten sekä tietokonerikollisuuden torjuntaan tarkoitetut tekniset välineet ja menetelmät.

---

[68] Direktiivin 95/46/EY 27 artiklan mukaisten käytännesääntöjen laatimiseen osallistuvat tietosuojatyöryhmä ja kansalliset tietosuojaviranomaiset. Nämä säännöt voivat koskea esim. direktiivin 97/66/EY soveltamisalaan koskevia asioita, kuten telekuuntelua.

[69] Lisätietoja Internetin nykyistä turvallisempaan käyttöön tähtäävästä toimintasuunnitelmasta saa verkko-osoitteesta http://158.169.50.95:10080/iap/.

IST-ohjelmalla, erityisesti avaintoimintoon 2 (*Uudet työtavat ja sähköinen kaupankäynti*) kuuluvilla *tietoturvaa, verkkoturvallisuutta ja muita luottamusta lisääviä tekniikoita* koskevilla toimilla, luodaan puitteet, joiden pohjalta voidaan vastata tietokonerikollisuuden ehkäisemiseen ja torjuntaan liittyviin teknisiin haasteisiin ja varmistaa turvallisuus- sekä tietosuojavaatimusten täyttyminen sekä EU:n, verkkoyhteisöjen että yksilöiden tasolla.

IST-ohjelman osana on lisäksi käynnistetty käyttövarmuutta koskeva aloite, jolla pyritään luottamuksen lisäämiseen muun muassa tietokonerikollisuuden ehkäisemisen ja tutkimisen avulla. Tällä aloitteella pyritään parantamaan käyttäjien luottamusta toisiinsa läheisesti liittyviin tietojärjestelmiin ja tiiviisti verkottuneisiin järjestelmiin lisäämällä tietoisuutta käyttövarmuuden merkityksestä ja käyttövarmuutta edistävästä tekniikasta. Aloitteeseen kuuluu kiinteänä osana myös kansainvälistä yhteistoimintaa. IST-ohjelma toimii joiltain osin yhteistyössä Yhdysvaltojen puolustusteollisuuden huippututkimushankkeita koordinoivan viraston (DARPA) ja kansallisen tiedesäätiön (NSF) kanssa. Lisäksi se on perustanut yhdessä Yhdysvaltojen ulkoasiainministeriön kanssa kriittisten järjestelmien suojaa käsittelevän EY:n ja USA:n yhteisen työryhmän, joka toimii EY:n ja USA:n tiede- ja teknologiayhteistyösopimukseen perustuvan yhteisen neuvoa-antavan ryhmän alaisena.[70]

Komission yhteinen tutkimuskeskus (YTK), joka on tukenut IST-ohjelman käyttövarmuusaloitetta, keskittyy kehittämään yhdenmukaisia toimenpiteitä, indikaattoreita ja tilastoja yhteistyössä muiden tahojen, kuten Europolin kanssa. Tavoitteena on laatia asianmukainen rikosluokitus ja lisätä tietoa laittomasta toiminnasta, sen maantieteellisestä levinneisyydestä ja yleistymisestä sekä sen torjumiseksi toteutettujen toimenpiteiden tehokkuudesta. YTK työskentelee tarpeen mukaan yhdessä muiden tutkimusyksiköiden kanssa ja ottaa niiden tutkimustulokset huomioon työssään. YTK ylläpitää asiaa käsittelevää Internet-sivustoa ja raportoi työnsä edistymisestä EU:n keskustelufoorumille.

## 7 PÄÄTELMÄT JA EHDOTUKSET

Tietokonerikollisuuden ehkäiseminen ja tehokas torjunta edellyttää välttämättä seuraavaa:

- Käytettävissä on ennalta ehkäisevää tekniikkaa. Tarvitaan asianmukainen sääntely-ympäristö, jossa on liikkumavaraa ja kannustimia innovaatioille ja tutkimukselle. Turvatekniikan kehittämistä ja käyttöä voi olla perusteltua tukea julkisin varoin.

- Turvallisuusriskit tiedostetaan ja osataan torjua.

