

Suomen Microsoft osajakumppaneiden yhdistys ry:n (IAMCP Finland) lausunto tiedonhankintalakiyöryhmän mietintöön

Puolustusministeriö on pyytänyt lausuntoja tiedonhankintalakiyöryhmän mietinnöstä ”Suomalaisen tiedustelulainsäädännön suuntaviivoja” 9.2.2015 päivätyllä lausuntopyyntöllä. Lausuntopyyntöissä pyydetään erityisesti kommentoimaan kehittämissuhteita ja johtopäätöksiä (luvut 6 ja 7) ja ehdotusten vaikutuksia lausunnonantajan toimintaan ja toimialalla.

IAMCP Finland on Microsoftin kumppaniverkoston yhteistyöfoorumi Suomessa.

1 Mietinnössä esitetyt kehittämissuhteet

Mietinnössä esitetään kolme tiedonhankinnan kehittämissuhteita: tietoliikennetiedustelu, ulkomaan henkilötiedustelu ja ulkomaan tietojärjestelmätiedustelu.

Tietoliikennetiedustelulla mietinnössä tarkoitetaan Suomen rajat ylittävien tietoliikenneyhteyksien kautta tapahtuvan viestinnän automaattista koneellista seuranta- ja suodattamista ja tiedusteluviranomaisen tekemää suodatetun tiedon käsittelyä ja analysointia kansallista turvallisuutta uhkaavia toimijoita ja toimintaa koskevan tiedon hankkimiseksi. Tarkoituksena olisi ylimmän valtiojohtoon päätöksenteon tukeminen välttämättömällä tilannekuvatiedolla.

Tietoliikennetiedustelu-termin käyttäminen tällaisesta toiminnasta on omiaan johtamaan lukijaa harhaan. Sen vuoksi esitämme termin korvaamisesta paremmin asiaa kuvaavalla **Viestintätiedustelu**-termillä, jota myös käytämme tässä lausunnossa.

Ulkomaan henkilötiedustelulla mietinnössä tarkoitetaan henkilökohtaiseen kanssakäymiseen tai henkilön tai muun kohteen henkilökohtaiseen havainnointiin perustuvaa tiedonhankintaa.

Ulkomaan tietojärjestelmätiedustelulla mietinnössä tarkoitetaan ulkomaisissa tietojärjestelmissä käsiteltävän tiedon hankintaa tietoteknisin menetelmin eli aktiivista tunkeutumista tietojärjestelmiin ja tietojen keräämistä järjestelmistä. Mietinnössä on rajattu aktiiviset hyökkäystoimet kuten tietojärjestelmien vahingoittaminen, tietojen tuhoaminen tai muuttaminen määritelmän ulkopuolelle.

2 Yleistä

Teknologian kehitys ja uudet innovaatiot mahdollistavat yhä paremmin ajasta ja paikasta riippumattoman viestinnän. Kehitys parantaa ratkaisevasti tuottavuutta, luo uusia työpaikkoja ja edesauttaa talouden kasvua. Kasvu toteutuu kuitenkin vain, jos huolehdimme siitä, että viestintäyhteydet paranevat, datan esteetön liikkuvuus rajojen yli mahdollistetaan ja pilviteknologian hyödyt otetaan käyttöön. Tämä on kuitenkin mahdollista vain käyttäjien luottaessa siihen, että tietoyhteiskunnan palvelut ovat toimintavarmoja ja ne suojaavat käyttäjien perusoikeuksia kuten oikeutta yksityiseen viestintään riittävällä tavalla. IAMCP Finlandin jäsenrytykset ovat keskeisinä toimijoina luomassa palveluita, joihin kansalaisten on voitava luottaa.

Digitaalinen talous ulottuu viestintä- ja tuottavuuspalveluiden ulkopuolelle kaikkialle teollisuuteen ja palveluihin. Digitaalisuuden täysimääräinen hyödyntäminen kaikilla teollisuuden aloilla on avain suomalaisen teollisuuden kilpailukykyyn ja tuottavuuden parantamisessa sekä talouden kasvun edistämiseksi.

