Liikenne- ja viestintäministeriö

15.12.2014

Digitaalisen yhteiskunnan tulevaisuus

Liikenne- ja viestintäministeriön edustajan eriävä mielipide tiedonhankintalakityöryhmän mietintöön

Liikenne- ja viestintäministeriön edustaja (myöh. liikenne- ja viestintäministeriö) ei voi tällä hetkellä saatavilla olevien tietojen perusteella suosittaa verkkovalvonnan mahdollistavan lainsäädännön valmistelua.

Eriävällä mielipiteellä ministeriö haluaa tarjota vaihtoehtoisen tavan hahmottaa digitaalista toimintaympäristöä. Mielipiteessä ministeriö esittää näkökulmia, joita ei ole huomioitu riittävästi tiedonhankintalakityöryhmän mietinnössä (myöh. mietintö). Lisäksi eriävällä mielipiteellä on tarkoitus mahdollistaa laajemman yhteiskuntapoliittisen keskustelun käyminen mietinnössä käsitellyistä aiheista ja erityisesti verkkovalvonnasta.

I. Ydinviestit

1. Tietoliikennetiedustelu on verkkovalvontaa.
   - Mietinnössä esitetty tietoliikennetiedustelu on verkkovalvontaa. Verkkovalvonnasta käytettään myös nimitystä massavalvonta, sillä siinä on kyse teknisestä pääsystä kaikkeen tietoliikenteeseen.
   - Verkkovalvonta kohdistuisi käytännössä kaikkeen tietoliikenteeseen, ei pelkästään kansainväliseen. Vaikka verkkovalvonnassa pyrittäisiinkin erottamaan kotimainen ja ulkomainen tietoliikenne, niin tiedustelu kohdistuu tosiasiassa myös suomalaisten viestintään.

2. Viranomaisille voidaan antaa vain toimivaltuuksia, jotka perustuvat niiden lakisääteisiin tehtäviin.
   - Tiedonhankintatoimivaltuudet ovat hyväksyttäviä vain, jos ne ovat välttämätön ja tehokas keino jonkin viranomaiselle säädetyn tehtävän hoitamiseksi.

3. Verkkovalvonnan tehokkuutta ei ole osoitettu, eikä vaihtoehtoja arvioitu.
   - Verkkovalvonta ei tuota tulevaisuudessa tietoa, jota sillä on ehkä aikaisemmin voitu saada.
   - Salaustekniikoiden kehittyminen ja käytön lisääntyminen sekä tietoliikenteen määrän kasvu vaikeuttavat verkkovalvontaa huomattavasti. Olennaisen tiedon löytäminen ja salauksen purkaminen vaativat merkittäviä resursseja, joita Suomella ei ole.
   - Työryhmätyöskentelyn tarkoituksena on näyttänyt olevan jo ennalta päätettyjen asioiden perusteleminen. Vaihtoehtoja työryhmän ehdottamalle verkkovalvonnalle ei ole esitetty.

4. Verkkovalvonnalla voi olla merkittäviä vaikutuksia yritystoimintaan.
   - Yritysvaikutukset vaikutukset on arvioitava huolellisesti. Verkkovalvonta vaikuttaa eri tavalla erityyppisiin yrityksiin.

- Verkkovalvonnalla voi olla vaikutuksia yritysten sijoittautumispäätöksiin, erityisesti tiedon hyödyntämiseen perustuvassa liiketoiminnassa.
- Suomi voisi käyttää kilpailuetunaan sitä, ettei täällä suoriteta verkkovalvontaa.

5. Verkkovalvonnalla rajoitetaan perusoikeuksia, erityisesti oikeutta yksityisyyteen.
   - Verkkovalvontatoimivaltuuksista säätäminen edellyttää perustuslain muuttamista.
   - Perustuslakia voidaan joutua muuttamaan, vaikka verkkovalvonta keskittyisi vain tunnistamistietoihin.

6. Verkkovalvonta ei parantaisi tietoturvaa, vaan heikentäisi sitä.
   - Verkkovalvonta tarkoittaisi käytännössä sitä, että tiedonhankinnan kohteeksi valikoidun viestinnän suojaukset yritettäisiin ohittaa tai murtaa.
   - Verkkovalvonta heikentäisi kaikkien niiden henkilöiden tietoturvallisuutta, joiden viestejä välitettäisiin niissä yleisissä viestintäverkoissa, joissa verkkovalvontaa suoritettaisiin.
   - Verkkovalvonta ei parantaisi yritysten tietoturvaa.

II. Johdanto

Tiedonhankintalakityöryhmä aloitti työskentelynsä tammikuussa 2014. Alun perin hallituksen esityksen muotoon kaavaillusta loppuraportista kasvoi noin 100-sivuinen mietintö. Mietinnössä kuvataan muuttuvaa turvallisuusympäristöä ja tiedonhankintatoimivaltuuksien nykytilaa. Tämän jälkeen mietinnössä vertaillaan eri maiden lainsäädäntöä ja esitetään lainsäädännön kehittämisehdotuksia. Työryhmä ehdottaa mietinnön johtopäätöksissä, että käynnistettäisiin tarvittavat toimenpiteet tiedustelua koskevan säädösperustan luomiseksi. Käytännössä tämä tarkoittaa lainsäädännön valmistelua.

Mietinnössä käsitellään kahta tiedustelukokonaisuutta: 1) tietoliikennetiedustelua ja 2) ulkomaan tiedustelua, joista jälkimmäinen jakaantuu henkilö- ja tietojärjestelmätiedusteluun. *Tietoliikennetiedustelulla* tarkoitetaan Suomen rajat ylittävissä tietoliikennekaapeleissa liikkuvaan tietoliikenteeseen kohdistuvaa tiedustelua. *Ulkomaan tietojärjestelmätiedustelulla* tarkoitetaan ulkomailla sijaitsevassa tietojärjestelmässä käsiteltäviin tietoihin kohdistuvaa tietoteknisin menetelmin tapahtuvaa tiedustelua. *Ulkomaan henkilötiedustelulla* tarkoitetaan ulkomaita koskevaa tiedustelua, joka perustuu henkilökohtaiseen kanssakäymiseen taikka henkilön tai muun kohteen henkilökohtaiseen havainnointiin. Tietoliikennetiedustelu ja ulkomaan tietojärjestelmätiedustelu menevät käsitteinä helposti sekaisin. Tässä eriävässä mielipiteessä käytetään tietoliikennetiedustelusta vastedes käsitettä verkkovalvonta.

Liikenne- ja viestintäministeriö katsoo, ettei se voi yhtyä tiedonhankintalakityöryhmän mietintöön kokonaisuudessaan. Tiedonhankintalakityöryhmä suosittelee mietinnössään, että Suomen tulisi harkita verkkovalvonnan käyttöönottoa. Liikenne- ja viestintäministeriö ei voi yhtyä tähän näkemykseen. Ministeriö ei kuitenkaan sulje pois mahdollisuutta muuttaa näkemystään verkkovalvonnasta, jos myöhemmin laadittava selvitys osoittaa sen tehokkaaksi tarkoitukseensa nähden sekä edut oletettua suuremmiksi ja haitat pienemmiksi. Näin ei toistaiseksi ole tapahtunut.

Liikenne- ja viestintäministeriö ymmärtää ja hyväksyy puolustusvoimien ja poliisin esittämät huolet siitä, etteivät ne kaikilta osin saa päätöksentekonsa tueksi tarpeeksi tietoa sotilaalliseen maanpuolustukseen tai rikoksiin liittyvistä uhkista. **Tällä hetkellä käytettävissä olevan tie-**

tämyksen perusteella mietinnössä suositeltu verkkovalvonta vaikuttaa kuitenkin olevan tarkoituksiinsa nähden tehoton ja haitallinen luottamuksellisen viestinnän suojalle ja elinkeinoelämälle.

