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.[1]

Muita esimerkkejä tekniikoista, joiden väärinkäyttöä on julkisessa keskustelussa pelätty, ovat anonyymipalvelimet (”anonyymit kunnianloukkaukset”), keskustelupalstat (”pomminteko-ohjeita”) 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.[2] Periaatteessa on yhtä helppoa puuttua siihen, kuin mistä ihmiset keskustelevat toreilla ja 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.

---

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

2 Freenet-projekti on esimerkki Internetissä toimivasta järjestelmästä, jossa mielipiteiden ja tietojen julkaisun estäminen tai anonyyminä esiintyvien henkilöllisyyden selvittäminen on tehty tarkoituksella lähes mahdottomaksi, ks.: http://freenetproject.org/

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[3] 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.[4]

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 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

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

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

ylläpitämiään viestintäkanavia käyttäen tehtyihin rikoksiin, joihin he eivät ole itse osallisina.[5] 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.[6] 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.[7]

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 tekijänoikeusrikkomusta.[8] 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

5 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

6 Ks.: http://www.effi.org/tekijanoikeus.var#PALVELUT

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

8 ”The Berman P2P Bill: Vigilantism Unbound”, EFF, http://www.eff.org/IP/P2P/20020802_eff_berman_p2p_bill.html

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[9] 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.[10] 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 vuosiksi 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 EFFIn keskusteluryhmässä (finet.toiminta.effi), joista kiitokset.

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

10 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