- Käytössä on riittävät aineelliset ja prosessioikeudelliset säännöt, jotka koskevat sekä kansallista että kansainvälistä rikollisuutta. Jäsenvaltioiden rikosoikeuden aineellisissa säännöissä on säädettävä riittävän laaja-alaisista, tehokkaista ja varoittavista seuraamuksista; tällöin ne auttavat ratkaisemaan kaksoisrangaistavuuteen[71] liittyviä ongelmia ja helpottavat kansainvälistä yhteistyötä. Prosessilainsäädännössä on sallittava lainvalvontaviranomaisten suorittaa viipymättä hakuja tietokonejärjestelmissä ja takavarikoida tai turvallisesti jäljentää tietokoneelle tallennetut tiedot, kun tähän on perusteltu syy. Tällöin on noudatettava Euroopan ihmisoikeussopimusta ja yhteisön oikeudessa määriteltyjä perusperiaatteita sekä säännöksiä tilanteista, joissa näistä

[70] Lisätietoja IST-ohjelmasta saa verkko-osoitteesta http://www.cordis.lu/ist.

[71] Tietyntyyppisen keskinäisen oikeusavun saamiseksi toisen maan viranomaisilta ja rikollisten luovuttamiseksi monissa oikeusjärjestelmissä edellytetään, että kyseessä on kummassakin maassa rangaistava rikos.

periaatteista voidaan poiketa. Komissio katsoo, että telekuuntelusäännösten osalta ei ole mahdollista edetä pitemmälle kuin mitä jäsenvaltiot ovat sopineet yleissopimuksessa keskinäisestä oikeusavusta rikosasioissa. Komissio seuraa sopimuksen täytäntöönpanoa jäsenvaltioiden, alan yritysten ja käyttäjien kanssa sen varmistamiseksi, että asiaan liittyvät aloitteet ovat tehokkaita, avoimia ja tasapainoisia.

- Koulutettuja lainvalvontaviranomaisia on riittävästi ja heillä on käytössään asianmukaiset välineet. Tiivistä koulutusyhteistyötä Internet-palveluntarjoajien ja teleoperaattoreiden kanssa kehitetään edelleen.

- Kaikkien toimijoiden — käyttäjien, kuluttajien, alan yritysten sekä lainvalvonta- ja tietosuojaviranomaisten — yhteistyötä tehostetaan. Tämä on ratkaisevan tärkeää tietokonerikosten tutkimisen ja yleisen turvallisuuden kannalta. Alan toiminnalle on asetettava selkeät säännöt ja velvoitteet. Hallitusten on tunnustettava, että lainvalvontaviranomaisten tarpeet voivat aiheuttaa rasitteita alan yrityksille, ja pyrittävä kohtuullisin toimenpitein minimoimaan näitä rasitteita. Samaten yritysten on liiketoiminnassaan otettava huomioon yleinen turvallisuus. Tämä edellyttää entistä aktiivisempaa yhteistyötä sekä yksittäisen käyttäjän ja kuluttajan tukemista.

- Alan yritysten ja yhteisön johdolla toteutettavia aloitteita jatketaan. Vihjelinjoja, joiden avulla voidaan jo nyt tehdä ilmoituksia laittomasta ja haitallisesta sisällöstä, voidaan laajentaa myös muuntyyppisiin väärinkäytöksiin. Alalla harjoitettava itsesääntely ja monialainen yhteistyöasiakirja voitaisiin ulottaa koskemaan mahdollisimman suurta kohderyhmää, ja niiden avulla voidaan monin eri tavoin edistää tietokonerikollisuuden ehkäisemistä ja torjuntaa sekä lisätä tietämystä ja luottamusta.

- Tutkimus- ja kehitystoiminnan saavutukset ja mahdollisuudet hyödynnetään mahdollisimman tehokkaasti. Keskeisenä strategisena tavoitteena on yhdistää kohtuuhintaisten ja tehokkaiden turvatekniikkojen ja muiden luottamusta lisäävien tekniikkojen kehittäminen ja EU:n poliittiset aloitteet.

Kaikissa EU:n tasolla hyväksyttävissä toimenpiteissä on otettava huomioon se, että sen jäseniksi ehdolla olevat maat on vähitellen tuotava EU:n sisäisen ja kansainvälisen yhteistyön piiriin ja että niistä ei saa tulla tietokonerikollisuuden pesäpaikkoja. On syytä harkita ehdokasmaiden edustajien kutsumista joihinkin tai kaikkiin tietokonerikollisuutta käsitteleviin EU-kokouksiin.

