Poliisiosaston julkaisu **2** ● 2003

Internetissä julkaistavan rikollisen materiaalin rajoittamista selvittäneen työryhmän raportti

ISSN 1236-049X
ISBN 951-734-503-8

SISÄASIAINMINISTERIÖ

KUVAILULEHTI

Julkaisun päivämäärä
15.1.2003

Tekijät (toimielimestä, toimielimen nimi, puheenjohtaja, sihteeri)	Julkaisun laji
Rikostarkastaja Ari Määttä, Keskusrikospoliisi, puh. joht. Rikosylikomisario Veli-Pekka Loikala, Keskusrikospoliisi Ylitarkastaja Sari Kajantie, Keskusrikospoliisi	Työryhmän raportti
	Toimeksiantaja Sisäasiainministeriö
	Toimielimen asettamispäivä 15.10.2002

Julkaisun nimi (myös ruotsinkielisenä)
Internetissä julkaistavan rikollisen materiaalin rajoittamista selvittäneen työryhmän raportti

Julkaisun osat
raportti ja liitteet

Tiivistelmä

Sisäasiainministeriön asettaman työryhmän tarkoitus oli selvittää sekä mahdolliset lainsäädäntöön liittyvät tarpeet että tekniset mahdollisuudet, jotta internetissä julkaistavan rikollisen materiaalin levittämistä voitaisiin rajoittaa tai estää. Raportissa käydään läpi erilaisia verkkoviestinnän muotoja ja punnitaan niiden valvontamahdollisuuksia. Työryhmä suosittaa, että rikollisen materiaalin julkaisemista tulisi ensisijaisesti rajoittaa koulutuksella, valistuksella ja tehokkaalla itsesääntelyllä. Myös oikeudelliset edellytykset tulee saattaa tasolle, joka mahdollistaa sisältörikosten selvittämisen ainakin kansallisissa tietojärjestelmissä. Yksi selvittämisen turvaamisen olennainen keino olisi säätää erilaisten viestien tunnistamistietojen säilyttämisestä.

Avainsanat (asiasanat)
internet, viestintä, verkkoviestintä, tietotekniikka, tietoverkkorikollisuus

Muut tiedot

Sarjan nimi ja numero	ISSN	ISBN
Sisäasiainministeriö, poliisiosaston julkaisusarja 2/2003	1236-049X	951-734-503-8

Kokonaissivumäärä	Kieli	Hinta	Luottamuksellisuus
45	suomi	-	julkinen

Jakaja	Kustantaja
Sisäasiainministeriö, poliisiosasto	Sisäasiainministeriö, poliisiosasto

Sisäasiainministeriölle

Sisäasiainministeriö asetti 15.10.2002 työryhmän selvittämään sekä mahdolliset lainsäädäntöön liittyvät tarpeet että tekniset mahdollisuudet, jotta internetissä julkaistavan rikollisen materiaalin levittämistä voitaisiin rajoittaa tai estää. Työssä tuli erityisesti ottaa huomioon jo vireillä olevat lainsäädäntöhankkeet. Työryhmän puheenjohtajaksi asetettiin rikostarkastaja Ari Määttä Keskusrikospoliisista ja jäseniksi rikosylikomisario Veli-Pekka Loikala ja ylitarkastaja Sari Kajantie Keskusrikospoliisista.

Toimeksiannon antamin valtuuksin työryhmä pyysi lausuntoja oikeuden ja tekniikan asiantuntijoilta. Lausunnon antoivat asianajaja, Euroopan parlamentin jäsen Matti Wuori, Telia Mobile Finlandin päälakimies Jari Perko, Viestinnän Keskusliiton toimitusjohtaja Håkan Gabrielsson, Electronic Frontier Finland ry:n puolesta FT, tutkija Kai Puolamäki, Teknisen korkeakoulun puolesta tietohallintopäällikkö Krister Sarlin, atk-erikoistutkija Timo Larmela, atk-erikoistutkija Kimmo Laaksonen ja tietoturva-asiantuntija Sami Koskinen. Tämän lisäksi työryhmä kuuli henkilökohtaisesti Opetushallituksesta Pirjo Immonen-Oikkosta DotSafe -projektista. Asiantuntijoiden lausunnot ovat olleet ohjaamassa tätä työtä ja lausunnot on liitetty raportin loppuun erillisiksi liitteiksi.

Työryhmän esittämät suositukset on esitetty luvussa 7 ja niistä vallitsi työryhmässä yksimielisyys.

Saatuaan työnsä valmiiksi työryhmä jättää kunnioittavasti laatimansa raportin sisäasiainministeriölle.

Vantaalla 15 tammikuuta 2003

Ari Määttä

Veli-Pekka Loikala

Sari Kajantie

SISÄLLYSLUETTELO:

1 Johdanto

Myyrmäen pommiräjäytyksen tutkinnan yhteydessä kävi ilmi, että räjäyttäjä oli keskustellut pommin valmistamisesta Internetin keskusteluryhmissä. Tämä aiheutti tiedotusvälineissä keskustelua Internetissä ilmenevistä haitallisista ilmiöistä sekä mahdollisuuksista viranomaistoimin puuttua niihin. Tiistaina 15. lokakuuta 2002 keskustelu eteni aina eduskuntaan asti, kun sisäministeri Ville Itälä antoi pääministerin ilmoituksen asian johdosta. Tuossa ilmoituksessa hän mainitsi julkisen vallan velvollisuudeksi turvata kaikkien kansalaisten perus- ja ihmisoikeudet. Näitten oikeuksien toteutuminen ja loukkauksiin viranomaistoimin puuttuminen tulee olla mahdollista myös Internetin kaltaisessa ympäristössä.

Internetin globaali luonne ja monimuotoisuus toimintaympäristönä on haasteellinen. Jo verkon rajat ylittävä luonne sekä mahdollisuus toimia anonyymisti tekee viranomaisten mahdollisuuden puuttua laittomaan ja haitalliseen sisältöön vaikeaksi. Internetissä on monia toimijoita, joiden asema järjestelmässä vaihtelee. On operaattoreita, palveluntarjoajia, kotikäyttäjiä, yrityskäyttäjiä ym.

Usein on sanottu, että kukaan ei pysty hallitsemaan verkkoa juuri sen globaalisuuden takia. Väite tarkoittaa itse asiassa samaa kuin väittäisimme, ettei kukaan hallitse maapalloa. Vaikka verkon kokonaisuus ei olekaan yksittäisen organisaation hallinnassa, se ei silti ole hallitsematon: Verkko muodostuu itsenäisistä osista, joilla kullakin on oma haltijansa. Eri organisaatioiden hallitsemien osien välistä kommunikaatiota sääntelevät tiukemmin lait sekä sopimukset ja löyhemmin verkon ylläpitäjien noudattama hyvä ylläpitotapa sekä käyttäjiä opastava netiketti eli käytännesäännöt. Teknisen kommunikoinnin taas mahdollistavat liikennöintistandardit.

Tietoverkkoja käytetään mitä erilaisimpiin palveluihin, sieltä haetaan tietoa, viihdettä, seuraa, mutta kuten yhteiskunnassa yleensä, ilmenee verkoissa myös yhteiskunnallisesti paheksuttavaa käyttäytymistä. Sisällöllisesti laittoman materiaalin levittäminen verkossa on teknisesti helppoa ja onnistuu nykyisin vähäisilläkin tietokonetaidoilla.

Rikoslain lähtökohta lainvastaisen materiaalin levittämiseen on selkeä. Tekijä vastaa teostaan. Sen sijaan muiden toimijoiden kuten operaattoreiden ja palveluntarjoajien vastuu laittomasta materiaalista on vielä tällä hetkellä jäsentymätön. Laki tietoyhteiskunnan palvelujen tarjoamisesta tuli voimaan 1 heinäkuuta 2002, jossa määriteltiin ensimmäisen kerran tietoyhteiskunnan palveluntarjoajan vastuuta laittomaan sisältöön. Sananvapauslain uudistaminen on kesken eduskunnassa ja tuossa laissa on tarkoitus säätää vastuu laittomasta verkkosisällöstä verkkojulkaisun ylläpitäjälle. Lakiehdotuksen sisällöstä on käyty voimakastakin keskustelua julkisessa sanassa eteenkin siltä osin, miten vastuu tulisi kohdistaa ja onko vastuun kohdistaminen oikeudenmukaista. Lakiehdotus tullee tämän raportin julkistamisen aikoihin eduskunnan käsittelyyn valiokunnista.

Tämän työryhmän tehtävänä on sisäasiainministeriön antaman toimeksiannon mukaisesti selvittää mahdolliset lainsäädäntöön liittyvät tarpeet sekä tekniset mahdollisuudet, jotta Internetissä julkaistavan rikollisen materiaalin levittämistä voitaisiin rajoittaa tai estää. Toimeksianto tarkentuu *valvonnan tehokkuuden arviointiin*. Työryhmä on rajoittanut työskentelynsä koskemaan vain toimeksiannossa tarkoitettua asiaa, joten siihen kysymykseen, tulisiko uusia sisältöön liittyviä kriminalisointeja tehdä, ei oteta kantaa. Työryhmä otti nimekseen "Nettityöryhmä".

2 Verkkoviestintämenetelmiä

Verkkoviestintä ei ole irrallaan muusta yhteiskunnasta. Verkkoviestinnän tekniikassa ja kulttuurissa on kuitenkin tiettyjä erityispiirteitä, joita on syytä ymmärtää ennen sääntelyä. Termejä käytetään tässä seuraavasti:

- *verkkokeskustelu* tarkoittaa toimittamatonta julkista verkkokeskustelua,
- t*iedonsiirto* menetelmiä, joilla voidaan tarjoa haettavaksi tai hakea tietoa, kuvia, ääntä, ohjelmia.
- *verkkoviestintä* on yhteisnimi, joka kattaa kummankin edellä mainitun

Tämän selvityksen ulkopuolelle jätetään varsinainen televisio- ja radiotoiminta. Tältä osin viitataan valmisteilla olevaan lakiin sanavapauden käyttämisestä joukkoviestinnässä. Tässä osassa on tarkoituksena esitellä erilaisia teknisiä verkkoviestinnän muotoja ja niiden hallintaa.

2.1 Viestintäkulttuurista

Verkkokeskustelu rinnastuu vahvasti avoimeen kahvilakeskusteluun. Keskustelu ei ole ennalta toimitettua, eikä osallistujilta vaadita vahvaa ennakkotunnistusta. Kukin seurue säätelee itse keskustelussa vallitsevat normistot: mistä puhutaan, millä tavoin sekä onko keskustelu kaikille avoin. Tilan tarjoava kahvila ei puutu keskustelun kulkuun, mutta säätelee normistot ja käytännöt vakavampien häiriöiden torjumiseksi.

Historiallisista syistä Internetissä on korostettu voimakkaasti yksilön vastuuta. Internetin verkkoviestintäkulttuurin pohja on akateemisessa maailmassa, jossa kunkin toimijan oma vastuu ja yhteisön itsesääntely on oleellisesti merkityksellisempää kuin muussa yhteiskunnassa.

Niinpä verkossa pätee yhä :

- Kirjoittajan vastuu: kukin vastaa omista kirjoituksistaan.
- Lukijan vastuu: verkon luonne on ymmärrettävä ja luettuun on suhtauduttava yhtä lähdekriittisesti kuin kahvilassa kuultuun.
- Yhteisön vastuu: itsesääntely.

Sekä myös

- Yksilön oikeus luottamukselliseen viestintään.
- Ylläpitäjän oikeus suojella järjestelmäänsä toimintaa häiritseviltä tekijöiltä, kuitenkaan loukkaamatta yksilön oikeuksia.

Verkkoviestinnän suurin voima on viestinnän vapaus, mutta se on myös heikkous silloin kun jokin toimijoista ei kykene kantamaan vastuutaan.

2.2 Suunnittelun lähtökohdat

Verkon tekniselle kehitykselle on ominaista orgaanisuus ja nopea reagointi ympäristöön. Jos jossakin ilmenee tekninen, taloudellinen tai hallinnollinen este, se kierretään suunnittelemalla viestintätapa tarvittavilta osin uudestaan.

Verkkokeskustelujärjestelmät on suunniteltu verkossa vallitsevaan kulttuuriin. Ne on alunperin pyritty kehittämään mahdollisimman tehokkaiksi ja vikasietoisiksi. Turvallisuus tai osallistujien tunnistettavuus ja jäljitettävyys eivät ole olleet suunnittelun kriteereitä, koska järjestelmät on suunniteltu ympäristöön, jossa vallitsee tietty luottamus. Nykyään turvallisuus tai jäljitettävyys jäävät usein huomiotta siksi, että ne ovat lisäkustannus ja hankaloittavat käyttöä.

Avoimet verkkorajapinnat ja tarkasti suunnitellut standardit merkitsevät käytännössä sitä, että kuka tahansa verkko-ohjelmointitaitoinen voi kehittää oman liikennöintikäytäntönsä. Tällä hetkellä kehityksen paino on erilaisissa vertaisverkoissa, mutta verkon luonteen huomioiden, huomenna se voi olla jotakin käsitteellisesti uutta.

2.3 Keskustelujärjestelmiä

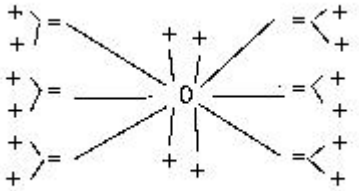
Verkossa on lukuisia erilaisia keskustelujärjestelmiä, joiden ominaispiirteet eroavat toisistaan suuresti. Järjestelmien rakenne asettaa reunaehtoja laittoman materiaalin levittämisen estämiselle. Joissakin järjestelmissä toimivat menetelmät eivät ole lainkaan mahdollisia joissakin muissa. Osa järjestelmistä on keskitetysti hallittuja, osan hallinta on täysin hajautettua. Osassa viestit ovat näkyvillä vain hetken, osassa viestit tallennetaan siten, että ne ovat luettavissa ajasta riippumatta.

Ohessa on ongelmakentän selventämiseksi kuvattu erilaisia avoimia ja julkisia keskustelujärjestelmätyyppejä. Esimerkit on valittu erilaisuuden ja laajan suomalaiskäytön mukaan.

2.3.1 Tallentuvia viestejä välittäviä järjestelmiä

Postituslistat:

0 – postilistapalvelin
= - listan jäsenen postipalvelin
+ - listan jäsen



Kuva 2.1: postituslista

Lyhyt kuvaus:

Postituslistassa listalle tarkoitettu viesti lähetetään postilistapalvelimelle osoitteeseen, joka on muodoltaan listan-nimi@lista.palvelin. Listapalvelin jakaa viestin edelleen kaikille listan jäsenille sähköpostitse.

Listan viestien vastaanottaminen sähköpostitse vaatii liittymisen listalle omalla sähköpostiosoitteella. Lähetys on myös usein sallittu vain jäsenille.

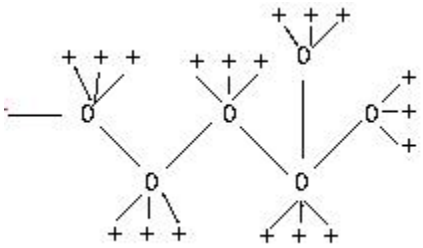
Hallinta:

Listan ylläpitäjä hallitsee jäsenlistaa ja viestien pääsyvalvontaa keskitetysti postituslistapalvelimessa. Listan ylläpitäjä määrittelee listan keskustelun normiston, ja voi määritellä pääsyvalvontaa viesteille, mutta ei voi poistaa listalta viestejä jälkikäteen, koska viestit tallentuvat jäsenten henkilökohtaisiin postilaatikoihin.

Postilistapalvelin yleensä tallentaa lokiin viestien lähetysajan, lähettäjäksi merkityn osoitteen, vastaanottajan sekä verkko-osoitteen, josta viesti on palvelimelle tullut.

News-järjestelmä[1]

0 – News-palvelin
+ - Newsien lukija



Kuva 2.2: News-järjestelmä

Lyhyt kuvaus:

News-järjestelmä ei nimestään huolimatta ole uutispalvelu, vaan hajautettu keskustelujärjestelmä, joka on toiminut Internetissä vuodesta 1979.

Käyttäjä lukee ja kirjoittaa News-artkkeleita oman organisaationsa News-palvelimen kautta. Artikkelit leviävät maailmalla ketjutetusti siten, että kullakin palvelimella on ”ylävirrassa” jakelija, jolta se saa artikkeleita, sekä ”alavirrassa” mahdollisesti jakelun kohteita, joille palvelin jakaa artikkeleita edelleen. Palvelin myös antaa ylävirtaan artikkelit, jotka on kirjoitettu palvelimessa itsessään tai jotka se on saanut alavirrasta.

News-artikkeleiden lukeminen ei vaadi rekisteröitymistä. Kirjoitus tapahtuu oman sähköpostiosoitteen nimissä, mutta sen oikeellisuutta ei tarkisteta.

[1] "News" on erisnimen kaltainen tunniste, jonka suomentaminen kadottaisi sanan merkityksen.

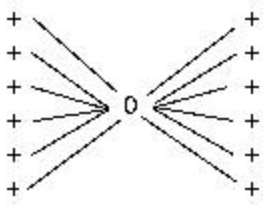
Hallinta:

News-palvelimen ylläpitäjä voi vaikuttaa etukäteen palvelimen ryhmävalikoimaan, mutta ei yksittäisten artikkeleiden vastaanottoon. Jälkikäteen palvelimen ylläpitäjällä on teknisesti mahdollisuus poistaa palvelun toimintaa haittaava tai laiton artikkeli, mutta poisto ei tällöin kohdistu muualle kuin omaan palvelimeen: muualla artikkeli säilyy yhä luettavana.

News-järjestelmässä on myös mekanismeja poistaa artikkeleita kaikilta palvelimilta, mutta Newsien hajautetun luonteen vuoksi näissä on sopimusteknisiä ongelmia, ja ne onkin tarkoitettu vain artikkelin kirjoittajan käyttöön. Newsien SPAM-torjuntajärjestelmissä ongelmat on kierretty siten, että haitallisten viestien poisto suoritetaan ennalta määritellyin teknisluontoisin kriteerein eikä sisällön tai viestintäosapuolten perusteella. Lisäksi kunkin palvelimen ylläpitäjä valitsee otetaanko torjunta palvelimella käyttöön vai ei.

WWW-keskustelupalstat

0 – WWW-keskustelupalvelin
+ - keskustelijat



Kuvaus 2.3: WWW-keskustelujärjestelmä

Lyhyt kuvaus:

WWW-keskustelupalstat ovat edellisistä poiketen yleensä täysin keskitettyjä siten että kaikki viestiliikenne ja palstan hallinta tapahtuvat yhdessä järjestelmässä.

Hallinta:

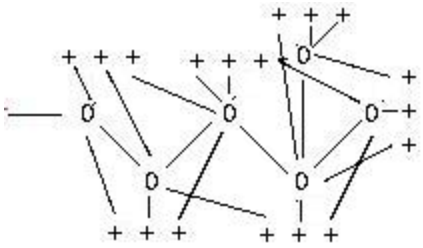
WWW-keskustelu on teknisesti täysin palveluntarjoajan hallittavissa. Hallinnoija voi määritellä keskustelun normit, sekä tarvittaessa poistaa haitallisia tai laittomia viestejä.

Käyttäjien rekisteröitymisvaatimukset vaihtelevat palveluntarjoajasta riippuen.