Digitalisaatio on muuttanut myös Suomeen ja suomalaisiin kohdistuvien uhkien luonnetta. Verkkorikollisuus on globaalia ja monet valtiolliset toimijat operoivat tietoverkoissa valtioiden rajoista välittämättä.

Tällaisessa jatkuvasti muuttuvassa toimintaympäristössä on entistäkin tärkeämpää, että jokainen toimija vastaa osaltaan turvallisuuden toteuttamisesta. Turvallisuutta ei voi ulkoistaa. Yritysten ja viranomaisten on varmistettava hallussaan olevien tietojen ja tietojärjestelmien riittävä suojaus ja käytettävä palveluiden toteuttamiseen luotettavia palveluntarjoajia. Toimijoilla on oltava riittävät valtuudet tehtäviensä hoitamiseen. Yritysten ja viranomaisten on toimittava yhteistyössä yhteisen tilannekuvan muodostamiseksi. Tilannekuvan on oltava kaikkien toimijoiden käytettävissä. Viranomaisten on kerrottava yrityksille viranomaisten tietoon saadut yrityksiin kohdistuvat uhat.

Mietinnössä on käsitelty useita eri asiakokonaisuuksia, jotka liittyvät toisiinsa varsin löyhästi. Esitetyt jatkotoimenpiteet on kuvattu varsin yleisluontoisesti, minkä vuoksi mahdollinen jatkovalmistelu voi johtaa lopputulokseen, jota mietinnössä ei ole kuvattu.

Pidämme hyvänä sitä, että työryhmä on tehnyt työtään varsin avoimesti ja kuullut laajasti eri osapuolia. Mahdollisessa jatkovalmistelussa tulisi valmistelun avoimuutta vielä parantaa ja varmistaa kaikkien osapuolien mahdollisuus osallistua työskentelyyn haluamassaan laajuudessa.

3 Tiedustelulainsäädännön jatkovalmistelusta

Jatkotyössä on syytä arvioida tiedustelulainsäädännön kehittämistarpeita. Mahdollisen lainsäädännön on oltava mahdollisimman selväsanaista ja yksitulkintaista, jotta toimintaympäristö säilyy ennustettavana sekä Suomessa jo toimivien että investointipäätöksiä harkitsevien yritysten kannalta. Mietinnössä esitetyt lainsäädäntöhankkeet tulisi valmistella erikseen kussakin vastuuministeriössä.

Valmistelussa tulee ottaa huomioon tiedustelu- ja viranomaistoiminnan kehittämistä tietoverkoissa ohjaavat yleiset periaatteet. Periaatteet on lyhyesti esitetty luvussa 4 ja laajemmin sivustolla <http://reformgovernmentsurveillance.com>.

3.1 Viestintätiedustelu

Viestintätiedustelun mahdollinen tarve tulee selvittää yleisellä tasolla osana tiedustelulainsäädännön valmistelutyötä. Viestintätiedustelua koskevan erityislain valmistelu voitaneen aloittaa tiedustelulainsäädännön käsittelyn jälkeen, mikäli toiminnan tarpeellisuudesta, hyödyistä ja kustannuksista sekä vaikuttavuudesta saavutetaan riittävän laaja yhteinen objektiivinen faktoihin perustuva näkemys.

Erityisesti tästä syystä yritysten osallistuminen jatkotyöskentelyyn on tärkeää.

Mikäli viestintätiedustelua koskevaa lainsäädäntöä aletaan jossain tulevaisuuden hetkessä valmistella, valmistelussa tulee pitää ohjaavina periaatteina mietinnössä ansiokkaasti esitetyt yritysten ja organisaatioiden toimintaa koskevat seikat täydennettyinä seuraavasti:

- Ohjelmistovalmistajia ja palveluntuottajia ei tule velvoittaa toteuttamaan ohjelmistoihin tai palveluihin takaportteja
- Organisaatioita ei tule velvoittaa luovuttamaan salausavaimia viranomaisille tai auttamaan viranomaisia salausten purkamisessa. Lainsäädäntöön ei saa sisällyttää salausmenetelmien tai muiden viestinnän luottamuksellisuutta turvaavien ja viestinnän osapuolia suojaavien menetelmien käyttökieltoja tai käyttörajoituksia.
- Viestintätiedustelun kohteena saa olla vain teleyritysten julkisten verkkojen rajat ylittävä liikenne. Viestintätiedustelua ei tule ulottaa organisaatioiden yksinomaisessa käytössä oleviin tietoliikenneyhteyksiin. Esittämämme rajoituksen tavoitteena on poistaa datakeskusinvestointeja

harkitsevilta toimijoilta viestintätiedustelun valmisteluun liittyvä epävarmuustekijä, joka on todennäköisesti pitkäkestoinen mahdolliseen lain valmisteluun liittyvien perustuslaillisten näkökohtien vuoksi.

- Tiedusteluviranomaisten tulee vastata täysimääräisesti mahdollisen viestintätiedustelun kustannuksista. Kustannuksia ei osittainkaan saa säilyttää yritysten kannettaviksi

Tiedustelulainsäädännön valmistelutyössä on tarkoin pidettävä mielessä, että toiminnan tarkoituksena on valtio johdon päätöksentekokyvyn mahdollistaminen. Tämän vuoksi olisikin harkittava sitä, että myös toiminta olisi tiukasti valtio johdon ohjauksessa. Tiedustelutoiminta rikkoo hyvinkin helposti muiden maiden lainsäädäntöä. Toimenpiteiden käynnistäminen vaatii poliittista harkintaa. Ratkaisut voitaisiin tehdä esimerkiksi ulko- ja turvallisuuspoliittisessa valiokunnassa tapauskohtaisesti.

3.2 Ulkomaan tietojärjestelmätiedustelu

Mahdolliseen ulkomaan tietojärjestelmätiedusteluun liittyy merkittävä periaatteellinen asia. Suomen ratifioimissa kansainvälisissä sopimuksissa tietojärjestelmiin tunkeutuminen on kriminalisoitu ja teot on määritelty kansallisessa lainsäädännössä rangaistaviksi.

Voidaan aiheellisesti kysyä, kasvaisiko kansalaisten ja yritysten luottamusta verkkoon ja sen palveluihin, jos viranomaisille sallittaisiin tällainen toiminta.

Suomi on toimillaan kansainvälisessä yhteisössä rakentanut menestyksekkäästi mainetta yhteistyön rakentajana ja rauhansovittelijana. Tätä taustaa vasten olisikin luontevampaa, että Suomi ottaisi kansainvälisillä foorumeilla aktiivisen roolin tietojärjestelmien turvallisuuden edistämässä ja edistäisi laajasti hyväksytyjen oikeushyvien turvaamista digitaalisessa toimintaympäristössä.

Suomi voisi toimia aktiivisesti erityisesti kansainväliseen oikeusapumekanismiin liittyvien toimintatapojen uudistamisessa ja mekanismin siirtämisessä globaalisti digiaikaan sekä valtioiden lainsäädäntöjen eroavuuksista johtuvien ristiriitojen ratkaisemiseen kykenevien foorumien luomisessa.

3.3 Mietinnön asiasisältö

Mietintö vaikuttaa lainsäädäntöä koskevien osuuksien osalta hyvin ja perusteellisesti valmistelulta. Näitä osuuksia voidaan käyttää hyvin jatkovalmistelun lähdemateriaalina.

Teknologian, tietoverkkojen, tietojärjestelmien, haittaohjelmien ja niiden havainnoinnin osalta mietinnön teksti on naivistista, perustuu vanhentuneisiin käsityksiin ja yksinkertaistettuihin mielikuviin. Teksti sisältää runsaasti virheellisyyskäsitteitä, perustelemattomia väitteitä ja mielipiteitä. Mietintöä ei näiltä osin tule käyttää valmistelun lähdemateriaalina, vaan valmistelun tulee perustua faktoihin ja objektiiviseen analyysiin tilanteesta ja tarvittavista toimenpiteistä.