Komission ehdotukset voidaan jakaa säädösehdotuksiin ja muihin ehdotuksiin.

### 7.1 Säädösehdotukset

Komissio esittää Euroopan unionista tehdyn sopimuksen VI osaston mukaisesti seuraavat säädösehdotukset:

- Ehdotus lapsipornografiarikoksia koskevan jäsenvaltioiden lainsäädännön lähentämisestä. Tämä aloite on osa laajempaa lasten seksuaalisen hyväksikäytön ja ihmiskaupan torjuntaa koskevaa ehdotuskokonaisuutta, josta ilmoitettiin joulukuussa 1998 annetussa ihmiskauppaa koskevassa komission tiedonannossa. Tällainen ehdotus vastaa täysin Euroopan parlamentin pyrkimystä muuttaa Itävallan aloitetta lapsipornografiaa koskevasta neuvoston päätöksestä siten, että tehtäisiinkin lakien lähentämistä edellyttävä puitepäätös. Lisäksi ehdotus käy yksiin Tampereen päätelmien ja järjestäytyneen rikollisuuden

vastaisen EU-strategian kanssa. Se on jo sisällytetty tulostauluun vapauteen, turvallisuuteen ja oikeuteen perustuvan alueen toteutumisen seuraamiseksi.

- Ehdotus rikosoikeuden aineellisten sääntöjen lähentämisestä entisestään huipputekniikkaan liittyvän rikollisuuden osalta. Tämä käsittää tietojärjestelmiin murtautumiseen ja ruuhkauttamishyökkäyksiin liittyvät rikokset. Komissio tarkastelee myös erilaisia vaihtoehtoja Internetissä esiintyvän rasismin ja muukalaisvihan torjumiseksi ja pyrkii laatimaan ehdotuksen Euroopan unionista tehdyn sopimuksen VI osaston mukaisesti tehtäväksi puitepäätökseksi rasistisen ja muukalaisvastaisen toiminnan torjumisesta sekä verkossa että sen ulkopuolella. Lisäksi on tarkasteltava huumeiden Internet-kaupan torjumista.

- Ehdotus vastavuoroisen tunnustamisen periaatteen soveltamisesta ennen oikeudenkäyntiä annettuihin määräyksiin ja vähintään kahta jäsenvaltiota koskevien tietokonerikostutkimusten helpottamisesta. Ehdotuksessa esitetään myös perusoikeuksien suojaamiseksi tarvittavat takeet. Ehdotus on vastavuoroisen tunnustamisen toimenpideohjelman mukainen, sillä toimenpideohjelmassa todetaan, että on syytä pohtia todistusaineiston esittämistä ja pidättämistä koskevia ehdotuksia.

Komissio arvioi tarvetta toteuttaa teleliikennetietojen säilyttämisen osalta lainsäädännöllisiä ja muita toimenpiteitä EU:n keskustelufoorumin tulosten perusteella ja muita osapuolia kuultuaan.

### 7.2 Muut ehdotukset

Toimenpiteitä on ehdotettu toteutettaviksi useilla osa-alueilla:

- Komissio perustaa EU:n keskustelufoorumin, jolla se toimii puheenjohtajana ja jolla lainvalvontaviranomaiset, palveluntarjoajat, verkko-operaattorit, kuluttajaryhmät ja tietosuojaviranomaiset pyrkivät tehostamaan yhteistyötään EU:n tasolla tuomalla yleiseen tietoisuuteen Internetiä hyväkseen käyttävien rikollisten aiheuttamat riskit, edistämällä tietotekniikan turvallisuuden kannalta parhaita käytäntöjä, kehittämällä tehokkaita rikostentorjuntavälineitä ja -keinoja tietokonerikollisuuden kitkemiseksi sekä edistämällä ennakkovaroitus- ja kriisinhallintajärjestelmien jatkokehittelyä. Kysymyksessä olisi unioninlaajuinen versio muutamissa jäsenvaltioissa jo aiemmin menestyksekkäästi perustetuista järjestelmistä. Komissio kannustaa myös jäsenvaltioita, joissa tällaisia järjestelmiä ei ole, perustamaan niitä. Kansallisten järjestelmien yhteistoimintaa voitaisiin edistää ja helpottaa EU-foorumin avulla.