Muilta osin liikenne- ja viestintäministeriö näkee, että puolustusvoimien tiedustelukyvyn kehittäminen on tärkeää. Ministeriö katsoo, että tulisi ryhtyä lainsäädännön valmisteluun sen varmistamiseksi, että puolustusvoimilla olisi perusteltu kyky ja selkeä toimivalta hankkia tehokkaasti sotilaallisen maanpuolustuksen kannalta keskeistä tietoa Suomen rajojen ulkopuolella sijaitsevista järjestelmistä. **Liikenne- ja viestintäministeriö pitää siten mietinnössä kaavailtua ulkomaille kohdistuvaa henkilö- ja tietojärjestelmätiedustelua perusteltuna.**

Poliisilla on ministeriön näkemyksen mukaan kattavat mahdollisuudet saada rikoksiin liittyvää tietoa Suomessa sijaitsevista tietojärjestelmistä poliisi- ja pakkokeinolain mukaisessa menettelyssä. **Jos poliisin valtuudet todetaan digitalisoituneessa ympäristössä riittämättömiksi, liikenne- ja viestintäministeriö pitää perusteltuna, että näiden salaisten pakkokeinojen nykyistä alueellista soveltamisalaa tai käytön edellytyksiä arvioidaan uudelleen.**

Työryhmän toimikauden aikana on ollut havaittavissa vastakkainasettelua liikenne- ja viestintäministeriön ja turvallisuusviranomaisten välillä. Liikenne- ja viestintäministeriö haluaa korostaa, ettei se kiistä tiedonsaantitarpeiden oikeellisuutta tai tärkeyttä yhteiskunnallisesti. Ministeriö on kuitenkin painokkaasti tuonut esille, että tiedonsaantitarpeet tulee esittää selkeästi ja perustella viranomaisten lakisääteisten tehtävien kautta. Tämän jälkeen keinot, joilla näihin tarpeisiin voitaisiin vastata, tulee eritellä, osoittaa niiden tehokkuus tarkoitukseensa nähden ja arvioida kaikki niiden vaikutukset.

Työryhmän työn suurin heikkous on ollut se, että se on keskittynyt työnsä alusta asti perustelemaan verkkovalvonnan käyttöönottoa. Työryhmä ei kuitenkaan ole pystynyt tyydyttävällä tavalla perustelemaan verkkovalvonnan tehokkuutta, eikä kuvaamaan sen vaikutuksia. Myöskään vaihtoehtoisiin tiedonhankintatapoihin ei ole perehdytty riittävästi.

Kuten tiedonhankintalakityöryhmän mietinnössä todetaan, ei puolustusvoimien tiedustelutoiminnasta säädetä tällä hetkellä laissa. Tästä huolimatta työryhmän asettamiskirje ja työryhmän tavoitteet on muotoiltu keskittymään vain niin sanottuun ”kybertoimintaympäristöön”.[1] Liikenne- ja viestintäministeriön näkemyksen mukaan työryhmän olisi tullut keskittyä vielä kokonaisvaltaisemmin tiedustelua koskevan lainsäädännön kehittämistarpeisiin, sillä yleislainsäädäntö tulisi lähtökohtaisesti säätää ennen erityislainsäädäntöä. Mahdollisessa seuraavassa vaiheessa tulisikin pohtia puolustusvoimien tiedustelua koskevan lainsäädännön laatimista, eikä keskittyä pelkästään tietoverkossa käytettäviin toimivaltuuksiin.

Työryhmän työskentely on ollut intensiivistä ja kokouksia on järjestetty noin kerran viikossa. Liikenne- ja viestintäministeriö on tiukasta aikataulusta huolimatta pyrkinyt parhaansa mukaan edistämään työryhmän työtä ja tarjoamaan omaa viestintäpolitiikkaan ja sähköiseen viestintään liittyvää osaamistaan työryhmän käyttöön. **Liikenne- ja viestintäministeriön esittämiä näkökulmia on otettu osaksi mietintötekstiä vasta työryhmän lopussa eikä silloinkaan sisällöllisesti merkityksellisellä tavalla.** Tämä ei ole riittänyt ministeriön ydinviestien huomioon ottamiseksi.

[1] Etuliitteen ”kyber” yksiselitteinen määritteleminen on haastavaa, mutta kybertoimintaympäristöllä viitataan yleisesti digitaalisen toimintaympäristöön, eli esimerkiksi toimintaan tietoverkoissa.

Eriävänä mielipide on laadittu liikenne- ja viestintäministeriön ydinviestien ympärille. Jokainen ydinviesti perustellaan omassa luvussaan. Viimeisessä luvussa kerrataan aiempia toimia, joita on tehty tietoturvan parantamiseksi sekä esitellään näkemyksiä internetin luotettavuuden kehittämiseksi. **Liikenne- ja viestintäministeriön eriävä mielipide keskittyy pääosin verkkovalvontaa koskevaan mietinnön osaan.**

Seuraavassa luvussa kuvataan, miten internetin massavalvontaa koskevat paljastukset ovat vaikuttaneet kansainväliseen keskusteluun. Lisäksi luvussa tarkastellaan internetin taloudelliseen hyödyntämiseen liittyvää kehitystä.

III. Toimintaympäristö

Mietinnössä on varsin laajasti kuvattu muuttuvaa turvallisuusympäristöä ja muun muassa kansalliseen turvallisuuteen kohdistuvia tietoverkkouhkia sekä tietoverkkorikollisuutta. Toimintaympäristön kuvaus on mietinnössä erittäin uhkakeskeinen. **Liikenne- ja viestintäministeriön näkemyksen mukaan mietinnössä olisi kuitenkin tullut kuvata laajemmin tiedusteluun liittyvää kansainvälistä ilmapiiriä ja internetin kehitystä sekä niiden vaikutuksia erityisesti verkkovalvonnan tehokkuuteen.**

Mietinnössä ei kuvata sitä muutosta, joka yritysten ja kansalaisten asenneilmapiirissä on tapahtunut sen jälkeen, kun Edward Snowden kertoi kesällä 2013 julkisuuteen tietoja USA:n ja muiden maiden harjoittamasta tietoliikenteen massavalvonnasta. Itse asiassa koko tietovuotoa tai kansainvälistä keskustelua valtioiden harjoittamasta ylimitoitetuista valvonnasta ei ole tarkemmin käsitelty mietinnössä.[2]

Esimerkkeinä verkkovalvontaan liittyvistä kansainvälisistä kannanotoista voidaan mainita YK:ssa käytävä keskustelu yksityisyydestä digitaaliaikana. YK:n ihmisoikeusneuvostoon kuuluvat erityisraportoijat ovat käsitelleet oikeutta yksityisyyden suojaan ja uuden informaatioteknologian mukanaan tuomia ihmisoikeushaasteita useista näkökulmista. YK:n yleiskokous hyväksyi joulukuussa 2013 ilman äänestystä päätöslauselman oikeudesta yksityisyyteen digitaaliaikana (A/RES/68/167). Uuden aloitteen taustalla olivat Brasilia ja Saksa ja myös Suomi suhtautui siihen positiivisesti. Huomattavaa oikeudellista ja poliittista kiinnostusta herättäneellä päätöslauselmalla ilmaistaan huoli sähköisen valvonnan sekä digitaalisen viestinnän urkinnan ja henkilökohtaisten tietojen keräämisen kielteisistä vaikutuksista ihmisoikeuksiin. Päätöslauselmalla pyritään vahvistamaan oikeutta yksityisyyden suojaan. Ihmisoikeuksia tulee suojella yhtäläisesti myös sähköisessä viestinnässä. Kansallisen lainsäädännön tulee olla yhdenmukaista kansainvälisten ihmisoikeusvelvoitteiden kanssa.[3]

Toisena esimerkkinä voidaan mainita Euroopan parlamentin päätöslauselma Yhdysvaltojen kansallisen turvallisuusviraston valvontaohjelmasta, eri jäsenvaltioiden valvontaelimistä ja niiden vaikutuksesta EU:n kansalaisten perusoikeuksiin ja transatlanttiseen yhteistyöhön oikeus- ja sisäasioissa.[4] Euroopan parlamentin päätöslauselmaa tulisi peilata erityisesti tiedonhankintalakityöryhmän mietinnön kansainvälistä vertailua koskevaan osuuteen. Mietinnössä verrokki-

[2] Verkkovalvonnan vaikutusarvioinnissa on maininta ”Snowden-tapauksesta” ja siitä kuinka sen jälkeisissä olosuhteissa Ruotsin selkeä tiedustelulainsäädäntö saattaa olla jopa kansainvälinen kilpailuetu.
[3] Ks. http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx. Lisäksi YK:n ihmisoikeuskomissaari on antanut aiheesta raporttinsa ja suositukset (A/HRC/27/37), joita on käsitelty YK:n 69. yleiskokouksessa syyskuussa 2014.
[4] Euroopan parlamentin päätöslauselma 12. maaliskuuta 2014 Yhdysvaltojen kansallisen turvallisuusviraston valvontaohjelmasta, eri jäsenvaltioiden valvontaelimistä ja niiden vaikutuksesta EU:n kansalaisten perusoikeuksiin ja transatlanttiseen yhteistyöhön oikeus- ja sisäasioissa (2013/2188(INI)).