4 Tiedustelutoimintaa ja viranomaisten tiedonhankintaa ohjaavat periaatteet

Suuret kansainväliset tietotekniikkatoimittajat ovat yhteistyössä koostaneet luettelon periaatteista, joita tulisi noudattaa kehitettäessä tiedustelutoimintaa ja viranomaisten tiedonhankintaa Internetistä ja pilvipalveluista koskevaa lainsäädäntöä. Periaatteet on tuotu esiin Yhdysvaltain liittovaltion tiedustelutoimintaa koskevan keskustelun yhteydessä. Ne on tarkoitettu kaikille valtioille, myös Suomelle. Periaatteiden tarkoituksena on turvata Internetin kehittyminen globaalina, kaikkien yksilöiden ja organisaatioiden käytettävissä olevana palveluna.

Esitämme, että Suomen valtion tulisi ottaa nämä periaatteet ohjenuoraksi tiedustelulainsäädännön kehitystyössä.

4.1 Viranomaisten oikeutta kerätä käyttäjien tietoja tulee rajoittaa

Valtioiden tulisi säätää järkevät rajoitukset viranomaisten toimivallalle kerätä käyttäjien tietoja palveluntuottajilta. Tietojen keruu tulee tapahtua vain tarkoin rajatuissa olosuhteissa ja se tulee tasapainottaa käyttäjien kohtuullisten yksityisyydensuojan odotusten kanssa ottaen huomioon toiminnan vaikutukset yksilöiden Internetiä ja verkkopalveluita kohtaan tuntemaan luottamukseen. Viranomaisten valvonnan tulee kohdistua vain lainsäädännössä määritellyillä perusteilla yksilöityjen käyttäjien tietoihin eikä viranomaisten tule kerätä tietoja tietoverkoista rajoituksetta.

4.2 Tiedonkeruun tulee olla valvottua ja vastuullista

Viranomaisten tietopyyntöjä ja tiedonkeruuta varten tulee olla selkeä lainsäädäntökehikko, jonka perusteella viranomaisten valtuuksia ja toimenpiteitä valvotaan riittävällä tarkkuudella. Toimintaa valvovien toimielimien tulee olla riippumattomia ja valvonnan kohteilla ja tietopyyntöjen vastaanottajilla tulee olla mahdollisuus valittaa päätöksistä. Viranomaisten ja valvontaelinten keskeiset päätökset tulee julkistaa viivytyksettä, jotta kansalaisvalvonta olisi mahdollista.

4.3 Tietopyyntöjä koskevan toiminnan tulee olla läpinäkyvää

Viranomaisten toimivaltuuksia ja valtuuksien perusteella toteutettavia valvontaohjelmia koskevan keskustelun mahdollistamiseksi toiminnan on oltava läpinäkyvää. Viranomaisten tulee antaa yritysten julkistaa erilaisten tietopyyntöjen lukumäärät ja luonne. Lisäksi viranomaisten itsensä tulee julkistaa vastaavat tiedot.

4.4 Vapaata tiedonkulkua tulee kunnioittaa

Valtioiden rajat ylittävä tietoliikenne on olennainen edellytys tämän vuosisadan globaalin talouden toiminnalle. Viranomaisten tulee sallia tiedon kulku tietoverkoissa. Lisäksi viranomaisten ei tule rajoittaa yksittäisten käyttäjien ja yritysten pääsyä laillisesti saatavissa olevaan toisten valtioiden alueella sijaitsevaan tietoon.

4.5 Valtioiden väliset mahdolliset ristiriidat tulee ratkaista

Jotta lainsäädännön ristiriitaisuuksilta vältyttäisiin, valtioiden tulee rakentaa kestäviä periaatteita noudattava ja läpinäkyvyyttä edistävä kehikko rajat ylittävien tietopyyntöjen hallintaan esimerkiksi vahvistamalla olemassa olevia maiden välisiä virka-apusopimuksia. Valtioiden tulee sopia keskenään menettelytavoista, joilla ratkaistaan eri maiden lainsäädäntöjen mahdollisista ristiriitaisuuksista aiheutuvat ongelmat.

Espoossa 9.4.2015



Sami Ensio

Puheenjohtaja, Suomen Microsoft osajakumppaneiden yhdistys ry (IAMCP Finland)

Toimitusjohtaja, Innofactor Oyj