2.3.2 Reaaliaikaiset keskustelujärjestelmät

IRC - The Internet Relay Chat

0 - IRC-palvelin
+ - IRC-keskustelija



Kuva 2.4: IRC-palvelu

Lyhyt kuvaus

IRC on suomalaisen Jarkko Oikarisen 1980-luvun lopulla kehittämä erittäin laajasti käytetty reaaliaikainen keskustelujärjestemä, jossa keskustelijat lähettävät tekstiä rivi kerrallaan IRC-palvelimelle, joka levittää ne edelleen muille kanavan käyttäjille sekä samalla palvelimella että muissa saman IRC-verkon palvelimissa. Käyttäjä voi kytkeytyä käytännöllisesti katsoen mihin tahansa IRC-palvelimeen, eikä ole millään tavoin sidoksissa oman organisaationsa palvelimeen.

IRCin reaaliaikaisuus tarkoittaa sitä, että viestiliikenne on nähtävissä lähetyshetkellä eikä IRC-palvelimen puolesta tallennu lainkaan. Yksittäisen keskustelijan on kuitenkin yleisissä IRC-asiakasohjelmistoissa mahdollista kerätä viestiliikennettä talteen.

IRCin kautta voi keskustelun lisäksi myös siirtää tiedostoja, ja IRC-tekniikka on käytössä myös erilaisissa vertaisverkkojen hallintajärjestelmissä.

IRCissä esiinnytään omalla kutsumanimellä, ja keskustelijan käyttämän koneen verkko-osoite on muiden keskustelijoiden nähtävissä.

Hallinta

Kunkin IRC-kanavan hallinnoija voi säädellä kanavan keskustelun normit, sekä poistaa osallistujia tarvittaessa kanavalta. Lähetettyjä viestejä ei ole teknisesti mahdollista poistaa näkyviltä.

WWW-chat

Lyhyt kuvaus

WWW-chatit ovat rakenteeltaan keskitettyjä aivan kuten WWW-keskustelujärjestelmät, mutta keskustelu on luonteeltaan reaaliaikaista eli perustuu samanaikaiseen keskusteluun eikä tallentuviin artikkeleihin.

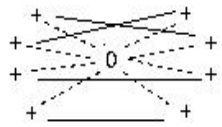
Käyttäjien rekisteröitymisvaatimukset vaihtelevat palveluntarjoajasta riippuen.

Hallinta

WWW-chat on teknisesti chatia ylläpitävän organisaation hallussa, mutta reaaliaikaisen luonteen takia viestejä ei yleensä seulota ennalta. Viestejä ei poisteta jälkikäteen, joskaan viestit eivät ole kauaa näkyvillä.

Vertaisverkot (peer-to-peer-verkot)

0 – (mahdollinen) hallintapalvelu
+ - keskustelija



Kuva 2.5: vertaisverkot

Lyhyt kuvaus

Vertaisverkoissa viestiliikenne tapahtuu suoraan kommunikoivien työasemien välillä. Yleiseen hallintaan, kuten keskustelukumppanien sijainnin selvittämiseen, käytetään usein hallintapalvelua, joka voi olla esimerkiksi erillinen palvelin tai vaikka IRC-kanava.

Vertaisverkkoja ovat esimerkiksi taannoin oikeudellisen arvioinnin alla ollut Napster, jota käytettiin musiikkitiedostojen jakeluun, sekä suosittu reaaliaikainen keskustelujärjestelmä ICQ.

Hallinta:

Vertaisverkot ovat liki täysin hajautetusti hallittuja, eikä edes ”hallintapalvelin” tiedä mitään keskustelijoiden välisistä yhteyksistä.

2.4 Tiedonsiirtomenetelmiä

Suurempia tietomääriä vaihdetaan keskustelujärjestelmien sijaan varsinaisilla tiedostonsiirtoyhteyskäytännöillä.

HTTP- tai FTP-siirroissa tiedon hakija ottaa yhteyden palvelimeen hakeakseen tiedon. Siirrettävä aineisto on teknisesti WWW- tai FTP-palvelimen ylläpidon hallittavissa, joten ylläpito voi tarvittaessa poistaa laittoman aineiston. Jäljet siirroista tallentuvat WWW- tai FTP-palvelun lokeihin.

Vertaisverkoissa tieto sijaitsee käyttäjän omalla koneella, joten operaattorilla ei ole teknisiä mahdollisuuksia poistaa laitonta aineistoa. Lokijälkiä vertaisverkkoliikenteestä ei yleisesti jää.

3 Tietotekniikan ja verkkoviestinnän vaikutus rikoslain kehitykseen

3.1 Rikoslain kokonaisuudistuksen I vaihe

Tietotekniikan ja verkkoviestinnän kehittyminen otettiin rikoslaissa ensimmäisen kerran huomioon säädettäessä rikoslain kokonaisuudistuksen ensimmäistä vaihetta, joka tuli voimaan 1991. Euroopan neuvosto oli asettanut vuonna 1985 asiantuntijakomitean, jonka tuli selvittää tietokonerikosten eri ilmenemismuotoja, arvioida niiden aiheuttamia

lainsäädännön uudistamistarpeita ja kehittää valtioiden välistä rikosoikeudellista yhteistyötä. Komitean työ siihen sisältyvine suosituksineen valmistui kesällä 1989 (Recommendation No. R (89) 9) ja Euroopan neuvoston ministerikomitea hyväksyi mainitut suositukset syksyllä 1989.[2] Tämä suositus oli vaikuttamassa rikoslain kokonaisuudistuksen ensimmäisen vaiheen työhön.

Rikoslain ensimmäisen vaiheen valmistelussa ei lähdetty rakentamaan uutta lainsäädäntöä vaan tarkistettiin luvatonta käyttöä, väärennöstä, vahingontekoa ja petosta koskevia rikoslain säännöksiä vastaamaan sen hetkistä tietoteknistä kehitystä. Näihin rikosnimikkeisiin kirjoitettiin tietotekniikan kehittymisen tuomat uudet, haitallisiksi katsotut tekomuodot osaksi tunnusmerkistökuvausta.

Luvatonta käyttöä koskevassa säännöksessä oli vanhan lain mukaan tunnusmerkistön toteutumisen edellytyksenä, että luvatta käytetty omaisuus oli käyttöhetkellä käyttäjän hallussa. Tämä edellytys aiheutti sen, että tietoverkkoa pitkin toisen tietokonejärjestelmään tunkeutuvaa ja sitä luvatta käyttävää ei voitu rangaista. Säännösmuutoksen jälkeen kyseinen toiminta tuli luvatonta käyttöä koskevan rikossäännöksen piiriin.

Väärennysrikosten osalta epäkohtana oli se, että automaattiseen tietojenkäsittelyyn soveltuvien tiedostojen muuntelut eivät kuuluneet silloisten väärennyssäännösten ulottuville.[3] Uudistuksen yhteydessä sisällytettiin väärennysrikoksia koskevaan rikoslain lukuun sellaisen todistuskappaleen määritelmä, joka voi olla väärennysrikoksen kohteena. Tuohon määritelmään otettiin tietotekniikan kehittymisen tuoma mahdollisuus tallentaa tietojärjestelmään tallenne, joka voi olla oikeudellisesti merkityksellinen. Tällaisen tallenteen väärentäminen tuli siten kriminalisoinnin piiriin.

Rikoslain aikaisempi sääntely vahingontekoa koskevissa rikoksissa rakentui ajatukselle omaisuuden fyysisestä vahingoittamisesta. Oli tulkinnanvaraista, voitiinko kyseistä säännöstä soveltaa siinä tapauksessa, että vahinko aiheutetaan turmelemalla tai muuntamalla tietojärjestelmään tallennettua tietoaineistoa ilman, että itse tietovälinettä fyysisesti vahingoitetaan.[4] Tästä johtuen säädettiin ns. tietovahingon aiheuttaminen, joka lisättiin vahingontekoa koskevan rikoslain 35 luvun 1 §:n 2 momenttiin. Säännöksen mukaan vahingonteosta tuomitaan myös se, joka toista vahingoittaakseen oikeudettomasti hävittää, turmelee, kätkee tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen.

Petosta koskevien rikossäännösten tarkoituksena on luoda edellytyksiä luottamukselle oikeuselämässä ja siten turvata tavaroiden ja palvelusten vaihdantaa sekä taloudellisten ja oikeudellisten asioiden hoitamista myös toisen puolesta.[5] Ennen rikoslain uudistusta epäkohtana oli se, että silloinen petossäännös edellytti aina jonkun ihmisen erehdyttämistä eikä näin välttämättä tapahtunut puututtaessa automaattiseen tietojenkäsittelyyn. Konetta ei voinut pettää. Tämä ongelma poistettiin säätämällä ns. tietojenkäsittelypetoksesta. Säännöksen mukaan petoksesta tuomitaan myös se, joka petostarkoituksessa syöttää vääriä tietoja tietojenkäsittelylaitteeseen tai muuten puuttumalla vääristää tietojenkäsittelyn lopputuloksen ja siten aiheuttaa toiselle taloudellista vahinkoa.

---

[2] Hallituksen esitys 94/1993 vp., s. 17.
[3] Korkeimman oikeuden päätös 1985 II 60.
[4] Hallituksen esitys 66/1988 vp., s. 122.
[5] Hallituksen esitys 66/1988 vp., s. 128

3.2 Rikoslain kokonaisuudistuksen II vaihe

Käsitellessään rikoslain kokonaisuudistuksen I vaihetta eduskunnan lakivaliokunta piti mietinnössään[6] välttämättömänä, että rikoslain kokonaisuudistuksen II vaiheessa kattavasti selostetaan, miten uusiutuva lainsäädäntömme täyttää Euroopan neuvoston tietokonerikoksia koskevan suosituksen. Tällainen selvitys otettiinkin lakia koskevaan hallituksen esitykseen.[7]

Euroopan neuvoston suosituksen pohjalta uusiin rikoslain pykäliin lisättiin jo aikaisemman lainvalmistelun tapaan uusia tietotekniikan esiin tuomia muutostarpeita ja rikoslakiin lisättiin muutamia uusia asiaan liittyviä säännöksiä. Tämän lisäksi tieto- ja viestintärikokset koottiin rikoslain 38 luvun alle. Tietotekniikan vaikutus näkyy mm. rikoslain 34 luvun 1 §:n tuhotyösäännöksessä, jossa tuhotyöstä tuomitaan myös se, joka tietojärjestelmän toimintaan oikeudettomasti puuttumalla aiheuttaa vakavan vaaran energiahuollolle, yleiselle terveydenhuollolle, maanpuolustukselle, oikeudenhoidolle tai muulle näihin rinnastettavalle yhteiskunnan tärkeälle toiminnolle. Rikoslain 30 luvun 4 §:n yritysvakoilua koskevan säännöksen mukaan laittomaan toimintaan syyllistyy se, joka oikeudettomasti hankkii tiedon toiselle kuuluvasta yrityssalaisuudesta tunkeutumalla ulkopuolisilta suojattuun tietojärjestelmään tarkoituksin oikeudettomasti ilmaista tällainen salaisuus tai oikeudettomasti käyttää sitä.

Rikoslain kokonaisuudistuksen I vaiheessa muutettu luvatonta käyttöä koskeva sääntely koskee nykyisellään riidattomasti myös tietojärjestelmän luvatonta etäiskäyttöä viestilinjojen välityksellä. Tämän lisäksi rikoslain 38 luvun 8 §:ään otettiin tietomurtoa koskeva rangaistussäännös, jonka tarkoituksena on kriminalisoida turvajärjestelyt ohittava, oikeudettomasti tapahtuva murtautuminen. Laitonta on nykyisin siis jo se, että murtautuu järjestelmään ilman, että luvatonta käyttöä ei tapahtuisikaan.

Viime vuosina yleistyneet palveluestohyökkäykset[8] on rikoslaissa kriminalisoitu 38 luvun 5-7 §:ään sisältyvien tietoliikenteen häirintää koskevien säännösten nojalla. Palveluestohyökkäykset ovat vakavia hyökkäyksiä tietojärjestelmää vastaan, joilta suojautuminen on vaikeaa.

Uusimpana tietoturvallisuutta palvelevana kriminalisointina rikoslakiin on sisällytetty tietokonevirusten ja järjestelmälle haitallisten ohjelmien valmistamisen ja saataville asettamisen kielto. Tämä rikoslain 34 luvun 9 §:n tarkoittama vaaran aiheuttaminen tietojärjestelmälle kriminalisoi myös virusohjeiden saataville asettamisen ja levittämisen.

3.3 Sisältörikokset verkkoviestinnässä

Edellä käsiteltiin tietotekniikan vaikutusta rikoslain säädöksiin lähinnä tietotekniseen järjestelmään kohdistuvan rikollisuuden kannalta. Nämä teot kohdistuvat pääsääntöisesti tietoturvan keskeisiin elementteihin eli tiedon luottamuksellisuuteen, eheyteen ja käytettävyyteen.

---

[6] Lakivaliokunnan mietintö n:o 6/1990 vp.
[7] Hallituksen esitys 94/1993 vp., s. 17 – 21.
[8] Hyökkäyksessä palvelimille lähetetään viestejä niin paljon, että palvelimet ylikuormittuvat ja tukkeentuvat siten, ettei esim. käyttäjä pääse palvelimissa oleville Internet –sivustoille.

Toinen verkkoviestinnässä ilmenevä rikollisuusmuoto on julkaistavassa sisällössä ilmenevät laittomuudet. Tästä ryhmästä voidaan käyttää nimeä sisältörikokset. Nämä rikokset eivät itsessään puutu tietojärjestelmän toimivuuteen vaan tietojärjestelmä toimii normaalisti tiedon siirtämisvälineenä ja julkaisuvälineenä. Internet on laajalle levinnyt ja tehokas verkkoviestinnän mahdollistava tietojärjestelmä, jolla voidaan hyvin nopeasti saattaa materiaalia suuren ihmisjoukon tietoisuuteen. Tällä on merkitystä mm. arvosteltaessa Internetissä tehdyn sisältörikoksen törkeysastetta.

Suomen rikoslaista löytyy yllättävän paljonkin rikoksia, jotka voivat täyttyä julkisuuteen saattamalla. Lisäksi joissakin tapauksissa on mahdollista, että rikoksen osallisuusmuodot eli yllytys, avunanto ja rikoskumppanuus voivat toteutua verkkoviestinnän välityksellä. Keskeisimmät rikoslaissa rangaistaviksi säädetyt rikokset, jotka perustuvat tai voivat perustua julkaistuun sisältöön, ovat nykyisin:

- kiihottaminen kansanryhmää vastaan (RL 11:8)
- sotaan yllyttäminen (RL 12:2)
- vakoilu (RL12:5)
- törkeä vakoilu (RL 12:6)
- turvallisuussalaisuuden paljastaminen (RL 12:7)
- tuottamuksellinen turvallisuussalaisuuden paljastaminen (RL 12:8)
- julkinen kehottaminen rikokseen (RL 17:1)
- uskonrauhan rikkominen (RL 17:10)
- väkivaltakuvauksen levittäminen (RL 17:17)
- sukupuolisiveellisyyttä loukkaavan kuvan levittäminen (RL 17:18)
- sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan hallussapito (RL17:19)
- sukupuolisiveellisyyttä loukkaava markkinointi (RL 17:20)
- sukupuolisiveellisyyden julkinen loukkaaminen (RL 17:21)
- yksityiselämää loukkaava tiedon levittäminen (RL 24:8)
- kunnianloukkaus (RL 24:9)
- törkeä kunnianloukkaus (RL 24:10)
- markkinointirikos (RL 30:1)
- kilpailumenettelyrikos (RL 30:2)
- yrityssalaisuuden rikkominen (RL 30:5)
- vaaran aiheuttaminen tietojenkäsittelylle (RL 34:9a)
- salassapitorikos (RL 38:1)
- salassapitorikkomus (RL 38:2)
- henkilörekisteririkos (RL 38:9)
- virkasalaisuuden rikkominen ja tuottamuksellinen virkasalaisuuden rikkominen (RL 40:5)
- tekijänoikeusrikos (RL 49:1)
- kurssin vääristäminen (RL 51:3)
- törkeä kurssin vääristäminen (RL 51:4)
- arvopaperimarkkinoita koskeva tiedottamisrikos (RL 51:5).[9]

Oleellista on havaita, että nämä rangaistussäännökset on rakennettu suojaamaan niitä arvoja, oikeuksia ja etuuksia, joita yhteiskunnassamme pidetään tärkeinä ja suojeltavina

[9] Hallituksen esitys 54/2002 vp. s. 68

kohteina. Näissä rikoksissa julkisuuteen saattaminen on yksi teon täyttymisen mahdollistava elementti, joten rikokset voidaan tehdä myös Internetin välityksellä.

Myyrmäen tapauksen esille nostattamana on pohdittu sitä, täyttääkö Internetin keskustelupalstoilla käyty keskustelu erilaisista räjähteiden valmistamiseen liittyvistä ohjeista mahdollisesti RL 17 luvun 1 §:n mukaisen julkisen kehottamisen rikokseen tunnusmerkistön tai vastaavasti avunannon tai yllytyksen RL 34 luvun 1 §:n tarkoittamaan tuhotyöhön. Tätä pohdintaa on tehty ja tehdään puhtaasti rikosoikeuden yleisten oppien perusteella ja tässäkin Internet on taustalla oleva välityskanava, yleinen keskustelun mahdollistava ympäristö.

3.4 Tietoverkkorikollisuutta koskeva uusin kansainvälinen kehitys

3.4.1 Euroopan neuvoston tietoverkkorikollisuutta koskeva kansainvälinen yleissopimus

Euroopan neuvosto on vuonna 1949 perustettu hallitustenvälinen järjestö, jossa on 41 jäsenmaata. Suomi liittyi järjestön jäseneksi vuonna 1989. Euroopan neuvosto pyrkii edistämään jäsenmaidensa yhtenäisyyttä, suojelemaan ihmisoikeuksia ja moniarvoista demokratiaa, parantamaan elinolosuhteita sekä edistämään inhimillisiä arvoja.

Helmikuussa 1997 Euroopan neuvosto ryhtyi valmistelemaan tietoverkkorikollisuutta koskevaa kansainvälistä yleissopimusta (ETS nro 185), jonka valmistuttua Euroopan neuvosto hyväksyi sen marraskuussa 2001 ja avasi allekirjoituksille. Suomi on allekirjoittanut sopimuksen 23. marraskuuta 2001.

Sopimus on kansainvälinen yleissopimus, joka koskee tietoverkkojen välityksellä tehtyjä rikoksia. Se sisältää säännöksiä tietotekniikkaan kohdistuvista rikoksista kuten tietomurrosta, viestintäsalaisuuden loukkaamisesta, datan vahingoittamisesta, tietojärjestelmän häirinnästä ja laitteiden ja ohjelmien väärinkäytöstä. Tietotekniikkaa hyväksikäyttäen tehtyjen rikosten osalta sopimuksessa on säännöksiä väärennöksestä, petoksesta, lapsipornografiasta ja tekijän- sekä teollisoikeuksien loukkauksesta. Sopimuksessa käsitellään avunantoa, yllytystä, yritystä sekä yhteisövastuuta liittyen tietoverkkorikollisuuteen. Sopimuksessa on säännöksiä rikosten johdosta tapahtuvasta luovuttamisesta ja pakkokeinojen käyttöä koskevasta kansainvälisestä oikeusavusta. Pakkokeinojen osalta sopimuksessa on lisäksi erityiset säännökset dataan kohdistuvista pakkokeinoista.

Euroopan neuvostossa on valmistunut tähän yleissopimukseen liittyvä lisäpöytäkirja[10], joka laajentaa sopimuksen aineellisoikeudelliset, proseduaaliset ja kansainväliseen yhteistyöhön liittyvät säännökset koskemaan myös rasistisen ja muukalaisvastaisen tiedon levittämistä.

