

**Lausunto luonnoksesta hallituksen esitykseksi
laiksi sähköisen viestinnän
tietosuojalain muuttamisesta**

17.8.2007

17.08.09

Electronic Frontier Finland ry

www.EFFI.org

1. Yleistä

Electronic Frontier Finland ry:n näkökulmasta nyt käsittelyssä olevalla esityksellä linjataan merkittävästi sitä, miten tavallisia verkkokäyttäjiä voidaan jatkossa valvoa. Vaikka esityksessä koitetaankin varsin tyylikkäästi ”kehystää” esitys koskemaan vain yritystoimintaa, tosiasiaa sen vaikutukset tuntuisivat yhtäläisesti tai jopa merkittävämminkin myös muissa yhteisötilaajissa kuten kouluissa, yliopistoissa tai kirjastoissa. Esimerkiksi kouluissa oppilaiden suojana ei ole yhteistoimintamenettelyn kaltaisia väärinkäytöksiltä suojaavia institutionaalisia suojaverkkoja. Ennen kuin esitys on valmis lähetettäväksi eduskuntaan, merkittävää lisäanalyysiä (ja asianosaisten kuulemisia) tarvittaisiinkin tästä näkökulmasta. Emme ole valitettavasti toiveikkaita sen suhteen, että näin tapahtuisi todellisuudessa.

EFFIn näkökulmasta selkeästi merkittävin uudistus esityksessä on 13 a §:n säännökset luvattoman käytön havaitsemiseksi ja lopettamiseksi. Sen sijaan julkisuudessa eniten olleen 13 b §:n merkitys jää järjestön arvion mukaan pieneksi - varsinkin kun 13 a §:n avulla voidaan toteuttaa käytännössä 13 b §:n mahdollistama valvonta ilman jälkimmäisestä pykälästä löytyviä ylimääräisiä rajoituksia.

Positiivista esityksessä on EFFIn näkökulmasta idea teknisten tietoturva-toimenpiteiden ensisijaisuudesta. Käytännössä kaikki yleisimmät tietoturvaongelmat voidaan ratkaista käyttäjän tietojärjestelmän käyttöä rajaavilla toimenpiteillä. Tästä herää kuitenkin väkisin kysymys – jos kerran hyvin hoidetussa teknisessä ympäristössä käytännössä kaikki ongelmat voidaan ratkaista etukäteisillä toimenpiteillä (esimerkiksi estämällä ylimääräisten ohjelmien tai palveluiden asentaminen tietokoneisiin, mikä on triviaalia) ja näiden toimenpiteiden käyttäminen on nimenomainen edellytys valvonnalle, valvottavia ongelmia ei kai pitäisi voida edes syntyä? Sama voidaan kääntää myös toisin päin eli väärinkäytöksiä voi ilmetä lähinnä niissä tilanteissa, joissa tietoturvaa ei ole hoidettu asiallisesti. Kyseessä on fundamentaali ristiriita, mihin esitys ei ota mitään kantaa.

EFFIn näkemyksen mukaan esitys ei voi mitenkään nyky muodossaan olla perustuslain mukainen, koska siitä murretaan hyvin laajasti viestinnän luottamuksellisuuden suojaa hyvin epämääräisin perustein. EFFIä paremmat perustuslain asiantuntijat ovat olleet laajasti tätä mieltä ja heidän analyysinsä ei ole edes vielä koskettanut järjestön mielestä esityksen ydinongelmaa, jota käsitellään

seuraavaksi. EFFI ei tule sen sijaan keskittymään tässä lausunnossa enää 13 b §:n ongelmiin, koska ko. kohtaa on tarpeeksi kritisoitu julkisuudessa.

2. 13 a § - yleisen verkkovalvonnan oikeutuslause?

EFFIn näkökulmasta ehdotuksen ehdottomasti pahin ongelma on 13 a §:n aivan liian avoimeksi kirjoitettu luonne. Näkemyksemme mukaan seuraavat kaksi skenaariota olisivatkin mahdollisia pykälän avulla:

Skenaario 1.

Teleoperaattori S:n toiminnasta on vuotanut inhottavia yksityiskohtia tietoja tiedotusvälineille. Yhtiön moraalitilanne on huonolla tolalla johdon pätemättömyyden vuoksi. Kriittistä suuttunut toimitusjohtaja määrää tietohallintopäällikön lopettamaan vuodot ja selvittämään niiden takana olevat henkilöt. Tietohallintopäällikkö ryhtyy toimeen; yhtiön verkkokäyttösopimus päivitetään kieltämään yhteydenotot tiedotusvälineisiin ja automaattinen hakutoiminto asetetaan valvomaan kieltoa. Tarvittava merkittävä haitta syntyy vuotojen seurauksena laskeneesta yhtiön pörssikurssista. Vuotajan henkilöllisyys paljastuu tiedotusvälineisiin menneiden sähköpostien manuaalisella tutkimisella ja yhtiö haastaa hänet oikeuteen.