maiksi on valittu vain maita, jossa verkkovalvontaa harjoitetaan. Vertailua tarkasteltaessa tulisi esimerkiksi huomioida, että Euroopan parlamentti on suhtautunut varsin varauksellisesti muun muassa Ruotsin ja Alankomaiden tiedustelua koskevaan lainsäädäntöön ja katsonut, että kyseiset lainsäädännöt voivat olla ongelmallisia EU:n perusoikeuksien näkökulmasta. Euroopan parlamentti on kehottanut kaikkia EU:n jäsenvaltioita kieltämään kaikenkattavat laajamittaiset valvontatoimet ja lisäksi kehottanut kaikkia EU:n jäsenvaltioita ja etenkin Yhdistynyttä kuningaskuntaa, Ranskaa, Saksaa, Ruotsia, Alankomaita ja Puolaa varmistamaan, että niiden nykyiset tai tulevat tiedustelupalvelujen toimintaa koskevat lainsäädäntökehykset ja valvontamekanismit ovat Euroopan ihmisoikeussopimuksen määräysten ja EU:n tietosuojalainsäädännön mukaisia. Terrorismin torjunnan osalta Euroopan parlamentti toteaa uskovansa vahvasti, ettei terrorismin torjunta voi koskaan oikeuttaa kohdentamattomia, salaisia tai jopa laittomia laajamittaisen valvonnan ohjelmia. Euroopan parlamentti katsoo, että tällaiset ohjelmat ovat tarpeellisuus- ja suhteellisuusperiaatteiden vastaisia demokraattisessa yhteiskunnassa.

Snowdenin paljastusten jälkeen maailmalla on havahduttu pohtimaan sitä, mitä teknistyminen ja jokapäiväisen elämämme yhä suurempi riippuvuus sähköisistä palveluista tarkoittaa. Digitalisaatio ratkaisee monia ongelmia ja tehostaa toimintaamme. Samalla se kuitenkin synnyttää uusia haasteita. Internetin ja mobiiliteknologian hyödyntäminen mahdollistaa tietojen keräämisen ja ihmisten seuraamisen aivan uudella tavalla. Myös valtiot pystyvät hyödyntämään tätä kehitystä tiedustelutoiminnassaan.

Tilannetta, jossa Euroopan unionin jäsenmaat urkkivat toisten maiden kansalaisten ja yritysten tietoja, voidaan pitää esteenä Suomen tärkeänä pitämien digitaalisten sisämarkkinoiden synnylle. **Liikenne- ja viestintäministeriö katsoo, että verkkovalvontatoimivaltuuksien sijaan Suomen tulisi aktiivisesti edistää kansainvälistä yhteistyötä viestinnän luottamuksellisuuden säilymisen puolesta.** Esimerkiksi EU:ssa voitaisiin pyrkiä löytämään yhteinen lähestymistapa sille, minkälaisissa tilanteissa ja millä tavoin toisen jäsenvaltion alueella asuvan ja toimivan kansalaisen tai yrityksen viestinnän luottamuksellisuutta voidaan rajoittaa.

Laajasti katsottuna toimintaympäristön muutoksessa on kyse internetin hyödyntämisestä. Tiedon säilyttämisen kustannukset ovat pienentyneet ja tiedosta on entistä helpompi saada liiketoiminnallista hyötyä. Palveluiden ansaintalogiikat perustuvat yhä useammin tietojen keräämiseen, käyttöön ja myyntiin. Internet-talous ja digitaaliset palvelut ovat merkittäviä talouden kasvun katalyytteja.

Kaikki mikä voidaan digitalisoida, tullaan digitalisoimaan. Tämä vaikuttaa käytännössä kaikkiin yhteiskunnan osa-alueisiin. Myös julkishallinnon palvelut siirtyvät verkkoon. **Digitaalisuus on kaikkia yhteiskunnan sektoreita läpileikkaava teema ja kyky sen hyödyntämiseen tulee pitkälti määrittelemään kansakuntien asemaa globaalissa kilpailussa.** Tieto- ja viestintäteknologian on arvioitu olevan merkittävin Suomen talouskasvuun viidentoista viime vuoden aikana vaikuttanut yksittäinen tekijä.[5] Oikeilla tieto- ja viestintäteknologiaa koskevilla päätöksillä voidaan parantaa tuottavuutta ja nopeuttaa talouskasvua. Päätöksenteossa tulee huomioida, että toimivia ja kilpailukykyisiä digitaalisia palveluita ei nykypäivänä pystytä rakentamaan ilman luottamusta. Luottamusta ei tule horjuttaa ilman erittäin tärkeäksi katsottua perustetta.

[5] Teknologiateollisuus ry:n julkaisu 9/2014: Suomi uuteen nousuun - ICT ja digitalisaatio tuottavuuden ja talouskasvun lähteinä (kirjoittanut Matti Pohjola).

Edellä esitetyn perusteella tiedustelutoimivaltuuksia on kansalaisiin ja yrityksiin kohdistuvien vaikutusten lisäksi harkittava myös laajemman tietoyhteiskuntakehityksen ja digitalisaation näkökulmasta.

1. Tietoliikennetiedustelu on verkkovalvontaa

Tiedonhankintalakityöryhmän mietinnössä kuvataan verkoissa toteutettavan tiedonhankinnan keinoja käsitteillä ”tietoliikennetiedustelu” ja ”tietojärjestelmätiedustelu”. Liikenne- ja viestintäministeriö käyttää kuitenkin tässä eriävässä mielipiteessään tietoliikennetiedustelusta käsitettä verkkovalvonta.[6]

Myös työryhmä on työskentelynsä aikana käyttänyt tietoliikennetiedustelusta käsitettävä verkkovalvonta. Syksyllä 2014 käsitteitä kuitenkin päätettiin vaihtaa, koska verkkovalvonnan koettiin herättävän liian kielteisiä ajatuksia mietintöä luettaessa. Toiminnasta käytetyn käsitteen muuttaminen ei kuitenkaan muuta itse toimintaa. Liikenne- ja viestintäministeriö katsoo, että verkkovalvonta kuvaa hyvin mietinnön tietoliikennetiedustelulla tarkoitettua toimintaa (”rajat ylittävissä tietoliikennekaapeleissa liikkuvaan tietoliikenteeseen kohdistuva tiedustelu”) ja vastaa myös julkisessa keskustelussa käytettyä käsitteistöä.

Liikenteen rajat ylittävyys

Verkkovalvonnan kohdentaminen ”rajat ylittävään tietoliikenteeseen” on vaikeaa tai käytännössä mahdotonta, koska palveluita tuotetaan nykyään entistä enemmän globaaleille markkinoille. Esimerkiksi pilvipalveluita käytettäessä tietoa tallentuu useammalle palvelimelle, jotka voivat sijaita eri puolilla maailmaa. Tämä tarkoittaa sitä, että Suomesta pilvipalvelusähköpostista (Gmail, MS Outlook) lähetetty sähköposti Suomessa olevalle vastaanottajalle saattaa kopioitua jo lähetyshetkellä useille palvelimille ympäri maailmaa.

Sen lisäksi, että tieto voi tallentua eri palvelimille, tietoliikenne myös yleensä ohjautuu reitittymään lyhintä tai nopeinta reittiä kohteeseensa. Liikenteen reitittyminen riippuu arvotetuista resursseista ja perustuu algoritmeihin. Tavallisella käyttäjällä ei lähtökohtaisesti ole mahdollisuutta vaikuttaa siihen, mitä reittiä esimerkiksi sähköpostiviestit kulkevat vastaanottajalle. Edellä mainittujen seikkojen takia **tietoliikenne on enenevässä määrin rajat ylittävää, vaikka se olisikin tarkoitettu liikkumaan vain Suomen sisällä lähettäjältä vastaanottajalle.**

Etuliitteen ”rajat ylittävä” käyttäminen mietinnössä hämärtää lukijan käsitystä siitä, mihin viestintään verkkovalvonta voisi kohdistua. Kun käytännössä ainakin tietoliikennetiedustelun ensivaiheessa (seulonta) rajat ylittävän liikenteen erottelu on vaikeaa tai mahdotonta, ei kaikkea tietoliikennetiedustelua voida katsoa kohdistuvaksi vain rajat ylittävään tietoliikenteeseen. Tämä ei tietenkään tarkoita sitä, etteikö verkkovalvontaan voitaisi säätää esimerkiksi käsittelykieltoa Suomen sisäiselle liikenteelle. Juridisesta näkökulmasta viestien rajat ylittävyydellä ei ole suurta merkitystä, sillä viestinnän luottamuksellisuuden suoja koskee kaikkea viestintää, joka on Suomen oikeudenkäytön piirissä. Vaikuttaisi siltä, että mietinnössä rajat ylittävyyden korostamisella on pyritty lähinnä hälventämään harhaanjohtavasti verkkovalvontaan kohdistuvia ennakkoluuloja, eikä niinkään kuvaamaan toimintaa itsessään.