Oikeusministeriö on asettanut 4.12.2002 työryhmän valmistelemaan yleissopimuksen voimaansaattamiseksi tarvittavaa lainsäädäntöä ja samalla selvittämään mahdollisia muita rikos- ja rikosprosessilainsäädännön muutostarpeita. Työryhmän tulee 1.6.2003

[10] Additional protocol to the convention on cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 7 marraskuuta 2002, PC-RX (2002) 24, viitattu 2.1.2003. Saatavilla WWW-muodossa:<URL: http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/ Cybercrime/Racism_on_internet/PC-RX(2002)24E.pdf>.

mennessä arvioida sopimuksen edellyttämät ja muut lainmuutostarpeet sekä valmistella ehdotus yleissopimuksen voimaansaattamiseksi tarvittavasta lainsäädännöstä ja mahdollisista muista lakimuutoksista.

3.4.2 Euroopan yhteisöjen komission ehdotus neuvoston puitepäätökseksi tietojärjestelmiin kohdistuvista hyökkäyksistä[11]

Euroopan unionissa aiotaan tehostaa tietojärjestelmiin kohdistuvien hyökkäysten torjuntaa lähentämällä jäsenvaltioiden rikostunnusmerkistöjä ja rangaistussäännöksiä, jotka koskevat luvatonta tunkeutumista tietojärjestelmään sekä tietojärjestelmien toiminnan häiritsemistä ja datan vahingoittamista. Tässä ehdotuksessa ei varsinaisesti ole määräyksiä tietoverkoissa ilmenevän laittoman materiaalin osalta.

Euroopan unionin neuvostossa ehdotusta käsitellään tällä hetkellä työryhmässä ja ehdotuksen valmisteluvaiheessa otetaan huomioon Euroopan neuvoston tietoverkkorikollisuutta koskeva sopimus.

Valtioneuvosto antoi asian 14.8.2002 tiedoksi eduskunnalle.

3.4.3 Euroopan yhteisöjen komission ehdotus neuvoston puitepäätökseksi lasten seksuaalisen hyväksikäytön ja lapsipornografian torjumiseksi[12]

Euroopan unionissa on valmisteilla puitepäätös, jonka tarkoituksena on löytää keinoja torjua mm. Internetissä esiintyvää lapsipornografiaa, jotta Euroopan unioni voi osoittaa soveltavansa yhteistä rikoslainsäädäntöä ja jotta Internetiä voitaisiin käyttää turvallisessa ja rikoksilta suojatussa ympäristössä. Asian käsittely Euroopan unionin neuvostossa on kesken. Valtioneuvosto on antanut asian 10.5.2001 tiedoksi eduskunnalle.

Puitepäätösehdotuksen johdosta oikeusministeriössä on asetettu 28.11.2002 työryhmä valmistelemaan ihmiskauppaa ja paritusta koskevia säännöksiä.[13] Työryhmän on vuoden 2003 loppuun mennessä valmisteltava myös laittoman maahantulon järjestämistä ja lapsipornografiaa koskevat rikoslain muutokset.

3.4.4 YK:n yleissopimus lasten oikeuksista

Suomi on ratifioinut 20.6.2001 YK:n yleissopimuksen lasten oikeuksista. Sopimus tuli voimaan kansallisesti 20.7.2001. Tähän sopimukseen liittyen on tehty vuonna 2000 valinnainen pöytäkirja lasten myynnistä, lapsiprostituutiosta ja lapsipornografiasta, jonka Suomi allekirjoitti 7.9.2000. Tätä pöytäkirjaa ei vielä ole saatettu voimaan kansallisesti.

Valinnaisen pöytäkirjan perusteluosassa todetaan se huolestuneisuus, että lapsipornografiaa on yhä enemmän saatavilla Internetin ja muun kehittyvän teknologian välityksellä. Pöytäkirjaan onkin otettu sopimusmääräys, jossa velvoitetaan jäsenvaltiot kieltä-

---

[11] Bryssel 19.04.2002, KOM(2002)173 lopullinen, 2002/0086 (CNS), viitattu 2.1.2003. Saatavilla WWW-muodossa:<URL: http://europa.eu.int/eur-lex/fi/com/pdf/2002/com2002_0173fi01.pdf>.

[12] Bryssel 21.12.2000,KOM(2000) 854 lopullinen, 2001/0024 (CNS), 2001/0025 (CNS), viitattu 2.1.2003. Saatavilla WWW-muodossa:<URL:http://europa.eu.int/eur-lex/fi/com/pdf/2000/ fi_500PC0854_01.pdf>.

[13] Viitattu 2.1.2003. Saatavilla WWW-muodossa:<URL :http://www.om.fi/16520.htm>.

mään mm. lapsipornografian tuottaminen, jakelu, levittäminen, tuonti, vienti, tarjoaminen, myyminen tai hallussapito yllä mainittua tarkoitusta varten.

Tämän valinnaisen pöytäkirjan vaatimukset otetaan huomioon edellä mainitun ihmiskauppaa ja paritusta koskevan työryhmän työssä.

4 Viestinnän sääntelymenetelmiä

Viestinnän sääntelyn keinoja valittaessa saavutetun hyödyn tulisi olla suhteessa aiheutettuun haittaan ja kuluihin. Yhteiskunnan ei tarvitse sietää laittoman aineiston vapaata jakamista, mutta sääntelyn keinot tulisi valita siten, että niiden aiheuttama haitta lailliselle viestinnälle on mahdollisimman vähäinen.

Mikäli suomalaisten verkkokeskustelujärjestelmien käyttö hankaloituu tai hidastuu kohtuuttomasti, haitta kohdistuu ensisijaisesti lailliseen keskusteluun. Sen sijaan laittoman rajamailla oleva materiaali siirtyy suljetumpiin vertaisverkkoihin ja ulkomaisiin palveluihin pois suomalaisviranomaisten ja keskusteluryhmien sosiaalisen kontrollin ulottuvilta.

Mikäli taas järjestelmien ylläpitokustannukset ylittävät lisäarvopalvelun tarjoamisesta saatavan hyödyn, operaattorit lakkaavat tarjoamasta julkisia keskustelupalveluita. Jälleen haitta kohdistuu eniten lailliseen keskusteluun, jota suurin osa keskustelusta on.

4.1 Ennakkoseulonta

Ennakkoseulonnassa palveluntarjoaja käy julkaistavaksi tarkoitettuja viestejä ennakolta läpi pyrkien estämään laittoman tai järjestelmän toimintaa haittaavan aineiston pääsyn keskustelujärjestelmiin.

4.1.1 Automaattinen ennakkoseulonta

Automaattisessa ennakkoseulonnassa liikennevirran suodatus toteutetaan ohjelmallisesti ennalta määrättyjen kriteerien perusteella. Suodatusperuste voi olla esimerkiksi viestien otsikkotietoihin (lähettäjä, aihe), sisältöön ("MAKE MONEY $$$$", haittaohjelman sormenjälki) tai välitystekniikkaan liittyvä seikka.

Automaattista ennakkoseulontaa voi käyttää millaisen tahansa verkkoliikenteen sääntelyyn, joskin viestien salaus estää sisältösuodatuksen käytön.

Sisältösuotimia käytettäessä verkkoliikenne ohjataan suotimiin, jotka keräävät kaiken liikennevirran, kokoavat verkkopaketit, ja vertaavat sisältöä suotimen sääntöihin. Sääntöihin osuvat viestit tai yhteydet estetään, mutta muut päästetään läpi.

Välitysteknisiin ehtoihin perustuvat suotimet käsittelevät puolestaan vain verkkoliikenteen otsikkokenttiä tai liikennöintitavan ohjaustietoa, joten ne ovat oleellisesti tehokkaampia. Viestien sisältöä ei tarvitse koota eikä verrata.

Etuja:

Seulonnalla voidaan estää seulontakriteereitä vastaava suotimen kautta kulkeva liikenne.

Ongelmia:

- Suotimet voidaan usein kiertää

  Jos palveluntarjoaja estää suotimella sanan "pommi" sisältävien viestien talletuksen, keskustelijan käyttävät sanaa "paukku".

  Teknisesti taitavat käyttäjät voivat myös etsiä keinon kuljettaa viesti suotimen ohi.

- Sisältösuotimet sekä vuotavat laittomia että karsivat laillisia viestejä

  Sisältösuotimet seulovat viestejä täsmälleen seulontakriteerien mukaisesti. Niinpä pääsyn estäminen sanan "uusnatsi" sisältäville WWW-sivustoille ei estä pääsyä "uus natsien WWW sivuille", mutta saattaa estää pääsyn ilmiötä käsittelevien tiedotusvälineiden ja tutkimuslaitosten WWW-palveluihin.

- Suotimet vaativat jatkuvaa ylläpitoa

  Erityisesti sisältöseulonta edellyttää virheellisiä osumia tuottavien suodatussääntöjen poistamista sekä jatkuvaa uusien sääntöjen lisäämistä.

- Sisältösuotimet vaativat prosessointitehoa

  Suuret lailliset viestit joudutaan käymään läpi kokonaan ja vertaamaan kaikkiin suotimessa oleviin suodatusehtoihin, joten ne eivät skaalaudu suuriin ympäristöihin.

- Suotimien tarjoamisen oltava oikeutettua

  Suotimia tarjottaessa on määriteltävä sopimuksin kenellä on oikeus määritellä suodatettavat kohteet.

Suotimet eivät kuitenkaan ole kategorisesti hyviä tai huonoja, vaan niiden käyttökelpoisuus riippuu käyttökohteesta.

Mahdollisia käyttökohteita:

Virustorjuntaohjelmisto on esimerkki hyödyllisestä ennakkoseulonnasta, joka ei puutu ihmisten väliseen kommunikaatioon, mutta pysäyttää tunnistamiensa haittaohjelmien kulun.

Automaattinen ennakkoseulonta on käyttökelpoinen apuväline myös sähköpostilistoilla, joissa sitä voidaan käyttää roskapostin esiseulontaan pois listalta. Tällöin listan ylläpitäjän on kuitenkin käytävä ajoittain suodatettu materiaali läpi, jos halutaan, että suodatin ei poista vahingossa myös joitakin listalle kuuluvia viestejä.

Suotimia voidaan käyttää WWW-liikenteen suodattamiseen pienissä ympäristöissä kuten lapsiperheissä tai kouluissa, joissa myöskään sopimukset eivät muodostu ongelmaksi.

Verkkoteknisillä suotimilla voidaan estää tietoturvapolitiikan mukaisesti jokin tietty liikennöintikäytäntö organisaation hallitsemassa verkossa tai estää yhteydet oman organisaation ja nimetyn kohteen välillä.

4.1.2 Manuaalinen

Manuaalinen ennakkoseulonta tarkoittaa toimitustyötä, jossa palvelua ylläpitävät henkilöt käyvät jokaisen viestin läpi ennen tallentamista keskustelujärjestelmään.

Etuja:

Ennakkoseulonnalla voidaan melko tarkkaan varmistua siitä, ettei järjestelmään tule talletetuksi järjestelmän toimintaa haittaavia tai laittomia viestejä.

Ongelmia:

Ennakkoseulonta

- Muuttaa keskustelujärjestelmien luonteen.

  Reaaliaikaiset keskustelujärjestelmät eivät ole mahdollisia ennakkoseulottuina.

- Vaatii ihmistyövoimaa, eli on kallista.

  Ennakkoseulonta ei olisi teknistaloudellisesti mahdollista suuren volyymin järjestelmissä.

  Esimerkiksi Teknillisen korkeakoulun tietojenkäsittelyopin laboratorion News- palvelimen sisään tulevien artikkeleiden lukumäärä ajanjaksolla 3.12.2002 - 11.12.2002 oli keskimäärin 860 905 artikkelia vuorokaudessa eli liki 600 artikkelia minuutissa.

- Todennäköisesti ajaisi laillisuuden rajamailla olevan keskustelun suljettuihin ryhmiin, joissa liikkuva tieto saattaa olla yksipuolisempaa kuin julkisissa ryhmissä.

Mahdollisia käyttökohteita:

Ennakkoseulonta on paikallaan sähköisissä julkaisuissa, joissa julkaisija vastaa arvovallallaan julkaisun toimitetun sisällön oikeellisuudesta sekä mielipidepalstan lainmukaisesta käytöstä.

4.2 Tekniset mahdollisuudet puuttua haittaavaan tai laittomaan aineistoon

Toimintamallissa järjestelmän toimintaa uhkaavat haittaohjelmat tai laittomat viestit poistetaan näkyviltä sen jälkeen kun palvelun ylläpitäjä saa niistä tiedon.

Poisto voidaan toteuttaa teknisestä alustasta riippuen joko poistamalla muilta kuin viestin omistajalta lukuoikeus viestiin tai poistamalla fyysisesti viesti.

Etuja:

Laittoman tai haittaavan tiedon poistaminen havaittaessa on toteutettavissa kohtuullisella vaivalla, eikä poistosta aiheudu haittaa muulle viestinnälle.

Ongelmia:

Viestien poisto jälkikäteen on teknisesti mahdollista vain keskitetyissä järjestelmissä, joita palvelun tarjoaja hallinnoi.

Oikeus poistaa laittomia ja haittaavia viestejä tulee määritellä ennalta käyttösopimuksessa.

Mahdollisia käyttökohteita:

Operaattori voi poistaa käyttösopimuksen nojalla näkyviltä palvelimellaan sijaitsevan laittoman WWW-sivun.

Verkkoyhteisön toimivasta itsesääntelystä hyvä esimerkki on News-järjestelmän SPAM-torjunta, jota ilman News-järjestelmä ei olisi enää toimintakykyinen. News-yhteisö on sopinut keskenään säännöt joiden puitteissa SPAM-torjunta tapahtuu[14], ja peruste on tekninen, ei viestin tekstisisältö.

4.3 Tekniset suojautumismahdollisuudet

Vaikka tietosisällöstä vastaa tiedon haltija, järjestelmän ylläpitäjä vastaa resurssiensa käytöstä.

Käytännön poliisityössä havaitaan jatkuvasti, että suuria tietomassoja levittävät tietosisältörikolliset pyrkivät hankkimaan käyttöönsä levytilaa tunkeutumalla oikeudettomasti puutteellisesti suojattuun järjestelmään ja ottamaan levy- ja linjakapasiteetin käyttöön omaan laittoman aineiston välitystoimintaan. Laittoman aineiston levittäminen vaikeutuisi oleellisesti, jos järjestelmät ylläpidettäisiin hyvän ylläpitotavan mukaisesti.

Yksityisten verkkojen haltijat (yritykset, virastot) voivat myös suojautua estämällä nimettyjen liikennöintikäytäntöjen käytön sisäverkon ja ulkoverkon välillä.

[14] <URL: http://www.faqs.org/faqs/usenet/spam-faq/>

4.4 Viestinnän oikeudellinen sääntely

4.4.1 Painovapauslaki ja radiovastuulaki sekä sananvapauslain uudistusehdotus

Suomessa painettua kirjallisuutta säädellään painovapauslailla (SK:1/1919) ja yleisradiotoimintaa radiovastuulailla (SK:219/1971), jotka ovat tällä hetkellä muutoksen alla. Nämä lait eivät sinänsä koske tietoverkoissa tapahtuvaa viestintää. Hallituksen esitys[15] sananvapauden käyttämisestä joukkoviestinnässä on eduskunnassa ja tarkoituksena on, että lailla korvattaisiin painovapauslaki ja radiovastuulaki. Ehdotetulla lailla annettaisiin perustuslain sananvapaussäännöksessä edellytettyjä tarkempia säännöksiä sananvapauden käyttämisestä joukkoviestinnässä mukaan lukien sähköinen viestintä. Lain yksi tarkoitus on myös estää sisällöltään selvästi lainvastaisen materiaalin levittäminen.

Laki toisi verkkojulkaisun määritelmän ja säätäisi velvollisuuden määrätä vastaava toimittaja sekä velvollisuuden tallentaa verkkoviestejä ja niitä koskevia tunnistamistietoja. Lisäksi käyttöön otettaisiin uusi pakkokeino, verkkoviestin jakelun keskeyttämismääräys. Säädöksen perusteella tuomioistuin voisi määrätä julkaisijan tai ohjelmatoiminnan harjoittajan yms. keskeyttämään julkaistun verkkoviestin pitämisen yleisön saatavilla, jos sisällön pitäminen saatavilla on ilmeisen laitonta. Määräys raukeaisi, ellei viranomainen tai loukattu tee tiettyjä oikeudellisia toimia kolmen kuukauden kuluessa.

Joissakin tapauksissa myös lähettimen, palvelimen tai muun vastaavan laitteen ylläpitäjällä itsellään olisi oikeus keskeyttää verkkoviestin pitäminen yleisön saatavilla.

Koska lakiehdotuksen käsittely eduskunnassa on tällä hetkellä kesken, ei työryhmä lähde tässä raportissa pohtimaan ehdotuksen vaikutuksia.

4.4.2 Laki tietoyhteiskunnan palvelujen tarjoamisesta

Heinäkuun alusta 2002 tuli Suomessa voimaan laki tietoyhteiskunnan palvelujen tarjoamisesta (SK:458/2002). Laki perustuu direktiiviin sähköisestä kaupankäynnistä.[16] Perustavoitteena on edistää sähköistä kaupankäyntiä Euroopan talousalueella varmistamalla ensinnäkin tietoyhteiskunnan palvelujen vapaa tarjonta. Yksi lain lähtökohdista on, että välittäjänä toimiva operaattori, esimerkiksi teleoperaattori, ei olisi vastuussa siirtämiensä tai tallentamiensa tietojen lainvastaisesta sisällöstä tai oikeudettomasta välittämisestä. Vastuuvapauden perusedellytys olisi se, että välittäjän toiminta on luonteeltaan teknistä eikä hän itse osallistu lainvastaisen sisällön tuottamiseen. Tallennuspalvelun tarjoajan on vastuuvapaus saadakseen poistettava palvelimeltaan lain tarkoittama lainvastainen sisältö.[17] Sisältö on poistettava, jos palvelun tarjoaja saa tietoonsa sitä koskevan tuomioistuimen määräyksen taikka, jos kysymyksessä on tekijänoikeuden tai lähioikeuden loukkaaminen, saatuaan tekijänoikeuden tai lähioikeuden haltijan tai hänen edustajansa yksilöidyn vaatimuksen. Lisäksi sisältö on poistettava, jos palvelun tarjoaja on saanut tosiasiallisesti tietoonsa, että tallennettu tieto on ilmeisesti rikoslaissa

---

[15] Hallituksen esitys 54/2002 vp.

[16] Euroopan parlamentin ja neuvoston direktiivi 2000/31/EY (300L0031); EYVL N:o L 178, 17.7.2000, s. 1., viitattu 3.1.2002. Saatavissa WWW-muodossa:<URL: http://europa.eu.int/ servlet/portail/RenderServlet?search=RefPub&lg=fi&nb_docs=25&domain=&in_force=NO&year=2000&month=7&day=17&coll=JOL&nu_jo=178&page=1 >.

[17] Hallituksen esitys 194/2001 vp., s.1.

tarkoitettu kiihottaminen kansanryhmää vastaan tai sukupuolisiveellisyyttä loukkaavan kuvan levittäminen.