Skenaario 2.

Lukio X:n opetukselle kriittinen videosarja on alkanut ilmestyä YouTubessa. Asiasta suuttunut koulun rehtori määrää koulun tietoturvasta vastaavan opettaja X:n tekemään tilaneelle jotain. Opettaja päivittää verkkokäyttösopimuksen kieltämään videopalveluiden käytön koulusta ja asettaa automaattisen hakutoiminnon valvomaan kieltoa. Tarvittava merkittävä haitta syntyy luonnollisesti kohonneesta verkkokäytöstä ja koulun heikentyneestä maineesta, joka on vähentämässä oppilasmääriä. Kohta oppilas X jääkin kiinni lähetettyään uusimman ohjelmansa hyödyntäen koulun nopeaa verkkoyhteyttä. X:llä annetaan kirjallinen huomautus ja hän saa huomata keskiarvonsa putoavan yllättävästi kiristyneen arvostelun seurauksena.

2.1 Merkittävän haitan määritelmä

Ministeriö on puolustanut 13 a §:ää sillä, että se rajautuu ainoastaan huomattavaan haittaan ja on näin riittävän tarkkarajainen ollakseen perustuslain mukainen. Esityksessä ei kuitenkaan määritellä mitenkään lain tasolla, mitä tarkoittaa ”on omiaan aiheuttamaan merkittävää haittaa tai vahinkoa.” Sen sijaan yksityiskohtaisissa perusteluissa asiasta todetaan seuraavaa:

”Säännöksessä tarkoitettua merkittävää haittaa voisi muun muassa olla lisääntyneet kustannukset tai sellainen lisääntynyt tiedonsiirtokapasiteetin käyttö, tietoturvauhka, tai muu vastaava syy, joka vaarantaa, vaikeuttaa tai hidastaa viestintäverkon tai palvelujen käyttöä niille suunniteltuun käyttötarkoitukseen.”

Kyseinen esimerkkilistaus on niin laaja, että vähääkään mielikuvitusta omaava henkilö (puhumattakaan juristista) kykenee jo sen avulla perustelemaan käytännössä aina, miksi valvonnan aloittamiselle on riittävät perusteet. Perustuslain suojaama viestinnän luottamuksellisuus tunnistetietojen osalta voitaisiin siis käytännössä murtaa pykälän avulla aina tarpeen mukaan.

Tilanteen korjaamiseksi nähdäksemme ainoa keino olisi merkittävän haitan käsitteestä luopuminen niin, että sen tilalle tulisi *suljettu lista viestintärikoksista*, jotka ovat jo valmiiksi sanktioituja rikosoikeudellisesti vähintään vankeusrangaistuksella ja jotka *kohdistuvat valvonnan suorittavaan yritykseen*. Muilta osin tutkintaoikeus tulee säilyttää pelkästään poliisilla. Pelkkä käyttöehtojen rikkominen ei missään tapauksessa saisi oikeuttaa viestinnän luottamuksellisuuden murtamista.

3. Tietosuojavaltuutetun resurssit

Esityksessä ollaan jälleen kerran lisäämässä tietosuojavaltuutetun velvollisuuksia lisäämättä kuitenkaan tarvittavia resursseja:

”Ehdotus ei lisäisi näiden valvontaelinten tehtäviä tavalla, jolla olisi vaikutuksia valtiontalouteen, koska valvovat viranomaiset voivat kohdentaa resurssejaan jossain

määrin uudelleen.”

Toisin sanoen ehdotuksen mukaan tietosuojavaltuutetun tulisi siirtää ”jossain määrin uudestaan” resursseja, joita ei tosiasiassa ole olemassa. Ehdotuksesta käy lisäksi ilmi, että valvonta olisi lähinnä tarkoitus toteuttaa raportointivelvollisuuden kautta ja pistokokeita ei olisi tarkoitus tehdä. Näin yhteisötilaaja voisi välttää käytännössä valvonnan jättämällä tekemättä valvontailmoitukset kaikissa muista tapauksista kuin niistä, joissa löytyi jotain niin kriittistä, että tapaukselle tarvitaan ex post -oikeutus. EFFIn mielestä olisikin suoraan sanottuna parempi, että esityksessä tunnustettaisiin rehellisesti, että sen valvonta tulee tapahtumaan vain jälkikäteisesti julkisuuteen vuotavien tapausten kautta.

Electronic Frontier Finland ry:n puolesta,

Ville Oksanen, varapuheenjohtaja