[6] Englannin kielessä verkkovalvonnasta käytetään yleisesti nimitystä ”mass surveillance”.

Mietinnössä on kuvattu tietoteknistymisen vaikutuksia henkilöiden väliseen kanssakäymiseen. Tietoteknistyminen ja sähköisten viestintävälineiden lisääntyvä käyttö kuvataan mietinnössä lähinnä niiden muodostamien uhkien kautta.[7] Ihmisillä ja yrityksillä on Euroopan yhdentymisen ja muun globalisaatiokehityksen johdosta enemmän sosiaalisia suhteita ulkomaille. Näitä suhteita on tehokasta, helppoa ja taloudellista ylläpitää esimerkiksi sähköpostilla tai sosiaalisen median sovellusten kautta. Tämän lisäksi Suomessa harjoitetaan merkittävässä määrin kansainvälistä liiketoimintaa, jonka voidaan arvioida lisääntyvän muun muassa digitalisoitumisen ansiosta.

Viestinnän luottamuksellisuus suojaa sellaistakin viestintää, jossa vain toinen osapuoli on suomalainen. Mietinnön johtopäätöksissä esitetty ajatus siitä, että verkkovalvonta voisi vaarantamatta viestinnän luottamuksellisuuden perusoikeussuojaa kohdistua pelkästään vieraan valtion tietoliikenteeseen vaikuttaa lähinnä teoreettiselta, jos otetaan huomioon internetissä liikkuvan tietoliikenteen ominaisuudet ja valtioiden rajat ylittävä luonne.

2. Viranomaisille voidaan antaa vain toimivaltuuksia, jotka perustuvat niiden lakisääteisiin tehtäviin

Suomen perustuslaissa säädetyn oikeusvaltioperiaatteen mukaan julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia.[8] Periaatteen toteutumisen kannalta on tärkeää, että viranomaisille esitetään ainoastaan sellaisia salaisia pakkokeinovaltuuksia tai tiedonhankintatoimivaltuuksia, joiden tarve on perusteltu kyseisen viranomaisen lakisääteisen tehtävän suorittamisen kannalta välttämättömäksi. Työryhmän mietinnössä toimivaltuuksien tarve on kuvattu epäselvästi ilman, että niitä on selkeästi sidottu kyseisten viranomaisten lakisääteisiin tehtäviin.

Mietinnössä poliisin ja puolustusvoimien tiedonhankinnan tarpeet on perusteltu sillä, että on olemassa ”yhteiskuntaa vakavasti vaarantavia uhkia”. Viranomaisten laissa määritellyt tehtävät ja mietinnössä esitetyt toimivaltuudet eivät kohtaa. Oikeusvaltioperiaatteen mukaan tiedonhankintaa koskevat uudet toimivaltuudet tulisi perustella täsmällisemmin sellaisten tietojen saannin tarpeilla, jotka ovat välttämättömiä poliisin ja puolustusvoimien laissa säädettyjen tehtävien toteuttamiseksi.

Kuten mietinnössäkin todetaan, yleinen kansainvälistymis- ja digitalisoitumiskehitys on tärkeää ja väistämätöntä. On selvää, että samalla turvallisuusympäristömme muuttuu ja monimutkaistuu. Tekniikan kehitystä voidaan käyttää hyvän lisäksi myös pahaan. Kansallista turvallisuutta vaarantavia tekoja voidaan toteuttaa entistä lyhyemmällä valmisteluajalla ja vakavammin seurauksin. Tietoverkkoja ja niiden päällä toimivia uusia teknologioita, voidaan hyödyntää paitsi suunnittelussa ja valmistelussa, myös tekovälineenä erilaisissa vakavissa turvallisuutta uhkaavissa toimissa. Tämän takia **liikenne- ja viestintäministeriö katsoo, että on tarpeellista pitää huolta siitä, että turvallisuusviranomaisillamme on riittävät ja oikeasuhtaiset toimivaltuudet kehittyvissä tietoverkoissa.**

[7] Esim. s. 18: " Kansalliseen turvallisuuteen kohdistuviin turvallisuusuhkiin liittyy globalisoitumisen seurauksena yhä useammin Suomessa ja ulkomailla olevien henkilöiden välisiä kytköksiä ja siitä seuraavaa tarvetta molemminpuoliseen kommunikointiin. Sähköisiä välineitä käytetään hyväksi uhkien taustalla olevien valtiollisten ja ei-valtiollisten tahojen viestinnässä, tehtäväksi annoissa, tehtävien toteuttamista koskevassa raportoinnissa, tekojen suunnittelussa, kohteita koskevassa tiedonhankinnassa, osallisten motivoinnissa ja radikalisoinnissa sekä uusien jäsenten rekrytoinnissa”.
[8] Suomen perustuslain (731/1999) 2 §.

Puolustusvoimien lakisääteisenä tehtävänä on muun muassa Suomen sotilaallinen puolustaminen.[9] On ilmeistä, että puolustusvoimilla on rauhan aikanakin tarve saada tietoa Suomeen kohdistuvasta aseellisen hyökkäyksen tai sitä vastaavan uhan kohdistumisesta Suomeen.

Liikenne- ja viestintäministeriö katsoo, että siviiliyhteiskuntaan kohdistuvan verkkovalvonnan sijasta tehokkaampaa ja yhteiskunnalle vähemmän vahingollista olisi hankkia tietoa kohdennetusti niistä ulkomailla sijaitsevista tietojärjestelmistä, joissa käsitellään Suomen sotilaalliseen puolustamisen kannalta olennaista tietoa aseellisen hyökkäyksen uhkasta tai siihen verrattavasta uhkasta. Kyse olisi tiedosta, joka hankittaisiin ulkomaisista sotilaallisista johtamisjärjestelmistä.

Työryhmä on käyttänyt kohdennetusta tiedonhankintakeinoista termiä *tietojärjestelmätiedustelu.* Käytännössä kyse olisi tiedonhankinnan kohteeksi määritettävien ulkomailla sijaitsevien johtamisjärjestelmiin liittyvien tietokoneiden tietoturvan loukkaamisesta sotilaallista maanpuolustusta koskevan tiedon hankkimiseksi. Teknisesti tietojärjestelmätiedustelu on toteutettavissa monella eri tavalla. Keinojen käyttöedellytyksiä ja mahdollista soveltamisalaa saattaa silti olla syytä arvioida kansainvälisen oikeuden näkökulmasta.

Liikenne- ja viestintäministeriö katsoo, että puolustusvoimille tulee turvata oikeus välttämättömiin, tehokkaisiin ja oikeasuhtaisiin toimivaltuuksiin sotilaallisen puolustamisen kannalta välttämättömien tietojen hankkimiseksi. **Liikenne- ja viestintäministeriö kuitenkin katsoo jäljempänä esitetyin perustein, ettei mietinnössä kuvattu verkkovalvonta ole välttämätön, tehokas ja oikeasuhtainen keino hankkia keskeisimpiä tietoja Suomen sotilaalliseksi puolustamiseksi.** Päinvastoin ministeriö pitää mietinnössä kuvatun kaltaista verkkovalvontaa epätehokkaana sotilaallisen puolustuksen perustellun tiedontarpeen kannalta. Lisäksi ministeriö katsoo, että verkkovalvonta voi vaikuttaa haitallisesti siviiliyhteiskunnan ja kansalaisten perusoikeuksien toteutumiseen, Suomessa toimivien yritysten toimintaedellytyksiin sekä yleiseen tietoyhteiskuntakehitykseen.

Sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyvien rikosten ennalta estämisestä ja paljastamisesta säädetään uudessa sotilaskurinpidosta ja rikostorjunnasta puolustusvoimista annetussa laissa (255/2014). Laki tuli voimaan 1.5.2014 ja siinä on määritelty ne salaiset pakkokeinot, joita puolustusvoimat voi käyttää mainittujen sen tehtäviin liittyvien rikosten tutkinnassa.[10] Työryhmän mietinnöstä ei ilmene, miltä osin nämä tutkintakeinot ovat riittämättömiä Suomen puolustamisen kannalta. Jos katsotaan, etteivät puolustusvoimien rikostorjuntaa koskevat toimivaltuudet ole riittäviä puolustusvoimien tehtävien suorittamiseksi, liikenne- ja viestintäministeriö pitää perusteltuna, että näiden pakkokeinojen nykyistä aineellista tai alueellista soveltamisalaa taikka käytön edellytyksiä arvioidaan uudelleen.