4.4.3 Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta

Televiestinnän yksityisyyden suojaa ja yleisen teletoiminnan tietoturvaa käsittelevä laki (SK: 565/1999) on erityislaki, joka pohjautuu Euroopan parlamentin ja neuvoston direktiiviin 97/66/EY henkilötietojen käsittelystä ja yksityisyyden suojasta televiestinnän alalla (15.12.1997).[18] Laissa on määräyksiä mm. viestinnän luottamuksellisuudesta, teleyritysten palveluksessa olevien vaitiolovelvollisuudesta ja viestintään liittyvien tunnistamistietojen käsittelystä. Laki on muuttumassa ja uusi sähköisen viestinnän tietosuojalakia koskeva hallituksen esitysluonnos on valmistunut liikenne- ja viestintäministeriöstä. Luonnos on saatavilla osoitteesta www.mintc.fi kohdasta Viestintätietoa.

5 Sisältörikosten selvittämisen keinot

5.1 Varautuminen

Ennakkovarautumisella luodaan edellytykset sille, että mahdollinen rikos on selvitettävissä jälkikäteen. Reaalielämän rikostutkinnassa voidaan turvautua silminnäkijähavaintoihin rikollisen liikkeistä. Verkossa tämä on mahdollista vain harvoissa erityistapauksissa, joten verkosta tarvitaan talteen reaalielämää enemmän teknistä kulkutietoa. Jotta verkkojäljistä olisi varautumismielessä hyötyä, ne tulisi myös kerätä tapahtumahetkellä. Tallennuskameran kytkeminen päälle rikoksen tapahduttua ei auta jo tapahtuneen rikoksen selvittämistä.

Kaikkien suomalaisten palveluntarjoajien kunnollinen varautuminen ei kansainvälisessä verkkoympäristössä toki takaa aukottomia mahdollisuuksia rikosten selvittämiselle, mutta varautumatta jättäminen on voimakas signaali yhteiskunnalta, ettei sähköinen kanssakäyminen nauti yhteiskunnan suojaa.

Varautuminen on kuitenkin toteutettava siten, ettei käyttäjien yksityisyyden suoja vaarannu, eikä varautumisesta aiheutuvat kustannukset ole kohtuuttomia suhteessa saavutettavaan hyötyyn. Varautumista on myös voitava soveltaa huomioiden eri järjestelmien tekniset rajoitteet.

5.2 Viestinnän talletus

Viestinnän talletus tarkoittaa tilannetta, jossa verkkokeskustelupalvelun ylläpitäjä tallentaa ylläpitämästään järjestelmästä kaiken julkisen viestinnän sellaisenaan ennalta määritellyksi määräajaksi.

Etuja:

---

[18] Direktiivi on kumottu 12.7.2002 direktiivillä 2002/58 EY henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän direktiivi). Tämä direktiivi tuli voimaan 31.7.2002. Viitattu 13.1.2003. Saatavilla WWW-muodossa:<URL: http://www.europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=FI&numdoc=32002L0058&model=guichett>

Viestinnän talletus on keino säilyttää näyttö viestin sisällöstä. Osassa järjestelmistä näin säilyy myös tieto vietin lähetysosoitteesta.

Ongelmia:

Keskitetysti hallituissa artikkeleita tallentavissa keskustelujärjestelmissä vanhempiakin artikkeleita usein säilytetään luettavissa pitkään. Sen sijaan suuren volyymin hajautetuille järjestelmille viestiliikenteen kuukausien pituinen tallennusvaatimus ei ole kohtuullinen .

Esimerkiksi TKK:n tietojenkäsittelyopin laboratorion News-palvelimella on 3.12.2002 - 11.12.2002 ollut artikkeleita keskimäärin 46,5 gigatavua lyhyehköillä säilytysajoilla. Kolmen kuukauden säilytysvaatimus saattaisi johtaa taloudellisesti ja jopa teknisesti mahdottomaan tilanteeseen.

Hajautetuissa järjestelmissä samat artikkelit olisivat myös tallessa jokaisessa suomalaisessa palvelussa sen lisäksi, että niitä arkistoidaan kansainvälisesti. Hyöty ei olisi suhteessa kustannuksiin.

5.3 Tapahtumien kirjaus lokiin

Lokitietojen tarkoituksena on mahdollistaa ongelmatilanteiden selvittäminen jälkikäteen. Lokeihin kirjataan vähintään verkkoyhteyden osapuolet ja tapahtuman aikaleima, mutta usein myös teknisten ongelmien selvittämistä helpottavaa tietoa. Vaikka lokien ensisijainen käyttökohde on teknisten häiriöiden selvittäminen, ne ovat korvaamaton apu myös verkossa tapahtuvan laittoman toiminnan jäljittämisessä.

Etuja:

Lokitietojen tallennus vaatii varsin paljon vähemmän tilaa kuin kokonaisten viestien tallennus, ja silti lokitiedot sisältävät enemmän tarpeellista informaatiota.

Esimerkinomainen suuruusluokka-arvio tarvittavasta tallennuskapasiteetista:

News-järjestelmä tallettaa käyttäjälokiin paljon tietoa käyttäjien luku- ja kirjoitusyhteyksistä, ryhmiin liittymisistä ja yhteyden päättymisestä, joista voitaisiin valita jälkikäteen arkistoitavaksi vain artikkeleiden kirjoitusta kuvaavat rivit.

Kun yksi rivillinen tietoa on noin 100 tavua, TKK:n eräälle News-palvelimelle viikossa kirjoitetuista 1500 viestistä syntyisi kirjoitustietoa noin 150 kilotavua viikossa. Sen sijaan kokonaisten News-artikkeleiden tallentamisvelvoitteesta syntyisi tallennettavaa materiaalia suuruusluokkaa 7 * 1 000 000 kilotavua viikossa.

Ongelmia:

Lokeja voidaan kerätä hyvin monenlaisista verkkotapahtumista, joista jotkut tuottavat paljon lokia, mutta vain vähän hyötyä väärinkäytösten selvittämiseen. Niinpä säilytysvelvollisuuden määrittely on tehtävä huolella, jos lailla edellytetään palvelu- ja teleoperaattoreilta lokitietojen säilytystä.

Lokitiedot dokumentoivat käyttäjien liikkeitä verkossa. Lokitiedot on ehdottomasti säilytettävä hyvän tietohallintotavan mukaisesti, jotta kansalaisille voidaan taata laillisessa verkkokäytössä anonymiteetti.

Käyttötarkoituksia:

Väärinkäytösten selvittämiseksi tarvitaan lokitietoja kahdesta eri kohteesta:

1. Viestintätapahtumien kirjaus lokiin viestintäpalvelun tarjoajalla.

Viestintätapahtumien kirjauksessa keskustelupalvelun ylläpitäjä kirjaa lokiin palvelimen kautta tehdyt viestintätapahtumat silloin, kun se on teknisesti mahdollista.

Oleellisimmat lokiin kirjattavat viestintätapahtumatiedot ovat viestintätapahtuman aika, verkko-osoite, josta lähetys on tullut, viestin yksilöllinen tunniste sekä lähettäjäksi merkitty tunniste (sähköpostiosoite, muu tunnus).

2. Verkkoon kytkeytymis- ja kirjautumistapahtumien kirjaus lokiin sekä viestintäpalvelun tarjoajalla että teleoperaattorilla.

Viestintätapahtumien lokitiedoista selviää mistä osoitteesta ja koska lähetys on tehty. Se ei kuitenkaan vielä riitä viestin lähettäjän henkilöllisyyden selvittämiseksi.

Jotta laittomuudesta epäillyn lähettäjän henkilöllisyys olisi selvitettävissä, myös verkkopalvelun tarjoajien kuten operaattorien tulisi ylläpitää kirjautumislokia, jonka perusteella olisi selvitettävissä kellä asiakkaalla on ollut nimetty verkko-osoite hallussaan nimettyyn aikaan.

5.4 Nykyiset oikeudelliset mahdollisuudet

Perusproblematiikka laittomaan sisältöön liittyvien rikosten selvittämisessä on poliisin tiedonsaantikeinojen ulottuvuus erilaisiin loki- ja asiakastietoihin. Kuten edellä on kerrottu, tekojen tapahtumisympäristöstä ei ole saatavissa kovinkaan paljoa sellaisia havaintoja tai jälkiä, jotka reaalimaailman rikoksissa ovat tavanomaisia. Tekojen selvittäminen nojaa täten vahvasti verkkoon jääneisiin jälkiin eli käytännössä lokitietoihin.

Rikostutkinnassa käytettävistä keinoista säädetään pakkokeinolaissa (450/1987) ja poliisilaissa (493/1995). Tämän lisäksi laissa yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999) annetaan muutamien rikosten osalta poliisille oikeus saada viestintään liittyviä tunnistamistietoja. Näitä rikoksia ovat muun muassa lähestymiskiellon rikkominen ja kotirauhan häirintä. Ko. laissa on määritelty salassapidettäviksi tunnistamistiedoiksi kaikki teleyhteyden toteuttamisen yhteydessä syntyneet tiedot.

Pakkokeinolain 5a luvun 1 §:n määritelmän mukaan televalvonnalla tarkoitetaan salassapidettävien tunnistamistietojen hankkimista televiesteistä, jotka on lähetetty yleisen tai muun teletoimintalain (183/87) soveltamisalaan kuuluvan televerkkoon kytketystä teleliittymästä tai vastaanotettu tällaiseen teleliittymään, sekä tällaisen teleliittymän tilapäistä sulkemista. Alun perin säännöksen tarkoituksena oli sallia viranomaisille mahdolli-

suus saada rikostutkinnan tarpeisiin tietoja siitä, mihin ja milloin jostakin tietystä puhelimesta on soitettu ja kuka ja koska on soittanut ko. puhelimeen. Telekuunteluvaltuuksia säädettäessä katsottiin, että nämä tiedot kuuluvat perustuslain puhelinsalaisuutta[19] suojaavaan vapauspiiriin, joten niistä tuli säätää lailla.

Televalvontasäännökset on tarkoitettu vakavien rikosten selvittämiseen. Suurin osa tietoverkoissa ilmenevistä sisältörikoksista on sellaisia, ettei niiden tutkinnassa voida käyttää televalvontaa. Ainoastaan laiton uhkaus (RL 25:7) ja oikeudenkäytössä kuultavan uhkaaminen (RL 15:9), jotka voidaan joissakin tapauksissa ajatella toteutettavaksi tietoverkkojen välityksellä, ovat rikoksia, joiden osalta on tehty televalvontasäännöksiin poikkeus.

Poliisin tiedonhankintaa koskevat yleiset säännökset löytyvät poliisilain 3 luvusta. Ko. lain 36 §:ssä on säädetty poliisin oikeudesta saada teletoimintaa harjoittavalta yhteisöltä yhteystiedot sellaisesta teleliittymästä, jota ei mainita julkisessa luettelossa, jos tietoja yksittäistapauksessa tarvitaan poliisille kuuluvan tehtävän suorittamiseksi. Poliisilla on vastaava oikeus saada postitoimintaa harjoittavalta yhteisöltä jakeluosoitetietoja. Säännöksen tarkoituksena oli alun perin turvata poliisille oikeus saada tietoja salaisista puhelinnumeroista.

Nykyisten säännösten sopimattomuus tietoverkoissa tapahtuneiden rikosten tutkintaa ilmenee erilaisina käsityksinä lakien sovellettavuudesta. Selkeiden säännösten puuttuessa tilanne on tällä hetkellä sellainen, että pääosassa sisältörikoksista poliisilla ei ole tiedonsaantioikeutta niistä verkkojäljistä eli teletoiminnan tietosuojalaissa määritellyistä tunnistamistiedoista, jotka mahdollistaisivat rikoksen tekijän käyttämän telepäätelaitteen ja sen asennusosoitteen selvittämisen. Nyt eduskunnan käsiteltävänä oleva sananvapauslain uudistus sekä Euroopan neuvoston tietoverkkorikollisuutta koskevan sopimuksen voimaanpano ratkaissevat problematiikan lähitulevaisuudessa.

6 Muut vaikutuskeinot

6.1 Koulutus ja valistus

Euroopan unionissa on hyväksytty Internetin käyttöturvallisuuden parantamista koskeva toimintasuunnitelma, jonka yhteydessä rahoitetaan toimia Internetin laittoman ja haitallisen sisällön torjumiseksi. Toimintasuunnitelman voimassaolo päättyi 31. joulukuuta 2002, mutta komissio on ehdottanut jatkettavaksi sitä kahdella vuodella.[20] Tämä suunnitelma on merkittävä osa komission toimista tällä alalla. Toimintasuunnitelman lähestymistapa on välittää tietoa laittomasta ja haitallisesta sisällöstä ja tarjota välineitä sen torjumiseksi periaatteella, että käyttäjälle annetaan mahdollisuus ottaa vastaan vain haluamansa sisältö.[21] Toimintasuunnitelman tarkoituksena on tukea erilaisia lainsäädännön ulkopuolisia toimenpiteitä. Sen kolme päätoimilinjaa ovat:

---

[19] Nykyisin asiasta säädetään perustuslain 10 §:n yksityiselämän suojaa koskevassa pykälässä, jonka 2 momentin mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.

[20] Internetin käyttöturvallisuuden parantamista maailmanlaajuisten verkkojen laitonta ja haitallista sisältöä torjumalla koskevan yhteisön monivuotisen toimintasuunnitelman jatkaminen, Bryssel 22.03.2002, KOM(2002) 152 lopullinen, 2002/0071 (COD), viitattu 2.1.2003. Saatavilla WWW-muodossa:<URL: http://europa.eu.int/information_society/programmes/iap/docs/pdf/programmes/followup/follow-up%20decision_acte_fi_%20fin.pdf>.

[21] Ibid. s. 3.

- turvallisemman käyttöympäristön luominen (Euroopan vihjelinjaverkoston perustaminen sekä itsesääntelyn ja käytännesääntöjen tukeminen),
- suodatin- ja luokitusjärjestelmien kehittäminen,
- tiedotustoimien edistäminen.[22]

Toimintasuunnitelman yksi osa on Turvallisempi Internetin käyttö (Safer Internet Action Plan) –toimintaohjelma. Suomessa tähän toimintaohjelmaan liittyvä näkyvin projekti on tällä hetkellä DotSafe –hanke. Tässä hankkeessa kahdeksan eurooppalaisen maan kouluviranomaiset Euroopan kouluverkoston johdolla kokosivat tukiaineiston kouluille Internetin turvallisesta käytöstä. Tämä aineisto on tarkoitettu opettajien tueksi ohjaamaan oppilaita Internetin vastuulliseen ja turvalliseen käyttöön. Hankkeeseen liittyvä materiaali löytyy Opetushallituksen tuottamassa Edu.fi –palvelusta osoitteesta www.edu.fi/virtuaalikoulu. Monikielinen aineisto on puolestaan osoitteessa www.eun.org. Opetushallitus on lisäksi teettänyt aineistosta kansion, joka lähetetään kaikille Suomen kouluille.

6.2 Itsesääntely

Itsesäänteylyllä tarkoitetaan tilanteita, joissa toimijat luovat oma-aloitteisesti toiminnalleen säännöt ja rajat. Termi on lainsäädännön vastakohta; lainsäädäntöä harjoittaa valtio tai valtioiden yhteisö. Käsitteellisestä sääntelystä on myös erotettava kansainväliset sopimukset, joilla valtio velvoittautuu saattamaan lainsäädäntönsä sopimuksella tarkoitetulle tasolle. Tämän lisäksi on vielä olemassa kansainvälistä mallilainsäädäntöä.[23] Tällaisista itsesääntelymenettelyistä yleisimpiä ovat erilaiset vihjelinjat, käytännesäännöt eli netiketti ja operaattoreiden sopimusmääräykset asiallisesta käyttäytymisestä tietoverkoissa.

Suomessa Pelastakaa Lapset Ry on käynnistänyt Internetissä toimivan vihjelinjan osoitteessa www.pela.fi/nettivihje/nettivihje.htm. Sivuston tarkoituksena on toimia osana kansainvälistä vihjepalveluyhteistyötä lapsipornografian materiaalivirran katkaisemiseksi. Nettivihje on Euroopan alueella toimivien vihjelinjojen Inhope –verkoston jäsen.[24] Myös Keskusrikospoliisilla on oma Internet –rikosvihjelinja osoitteessa vihje.internet@krp.poliisi.fi, johon voi ilmoittaa havaitsemansa Internettiin liittyvän rikoksen.

Suurimmat operaattorit julkaisivat 14.2.2001 Netiketin, jossa on ohjeita hyvään käyttäytymiseen Internetissä. Netiketin lähtökohtana on ohjata käyttäjiä mukavaan ja hyödylliseen Internetin käyttöön ja samalla kertoa toivotuista käyttäytymistavoista. Netiketillä on myös vaikutusta operaattoreiden palvelusopimuksien tulkinnassa, sillä niissä yleensä kielletään Intenetin lain / hyvän tavan vastainen käyttö ja operaattoreilla on tällaisen käyttäytymisen perusteella oikeus purkaa sopimus. Netiketissä olevat käytännesäännöt

---

[22] Ibid, s. 4.
[23] Liikenne- ja viestintäministeriön julkaisu 1/2002 Itsesääntely - haitalliset verkkosisällöt, s.1, kirjoittanut prof. Jukka Kemppinen, viitattu 13.1.2003. Saatavana WWW-muodossa:<URL: http://www.mintc.fi/www/sivut/dokumentit/julkaisu/julkaisusarja/2002/ju050202544fin.htm>
[24] <URL:http://www.inhope.org>

ovat operaattoreiden näkemys hyvän tavan mukaisesta käyttäytymisestä, joten ainakin näiden sääntöjen vastainen menettely on sopimusrikkomus.

7 Työryhmän suositukset

Rikollisuutta ilmiönä on esiintynyt niin kauan kuin on ollut yhteisöjä, joissa on luotu oikein toimimisen sääntöjä. Yhteiskuntien toimet rikollisuuden rajoittamiseksi ovat vaihdelleet aikakausittain riippuen vallinneesta yhteiskuntajärjestelmästä ja yhteisöjen uskomuksista, arvoista ja moraalikäsityksistä. Rikollisuus on hakenut leviämisreittinsä ja vaikutuskanavansa aina sieltä, missä on ollut sille otollinen maaperä. Rikollisuus tietoverkoissa ei muodosta tästä minkäänlaista poikkeusta. Internet on vapaa ja avoin kanava, jossa anonyymi toiminta on mahdollista, verkkoon pääsy on helppoa ja houkuttelevia tilaisuuksia toimia väärin on paljon.

Perinteisesti rikollisuuteen on puututtu preventiivisillä ja repressiivisillä keinoilla. Nämä keinot eivät tietoverkkorikollisuudessa toimi vielä vastaavalla tavalla kuin muussa yhteiskunnassa esiintyvässä rikollisuudessa. Kuten raportissa on kuvattu, toimenpiteitä tietoverkkorikollisuuden ehkäisemiseksi on mietitty jo useilla kansainvälisillä foorumeilla ja tämän rikollisuuden muodon vaikutuksia näkyy jo kansallisessa lainsäädännössämmekin. Työryhmä näkeekin tärkeänä, että tätä työtä jatketaan kansainvälisesti ja kansallisesti. Erityisen tärkeänä työryhmä pitää Euroopan yhteisön ja Euroopan neuvoston piirissä tehtävää työtä kansainvälisen yhteisymmärryksen saavuttamiseksi siitä, mitä säännellään ja millä tavoin ja millaisin keinoin. Kansallisesti tätä kehitystä on seurattava tarkkaa ja oltava aktiivisesti mukana vaikuttamassa tulevaisuuden päätöksiin.