- Komissio edistää edelleen turvallisuutta ja luottamusta *e*Europe-aloitteen, Internet-toimintasuunnitelman, IST-ohjelman ja seuraavan TTK-puiteohjelman avulla. Tämä tarkoittaa muun muassa riittävän turvallisten tuotteiden ja palvelujen saatavuuden sekä tehokkaiden salaustuotteiden aiempaa vapaamman käytön edistämistä kaikkien osapuolten vuoropuhelun avulla.

- Komissio edistää nykyisten ohjelmien avulla uusia hankkeita, joilla tuetaan lainvalvontaviranomaisille annettavaa koulutusta huipputekniikkaan liittyvää rikollisuutta koskevissa asioissa ja edistetään tietokonerikosten jälkien tutkimista.

- Komissio tutkii mahdollisuuksia parantaa COMCRIME-tutkimuksen yhteydessä laaditun kansalliset lait käsittävän tietokannan sisältöä ja käynnistää tutkimuksen, jonka tarkoituksena on aiempaa paremmin selvittää jäsenvaltioissa harjoitettavan tietokonerikollisuuden luonne ja laajuus.

### 7.3 Muu kansainvälinen toiminta

Komissio pyrkii edelleen aktiivisesti koordinoimaan tietoverkkorikollisuutta koskevia jäsenvaltioiden kannanottoja Euroopan neuvostossa, G8-maiden kokouksissa ja muissa kansainvälisissä yhteyksissä. Komission aloitteissa jäsenvaltioiden lainsäädännön lähentämiseksi otetaan täysin huomioon saavutetut tulokset.

* * * * *

# RAHOITUSSELVITYS

## 1. TOIMENPITEEN NIMI

Turvallisempaan tietoyhteiskuntaan tietojärjestelmien turvallisuutta parantamalla ja tietokonerikollisuutta ehkäisemällä.

## 2. BUDJETTIKOHDAT

B5-302

B5-820

B6-1110, B6-2111, B6-1210

## 3. OIKEUSPERUSTA

EY:n perustamissopimuksen 95, 154 ja 155 artikla, EU:sta tehdyn sopimuksen 29 ja 34 artikla

## 4. TOIMENPITEEN KUVAUS

### 4.1. Toimenpiteen yleistavoite

Komissio perustaa EU:n keskustelufoorumin ja toimii sen puheenjohtajana. Foorumin tarkoituksena on tarjota lainvalvontaviranomaisille, Internet-palveluntarjoajille, teleoperaattoreille, kansalaisoikeusjärjestöille, kuluttajien edustajille, tietosuojaviranomaisille ja muille osapuolille tilaisuus tutustua toisiinsa paremmin ja tehostaa yhteistoimintaansa EU:n tasolla. Näin pyritään tuomaan yleiseen tietoisuuteen Internetiä hyödyntävien rikollisten aiheuttamia riskejä, edistämään turvallisuuden kannalta parhaita käytäntöjä, kehittämään tehokkaita välineitä ja keinoja tietokonerikollisuuden torjumiseksi sekä kehittämään ennakkovaroitus- ja kriisinhallintajärjestelmiä edelleen. Foorumin Internet-sivuilla julkaistaan näihin aiheisiin liittyviä asiakirjoja.

### 4.2. Toimenpiteen kesto ja sen uusiminen

2001–2002. Foorumin jatkosta päätetään vuonna 2002 tehtävän arvioinnin perusteella.

## 5. MENOJEN JA TULOJEN LUOKITUS

### 5.1. Ei-pakollinen

### 5.2. Jaksotetut määrärahat

## 6. MENO-/TULOLAJI

| | | | |
|---|---|---|---|
| **Kokoukset: asiantuntijoiden matkakulujen korvaaminen** | | | |
| B5 302A | 2001 | | 27 000 € |
| B5 302A | 2002 | | 40 500 € |
| **Käytännön järjestelyt, Internet-sivuston ylläpitäminen** | | | |
| B6 1110 | 2001 | YTK:n virkamatkat | 10 000 € |
| B6 2111 | 2001 | YTK:n erityismäärärahat (sekalaiset) | 15 000 € |
| B6 1210 | 2001 | YTK:n yleiskulut | 50 000 € |
| B6 1110 | 2002 | YTK:n virkamatkat | 10 300 € |
| B6 2111 | 2002 | YTK:n erityismäärärahat (sekalaiset) | 15 450 € |
| B6 1210 | 2002 | YTK:n yleiskulut | 51 500 € |
| **Tutkimukset** | | | |
| B6 2111 | 2001 | YTK:n erityismäärärahat (tutkimukset) | 25 000 € |
| B6 2111 | 2002 | YTK:n erityismäärärahat (tutkimukset) | 25 750 € |
| Yhteensä | 2001 + 2002 | | 270 500 € |