---

[9] Laki puolustusvoimista (551/2007) 2 §. Säännöksen mukaan Suomen sotilaalliseen puolustukseen kuuluu a) maa-alueen, vesialueen ja ilmatilan valvominen sekä alueellisen koskemattomuuden turvaaminen; b) kansan elinmahdollisuuksien, perusoikeuksien ja valtiojohdon toimintavapauden turvaaminen ja laillisen yhteiskuntajärjestyksen puolustaminen; c) sotilaskoulutuksen antaminen ja vapaaehtoisen maanpuolustuskoulutuksen ohjaaminen sekä maanpuolustustahdon edistäminen. Lain 4 §:n mukaan puolustusvoimat turvaa Suomen aluetta, kansan elinmahdollisuuksia ja valtiojohdon toimintavapautta sekä puolustaa laillista yhteiskuntajärjestystä tarvittaessa sotilaallisin voimakeinoin *aseellisen hyökkäyksen tai sitä vastaavan ulkoisen uhan* kohdistuessa Suomeen. Sotilaallisten voimakeinojen tulee olla sopusoinnussa Suomea sitovien kansainvälisten velvoitteiden kanssa. Sotilaallisilla voimakeinoilla tarkoitetaan sotilaan henkilökohtaisen aseen ja sitä voimakkaampaa asevoiman käyttöä.

[10] Lain 89 §:n mukaan puolustusvoimilla on toimivaltuudet mm. seuraaviin tutkintakeinoihin: 1) Tukiasematietojen hankkiminen; 2) suunnitelmallinen tarkkailu; 3) peitelty tiedonhankinta; 4) tekninen kuuntelu; 5) tekninen katselu; 6) tekninen seuranta; 7) teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen. Pykälän mukaan puolustusvoimat saa käyttää edellä mainittuja tutkintakeinoja seuraavien rikosten paljastamisessa: 1) Suomen itsemääräämisoikeuden vaarantaminen; 2) sotaan yllyttäminen; 3) maanpetos ja törkeä maanpetos; 4) vakoilu ja törkeä vakoilu; 5) turvallisuussalaisuuden paljastaminen; sekä 6) luvaton tiedustelutoiminta.

Poliisin lakisääteisenä tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen. Poliisin toiminnan tehokkuus perustuu monella tapaa järjestykseen ja rikoksiin liittyvän tiedon hankintaan. Poliisille onkin poliisi- ja pakkokeinolaeissa säädetty lukuisia välttämättömiä toimivaltuuksia poliisin lakisääteisiin tehtäviin liittyvän tiedon hankkimiseksi.

Uudistetut poliisilaki (872/2011) ja pakkokeinolaki (806/2011) tulivat voimaan 1.1.2014.[11] Lait antavat poliisille oikeuden hankkia tietoja rikoksesta epäillyn luottamuksellisesta viestinnästä ja tämän käyttämistä tietokoneista monin keinoin.[12] Lisäksi poliisi sai uutena toimivaltuutena oikeuden tehdä teknistä laitetarkkailua, joka käytännössä tarkoittaa tiedon hankkimista salaa rikoksesta epäillyn tietokoneelta loukkaamalla tämän tietoturvallisuutta. Kyse on teknisesti samankaltaisesta toiminnasta kuin tietojärjestelmätiedustelu. Työryhmä ei ole mietinnössään kattavasti arvioinut näiden lakien mukaisten salaisten tiedonhankinnan toimivaltuuksien käyttöä ja tehokkuutta, riittävyyttä tai riittämättömyyttä poliisin lakisääteisten tehtävien hoitamisessa. Liikenne- ja viestintäministeriölle on epäselvää, minkälaisten rikosten torjumiseksi poliisin käytössä olevat tiedonhankinnan keinot eivät ole riittäviä.

Liikenne- ja viestintäministeriö pitää tärkeänä, että poliisilla on kattavat mahdollisuudet saada rikoksiin liittyvää tietoa Suomessa sijaitsevista tietojärjestelmistä poliisi- ja pakkokeinolain mukaisessa menettelyssä. **Jos katsotaan, että poliisin nykyiset valtuudet eivät ole riittäviä poliisin tehtäviin nähden, liikenne- ja viestintäministeriö pitää perusteltuna että näiden salaisten pakkokeinojen nykyistä alueellista tai aineellista soveltamisalaa taikka käytön muita edellytyksiä arvioidaan uudelleen.** Tällaiset mahdolliset lainsäädännön tarkastelut tulisi tehdä normaalilla tavalla valtioneuvoston ohjesäännön mukaisesti.[13]

Liikenne- ja viestintäministeriö katsoo, että perusoikeussuojan piirissä olevien kansalaisten yksityiselämää ja viestinnän luottamuksellisuuden suojaa loukkaavien poliisin salaisten pakkokeinovaltuuksien käytön edellytyksenä on aina oltava riippumattoman tuomioistuimen konkreettisen rikosepäilyn johdosta antama lupa. Ministeriön mielestä ei ole perusteltua, että tästä lainsäädännössä ja perustuslakivaliokunnan lausuntokäytännössä vakiintuneesta käytännöstä poikettaisiin.[14] Verkkovalvontaan myönnetty lupa ei samalla tavalla kohdistuisi konkreettiseen rikosepäilyyn yksittäistapauksessa.

---

[11] Pakkokeinolain salaisia pakkokeinoja koskevassa 10 luvussa säädetään, että telekuuntelua, tietojen hankkimista telekuuntelun sijasta, televalvontaa, tukiasematietojen hankkimista, suunnitelmallista tarkkailua, peiteltyä tiedonhankintaa, teknistä tarkkailua (tekninen kuuntelu, tekninen katselu, tekninen seuranta ja tekninen laitetarkkailu), teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimista, peitetoimintaa, valeostoa, tietolähdetoimintaa ja valvottua läpilaskua voidaan käyttää *esitutkinnassa* salassa niiden kohteilta.

[12] Poliisilain salaisia tiedonhankintakeinoja koskevassa 5 luvussa säädetään telekuuntelun, tietojen hankkimisen telekuuntelun sijasta, televalvonnan, tukiasematietojen hankkimisen, suunnitelmallisen tarkkailun, peitellyn tiedonhankinnan, teknisen tarkkailun (tekninen kuuntelu, tekninen katselu, tekninen seuranta ja tekninen laitetarkkailu), teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisen, peitetoiminnan, valeoston, tietolähdetoiminnan ja valvotun läpilaskun käyttämisestä *rikoksen estämiseen, paljastamiseen tai vaaran torjumiseen*. Näitä tiedonhankintakeinoja voidaan käyttää salassa niiden kohteilta. Lisäksi edellä mainittuja keinoja saadaan käyttää seuraavien *rikosten paljastamisessa*: 1) Suomen itsemääräämisoikeuden vaarantaminen; 2) sotaan yllyttäminen; 3) maanpetos, törkeä maanpetos; 4) vakoilu, törkeä vakoilu; 5) turvallisuussalaisuuden paljastaminen; 6) luvaton tiedustelutoiminta; 7) rikoslain 34 a luvun 1 §:n 1 momentin 2–7 kohdassa tai mainitun pykälän 2 momentissa tarkoitettu terroristisessa tarkoituksessa tehtävä rikos; 8) terroristisessa tarkoituksessa tehtävän rikoksen valmistelu; 9) terroristiryhmän johtaminen; 10) terroristiryhmän toiminnan edistäminen; 11) koulutuksen antaminen terrorismirikoksen tekemistä varten; 12) värväys terrorismirikoksen tekemiseen; 13) terrorismin rahoittaminen.

[13] Valtioneuvoston ohjesäännön (262/2003) 14 §:n mukaan oikeusministeriön toimialaan kuuluu mm. lainvalmistelu rikos- ja prosessioikeuden alalla.

[14] PeVL 8/1994 vp.