Nyt jo säädetty laki tietoyhteiskunnan palvelujen tarjoamisesta on tuonut keinoja ja velvoitteita puuttua sisällöllisesti rikolliseen materiaaliin Internetissä. Sananvapautta koskeva lakiuudistus tuonee myös mukanaan lisää sääntelyä. Pakkokeinolain uudistaminen antaa poliisille nykyistä enemmän mahdollisuuksia puuttua tietoverkkorikollisuuteen ja Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen määräyksien voimaanpano toivottavasti saattaa suomalaisen lainsäädännön tasolle, jolla mahdollistettaisiin ainakin oikeudelliset keinot selvittää rikollisen materiaalin levittäjä kansallisissa tietojärjestelmissä.

Erityisen kannatettavana työryhmä pitää sananvapauslain uudistusehdotuksessa mainitun verkkoviestin lähettäjää koskevien tunnistamistietojen säilyttämisvelvollisuutta. Miten tälle velvollisuudelle käy eduskuntakäsittelyssä on vielä tässä vaiheessa arvoitus. Työryhmän mielestä tietoliikenteen tunnistamistietojen säilyttämisvelvoitetta tulisi arvioida myös tietoturvallisuuden toteutumisen kannalta. Erilaiset tietojärjestelmiin kohdistuneet hyökkäykset eivät varsinaisesti ole sananvapauslaissa tarkoitettuja verkkoviestejä. Esimerkiksi perinteisessä tietomurrossa murtautuja ei lähetä minkäänlaista viestiä, joka olisi tarkoitettu julkisuuteen tai jonkun henkilön tietoon. Murtautujan tarkoitus on aiheuttaa tietoverkon kautta kohteeseen tekninen häiriö, jota kautta hän saa käyttöönsä uhrin tietokoneen tai tietojärjestelmän. Näitten rikosten menestyksellinen selvittäminen edellyttää, että otetuista yhteyksistä löytyy merkintä niistä palvelimista ym. laitteista, joiden kautta murtautuminen on tehty. Tunnistamistietojen säilyttämisvelvollisuus tietoturvaloukkausten selvittämisen turvaamiseksi olisi näkemyksemme mukaan tarpeen tehdä erillään sananvapauslain uudistamistyöstä, koska kyseessä ei sinänsä ole sananvapauden käyttämisestä.

Vaikka tekniset keinot eivät voi olla ratkaisu sosiaalisille ongelmille, niillä voidaan vähentää ongelmien aiheuttamaa haittaa eli säilyttää verkon toimintakykyisyys ja käyttökelpoisuus. Kehitystyötä tulisi kohdistaa tietoverkoissa käytettäviin teknisiin välineisiin, joilla mahdollistetaan käyttäjien ja järjestelmien ylläpitäjien oikeus kieltäytyä vastaanottamasta laitonta ja haitallista materiaalia. Lasten ja nuorten kohdalla erityisten helppokäyttöisten suodinten kehittäminen on kannatettavaa jo vanhempien kasvatusmahdollisuuden takaamiseksi.

Yhteiskunnassa erilaisiin haitallisiin ilmiöihin puuttuminen rikosoikeudellisin keinoin tulisi olla aina viimekätinen keino. Työryhmä korostaakin, että ensisijaisena vaikutuskanavana tulisi käyttää koulutusta ja valistusta sekä tehokkaan itsesääntelyn mahdollistavien sopimusten tekemistä.

Itsesääntelystä hyvänä esimerkkinä on suurten operaattoreiden yhdessä sopima netiketti, sekä netiketin huomioivat käyttösopimukset, jotka varaavat operaattorille oikeuden poistaa laiton tai haitallinen aineisto palvelimelta saatuaan sen olemassaolosta tiedon.

Koulutuksesta ja valistuksesta esimerkkinä mainittakoon raportissa kuvattu DotSafe – projekti, jossa opettajille annetaan helppokäyttöisessä muodossa materiaalia opettamisen tueksi Internetin vaaroista sekä tietoa käytännesäännöistä. Tietoyhteiskunnan leviäminen yhä laajemmalle on kannatettava suuntaus ja tätä tulisi edistää myös koulujärjestelmässämme siten, että kouluissa olisi toimivat ja helppokäyttöiset käyttäjän tunnistavat tietojärjestelmät sekä järjestetty ylläpito, joka vastaa järjestelmän toimivuudesta hyvän tietohallintotavan mukaisesti. Anonyymi ilmaisu ja liikkuminen Internetissä tulee olla mahdollista, mutta taustalla tulee myös olla tietoisuus siitä, että väärinkäyttötapauksissa tekijä on jäljitettävissä.

8 Liitteet

Liite 1 Teknisen korkeakoulun lausunto

1. Toimeksianto

Tämä lausunto perustuu seuraavaan lausuntopyyntöön:

Tietohallintopäällikkö Kristel Sarlin, Teknillinen korkeakoulu

Sisäasiainministeriö asetti 15.10.2002 työryhmän selvittämään sekä mahdolliset lainsäädäntöön liittyvät tarpeet että tekniset mahdollisuudet, jotta internetissä julkaistavan rikollisen materiaalin levittämistä voitaisiin rajoittaa tai estää.

Työryhmän puheenjohtajana toimii rikostarkastaja Ari Määttä ja jäseninä Veli-Pekka Loikala sekä ylitarkastaja Sari Kajantie Keskusrikospoliisista. Työryhmän määräaika on 31.12.2002.

Toimeksiannon valtuuttamana työryhmä on päättänyt pyytää lausuntoja sekä tekniikan että lainsäädännön asiantuntijoilta erilaisista näkökulmista. Pyydämme sinulta lausuntoa seuraaviin kysymyksiin:

1. Millaiset tekniset tai lainsäädännölliset keinot puuttua internetissä ilmenevään rikolliseen sisältöön olisivat

TKK:n näkökulmasta mahdollisia ja kohtuullisia?

2. Millaisista viesti- tai liikennemääristä puhutaan News-liikenteen osalta News-palvelimellanne? (Ilmoitettavan suureen ja aikajakson voitte valita sen mukaan mikä on helpointa selvittää)

3. Mikä on arvionne peer-to-peer- ja irc- liikennemääristä omassa tai kyläverkossanne?

4. Millaisiksi arvioisitte teknisestä ylläpitäjänäkökulmasta seuraukset, jos Suomessa edellytettäisiin julkisten keskustelujärjestelmien ennakkosensuuria?

2. Lausunto

Tämän lausunnon antaa Teknillisen korkeakoulun turvaryhmästä tietohallintopäällikkö Kristel Sarlin, atk-erikoistutkija Timo Larmela, atk-erikoistutkija Kimmo Laaksonen ja tietoturva-asiantuntija Sami Koskinen.

2.1 Kysymys 1

"Millaiset tekniset tai lainsäädännölliset keinot puuttua internetissä ilmenevään rikolliseen sisältöön olisivat TKK:n näkökulmasta mahdollisia ja kohtuullisia?"

Tällä hetkellä verkossa esiintyvään rikolliseen sisältöön puututaan seuraavasti:

1) Jos joku TKK:n verkon käyttäjä tai ulkopuolinen taho Suomesta tai muualta maailmasta on havainnut jotain, joka on selvästi rikollista tai on vahva epäily siitä, että tapahtuu rikollista toimintaa, ja hän siitä ilmoittaa, niin siihen puututaan tapauksesta riippuen seuraavasti:

Lievin tapaus on se, että joku levittää jotain elokuvaa, musiikkia tms. todennäköisesti tekijänoikeuden alaista materiaalia. Levittäjää pyydetään poistamaan materiaali verkosta ja häneltä pyydetään selvitystä, mitä hän oli tekemässä. Näin toimitaan, kun on esimerkiksi saatu ilmoitus, mutta ei ole välitöntä havaintoa, että levitystä tapahtuu, jonka huomaa esimerkiksi suuresta liikennemäärästä.

Havaittaessa laittoman materiaalin levittämistä, levittämisestä epäillyn oikeudet käyttää TKK:n tietojärjestelmiä peruutetaan ja materiaali poistetaan saatavilta. Materiaali talletetaan joksikin aikaa mahdolliseksi todisteeksi tai palautettavaksi, jos käy ilmi. että kyse ei ole rikollisesta materiaalista. Tapauksesta riippuen oikeudet käyttää TKK:n tietojärjestelmiä voidaan palauttaa asian selvittämisen jälkeen.

Käyttösääntöjemme mukaan käyttäjät eivät saa pystyttää omia verkkopalveluja atk-keskuksen ylläpitämiin laitteistoihin. Jos käyttäjä levittää mitä tahansa, laitonta tai laillista, materiaalia atk-keskuksen järjestelmiin pystyttämän oman palvelunsa kautta, tähän puututaan käyttösääntöjen rikkomisen nojalla sulkemalla käyttäjätunnus.

Käyttöoikeudet saa takaisin vain siten, että kirjallisesti selvittää mitä on tehnyt, ja käy johtajan puhuttelussa. Vakavimmissa tapauksissa harkitaan esimerkiksi rehtorin puhuttelua tai muuta kurinpidollista toimenpidettä.

Suurinta osaa tapauksista ei viedä eteenpäin. Jos epäillään laittoman materiaalin levitystä, selvää yllytystä rikokseen tai tietomurtoa, otetaan yhteys poliisiin. Yhteydenoton tarkoitus on tiedottaa asiasta, koska siitä voi olla hyötyä jonkun muunkin rikoksen selvittämisessä, sekä alustavasti selvittää, kuinka vakavasta asiasta on kyse. Kaikista väärinkäytöksistä ei kannata tehdä rikosilmoitusta, koska niiden selvittäminen voi olla erittäin hankalaa ja työlästä, ja poliisin sekä

ylläpidon resurssit eivät riitä kaiken tutkimiseen. Yhteydenoton ja alustavan selvityksen perusteella TKK:n johto päättää, tehdäänkö asiasta rikosilmoitus (asianomistajarikos) tai poliisi päättää, aloitetaanko rikostutkinta (yleisen syyttäjän alainen rikos).

2) Jos verkossa havaitaan sen epänormaalin toiminnan tai tilastollisen seurannan perusteella, että on syytä epäillä, että joku rikkoo käyttösääntöjämme, ryhdymme edellä kuvattuihin toimenpiteisiin. Esimerkiksi, jos jostain erikoisesta portista lähtee ulos suuri määrä liikennettä, voi epäillä, että se ei ole asiallista.

3) Jos poliisi ottaa yhteyttä virka-apupyynnön muodossa ja pyytää, että jokin aineisto poistetaan ja/tai pistetään talteen ja toimitetaan poliisille todistusaineistoksi, annamme poliisille virka-apua. Jos poliisilla on tuomioistuimen päätös, niin annamme virka-apua esimerkiksi myös tietoliikenteen seurannassa.

Lain mukaan meillä ei ole oikeutta seurata liikenteen sisältöä, lukea ihmisten sähköposteja tai tutkia tiedostojen sisältöä muulloin kuin silloin, kun annamme virka-apua poliisille, hänen soveltaessaan lain mukaisia pakkokeinoja.

4) Kaikki sähköpostit kulkevat virusssuodattimen ja roskapostisuodattimen läpi. Jos havaitaan virus, se poistetaan postista, ja siitä tulee ilmoitus postin vastaanottajalle. Roskapostisuodatin antaa postille pisteitä sen mukaan. miten todennäköisesti se on roskapostia. Käyttäjä voi pisteytyksen perusteella tehdä postille mitä haluaa, mutta sitä ei automaattisesti poisteta eikä sen sisältöä muuteta.

Nämä ovat ainoat tapaukset, jolloin sisälle tulevaa tai uloslähtevää tietoa analysoidaan sisällön perusteella. Tämäkin analyysi tapahtuu ohjelmallisesti siten, että kukaan ihminen ei ole tietoinen siitä, mikä on postin sisältö. Virussuodattimena on RAV AntiVirus for Mail Servers -niminen ohjelma, ja roskaposteja etsitään SpamAssassin-ohjelmalla.

Ainakin tiedustelupalveluilla lienee käytössään ohjelmia, joilla voidaan valvoa verkon liikennettä siten, että siitä voidaan tehdä sisällöllisiä analyysejä. Meillä ei ole muita kuin edellä mainittuja virustentorjuntaan ja roskapostien tunnistamiseen soveltuvia ohjelmia. Toisaalta sisällöllisellä analyysilla on vaikea havaita, mikä materiaali on rikollista ja mikä ei. Lisäksi aineisto voidaan, ja myös salakirjoitetaan, sekä esimerkiksi kuviin on helppo piilottaa muutakin tietoa, jonka havaitseminen on käytännössä mahdotonta, ainakin sellaisilla ohjelmistoilla joita Teknillisellä korkeakoululla on käytössään.

Periaatteessa on mahdollista ylläpitää rekisteriä, kuka liikennöi ja milloin, pisteestä A pisteeseen B. Käsittääksemme tällöin syntyy sellainen henkilörekisteri, jonka pitäminen on laitonta. Lokeissa on tietoa, joista poliisi periaatteessa voi rikostutkinnan yhteydessä luoda tällaisia rekistereitä, mutta valmiina niitä ei ole. Lokien määrä on myös niin suuri, että niitä ei voi kovin pitkään säilyttää.

Jos joku haluaa siirtää rikollista materiaalia, niin se voidaan tehdä myös siten, että se kulkee sellaisen protokollan päällä, että sitä on vaikea havaita, portteja voidaan koko ajan vaihtaa yms. Käytännössä on lukematon määrä tapoja, joilla rikollisen materiaalin siirtäminen voidaan suorittaa ilman että sitä havaitaan. Aktiivinen yritys paljastaa kaikki epäilyttävä, johtaisi kilpajuoksuun, jolle ei ole loppua, joka vaatisi jatkuvasti kasvavia investointeja laitteisiin ja ohjelmistoihin sekä henkilökunnan määrän jatkuvaa kasvattamista.

Lainsäädännön mukaan (perustuslaki, laki yksityisyyden suojasta työelämässä jne.) mukaan meidän tehtävämme ei voi olla aktiivinen liikenteen sisällön seuraaminen tai sen selvittäminen kuka vaihtaa tietoa ja kenen kanssa. Poliisin tehtävä on selvittää, tapahtuuko rikollista toimintaa. Rikollisen materiaalin tunnistaminen vaatii käytännössä myös sen, että ihmisen tulee tunnistaa se rikolliseksi. Tätäkään emme voi tehdä, mutta emme myöskään halua, koska se on vastoin niitä periaatteita, joille Suomen ja EU:n yhteiskunta-

rakenne perustuu.

TKK on yliopisto, jolle on oleellista tutkimuksen vapaus ja mahdollisuus vaihtaa tietoa kaikkien maiden tutkijoiden kanssa sekä pitää IT-infrastruktuuri niin avoimena kuin mahdollista. Tämän takia TKK:ta ei voi eristää muusta Internetistä samalla tavalla kuin firmoissa voidaan tehdä.

Periaatteessa on teknillisesti mahdollista suodattaa liikennettä kuten tehdään esimerkiksi Kiinassa tai Saudi-Arabiassa tai asentamalla suodatin-ohjelmia, joita on tarjolla lukematon määrä, joilla esimerkiksi suojellaan lapsia siltä, että he eivät kotikoneelta pääsisi katselemaan pornosivuja. Yhtä mahdollista on myös kiertää nämä tekniset rajoitukset. Sen lisäksi liikennemäärä on niin suuri, että käytännössä ei ole mahdollista hankkia laitteistoja ja ohjelmistoja, joilla kaikki liikenne analysoitaisiin ilman että verkon ja/tai koneiden suorituskyky ei romahtaisi lähes nollaan.

Yhteenvetona voidaan todeta, että TKK:n kannalta mikään sellainen, joka vaatisi selvittämään tietoliikenteen ja tiedostojen sisältöä, ei ole kohtuullista. Sen sijaan tärkeää on opettaa ihmiset toimimaan verkossa siten, että he ottavat huomioon toistensa tarpeet ja toimivat siten, että eivät tahallaan tai vahingossa aiheuta ongelmia ja että he asiallisesti osaavat tunnistaa haittaa aiheuttavat asiat ja rikollisen toiminnan ja raportoivat siitä ylläpidolle.

2.2 Kysymys 2

"Millaisista viesti- tai liikennemääristä puhutaan News- liikenteen osalta News-palvelimellanne? (Ilmoitettavan suureen ja aikajakson voitte valita sen mukaan mikä on helpointa selvittää)"

Tarkasti ottaen TKK:lla ei ole omaa varsinaista news-palvelinta. Internetin news-ryhmät välitetään tänne nntp.hut.fi- ja news.cs.hut.fi-palvelimien kautta. Tänne välitetään lähes kaikki Usenetin ryhmät lukuunottamatta binaariryhmiä (alt.binaries), joita ei välitetä kapasiteettisyistä nntp.hut.fi:lle.

Ylioppilaskunnalla on news-palvelin, otax.hut.fi, jossa on monenlaisia opiskeluun ja harrastustoimintaa liittyviä ryhmiä sekä muutamia virallisia TKK:n keskustelu- ja tiedotusryhmiä.

Tietojenkäsittelyopin laitoksella on kolmas news-palvelin, news.cs.hut.fi. Sen kautta välitetään enemmän Usenetin ryhmiä kuin edellä mainittujen.

2.2.1 Nntp.hut.fi-palvelin

Atk-keskuksen hallinnassa olevan news-palvelimen nntp.hut.fi osalta liikennemäärää kuvaavat seuraavat luvut:

aika: 12.10.2002 - 4.12.2002
sisään tuleva liikenne (per päivä):
artikkelien lukumäärän keskiarvo: 456 005 kpl
artikkelien yhteiskoon keskiarvo: 10,05 Gt

aika: 1.12.2002 - 4.12.2002
ulospäin lähtevä liikenne: (kokonaismäärä ajanjaksolta)
artikkeleiden lukumäärä: 929 007 kpl
artikkeleiden keskiarvo (per päivä): 232 252 kpl

palvelimen statistiikkaa:
artikkeleita keskimäärin: 22 Gt
artikkeleiden lukumäärä: 3 289 547 kpl

2.2.2 Otax.hut.fi-palvelin

Teknillisen korkeakoulun ylioppilaskunnan news-palvelimelle (news.tky.hut.fi aka otax) käyttäjät kirjoittavat noin 1500 uutta viestiä viikossa.

2.2.3 News.cs.hut.fi-palvelin

Newsfeediä tulee ja menee funetille, nntp:lle ja song.fi:lle. Liikennemäärää kuvaavat seuraavat luvut:

aika: 3.12.2002 - 11.12.2002

sisään tuleva liikenne (per päivä):
artikkeleiden lukumäärän keskiarvo: 860 905 kpl
artikkeleiden yhteiskoon keskiarvo: 10 Gt (*)
(*) tämä on arvio, koska tästä ei ole tarkkaa lokia

ulospäin lähtevä liikenne: (kokonaismäärä ajanjaksolta)
artikkeleiden kokonaismäärä: 1 414 980 kpl
artikkeleiden keskiarvo (per päivä): 157 220 kpl

palvelimen statistiikkaa:
artikkeleita keskimäärin: 46,5 Gt
artikkeleiden lukumäärä:5 555 137 kpl

2.3 Kysymys 3

"Mikä on arvionne peer-to-peer- ja irc- liikennemääristä omassa tai kyläverkossanne?"

MRTG-statistiikkojen perusteella irc-serverin (lähinnä clienteille) ulospäin menevä liikenne vaihtelee melko ennustettavasti päivittäin välillä 10-50 kilotavua sekunnissa ja sisäänpäin tuleva liikenne vaihtelee välillä 10-20 kilotavua sekunnissa.

Nämä lukemat eivät kuitenkaan heijastele millään tapaa ircin avustuksella siirrettävien tiedostojen kokoja, koska ircin tiedostosiirto tapahtuu clienttien välillä suoralla TCP-yhteydellä jonka kanssa serveri on tekemisissä vain porttinumerotietojen välittäjänä. Nämä välitystiedot voitaisiin periaatteessa lokittaa, mutta niitä ei tällä hetkellä lokiteta.