## 7. RAHOITUSVAIKUTUKSET

**Toimenpiteen kokonaiskustannusten laskutapa (yksittäisten ja yhteenlaskettujen kustannusten välinen suhde)**

Kokousten osanottajille korvataan matkakulut. Vuonna 2001 on tarkoitus järjestää kaksi ja vuonna 2002 kolme kokousta. Kunkin kokouksen osalta korvataan 15 asiantuntijan matkakustannukset. Keskimääräisen korvauksen arvioidaan olevan 900 euroa.

Infrastruktuuriin, hallintotukeen ja tekniseen tukeen liittyvät henkilöstökulut ja erityismäärärahat kohdennetaan suhteessa toimintaan osallistuvan henkilöstön määrään. Tutkimusmäärärahatarve perustuu arvioon, jonka mukaan tehdään kaksi tutkimusta vuodessa ja kunkin vaatima työmäärä on 1 henkilötyökuukausi.

## 8. PETOSTENVASTAISET TOIMENPITEET

Rutiinitarkastukset. Lisätoimenpiteitä ei ole tarkoitus toteuttaa.

## 9. KUSTANNUSVAIKUTTAVUUSANALYYSI

### 9.1. Tavoitteet ja kohderyhmä

Eri eturyhmien keskinäisen tuntemuksen ja yhteistyön edistäminen EU:n tasolla. Kohderyhmä: lainvalvontaviranomaiset, Internet-palveluntarjoajat, teleoperaattorit, kansalaisoikeusjärjestöt, kuluttajien edustajat, tietosuojaviranomaiset ja muut osapuolet.

### 9.2. Toimenpiteen perustelut

Foorumin tarkoituksena on parantaa eri eturyhmien keskinäistä tuntemusta ja edistää niiden yhteistoimintaa EU:n tasolla. Foorumin yhteydessä pyritään tuomaan yleiseen tietoisuuteen Internetiä hyödyntävien rikollisten aiheuttamia riskejä, edistämään turvallisuuden kannalta parhaita käytäntöjä, kehittämään tehokkaita välineitä ja keinoja tietokonerikollisuuden torjumiseksi sekä kehittämään ennakkovaroitus- ja kriisinhallintajärjestelmiä edelleen.

### 9.3. Toimenpiteen seuranta ja arviointi

Komissio järjestää foorumin kokoukset ja toimii niissä puheenjohtajana sekä hoitaa foorumin Internet-sivustoa. Vuonna 2002 arvioidaan, onko foorumin toimintaa syytä jatkaa vuonna 2003 ja sen jälkeen.

## 10. HALLINTOMENOT

Toiminta pystytään hoitamaan nykyisellä henkilöstöllä.

### 10.1. Vaikutus henkilöstön määrään

| Henkilöstön laji | Toimen hallinnointiin osoitettu henkilöstö | | Jakauma | | Kesto |
|---|---|---|---|---|---|
| | Vakinainen henkilöstö | Väliaikainen henkilöstö | Pääosastojen nykyinen henkilöstö | Lisätarve | |
| Virkamiehet A<br>tai B<br>väliaikaiset C<br>toimihenkilöt | 0,05 | 1,75<br>0,15 | 1,75<br>0,15<br>0,05 | | Vuotta kohden kahden vuoden ajan |
| Muu henkilöstö | | | | | |
| Yhteensä | 0,05 | 1,9 | 1,95 | | |

### 10.2. Lisähenkilöstöstä aiheutuvat kokonaiskustannukset

| | Määrä | Laskutapa (2001 - 2002) |
|---|---|---|
| Virkamiehet | 421.200 € | 2 vuotta x 108 000 € x 1,95 henkilötyövuotta |