”Tiedustelu” tai ”uhkien torjunta” eivät ole puolustusvoimien tai poliisin lakisääteisiä tehtäviä. Jos tiedustelutoiminnasta on tarve säätää lailla, tulee tiedustelutoimintaa tarkastella samoin perustein kuin muitakin viranomaisten lakisääteisten toimivaltuuksien käyttöä. Liikenne- ja viestintäministeriö pitää itsestään selvänä, ettei millekään viranomaiselle ole perusteltua säätää laajempia perusoikeussuojaa loukkaavia toimivaltuuksia kuin mikä on välttämätöntä kyseisen viranomaisen lakisääteisten tehtävien suorittamisen kannalta. Liikenne- ja viestintäministeriö kehottaa oikeusministeriötä arvioimaan, onko Suomessa tarvetta yleiselle tiedustelulainsäädännölle, jossa arvioitaisiin huolellisesti poliisin ja puolustusvoimien salaiseen tiedonhankintaan liittyvien tehtävien määrittelyn tarkoituksenmukaisuutta ja vasta sen jälkeen tehtävien suorittamiseksi tarvittavia välttämättömiä ja tehokkaita tiedustelukeinoja sekä toimivaltuuksia.

3. Verkkovalvonnan tehokkuutta ei ole osoitettu, eikä vaihtoehtoja arvioitu

Kuten todettu tiedonhankintalakityöryhmän mietinnössä on käsitelty kolmea tiedustelutoimivaltuutta, eli kolmea keinoa hankkia kansallisen turvallisuuden kannalta välttämätöntä tietoa (verkkovalvonta, ulkomaan henkilö- ja tietojärjestelmätiedustelu). Mietinnössä on painotettu, ettei millään yksittäisellä tiedustelumenetelmällä saada kaikkea kansallista turvallisuutta koskevaa tietoa, vaan tieto joudutaan hankkimaan ja varmistamaan useilla toisiaan tukevilla tiedustelumenetelmillä. Myöskään mietintöön valituissa verrokkimaissa ei ole tyypillisesti säädetty vain yhdestä tiedustelumenetelmästä. Lisäksi mietinnössä todetaan, etteivät siinä esitetyt tiedustelumenetelmät korvaa toisiaan, koska ne ovat luonteeltaan osittain erilaisia.

Käytännössä mietinnössä ei ole esitetty vaihtoehtoehtoisia tiedonhankintamenetelmiä verkkovalvonnalle, eikä verkkovalvontaa ole esimerkiksi vertailtu suhteessa ulkomaan tietojärjestelmätiedusteluun. Vaikka **verkkovalvonnalla ja tietojärjestelmätiedustelulla ei kaikilta osin voitaisi vastata samaan tiedonhankintatarpeeseen, olisi verkkovalvonnalle silti pitänyt pyrkiä löytämään vaihtoehtoisia tiedonhankintamenetelmiä.** Kaiken kaikkiaan vaikuttaa siltä, ettei muita menetelmiä ole tunnistettu tai haluttu ottaa harkittavaksi.

<u>Tietoliikenteen salaaminen</u>

Suomen lainsäädäntö turvaa kaikille oikeuden suojata käytössä olevin teknisin mahdollisuuksin sähköisen viestin ja tunnistamistiedot. Viestintävirasto onkin useissa yhteyksissä kannustanut käyttäjiä salaamaan viestintänsä. Tietojen salaamista voidaan käyttää myös yhtenä keinona, kun halutaan toteuttaa henkilötietojen suojaamista koskevia velvoitteita.

Tiedonhankintalakityöryhmän työskentelyn aikana on useamman kerran kuultu, kuinka tietoliikenteen salaamisen lisääntyminen vaikeuttaa tiedonhankintaa. Salauksen lisääntymiselle on nähtävissä useita syitä. Mitä arvokkaammaksi data käy yritysten liiketoiminnalle, sitä enemmän sitä halutaan suojata. Myös suuria asiakasrekistereitä ylläpitäviin yrityksiin ja yhteisöihin kohdistuneet tietomurrot vaikuttavat innokkuuteen salata liikennettä. Salaamisen lisääntyminen ei kuitenkaan selity pelkästään edellä mainituilla. Tietovuotaja Edward Snowdenin paljastamalla laajamittaisella viranomaisten suorittamalla massavalvonnalla on merkittävä osuutensa asiaan.

Tarkasteltaessa millaisilla sivustoilla internetissä käydään kaikista eniten[15], voidaan todeta, että liikennettä ohjautuu eniten hakukoneisiin, sosiaalisen median sivustoille, videopalveluihin ja nettikauppoihin. Tämä kuvaa internetin kehitystä yhä palvelualustakeskeisemmäksi.[16] Jos paljon liikennettä keräävät sivustot ja niiden tarjoamat palvelualustat käyttävät käyttäjän ja sivuston välisessä yhteydessä esimerkiksi SSL-salausta ja salaavat palvelustaan lähtevän liikenteen, tarkoittaa tämä käytännössä sitä, että tietoon on yhä vaikeampi päästä käsiksi. Isot teknologiayritykset ovat viimeisen vuoden aikana ilmoittaneet ottavansa yhä laajemmin käyttöön liikenteen salaustekniikoita. Esimerkiksi Google Gmail, Facebook ja Yahoo salaavat kaikki lähtevät viestit.[17] Sovellusten sisäisen ja niihin kohdistuvan liikenteen salaaminen vaikeuttaa myös tunnistamistietojen keräämistä.

Snowdenin paljastusten jälkeen tietoliikenteen salaaminen on lisääntynyt erityisesti Euroopassa.[18] On myös nähtävissä, että ihmisten tietoisuus yksityisyyden suojasta ja tietoturvasta internetissä on lisääntynyt.[19] Käyttäjien lisääntyvä tietoisuus yksityisyydensuojasta internetissä luo myös yrityksille painetta salata tarjottujen palveluiden tietoliikennettä ja panostaa tietoturvaan.

Tietoliikenteen salauksia on mahdollista purkaa. Salauksen avaaminen on kuitenkin aina huomattavasti hankalampaa kuin tiedonsalaaminen. Salauksen purkaminen voi myös viedä merkittävästi aikaa. Salauksen purku ei ole ongelma, jos käytössä on salauksen purkuun tarvittavat salausavaimet. Tiedonhankintalakityöryhmän mietinnössä kuitenkin painotetaan, ettei yrityksiä velvoitettaisi luovuttamaan salausavaimia tai asentamaan takaportteja järjestelmiinsä, mitä liikenne- ja viestintäministeriö pitää erittäin hyvänä.

Liikenne- ja viestintäministeriön näkemyksen mukaan tietoliikenteen salaaminen pienentää verkkovalvonnan mahdollisuutta tuottaa päätöksenteon tueksi ajanmukaista tietoa. Lienee selvää, että Suomen sotilaallisen puolustuksen kannalta keskeiset tiedot eivät kulkisi salaamattomana yleisissä viestintäverkoissa. Päinvastoin, juuri sotilaallinen viestintä on perinteisesti ollut hyvin salattua.

Mietinnössä on todettu verkkovalvonnan osalta, että tiedustelutiedon luovuttamisen edellytyksistä kansainvälisille yhteistyötahoille tulisi olla säännökset. Mietinnön mukaan lähtökohtana voisi olla se, että tietoluovutuksella edistetään kansallista turvallisuutta eikä sillä vaarannettaisi Suomen etuja, mukaan lukien kansantaloudelliset edut. Liikenne- ja viestintäministeriön näkemyksen mukaan verkkovalvonnan tehokkuutta ja sitä kautta sen oikeasuhtaisuutta ei voida perustalla kansainvälisen yhteistyön kautta saadulla esimerkiksi salauksen purkuun liittyvällä avulla. Tiedustelutoiminnasta säädettäessä tulee ratkaista mitä tietoja voitaisiin Suomen lainsäädännön nojalla vaihtaa kansainvälisessä tiedusteluyhteistyössä. **Liikenne- ja viestintäministeriö ei pääsääntöisesti voi pitää hyväksyttävänä sitä, että käytännössä suomalaista tietoliikennettä käsiteltäisiin jossain ulkomaisessa tiedusteluorganisaatiossa.**