Välitystiedoista ei myöskään selviä, millaista materiaalia kahden irc-clientin välillä todellisuudessa liikkuu, koska irc-palvelin ei sitä näe.

Hyvin usein tätä ominaisuutta kuitenkin käytetään laittoman materiaalin levittämiseen. Ominaisuuden poistaminen tarkoittaisi laillisen käytön rampauttamista ja laittoman materiaalin siirtymistä muiden irc-palvelinten yhteyteen tai kokonaan toisille tekniikoille.

Meillä ei ole tietoa siitä, mitä IRCnetin ulkopuolelle suuntautuvaa irc-liikennettä TKK:n verkossa kulkee, emmekä välttämättä tiedä kaikkea IRCnet-liikennettäkään. Erilaisia julkisia irc-verkkoja maailmalla on useita, yksityisiä ei kannata yrittää edes arvioida.

Kokonaisuudessaan pelkästään IRCnetillä on noin 120 000 käyttäjää, ks. <http://ircnet.org@irc.tu-ilmenau.de/all_servers/>.

Irc.cs.hut.fi -koneeseen on yhteydessä karkeasti ottaen 1000-2000 clienttiä.

Peer-to-peer liikennettä ei ole koskaan mitattu. Kyläverkosta lähtee maailmalle koko ajan n. 9 Mt sekunnissa, josta ilmeisesti suuri osa on peer-to-peer-liikennettä. Sisäänpäin menee yhteensä 3-4 Mt sekunnissa.

2.4 Kysymys 4

"Millaisiksi arvioisitte teknisestä ylläpitäjänäkökulmasta seuraukset, jos Suomessa edellytettäisiin julkisten keskustelujärjestelmien ennakkosensuuria?"

Asiaa voidaan tarkastella monelta kannalta.

Julkisten keskustelujärjestelmien suurten viestimäärien vuoksi se ei olisi teknisesti mitenkään helppo asia hoitaa järkevästi. Siltä osin kuin jokainen viesti pitäisi tarkistaa, se olisi käytännössä mahdotonta, koska niin suurta määrää ihmisiä kuin tarvittaisiin tähän, ei ole mahdollista palkata. Sen lisäksi tällaisten, ns. moderoitujen ryhmien viestien väärentäminen on erittäin helppoa eli ennakkosensuuri voitaisiin ohittaa. Jos julkisiin keskustelujärjestelmiin kaavailtu päätoimittajavastuu toteutuu, se merkitsee keskusteluryhmien lopettamista, koska päätoimittaja joutuisi vastaamaan viesteistä, jotka menevät hänen kontrollinsa ohi joko siten, että niitä on niin paljon, että niitä ei voi tarkistaa, tai sitten niitä väärennetään.

Moderointitietojen väärentämisen yksinkertaisuus pätee erityisesti nntp-järjestelmiin, kuten USENET News. Www-foorumit ovat eri asia, mutta niissäkin voi olla toiminnallisia puutteita, joita voidaan käyttää hyväksi.

Muutamia vuosia sitten Soneralla oli tarjolla palvelu, jolla sai lähettää tekstiviestin haluamaansa numeroon ja viestin lähettäjän puhelinnumeroksi sai antaa vapaavalintaisen numerosarjan. Näin ollen ei ole mitenkään varmaa, etteikö tekstiviestienkin tunnistetietoja voisi väärentää edelleen, joskaan se ei varmasti ole yhtä yksinkertaista kuin tuolloin.

On siis mahdollista, että tekstiviestien oletettu turvallisuus liittyen erilaisiin sms chat -foorumeihin, on illuusio. Nämä foorumit ovat poikkeuksetta tehtävään palkatun ihmisen moderoimia, ainakin toistaiseksi. Näiden viestivolyymi on iso, ja koska jokainen viesti maksaa, on odotettavissa, että joku toteuttaa vastaavan järjestelmän siten, että se toimii kuten irc, eikä sitä istu joku koko ajan valvomassa. Kaikki tekniset mahdollisuudet ovat olemassa, ja uudet multimediakännykät voivat luoda tällaiselle omat paineensa. Televisiokanavien sms-chatit eivät oikeastaan poikkea juuri ollenkaan verkossa tarjolla olevista nk. chat-sivuista (wwwchat) muuten kuin siten, että chat-sivujen liikennettä ei yleensä moderoida.

Jo usean vuoden ajan erityisesti ircissä eräät keskustelijat aivan muodon vuoksi ovat käyttäneet vahvaa salausta myös julkisessa keskustelussa. Reaaliaikaisen keskustelun moderointi niin ikään myös tappaisi reaaliaikaisuuden.

Koska keskusteluryhmiä voi perustaa missä tahansa Internetin osassa ja Internet on maailmanlaajuinen, niin keskustelu, jota täällä sensuroitaisiin, siirtyisi muualle Suomen rajojen ulkopuolelle.

Jos ei-toivottu liikenne haluttaisiin estää ja sulkea osa reiteistä, niin se tulkitaan tietoliikenneverkon virheeksi, ja Internetin rakenteen perusteella vikapaikka kierretään. Se on siis käytännössä mahdotonta.

Jos keskustelujärjestelmiä (news, irc, aim, icq, wwwchat ja tuhansia muita) haluttaisiin ennakkosensuurin piiriin ja valvoa reaaliaikaisesti, niin siihen ei yksinkertaisesti ole teknisiä välineitä eikä ihmisresursseja. Paljon yksinkertaisempaa olisi maantieliikenteen valvonta siten, että jokaisessa Suomen tienristeyksessä olisi 24 tunnin poliisipartiovalvonta, mikä myös on mahdotonta.

Ennakkosensuurin toteuttaminen johtaisi myös siihen, että julkiset keskustelujärjestelmät muuttuisivat suljetuiksi keskustelujärjestelmiksi, joissa olisi itse asiassa helpompi kuin julkisissa, käydä arveluttavaa keskustelua ja/tai välittää rikollista materiaalia.

Koska www-sivut ovat itsessään osa julkista keskustelua, ja niiden kautta voidaan sitä käydä monella tavalla, ennakkosensuuri merkitsisi jokaisen www-sivun ennakkosensuuria sekä valvontaa, että sivua ei muuteta ilman uutta tarkistusta. Käytännössä tämä ei ole mahdollista ilman Internetin sulkemista. Ja vaikka www-sivut rajattaisiin pelkästään esimerkiksi TKK:n sisälle (yhteydet ulos olisi suljettu), niin ei olisi mitään mahdollisuuksia valvoa 14 000 - 15 000 henkilön verkkosivuja, ja samalla myös tieteellinen tutkimus loppuisi yhteyksien katkettua.

Periaatteessa on mahdollista toteuttaa www-sivujen ennakkotarkastus määrittämällä tarkastamattoman sivun julkaisu rikolliseksi. Kokonaan toinen asia taas on, mistä Suomeen saataisiin ne tarkastajat, jotka tarkastavat joka ikisen Suomen maaperällä julkaistavan www-sivuston lainvastaisuuksien varalta ja kuka sen maksaisi. Samalla voitaisiin sanoa hyvästit nykyiselle demokraattiselle ja vapaalle yhteiskuntajärjestykselle.

Mielenkiintoista olisi myös se, miten suhtauduttaisiin materiaaliin, joka sijaitsee fi-juuren alta löytyvässä domainissa, mutta itse sivusto taas on jossakin aivan toisessa maassa? Minkä maan lakia sivustoon sovellettaisiin ja millä perusteella?

Liite 2 Viestinnän keskusliiton lausunto

Keskusrikospoliisi
Rikostarkastaja Ari Määttä
(ari.k.maatta@krp.poliisi.fi)
PL 285
01301 Vantaa

30.12.2002

Asia: Viestinnän Keskusliiton kirjallinen lausunto internetissä julkaistavan rikollisen materiaalin levittämistä pohtivan työryhmän kysymykseen

9 Viestinnän Keskusliitto

Viestinnän Keskusliiton (jäljempänä myös liitto) tarkoituksena on edistää joukkoviestintäalan yritysten yleisiä ja erityisiä toimintaedellytyksiä. Edunvalvonta ja vaikuttaminen, muun muassa toimialalle yhteiset lainsäädäntöasiat, on keskitetty alan yhteisten asioiden osalta alla olevilta jäsenliitoilta Viestinnän Keskusliitolle.

Viestinnän Keskusliiton jäsenliitot ovat Aikakauslehtien Liitto, Graafinen Teollisuus, Sanomalehtien Liitto, Suomen Kustannusyhdistys ja Viestintätyönantajat VTA.

Aikakauslehtien Liittoon kuuluu 244 aikakauslehden kustantajaa ja 456 jäsenlehteä. Graafinen Teollisuus on graafisen teollisuuden elinkeinopoliittinen toimiala- ja edunvalvontajärjestö. Liitolla on 260 jäsenyritystä. Sanomalehtien Liittoon kuuluu 148 sanomalehden kustantajaa, jotka julkaisevat 199 sanomalehteä. Suomen Kustannusyhdistys on suomalaisten kirjankustantajien etujärjestö, jolla on 90 jäsenyritystä. Viestintätyönantajat VTA ry palvelee jäseniään graafisen teollisuuden ja muun viestinnän työnantajapoliittisissa kysymyksissä. Liitolla on 387 jäsenyritystä.

- Työryhmän esittämään kysymykseen ”*Millaisena näette sananvapauden ja internetissä julkisesti levitettävän, sisällöltään laittoman materiaalin välisen suhteen*”, liitto esittää kunnioittavasti seuraavan.

Internetissä julkisesti levitettävien tietojen, ajatusten, mielipiteiden tai muiden viestien levittämisen ennakollinen rajoittaminen viranomaisten tai muiden toimesta ei ole mahdollista.

Edellä mainittu johtuu siitä, että perustuslain 12 §:ään kirjattu sananvapaussäännös antaa jokaiselle oikeuden kenenkään ennakolta estämättä levittää sisällöltään kaikenlaista materiaalia. Ennakkoesteiden kielto on ehdoton. Ainoastaan lasten suojelemiseksi voidaan lailla asettaa välttämättömiä rajoituksia. Sananvapauden käyttämisestä säädetään erikseen. Tällä hetkellä sananvapauden käyttämisestä säännellään muun muassa painovapauslaissa. Uutta lainsäädäntöä on vireillä: nykyisen eduskunnan käsiteltävänä on ehdotus laiksi sananvapauden käyttämisestä joukkoviestinnässä (HE 54/2002).

Sananvapausjärjestelmä lähtee siitä, että jos julkisesti levitetty ajatus, mielipide, tieto tai muu viesti sisältää laitonta materiaalia, voidaan asiaa puuttua jälkikäteisin keinoin. Esimerkiksi henkilön kunniaa tai yksityiselämää loukkaavaan kirjoituksen voidaan puuttua siten, että asia käsitellään asianmukaisessa järjestyksessä tuomioistuimessa, ja vasta tuomioistuimen suorittaman arvioinnin jälkeen voidaan todeta, onko asiassa syyllistytty viestin sisältöön perustuvaan rikokseen. Viranomainen ei voi ennakolta sitovasti arvioida tai päättää, onko jossain materiaalissa laitonta sisältöä.

Tietyissä poikkeuksellisissa tilanteissa muu kuin tuomioistuin voisi ryhtyä toimenpiteisiin sananvapauden rajoittamiseksi. Tätä on ehdotettu edellä mainitussa ehdotuksessa laiksi sananvapauden käyttämisestä joukkoviestinnässä. Ehdotuksen 5 luvun 20 §:n mukaan ”lähettimen, palvelimen tai muun sellaisen laitteen ylläpitäjällä on oikeus keskeyttää verkkoviestin pitäminen yleisön saatavilla, jos on ilmeistä, että viesti täyttää rikoslain 11 luvun 8 §:ssä tai 17 luvun 18 §:ssä rangaistavaksi säädetyn teon tunnusmerkit.”

Ehdotusta on perusteltu sillä, että säännöksissä mainituissa tilanteissa on kyse sellaisista tekomuodoista, joiden moitittavuudesta vallitsee laaja yksimielisyys. Lähettimen tai palvelimen ylläpitäjän pitää selvästi materiaalin – kuvan tai tekstin – perusteella pystyä arvioimaan että kyse on mainituista teoista. Useimpien aineistojen ja materiaalien osalta tällainen arviointi ei ole mahdollista. Tästä syystä verkkoviestin keskeyttämisoikeus on rajattu vain edellä mainittuihin kahteen tekomuotoon.

Liiton mielestä internetissä olevan laittoman aineiston osalta ei ole tarvetta ryhtyä lainsäädäntötoimenpiteisiin. Laittomaan aineistoon voidaan puuttua jälkikäteisin keinoin niissä tilanteissa, joissa puuttuminen on aineiston sisällön perusteella mahdollista rikoslaissa säädetyissä tekomuodoissa.

Vaikka joissain yksittäistapauksissa näyttäisi siltä, että uusiin kriminalisointeihin tai sananvapauden käyttämistä koskeviin rajoituksiin olisi tarvetta, ei lainsäädäntöä tule kuitenkaan tehdä sellaiseksi, että sillä ”paikattaisiin” yksittäisiä ja satunnaisia ongelmatilanteita.

Liiton edustamalla toimialalla toimivat sähköisen aineiston julkaisijat noudattavat sekä voimassa olevia säännöksiä että oman alansa itsesääntelyohjeita. Korkeas-

ta eettisestä tasosta kertoo muun muassa se, että kaikille sähköisille joukkoviestintää harjoittaville julkaisuille on nimetty päätoimittaja, vaikka nykyinen lainsäännö ei tällaista edellytä.

Oikeudelliselta kannalta sananvapauden ja internetissä julkisesti levitettävän, sisällöltään laittoman materiaalin välinen suhde ei ole ongelmallinen. Sisällöllisesti laittomaan materiaaliin voidaan puuttua jälkikäteen niissä tilanteissa, joissa puuttuminen on lainsäädännön perusteella mahdollista. Painetun ja sähköisen aineiston sisältöön puuttuminen jälkikäteen ei pidä olla erilaista. Oikeudellisesti ei ole perusteita sille, miksi sääntelyn pitäisi ylipäätään olla erilaista. Näin ollen koko kysymystä sananvapauden ja sisällöltään laittoman aineiston välisestä suhteesta tulee ajatella suurempana kokonaisuutena, ei ainoastaan kysymyksenä internetissä olevan materiaalin laittomuutena.

Tekniseltä kannalta internetissä olevan aineiston saannin tai levittämisen rajoittaminen ei ole käsityksemme mukaan mahdollista muutoin kuin erittäin huomattavien resurssien käyttämisellä. Internetin tekninen valvonta ja rajoittaminen vaatisi satoja ellei peräti tuhansia miestyövuosia. Siitä huolimatta keskustelupalstat tai muut vastaavat tietojen, ajatusten tai mielipiteiden virtuaaliset vaihtopaikat olisi yksinkertaista siirtää yhä uudelleen sellaiseen paikkaan, jonne teknistä valvontaa tai rajoittamista olisi mahdotonta ulottaa.

Liiton johtopäätös käsillä olevassa asiassa on edellä mainittujen näkökohtien perusteella se, että oikeudellista kannalta sananvapauden ja internetissä olevan sisällöltään laittoman aineiston välinen suhde ei ole ongelmallinen niin kauan kuin perustuslain 12 §:n ennakkoesteiden kieltoa kunnioitetaan. Sananvapauden käyttämisen ennakolliseen rajoittamiseen ei saa eikä voida puuttua ryhtymällä satunnaisia yksittäistilanteita korjaaviin lainsäädäntötoimenpiteisiin.

Internetissä olevan laittoman aineiston valvonta on lähinnä resurssikysymys; miten poliisi ja muut viranomaiset pystyvät seuraamaan verkossa levitettävää aineistoa teknisesti siten, että laittoman aineiston levittämiseen pystyttäisiin puuttumaan jo nykyisen lainsäädännön sallimalla tavalla.

Liitto antaa mielellään lisätietoja tässä lausunnossa esitettyihin näkemyksiin. Tarpeen vaatiessa asiaan vastaa joko allekirjoittanut tai johtaja Valtteri Niiranen.

Viestinnän Keskusliitto

Håkan Gabrielsson (hakan.gabrielsson@sanomalehdet.fi)
Toimitusjohtaja
Viestinnän Keskusliitto

Liite 3 Telia Mobile Finlandin lausunto

Jari Perko 16.12.2002 Telia Mobile Finland

Millainen on teleoperaattorin näkökulma puuttua teknisesti tai lainsäädännön keinoin internetissä ilmenevään rikolliseen sisältöön?

Millaisia muita vaikuttamiskeinoja teleoperaattorilla olisi internetissä ilmenevän rikollisen sisällön ehkäisemikseksi tai siihen puuttumiseksi?

Vastauksessa internet on ymmärretty laajasti mukaan lukien kaikki käyttäjien saatavilla oleva sisältötarjonta verkoista, yhteystavoista ja tekniikoista riippumatta.

Ottaen huomioon internetin teknisen ja rajat ylittävän luonteen sekä voimassa olevat oikeusperiaatteet ja lainsäädännön operattorilla ei tosiasiallisesti ole tehokkaasti mahdollisuutta puuttua internetin rikolliseen sisältöön. EU:ssa on jo otettu selvä kanta operaattorin asemaan internetin rikolliseen sisältöön puuttumisessa. Ns. sähkökauppadirektiivin (2000/31/ EY, 15 artikla 1 kohta) mukaan ”*Jäsenvaltiot eivät saa asettaa palvelun tarjoajille 12, 13 ja 14 artiklassa tarkoitettujen palvelujen toimittamisen osalta yleistä velvoitetta valvoa siirtämiään tai tallentamiaan tietoja eivätkä yleistä velvoitetta pyrkiä aktiivisesti saamaan selville laitonta toimintaa osoittavia tosiasioita tai olosuhteita”.* Suomen implementointi sähkökauppadirektiivistä on ennustettavuuden ja toimivuuden kannalta Euroopan parhaita ellei jopa paras. Laissa on lähtökohdaksi ja peruskehykseksi otettu terveellä ja toimivalla tavalla selkeä sisällöntuottajan vastuu sisällöstä ja viranomaisaloitteinen aineiston poisto internetistä. Viranomaisaloitteisen poiston osalta tulisi kehittää nopeampia ja tehokkaampia viranomaismenettelyitä.

Tärkeä osa internetin sekä haitalliseen että rikolliseen sisältöön puuttumista ja tällaisen sisällön syntymisen ja sen käytön estämistä on eri tahoille suuntautuva valistus- ja tiedotustoiminta yhteistyössä eri osapuolten kesken. Useita tällaisia hankkeita on käynnissä eurooppalaisella ja kansallisella tasolla ja niiden jatkuva ja tarkasti punnittu toteuttaminen on jatkossakin tärkeää. Tämä sektori sisältää kysymyksenasettelussa mainittuja operaattorin ”muita vaikuttamiskeinoja”. Pääasiassa yhteys- ja siirtopalveluiden tarjoajana operaattoreiden ei tulisi olla valistus- ja tiedotustoiminnan pääroolissa, mutta operaattoreiden mukanaolo kokonaisuuden toteuttamisessa on toivottavaa ja välttämätöntä.

Operaattoreiden palveluehtojen tulee pyrkiä sopusointuun sääntely- ja valituskokonaisuuden kanssa lähtien kuitenkin kaupallisen toimintavapauden ja palvelutarjonnan joustavuuden pohjalta.

Operaattorin toimiessa sisällöntuottajana tai sisältöön liittyvien muiden kuin operaattoripalveluiden tarjoajana koskee tätä toimintaa omat säännöksensä. Kuten käynnissä oleva keskustelu sananvapauslakiesityksestä osoittaa, on kaikkeen internetissä saatavilla olevaan aineistoon tai palvelutarjontaan erittäin vaikeaa, epätarkoituksenmukaista, tehotonta tai jopa haitallista soveltaa perinteistä sisältöpalvelun tarjontaa koskevia säädöstöä liian laajassa mitassa. Riippumatta tulevan sananvapauslain lopullisesta sisällöstä on tärkeää, että uusien säännösten toimivuutta ja vaikutusta eri sisältö- ja palvelutarjonnan muotoihin konkreettisesti seurataan.

Sananvapauslakiehdotukseen sisältyy ja muissakin yhteyksissä ja ehdotuksissa esiintyy ajatus operaattoreille tai palveluntarjoajille asetettavasta tallennusvelvoitteesta eri muodoissaan. Internetin rikolliseen sisältöön puuttumisessa liittyvissä toimenpiteissä on erittäin tärkeää suhteellisuus- ja tarpeellisuusperiaatteen noudattaminen. Tallennusvelvoitteet massiivisia liikenne- ja tapahtumamääriä sisältävässä kokonaisuudessa eivät palvele em. tavoitteiden asianmukaista ja tarkoituksenmukaista toteutumista. Palveluntarjoajien muuttaminen massiivisen, potentiaalisen esitutkinta-aineiston säilytys- ja hallintapaikoiksi ei palvele tehokkaasti rikostutkintaa eikä vastaa voimassa olevia oikeusperiaatteita eikä hallitusohjelmaa asettaen kohtuuttomia rasitteita yrityksille.

Edellä selostettuun viitaten tosiasiallisia muutostarpeita sisältäväksi osa-alueeksi jää lähinnä operaattorin asema rikolliseen sisältöön kohdistuvan viranomaistutkinnan avustavana osapuolena. Käytännössä tämä tarkoittaa operaattorin roolia osana esitutkintaa perinteisine pakkokeinoineen, joista mm. sähkökauppadirektiivin ja televiestinnän tietosuojadirektiivin sallimissa rajoissa on tällä hetkellä valtioittain eriytynyttä kansallista sääntelyä. Cyber Crime Conventionin voimaan saattaminen tulee osaltaan yhtenäistämään tätä säännöstöä eurooppalaisella tasolla.

Operaattorin näkökulmasta rikolliseen sisältöön liittyvää tutkintaa voi edistää kahdella tavalla: parantamalla kuunteluun ja valvontaan liittyvää käytännön toimintaa ja yhteistyötä sekä uudistamalla televalvontaa koskevaa lainsäädäntöä.

Telekuuntelun ja -valvonnan käytäntöjen ja siihen liittyvien teknisten ja toiminnallisten asioiden kehittäminen on jatkuvaa eri osapuolten välistä pitkäjänteistä toimintaa ja sitä tulee edelleen kehittää. Tulevan viestintämarkkinalain asiaa koskevat säännökset antavat tälle työlle aikaisempaa paremman säädöskehyksen.

Sekä poliisin että operaattorin kannalta televalvontaa koskevat säännökset ovat luoneet käytännön ongelmia. Poliisin toiminnasta on selkeästi käynyt ilmi, että poliisi pitää voimassa olevia säännöksiä televalvonnasta riittämättöminä. Eduskunnan käsittelyssä oleva pakkokeinolain muutos parantaa osaltaan tilannetta. Tutkintapaine poliisin puolella on johtanut siihen, että poliisi on yrittänyt saada muiden kuin televalvontatietojen saantia koskevien yleissäännösten avulla operaattoreilta tunnistamistietoja. Tämä ei ole sopusoinnussa voimassa olevan yleis- ja erityissääntelyn jaon kanssa ja on saattanut operaattorit käytännössä erittäin hankalaan tilanteeseen, koska viestintäsalaisuuden piirissä olevat tunnistamistiedot kuuluvat operaattoreita sitovan vaitiolovelvollisuuden piiriin. Myös tunnistamistietoja koskevien televalvontasäännösten soveltuvuutta on yritetty laajentaa televalvontapyynnöissä tavalla, joka on aiheuttanut ongelmia operaattoreille (mm. EOA ns. tolppalupapyynnöistä).

Televalvontaa ja myös –kuuntelua koskevat säännökset ovat hajautuneet useisiin eri hallinnonalan lakeihin (OM, SM, LVM) ja tämä aiheuttaa käytännössä jatkuvasti tulkintaongelmia mm. soveltamisalan ja tekniikkaneutraalisuuden suhteen. Poliisilla vaikuttaa olevan tarpeita käyttää televalvontatietoja yhä erilaisimmissa tapauksissa yhä erilaisimmin tavoin, mikä tarkoittaa yhä vaativampia tieto- ja seurantapyyntöjä operaattoreille edellyttäen usein päivystyshenkilökunnan ympärivuorokautista toimintaa valvontapyynnön toteuttamiseksi. Televalvontaa ja –kuuntelua koskevat säännökset tulisi ehdottomasti keskittää yhteen säädökseen ja samalla huolehtia poliisin tutkintatarpeen tyydyttämisestä ottaen huomioon pakkokeinojen sääntelyn yleiset periaatteet, yksityisyyden

suoja, viestintäsalaisuus, jatkuvasti muuttuva tekninen kehitys sekä yrityksille aiheutuvat rasitukset.

Telekuunteluun ja televalvontaan sekä muuhun viranomaisavustamiseen tulisi johdonmukaisesti soveltaa pakkokeinolaissa omaksuttua pääperiaatetta avustuskustannusten korvaamisesta operaattorille. Viranomaisten budjettisuunnittelussa tulee nopeasti ja tehokkaasti huomioda jatkuvasti kasvavan televalvonnan tarpeet. Oikeus- ja sisäasianministeriön välistä yhteistyötä tulee kehittää. Viranomaisten välistä kansainvälistä yhteistyötä tulee tehostaa.

Rikollisiin sisältöihin liittyviä punnintoja tehdessä internetin luonne palvelu- ja sisältöalustana sekä tähän liittyvä siirto- ja yhteyspalvelutarjonta tulee selkeästi erottaa sisällön tuottamisesta. Internetin rikollisen sisällön arvioinnissa on aina syytä lähteä sisällön rikollisuuden tekniikkaneutraalista ja kiihkottomasta arvioinnista voimassa olevan rikoslain säännöksistä käsin. Uusia keinoja harkittaessa tulee ottaa aina huomioon internetin avoimuus, anonyymisuus ja rajat ylittävä luonne yhdessä suhteellisuus- ja tarpeellisuusperiaatteiden kanssa. Rikollisen toiminnan kytkeytyminen osaltaan internetiin ei tarkoita internetin kokonaisuuden osana olevan ongelman lähde tai ydin eikä sitä, että rikollinen toiminta estyisi tähän kokonaisuuden osaan kohdistuvilla toimenpiteillä.

Liite 4 Electronic Frontier Finland ry:n lausunto

Lausunto puuttumisesta Internetissä ilmenevään rikolliseen sisältöön

11.12.2002

Kai Puolamäki

FT, tutkija
Teknillinen korkeakoulu
Electronic Frontier Finland – EFFI ry

PL 9800 – 02015 TKK – 050 522 8111 – (09) 755 4892 (faksi)
Kai.Puolamaki@iki.fi – http://www.iki.fi/kaip/

Filosofian tohtori, tutkija **Kai Puolamäki** on työskennellyt Fysiikan tutkimuslaitoksella ja hoitanut vuodesta 2001 lähtien opettavan tutkijan virkaa Teknillisen korkeakoulun Informaatiotekniikan laboratoriossa. Kai Puolamäki on toiminut EFFIn puolesta asiantuntijana, avustanut viranomaisia ja antanut esitelmiä muun muassa ei-toivottua sähköistä viestintää ja joukkoviestinnän vastuulakia koskevissa asioissa.

Electronic Frontier Finland – EFFI ry on perustettu käyttäjien ja kansalaisten oikeuksien puolustamiseen Internetissä. Yhdistys pyrkii vaikuttamaan muun muassa lainsäädäntöhankkeisiin sananvapaudesta, tekijänoikeudesta ja tietokoneohjelmien patentoinnista Suomessa ja Euroopassa. Lisätietoja EFFIn kotisivulta osoitteessa http://www.effi.org/.

Johdanto

Sisäasianministeriön työryhmä pyysi 14.11.2002 päivätyssä kirjeessä vastausta seuraavaan kysymykseen:

> Millaiset tekniset tai lainsäädännölliset keinot puuttua Internetissä ilmenevään rikolliseen sisältöön olisivat EFFIn näkökulmasta hyväksyttäviä?

Kysymys koskee selvästi laitonta sisältöä, kuten petoksia (RL 36:1), kunnianloukkauksia (RL 24:9), yksityiselämää loukkaavan tiedon levittämistä (RL 24:8) tai sukupuolisiveellisyyttä loukkaavia lasta esittäviä kuvia (RL 17:18-19). Tämä lausunto ei sisällä kannanottoa siihen, mikä sisältö pitäisi tulkita rikolliseksi ja mikä ei.

Mielestämme rikolliseen toimintaan puuttumisessa on otettava huomioon seuraavat seikat, jotka perustelemme jäljempänä:

- Internet ei tee rikoksia
- Tekniikka ei ole rikollista
- Vain rikolliseen toimintaan tulee puuttua
- Jos tietoja kerätään, niitä käytetään väärin
- Puuttumiskeinojen on oltava perusteltuja ja järkevässä suhteessa tapahtuneeseen rikokseen
- Vain rikokseen syylliset ovat vastuussa teosta
- Vain viranomaiset voivat käyttää erioikeuksia
- Valistaminen ja itsesäätely ovat tehokkaita keinoja
- Rikollisia ei aina saada kiinni

Internet ei tee rikoksia

Internet tarjoaa ennenkuulumattoman tehokkaan tavan viestiä ja levittää informaatiota. Internettiä voi perustellusti pitää yhtenä ihmiskunnan merkittävimmistä keksinnöistä.

Internet on yksi inhimillisen kanssakäymisen muoto. Internetillä on kahvilakeskusteluihin, postiin, puhelinjärjestelmään, kirjakauppoihin tai kirjastoihin verrattuna seuraavia erityispiirteitä:

- Internet on kansainvälinen.
- Internetin rakenne on verkkomainen, eikä Internet-viestinnällä tyypillisesti ole keskitettyä "ylläpitäjää".
- Internet mahdollistaa tehokkaan ja maailmanlaajuisen tiedon haun ja viestinnän.

Internettiä – kuten muitakin inhimillisen kanssakäymisen muotoja – voi käyttää apuna rikosten tekemisessä. On kuitenkin tärkeää muistaa, että Internet ei tee rikoksia, vaan jotkut sitä käyttävät ihmiset, ja että Internetistä yhteiskunnalle aiheutuneet hyödyt ovat moninkertaisia verrattuna väärinkäytöksistä aiheutuneisiin haittoihin.

Tekniikka ei ole rikollista

Lähes kaikkia teknisiä keksintöjä, joilla on oikeutettuja käyttötarkoituksia, voi myös käyttää apuna rikosten tekemisessä. Pelkoja siitä, että tällaista tekniikkaa voidaan käyttää väärin, ei kuitenkaan saisi käyttää perusteena tämän tekniikan kieltämiselle tai rajoittamiselle.

Esimerkkinä tällaisesta tekniikasta ovat salausjärjestelmät (kryptografia). 1980- ja 1990-luvuilla argumentoitiin yleisesti, että rikolliset voivat käyttää tehokkaita salausjärjestelmiä piilottamaan tietoja viranomaisilta. Useat valtiot, kuten Ranska ja Yhdysvallat, yrittivät muun muassa tästä syystä rajoittaa salaustekniikoiden leviämistä lainsäädännöllisin keinoin. Nykyään kuitenkin ymmärretään, että salausjärjestelmät ovat välttämättömiä tietoturvan takaamiseksi, eikä salausjärjestelmien rajoittamisesta juuri enää puhuta.[25]

Muita esimerkkejä tekniikoista, joiden väärinkäyttöä on julkisessa keskustelussa pelätty, ovat anonyymipalvelimet ("anonyymit kunnianloukkaukset"), keskustelupalstat ("pommintekoohjeita") ja vertaisverkot ("tekijänoikeusrikkomuksia"). Kaikilla näillä tekniikoilla on kuitenkin myös runsaasti oikeutettuja käyttötarpeita, joita kaikkia ei vielä välttämättä edes täysin ymmärretä. Siksi mahdollisten kieltojen tulisi kohdistua itse rikolliseen toimintaan, ei tekniikoihin. Eihän postilaatikkojakaan kielletä sillä perusteella, että niihin voi jättää anonyymejä kunnianloukkauskirjeitä, tai ihmisten pääsyä yliopistoihin rajoiteta sillä perusteella, että niissä oppii tekemään pommeja.

Vain rikolliseen toimintaan tulee puuttua

Netin kansainvälisyys ja verkkomainen rakenne tekevät Internetin sisällön tehokkaasta sääntelystä tai hallinnasta melkein mahdottoman urakan. Erilaiset tekniset tai oikeudelliset esteet ja viranomaisten valvontayritykset voidaan kiertää. Esimerkiksi webbisivut, joilla on ei-toivottua sisältöä, voidaan määrätä poistettavaksi, mutta tämä ei estä sisällön ilmestymistä ulkomaisille palvelimille tai sitä, että asiasta kiinnostuneet voivat levittää tietoa vaikkapa sähköpostin välityksellä.[26] Periaatteessa on yhtä helppoa puuttua siihen, kuin mistä ihmiset keskustelevat toreilla ja

[25] Suomikin allekirjoitti vuonna 1998 salausjärjestelmiä rajoittavan Wassenaarin järjestelyn, ks.: http://www.iki.fi/kaip/wassenaar/

[26] Freenet-projekti on esimerkki Internetissä toimivasta järjestelmästä, jossa mielipiteiden ja tietojen julkaisun estäminen tai anonyyminä esiintyvien henkilöllisyyden selvittäminen on tehty tarkoituksella lähes mahdottomaksi,

kodeissa, kuin mistä he keskustelevat Internetissä.

Tämä on havaittu monessa totalitäärisessä valtiossa, joissa viranomaiset ovat menettäneet monopolinsa tietoon, mikä on hyvä asia. Ihmisillä on oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä. Ennakkosensuuri ei kuulu oikeusvaltioon.

Yksityiselämän ja viestinnän suoja on loukkaamaton. Kenellekään tuskin tulisi mieleen ehdottaa, että talonmiesten pitäisi pitää kirjaa kaikista kodeissa käyvistä ihmisistä ja tallettaa tiedot useiksi vuosiksi siltä varalta, että joku näistä ihmisistä syyllistyisi joskus rikokseen. Valitettavasti kun puhutaan Internetistä, tuntuvat tällaiset ehdotukset tunnistamistietojen pakollisesta tallentamisesta olevan arkipäiväisiä. Oikeusvaltioon ei kuulu, että viestintää valvotaan vain siltä varalta, että joku seuratuista syyllistyisi joskus rikokseen.

Ennakkosensuuri tai ihmisten valvominen "varmuuden vuoksi" ei ole hyväksyttävää. Viranomaisten tulee puuttua Internet-viestintään vain, jos heillä on perusteltu syy epäillä rikosta.

Jos tietoja kerätään, niitä käytetään väärin

Jos tietoja kerätään, niin niitä käytetään ennemmin tai myöhemmin väärin, joko viranomaisten tai esimerkiksi teleoperaattorin toimesta. Siksi kaikkea tarpeetonta Internet-viestinnän seurantaa tulee välttää.

Lisäksi on hyvä muistaa, että kerätyt tiedot eivät tule ainoastaan Suomen käyttöön. Cybercrime-sopimuksen[27] perusteella Suomella on velvollisuus antaa virka-apuna tätä informaatiota maihin, joiden oikeusjärjestelmä ei ole läheskään Suomen tasolla, kuten esimerkiksi Albaniaan ja Azerbaidžaniin.

Yksityisyyden suojan piiriin kuuluvia tietoja ei tule luovuttaa vieraille valtioille tai kotimaisille tai kansainvälisille järjestöille, jos tietojen käyttöä ei voida valvoa tehokkaasti parlamentaarisin keinoin. Esimerkki jälkimmäisen kaltaisesta järjestöstä on Tampereen EU-kokouksessa 11.10.1999 perustettu "The Police Chiefs Operational Task Force" (PCOTF). 11.9.2001 jälkeen PCOTF:n tehtävät laajennettiin koskemaan muun muassa tiedustelutietojen vaihtoa. PCOTF ei ole luovuttanut pöytäkirjojaan niitä pyydettäessä, eikä mikään ulkopuolinen taho valvo sen toimintaa.[28]

Samalla tavalla on tärkeää, että Internettiin liittyviä valvonta- ja pakkokeinojärjestelmiä ja lainsäädäntöä valmistellaan avoimesti, ei suljettujen ovien takana.

Puuttumiskeinojen on oltava perusteltuja ja järkevässä suhteessa epäiltyyn rikokseen

Viranomaisten tulee puuttua Internet-viestintään vain, jos on perusteltu syy epäillä rikosta. Silloinkin keinojen on oltava perusteltuja ja järkevässä suhteessa epäiltyyn rikokseen.

Jos todennäköinen seuraus rikoksesta on pitkä vankeustuomio, oikeuttaa se raskaampiin toimiin kuin jos kyse olisi rikoksesta, josta todennäköinen rangaistus on sakkoa. Esimerkiksi tietokoneen kovalevyn sisällön tutkimiseen tai viestinnän seuraamiseen pitää suhtautua samalla tavalla kuin

---

ks.: http://freenetproject.org/

[27] Ks.: http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm
http://www.privacyinternational.org/issues/cybercrime/

[28] Ks. Statewatch analysis no 13, The "war on freedom and democracy" by Tony Bunyan, http://www.statewatch.org/news/2002/sep/analysis13.htm

kotietsintään tai puhelujen kuunteluun.

Tarpeettomat yksityisyyden tai omaisuuden suojan loukkaukset eivät ole hyväksyttäviä. Jos rikollinen materiaali on esimerkiksi julkisella WWW-sivulla, sen sisältö voidaan tallettaa verkon kautta sen sijaan, että todistusaineisto kerätään takavarikoimalla sivua tarjoava palvelin.

Vain rikokseen syylliset ovat vastuussa teosta

Rikoksen tekemisessä voidaan käyttää apuna esimerkiksi Internet-palveluntarjoajan ylläpitämää WWW-palvelinta tai ylläpidettyä keskustelupalstaa.

Ylläpitäjille ei tule asettaa tarpeettomia lisävelvoitteita eikä heitä tule saattaa vastuuseen heidän ylläpitämiään viestintäkanavia käyttäen tehtyihin rikoksiin, joihin he eivät ole itse osallisina.[29] Tällainen vastuu johtaa ennakkosensuuriin: ylläpitäjän kannattaa sensuroida käyttäjiensä viestintää, jos on olemassa pienikin mahdollisuus, että käyttäjä syyllistyisi rikokseen. Tyypillisenä esimerkkinä tästä ovat yksittäisen kuluttajan WWW-kotisivuillaan tai keskustelupalstoilla elinkeinonharjoittajasta esittämät kriittiset väitteet. WWW-palvelimen tai keskustelupalstan ylläpitäjä ei voi mitenkään tietää, ovatko kuluttajan esittämät väitteet perättömiä ja siten ehkä laittomia tai rikollisia.