---

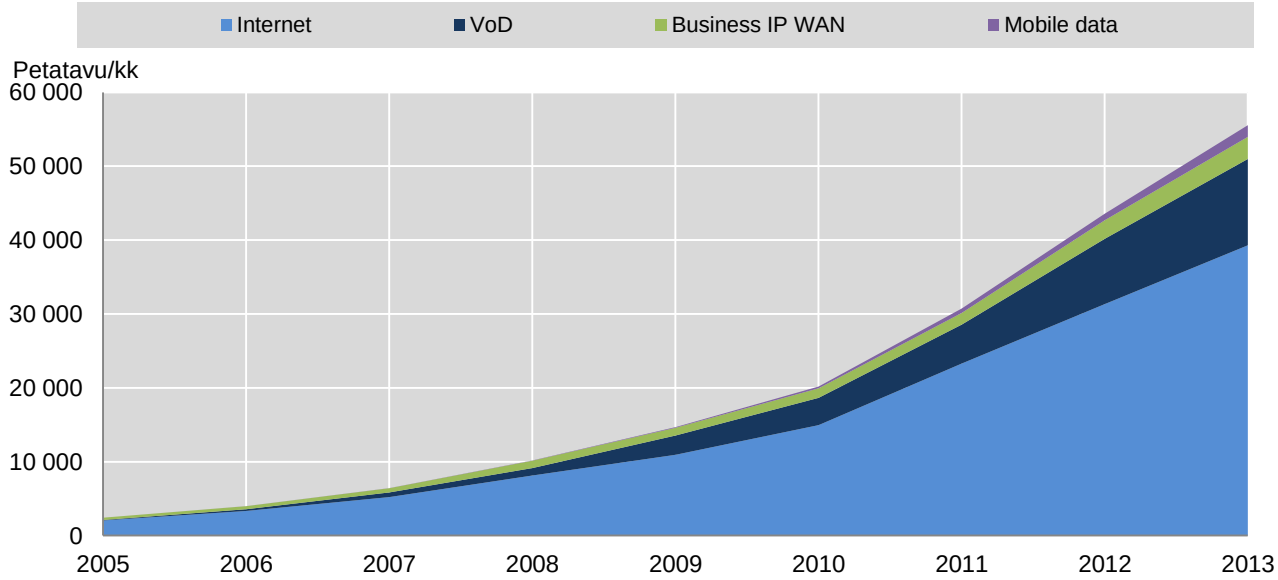
[15] Ks. esim. http://www.alexa.com/topsites, tai https://www.quantcast.com/top-sites.
[16] Alustakeskeisyydestä http://www.economist.com/news/special-report/21593583-proliferating-digital-platforms-will-be-heart-tomorrows-economy-and-even.
[17] Ks. esim. http://www.digitoday.fi/tietoturva/2014/06/04/google-facebook-ja-yahoo-salaavat-sahkopostit-comcast-ja-verizon-eivat/20147868/66.
[18] Ks. esim. http://www.wired.com/2014/05/sandvine-report/ ja https://www.sandvine.com/downloads/general/global-internet-phenomena/2014/1h-2014-global-internet-phenomena-report.pdf .
[19] Ks. esim. http://www.cigionline.org/internet-survey jossa 64 %:lla vastaajista jonkinasteinen huoli yksityisyydestä tietoverkoissa oli lisääntynyt viimeisen vuoden aikana.

Mietinnön mukaan verkkotiedustelulla voidaan salauksesta huolimatta saada kansallisen turvallisuuden kannalta merkittävää tietoa esimerkiksi tunnistamistietojen perusteella. Lisäksi salaamisella ei mietinnön mukaan ole vaikutusta tietoverkkohyökkäysten havaitsemiseen. Väitteitä ei ole perusteltu mietinnössä. Vaikka liikenne- ja viestintäministeriö on lähtökohtaisesti sitä mieltä, että tunnistamistietoja analysoimalla voidaan saada tietystä henkilöstä erittäin yksityiskohtaistakin tietoa selville, on mietinnössä esitetty väite tulkinnanvarainen. Tiettyjä tunnistamistietoja kuten sitä, mistä maasta tietty liikenne on peräisin, on jopa suhteellisen helppo salata erilaisilla palomuureilla tai hyödyntämällä salatuttuja erillisverkoja (VPN-yhteyksiä). Lisäksi esimerkiksi anonyymin verkkoselailun mahdollistavaa TOR-verkkoa käytettäessä käyttäjien anonymiteetti pyritään varmistamaan IP-osoitteita vaihtelemalla.[20] On todennäköistä, että tulevaisuudessa myös viestinnän tunnistamistietoja pyritään aktiivisemmin salaamaan.

Liikenteen määrän kasvu

Salaamisen kanssa rinnakkaisena ilmiönä tulee kiinnittää huomiota yleisissä viestintäverkoissa liikkuvan liikenteen määrän kasvuun tulevaisuudessa. Tämä selittyy paitsi internetin käytön lisääntymisellä niin myös teollisella internetillä, joka liittää yhä suuremman määrän laitteita verkkoon. On arvioitu, että vuoteen 2015 mennessä internetiin yhteydessä olevia laitteita on 25 miljardia ja että määrä kasvaa 2020 mennessä 50 miljardiin.[21] Lisäksi uutta tietoa arvioidaan syntyvän päivittäin miljardi gigatavua ja suurin osa siitä liikkuu internetissä.[22] Internetliikenteen määrän räjähdysmäistä kasvua kuvaa hyvin myös se, että liikenteen arvioidaan vuonna 2018 olevan 64-kertainen suhteessa vuoden 2005 liikennemäärään.[23] Kuten alla olevasta taulukosta ilmenee, IP-liikenteen määrä on OECD:n lukujen mukaan kovassa kasvussa.[24]

Global Internet Protocol (IP) traffic, 2005-13



OECD Science, Technology and Industry Scoreboard 2013 - © OECD 2013

[20] Internet toimii IP- eli Internet Protocol -osoitteilla. Kaikilla internetin verkko- ja päätelaitteilla, kuten tietokoneilla ja älypuhelimilla, on oma IP-osoitteensa. Osoitteet tarvitaan, jotta laitteet osaavat lähettää toisilleen viestejä. IP-osoitteita voikin verrata postiosoitteisiin. Ks. lisää http://pilvi.viestintavirasto.fi/internetpuhelin/internet/ip-osoitteet.html.
[21] http://share.cisco.com/internet-of-things.html.
[22] http://blogs.cisco.com/wp-content/uploads/GITR-2014-Cisco-Chapter.pdf.
[23] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html.
[24] http://www.oecd-ilibrary.org/science-and-technology/oecd-science-technology-and-industry-scoreboard-2013_sti_scoreboard-2013-en;jsessionid=mvepxnwi8azd.x-oecd-live-02.

Tiedonhankinnan kannalta uusien laitteiden liittäminen internetiin tarkoittaa sitä, että tietoverkoissa tulee liikkumaan yhä enemmän myös koneiden välistä viestintää. Tietoliikenteen määrän kasvaessa myös potentiaalisesti hyödyllisen tiedon määrä tietoverkoissa lisääntyy. Liikenteen määrän ja salauksen lisääntymisen yhteisvaikutuksena hyödyllisen tiedon löytämisestä tulee kuitenkin yhä vaikeampaa ja se voi vaatia yhä enemmän resursseja ja kapasiteettia. Tietoliikenteen määrän huomattava kasvu edellyttäisi myös kasvavia resursseja tiedon hankintaan, käsittelyyn ja salauksen purkamiseen. Näitä ei ole mietinnössä arvioitu.

4. Verkkovalvonnalla voi olla merkittäviä vaikutuksia yritystoimintaan

Työryhmä on työskentelynsä aikana pyrkinyt selvittämään elinkeinoelämän näkemyksiä verkkotiedustelutoimivaltuuksien mahdollisista vaikutuksista. Verkkovalvonnan osalta liikenne- ja viestintäministeriö on tuonut esille, että sillä voi olla negatiivisia vaikutuksia elinkeinoelämän kilpailukykyyn ja investointien suuntautumiseen.[25]

Liikenne- ja viestintäministeriö myöntää, että lopulliset vaikutukset ovat vaikeasti arvioitavissa, mutta korostaa, että yritysvaikutuksia on silti arvioitava perusteellisesti. Arvioinnissa olisi huomioitava erityisesti Snowden-paljastusten jälkeinen aika, tietointensiivisen teollisuuden taloudellinen merkitys tulevaisuudessa ja toimialan kasvunäkymät sekä yleinen digitalisaatiokehitys ja markkinatilanne. Lisäksi tulisi huomioida, että Suomella pitkät perinteet ja paljon osaamista digitaalisen talouden alalla.

Liikenne- ja viestintäministeriö korostaa, että vaikutukset yritystoiminnalle voivat olla erilaisia riippuen muun muassa yrityksen toimialasta, koosta ja sen harjoittamasta kansainvälisestä toiminnasta. Selkeimmin verkkovalvonnan voidaan katsoa vaikuttavan teleyrityksiin, jotka joutuisivat osallistumaan verkkovalvonnan tekniseen toteuttamiseen. Teleyritysten lisäksi verkkovalvonnalla voisi olla vaikutuksia lähes kaikkiin yrityksiin, jotka jollain tavalla toimivat internetin kautta. Erityisesti sillä voi olla vaikutuksia ICT- ja tietoturvayrityksiin, joiden asiakaslupaukset sisältävät elementtejä tiedon ja viestinnän luottamuksellisuudesta. Suorien yritysvaikutusten lisäksi on otettava huomioon epäsuorat vaikutukset kulutuskäyttäytymiseen ja vaikutukset niihin mielikuviin, joiden perusteella kuluttajat käyttävät erilaisia sisältöjä ja palveluita.