Toisena esimerkkinä Skientologikultti on kunnostautunut vaatimalla yhdysvaltalaiseen tulkinnanvaraiseen tekijänoikeuslakiin vedoten Internet-palveluntarjoajia (mm. hakukone Googlea) poistamaan palvelimiltaan muiden tuottamaa Skientologien toimintaa arvostelevaa materiaalia ja linkkejä tällaiseen materiaaliin.[30] Skientologikultti tulkitsee tekijänoikeuslakia laajentavasti. Kultin esittämät poistopyynnöt lienevät melkein aina perusteettomia, mutta Internet-palveluntarjoajat yleensä mieluummin suostuvat poistopyyntöihin kuin puolustavat asiakkaidensa oikeuksia kalliissa ja aikaa vievissä oikeudenkäynneissä.[31]

Tämän vuoksi on tärkeää, että vastuu Internettiä käyttäen tehdystä rikoksesta kuuluu yksinomaan rikokseen syyllistyneelle. Lisäksi vastuu sen määrittelemisestä, että onko kyse rikoksesta, kuuluu yksinomaan tuomioistuimelle. Näitä vastuita ei saa miltään osin sälyttää vahingonkorvauksen tai rangaistuksen uhalla esimerkiksi Internet-palveluntarjoajien harteille. Erilaiset “notice and take down“ -menettelyt ovat tästä syystä erittäin ongelmallisia.

Jos ylläpitäjiä velvoitetaan johonkin, on tämän tapahduttava vasta viranomaisen antaman määräyksen jälkeen. Ylläpitäjällä voi toki olla oikeus poistaa materiaali ilman erillistä viranomaisen antamaa määräystäkin, mutta velvoitetta tähän ei pidä olla.

Vain viranomaiset voivat käyttää erioikeuksia

Vain viranomaisilla tulee olla oikeus käyttää pakkokeinojen tai valvonnan kaltaisia erioikeuksia ilman pakkokeinojen tai valvonnan kohteen hyväksyntää.

Yhdysvalloissa on ehdotettu lainsäädäntöä, jonka mukaan tekijänoikeuden haltijoilla olisi oikeus tehdä tietomurto tai syyllistyä tietoliikenteen häirintään, jos heillä on syy epäillä tekijänoikeus-

[29]Ehdotettu laki sananvapauden käyttämisestä joukkoviestinnässä (HE 54/2002 vp) asettaisi keskustelupalstan ylläpitäjän joissain tilanteissa rikosoikeudelliseen ja vahingonkorvausvastuuseen keskustelupalstalla julkaistuista artikkeleista. Ks.: http://www.effi.org/sananvapaus.var

[30]Ks.: http://www.effi.org/tekijanoikeus.var#PALVELUT

[31]Laki tietoyhteiskunnan palvelujen tarjoamisesta sisältää samankaltaisen palveluntarjoajia velvoittavan määräyksen tekijänoikeuksia mahdollisesti rikkovan materiaalin poistamisesta palvelimelta tekijänoikeuden haltijan määräyksestä.

rikkomusta.[32] Tämä ei ole hyväksyttävää.

Internet-palveluntarjoajilla voi olla käyttäjien hyväksymiin käyttöehtoihin perustuva oikeus tutkia väärinkäytöksiä ja puuttua niihin. On kuitenkin tärkeää, että tällaiset käyttöehdot on kirjoitettu selkeästi ja ymmärrettävästi ja että palveluntarjoajien suorittama valvonta on perusteltua ja järkevässä suhteessa suojeltavaan etuun nähden ja että perusoikeuksia, kuten henkilötietojen ja yksityisyyden suojaa, kunnioitetaan.

Valistaminen ja itsesäätely ovat tehokkaita keinoja

Internetin rikollinen sisältö koskettaa tavallista käyttäjää usein esimerkiksi sähköpostin liitetiedostoissa leviävien haittaohjelmien muodossa. Rikollisen sisällön lisäksi Internetistä on saatavana laillista materiaalia, kuten pornografiaa, joka ei kuitenkaan sovellu esimerkiksi lasten nähtäväksi. Paras apu näihin ongelmiin on valistustyö. Muillakin elämänalueilla on hyvä tietää, miten kannattaa toimia ja miten ei. Tiettyjä kaupunginosia kannattaa välttää ja katua ylittäessä on oltava varovainen. Vastaavia kansalaistaitoja tarvitaan myös Internetissä: kaikkia liitetiedostoja ei kannata avata, käyttöjärjestelmän tietoturvapäivitykset tulee asentaa säännöllisesti ja joillekin sivustoille ei kannata mennä.

Samaten ihmisten tulisi ymmärtää, että viranomaiset eivät voi eikä heidän pidä valvoa kaikkea toimintaa ja estää kaikkia rikoksia ennalta. Kuten muillakin elämänaloilla, jos ihmiset havaitsevat, että on tapahtunut rikos, voivat he ilmoittaa asiasta viranomaisille.

Tehokas vaikutustapa tietoturvauhkiin on CERT-toiminta[33] ja tietoturvauhkista ja ohjelmien haavoittuvuuksista tiedottaminen mahdollisimman tehokkaasti ja avoimesti. Valtiovallan tulisi osaltaan rohkaista tällaista avointa tietojen vaihtoa ja tietoturvaongelmista ja Internetin ongelmista käytävää keskustelua ja vapaaehtoisuuteen perustuvien toimintamallien kehittämistä.

Rikollisia ei aina saada kiinni

Internet tarjoaa valtavia mahdollisuuksia. Internet tarjoaa myös mahdollisuuksia laajamittaiseen sensuuriin ja valvontaan. Euroopan unionissakin on ehdotettu Internet-liikenteen tallentamista useiksi vuosiksi.[34] Tämä ei kuulu oikeusvaltioon.

Koska talonmiehet eivät pidä kirjaa kodeissa käyvistä ihmisistä, ei todistusaineistoa kerry niin paljon kuin poliisivaltiossa olisi mahdollista. Oikeusistuimet toimivat sillä periaatteella, että on parempi, että kymmenen syyllistä päästetään vapaaksi kuin että yksi syytön tuomitaan. Rikollisia ei siis aina saada kiinni, Internetissäkään.

Yhteenveto

Internetissä olevaan rikolliseen sisältöön tulee puuttua samoin periaattein kuin muillakin elämänaloilla. Ennakkosensuuri tai tunnistamistietojen pakollinen tallentaminen vain varmuuden vuoksi tai siksi, että viranomaisille ei ole annettu tarpeeksi voimavaroja Internettiin liittyvien rikosten selvittämiseksi, ei ole hyväksyttävää. Muillakaan elämänaloilla tietoja ei tallenneta vuo-

[32] "The Berman P2P Bill: Vigilantism Unbound", EFF, http://www.eff.org/IP/P2P/20020802_eff_berman_p2p_bill.html

[33] Viestintävirasto, Tietoturvaloukkausten havainnointi ja ratkaisu (CERT), http://www.ficora.fi/suomi/tietoturva/cert.htm

[34] Sähköisen viestinnän tietosuojadirektiivi (2002/58/EY) oikeuttaa jäsenvaltiot keräämään ja tallettamaan teletunnistamistietoja. Suomi on äskettäin ehdottanut EU:ssa kaikkien teletunnistetietojen pakollista tallentamista kahdeksi vuodeksi, ks.: http://www.effi.org/lehdistotiedote-2002-11-25.html

siksi vain siltä varalta, että joku syyllistyisi joskus rikokseen.

Vain viranomaisilla tulee olla oikeus käyttää erioikeuksia rikolliseen sisältöön puuttumiseen. Puuttumiskeinojen tulee kuitenkin olla perusteltuja ja järkevässä suhteessa epäiltyyn rikokseen nähden.

Helsingissä 11.12.2002

Kai Puolamäki

Kiitokset

Sain tämän lausunnon kirjoittamista varten lukuisia hyödyllisiä ehdotuksia sähköpostitse ja EF-FIn keskusteluryhmässä (finet.toiminta.effi), joista kiitokset.

Liite 5 Euroopan parlamentin jäsen Matti Wuoren lausunto

Helsinki 5.12.2002

Keskusrikospoliisi
Rikostarkastaja Ari Määttä
PL 285
01301 Vantaa

Sisäasianministeriön internet-työryhmän pyytämä lausunto

Otsikkoasiassa pyydettynä lausuntona esitän kohteliaimmin seuraavaa:

Lausuntopyynnössä 6.11.2002 (*liitteenä 1.*) esitetyt kysymykset kietoutuvat siinä määrin temaattisesti yhteen, että vastaan niihin erittelemättä niitä omiksi jaksoikseen.

Euroopan unioni ei ole Euroopan neuvoston eikä sen ihmisoikeussopimuksen jäsen. Tästä huolimatta unionin perussopimuksissa ja lukuisissa muissa keskeisissä asiakirjoissa tähdennetään ihmisoikeuksien ja ihmisoikeusmääräysten perustavaa merkitystä sekä yhteisön arvopohjana että sitä poliittisesti ohjaavana normistona. Niin sanotut Kööpenhaminan kriteerit ja niiden myötä syntynyt käytäntö osoittavat, että ihmisoikeusmääräykset ovat osa EU:n jäsenyysvaatimuksiin kuuluvaa *acquis communautaire*a ja että ne ovat selvästi sitovampia kuin vain eettiset ohjeet (ns. *acquis éthique*). Tämä näkökohta korostuu unionin hyväksyttyä Nizzan huippukokouksessaan erityisen perusoikeuskirjan (*Charter of Fundamental Rights*), jossa Euroopan ihmisoikeussopimuksen normeja on edelleen kehitelty ja laajennettu. Vaikka peruskirjalla ei vielä ole oikeudellista sitovuutta, se on jo nyt merkittävä oikeuslähde, jota EY-tuomioistuin voi soveltaa tulevassa oikeuskäytännössään.

Euroopan ihmisoikeussopimuksen 10 artiklan mukaan sananvapautta voidaan rajoittaa vain, mikäli se on *välttämätöntä demokraattisessa yhteiskunnassa* (ks. myös YK:n kansalaisoikeuksia ja poliittisia oikeuksia koskevan yleissopimuksen eli ns.KP-sopimuksen 19 artikla). Kansanvaltaiseen järjestelmään kuuluu samalla, että yleisöllä on mahdollisimman vapaa ja esteetön oikeus tiedonsaantiin silloinkin, kun informaatio on esimerkiksi viranomaisten kannalta epämiellyttävää.

Internetissä leviävän aineiston rajoittamista tai valvontaa koskevat suoranaiset normit puuttuvat EU:n tasolla, vaikka niitä ollaan eri jäsenmaissa erivaiheisesti valmistelemassa (ks. kuitenkin jäljempänä

s. 3 mainittu puitepäätös). Suomessa tämä liittyy **painovapauslain-säädännön** kokonaisuudistukseen ja siihen sisältyviin säännösehdotuksiin, jotka koskevat muun ohella vastuuta sähköisesti ja tietoverkkojen kautta levitettävien viestien sisällöstä ja oikeudellisia mahdollisuuksia vaikuttaa siihen.

Kun selvittely- ja valmistelutyö on niin EU:ssa kuin kotimaassakin meneillään, en pidä suotavana että joidenkin Myyrmäen pommi-iskun kaltaisten yksittäistapausten johdosta ryhdyttäisiin sellaiseen *kansalliseen erillis- ja erityissääntelyyn ad hoc*, joka vääjäämättä vaikuttaisi tämän alueen kannalta keskeisten perus- ja ihmisoikeuksien, kuten sananvapauden tai yksityisyyden toteutumiseen. Käsillä on herkkä ja monitahoinen ongelmavyyhti, joka jo asiaan liittyvien teknisten näkökohtien vuoksi – kun kysymyksessä on maailmanlaajuinen, globaali viestintämuoto, yhden valtion toimet internetin käytön rajoittamiseksi tai valvomiseksi oman jurisdiktionsa puitteissa jäävät käytännössä helposti tehottomiksi tai tarkoituksettomiksi – on syytä pyrkiä ratkaisemaan kokonaisvaltaisesti ja laajan kansallisen ja kansainvälisen yhteistyön kautta. Näin siitä huolimatta, että esimerkiksi EU:n niin sanottuun terrorismin vastaiseen pakettiin kuuluu myös velvollisuus kaiken viestinnän tallentamisesta 12 ja jopa 24 kuukaudeksi.

Preventiiviset keinot tulevat viestinnän luonteen vuoksi ylipäänsä harvoin kysymykseen, ellei olla valmiita hyväksymään Kiinan Kansantasavallan ja eräiden muiden valtioiden omaksumaa voimakasta sananvapauden tukahduttamista. Myös *repressiivisten* keinojen käyttömahdollisuudet poikkeavat perinteisen viestinnän kentästä (vaikka Suomessa on ainakin yhdessä tapauksessa, *sjä > Rantalainen ym.*, katsottu, että vastaava ohjelmatoimittaja voi joutua radiovastuulain mukaiseen rangaistus- ja korvausvastuuseen suorassakin televisiolähetyksessä esitettyjen lausumien johdosta).

Laatimassani ja Euroopan parlamentin täysistunnossaan 5.7.2001 hyväksymässä mietinnössä ’Ihmisoikeudet maailmassa ja EU:n politiikka 2001’ (*liitteenä 2.*), jonka keskeisenä painopisteenä on sanan- ja ilmaisuvapauden käyttö, on käsitelty myös uusmedian ja sähköisten viestintäkanavien yleistymisen luomia ongelmia. Mietinnön esipuheessa (*s. 8*) sekä perustelujen internetiä koskevassa jaksossa (*s. 67-69*) on kiinnitetty huomiota tarpeeseen löytää yhä pidäkkeettömämmän ja rajattomamman viestinnän ja informaation vaihdon oloissa oikea ja tasapainoinen suhde sinänsä legitiimien valvonnan tarpeiden, internet-rikollisuuden torjunnan ja yksilön henkilökohtaisen suojan sekä mahdollisimman esteettömän mielipiteen ja tiedonvälityksen vapauden välille. Lähtökohdaksi on otettu se, että epäselvissä tapauksissa olisi päädyttävä sananvapautta vahvistavien vaihtoehtojen kannalle. Perusteluissa katsotaan (s. 68), että monet uusista ongelmista voidaan ratkaista soveltamalla harkiten nykyisiä normeja, ja että yleisesti ottaen teknologiset ratkaisut ja innovaatiot ovat suositeltavampia kuin lainsäädäntötoimet tai muut rajoittavat toimenpiteet. Julkilausumaosassa (**67.-69**, *s. 31*) korostetaan muun ohella tiedonsaannin ja –välityksen vapautta, puuttumattomuutta niiden toteutumiseen sekä oikeutta käyttää sähköpostia ja internetiä vapaasti ja ilman sensuuria. Lisäksi parlamentti painottaa erikseen (**70.**) lähdesuojan merkitystä.

Euroopan unionilla on ollut nelivuotinen internetin käyttöturvallisuuden parantamista koskeva toimintasuunnitelma, jonka yhteydessä rahoitetaan toimia laittoman ja haitallisen sisällön torjumiseksi. Nykyinen toiminta-suunnitelma päättyy kuluvan vuoden lopussa. Toimintasuunnitelmaa ehdotetaan jatkettavaksi toisella vaiheella, joka kestäisi kaksi vuotta. Viittaan komission tiedonantoon toimintasuunnitelman jatkamisesta (http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=FI&numdoc=52002SC0152&model=quichett).

Toimintasuunnitelmassa viitataan sekä laittomaan että ns. haitalliseen aineistoon. Toimintalinjojen pääkohdat ovat:

1) Turvallisemman käyttöympäristön luominen
2) Suodatin- ja luokitusjärjestelmän kehittäminen
3) Tiedotustoiminnan edistäminen
4) Tukitoimet

Muut linjat koskevat ennen muuta ei-oikeudellisia toimia, mutta tukitoimien toimintalinjassa oli tarkoitus tutkia internetin käytön tai sisällön esiin nostamia oikeudellisia ongelmia. Euroopan parlamentin kansalaisvapauksien valiokunnassa on ollut käsittelyssä William Newton Dunnin mietintö toimintasuunnitelman jatkamisesta. Siinä esitetyn tilannearvion mukaan tällaisten tutkimusten suhteen ei ole toistaiseksi juuri ryhdytty käytännön toimiin. Komission uusimmassa tiedonannossa hanketta oikeudellisen selvityksen toteuttamiseksi ei lainkaan mainita. (Newton Dunnin raportti, jonka käsittely EP:ssa on edelleen kesken, löytyy kokonaisuudessaan osoitteesta http://www.europarl.ep.ec/meetdocs/committees/libe/20020617/470758FI.pdf).

EU:n komissio on kaiken kaikkiaan työskennellyt rikollisen internet-materiaalin levittämisen estämiseksi vuodesta 1996. Mahdollisuuksista saada aikaan yhteistä lainsäädäntöä on erilaisia arvioita. Toistaiseksi pidetään tärkeimpänä panostaa tietoisuuden tason nostamiseen ja muun muassa tiedottamiseen sekä teknisten estolaitteiden kehittämiseen.

Varsinaista EU-lainsäädäntöä on lähinnä sähköistä kaupankäyntiä (e-commerce) koskevassa direktiivissä (internet-palvelujen tarjoajien vastuu) sekä ministerineuvoston puitepäätöksessä lapsipornon levittämisen ehkäisemisestä.

Eräät niin EU:ssa kuin kansallisestikin kaavaillut projektit näyttäisivät tyrehtyneen pääasiassa rahoituksen puutteeseen; näin esimerkiksi eSafe – hankkeessa, jossa on kysymys laittoman materiaalin levittämisen ehkäisemisestä. Tiedotussuunnitelmat ovat kärsineet koordinaation ja rahoituksen puutteesta, minkä vuoksi komission Safer Internet Action Plan – toimintasuunnitelman puitteissa on toivottu, että kansalliset viranomaiset – Suomessa ennen muuta sisäasiain-, oikeus-, liikenne- ja opetusministeriöt – tiivistäisivät yhteistyötään. Myös eräät kansalaisjärjestöt ovat olleet aktiivisia. Suomessa esimerkiksi Pelastakaa Lapset ry:llä on erityinen lapsi-pornoa seuraava Nettivihje-kuuma linja (www.pela.fi/nettivihje), jonka myös suurempi yleisö on ilmeisesti alkanut löytää (lisätietoja tästä suvi.kuikka@pela.fi). Hanke perustuu osaltaan yhteistyöhön internet-operaattorien, Helsingin kaupungin, rikostorjunta- ja –tutkintaviran-

omaisten kesken. Ongelmana tässäkin on se, että useimmat porno-sivut toimivat Yhdysvalloissa, Suomea lähimmät varsinkin Venäjältä ja Virosta käsin.

Euroopan parlamentissa on lisäksi parhaillaan käsittelyssä henkilö-tietojen käsittelyä ja yksityisyyden suojaa sähköisen viestinnän alalla koskeva direktiivi, jota käsitellään Marco Cappaton laatimassa mietinnössä (15396/2/2001 – C5-0035/2002 – 2000/0189(COD)), joka on hyväksytty parlamentin ensimmäisessä lukemisessa 14.5. 2002. Kun se valaisee osaltaan useista nyt käsiteltävän viestinnän kannalta olennaisista kysymyksistä käytävän keskustelun nykyvaihetta, oheistan mietinnön tähän kokonaisuudessaan (*liite 3.*).

Olen mielelläni valmis antamaan lisätietoja ja –selvityksiä tarvittaessa.

Matti Wuori
asianajaja, Euroopan parlamentin jäsen
MWuori@europarl.eu.int & matti.wuori@mattiwuori.fi