Yritysvaikutuksina on huomioitava myös vaikutukset yritysten sijoittautumispäätöksiin, eli investointeihin Suomeen. Kun tietointensiivisen teollisuuden yritykset tekevät sijoittautumispäätöksiä, ne pyrkivät ennakoimaan toimintaansa kohdistuvat oikeudelliset riskit. Huomion kohteena ovat tällöin erityisesti sijoittautumisvaltion lainsäädännön soveltuminen sekä sen aikaansaamat myönteiset ja kielteiset vaikutukset yrityksen liiketoimintaan.[26]

Kun tietointensiivisen teollisuuden yritys tekee sijoittautumispäätöksiä ja liiketoimintasuunnitelmia, eli esimerkiksi päätöstä siitä sijoitetaanko tietty palvelinkeskus Suomeen, yritys huomioi sääntelyn, joka koskee ulkopuolisten tahojen kuten viranomaisten pääsyä yritysten tie-

[25] Tiedonhankintalakityöryhmän mietinnön liitteenä 2. on yhteenveto työryhmän työskentelyn aikana kuultujen sidosryhmien ja asiantuntijoiden kannanotoista. Lisäksi puolustusministeriön internet-sivuilta löytyy tietoja elinkeinoelämälle 29.4.2014 järjestetystä kuulemistilaisuudesta: http://www.defmin.fi/index.phtml?s=767.

[26] Dittmar & Indreniuksen liikenne- ja viestintäministeriölle tekemä selvitys aiheesta: Dataintensiivisen teollisuuden sijoittautumisen edellytykset, 2014.

toon.[27] Tämän lisäksi se arvioi tietosuojaan ja viestinnän luottamuksellisuuteen sekä tietoyhteiskunnan palveluntarjoajiin liittyvät säännökset ja niiden kattavuuden. Tällä hetkellä Suomen rajoitetut viranomaisvaltuudet ja -käytännöt tukevat käsitystä Suomen korkeasta tietosuojan tasosta ja palveluiden piirissä olevien tietojen luottamuksellisuudesta. Toisaalta sijoittautumispäätökset ovat kokonaisarviointeja, joissa huomioidaan myös tekijöitä kuten verotus, sähkön hinta ja saatavuus, työvoimaan liittyvät velvoitteet, yhteiskunnallinen ja poliittinen vakaus, ilmasto ja niin edelleen.

Sijoittautumispäätösten yhteydessä on huomioitava, että yleisen teknistymiskehityksen myötä myös sellaiset alat, jotka eivät perinteisesti ole nojanneet dataan liiketoiminnassaan, ottavat käyttöön analytiikkaa ja muita digitaalisen tiedon hyödyntämisen välineitä. Tämä tarkoittaa, että teollisen internetin sovellutukset ja tietointensiivinen teollisuus tulee lisääntymään lähivuosina voimakkaasti.

Työryhmän mietinnössä viitataan harhaanjohtavasti tutkimus- ja konsulttiyhtiö Gartnerin tutkimukseen. Tutkimuksen mukaan Ruotsi ja Norja koetaan houkuttelevina konesalien sijoituspaikkoina ja todetaan, ettei niiden tiedustelulainsäädäntö ole noussut tutkimuksessa esille.[28] Kyseisessä tutkimuksessa ei ole varsinaisesti eritelty eri maiden houkuttelevuutta konesali-investoinneille lainsäädännön näkökulmasta, vaan siinä on lähinnä pyritty toteamaan asioita, joita sijoittautumisessa olisi huomioitava. Lisäksi tutkimuksessa on laskettu sähkön hinnan vaikutusta konesalien ylläpitämisen kustannuksiin. Ruotsissa ja Norjassa sähkön hinta on laskenut verrattuna Keski-Eurooppaan. Yhtenä sijoittautumiseen vaikuttavana tekijänä Gartnerin tutkimuksessa on mainittu turvallisuusvaatimusten noudattaminen, jonka yksi osa on kohdemaan tietosuojasääntely.

Työryhmä viittaa mietinnössä myös Gearshift Group Oy konsulttitoimistolla teettämäänsä selvitykseen.[29] Selvityksen otsikon mukaan työssä on arvioitu tiedustelulainsäädännön kehittämisen näkökulmasta IT-sektoriin kohdistuvien ulkomaisten investointien kehittymistä ja Ruotsin signaalitiedustelua koskevan niin sanotun FRA-lain mahdollisia vaikutuksia toteutuneeseen investointitoimintaan Ruotsissa. Selvitys on rajattu vuosiin 2008–2013. Käytännössä mietintö ei siis kata Snowden-paljastusten jälkeistä aikaa.[30] Nimenomaan paljastusten jälkeiset arviot investointien suuntautumisesta, olisivat olleet verkkovalvonnan arvioinnin kannalta hyödyllisiä. Selvityksessä ei myöskään ole investointien osalta käytetty materiaalina IT-investointeihin keskittyviä tilastoja.[31] Selvityksessä investointien kehitystä on käsitelty yleisten talouden indikaattorien perusteella, eikä niistä ole yksilöitävissä digitaalista taloutta ja vasta kehittymässä olevaa tietointensiivistä teollisuutta.

Gearshift Group Oy:n selvityksen mukaan Ruotsin selkeä tiedustelulainsäädäntö saattaa olla jopa kilpailuetu.[32] Selkeä sääntely ja sääntelyn sovellettavuus ovat yritystoiminnan ennakoitavuuden kannalta tärkeä tekijä ja myös mahdollinen kilpailuvaltti. Liikenne- ja viestintäministeriön vuonna 2014 teettämän konesalien sijoittumiseen liittyvän Gearshift Group Oy:n laatiman selvityksen mukaan sen sijaan, Snowden-paljastukset voidaan katsoa yhdeksi sellaiseksi markkina-ajuriksi, joka ohjaa yritysten mielenkiintoa nimenomaan Yhdysvalloista Euroop-

[27] Ks. Dittmar & Indreniuksen liikenne- ja viestintäministeriölle tekemä selvitys aiheesta: Dataintensiivisen teollisuuden sijoittautumisen edellytykset, 2014.
[28] Lisätietoa tutkimuksesta: http://www.gartner.com/newsroom/id/2884318.
[29] Selvitys on liitteenä mietinnössä. Se on otsikoitu: ” IT sektoriin kohdistuvien ulkomaisten investointien kehittyminen Ruotsissa ja Suomessa vuosina 2008 - 2013 ja Ruotsin ”FRA-lain” mahdolliset vaikutukset investointeihin”.
[30] Selvityksessä monet esitetyistä kuvioista ja taulukoista koskevat aikaa ennen vuotta 2013. Ks. Gearshift Group Oy:n selvitys tiedonhankintalakityöryhmälle, s. 5-8, 11.
[31] Ks. Gearshift Group Oy:n selvitys tiedonhankintalakityöryhmälle, s. 5-6.
[32] Ks. Gearshift Group Oy:n selvitys tiedonhankintalakityöryhmälle, s. 10.

paan.[33] Lisäksi tieto siitä, että verkkovalvontaa ei maassa harjoiteta lisää yhtälailla yritystoiminnan ennakoitavuutta.

Investointien menetyksestä ja verkkovalvonnan mahdollisesti aiheuttamasta mainehaitasta on vaikeaa antaa kattavaa arviointia. Kuten aiemmin kuvattiin, esimerkiksi investointien suuntautuminen perustuu monipuoliseen vaikutustenarviointiin yrityksen liiketoiminnan kannalta. Kun pilvipalvelumarkkinat edelleen kasvavat, tarvitaan konesaleja kuitenkin lisää. Onkin havaittavissa, että isoja palvelinkeskusten investointipäätöksiä tehdään seuraavien vuosien aikana ja nyt tehtävät päätökset vaikuttavat toimialan kehitykseen seuraavat 15 vuotta.[34] Sijoittautumispäätökset ja konesalien rakentaminen Suomeen ovat jo itsessäänkin tavoiteltavia investointeja, mutta vielä merkittävämpänä mahdollisuutena voidaan nähdä konesalien yhteyteen muodostuvat laajemmat ekosysteemit. Pelkkien palvelimien sijaan datakeskuksen ympärille voi kehittyä muutakin toimintaa kuten lisäarvopalveluita ja tutkimus- ja tuotekehitystoimintaa.[35]

Snowdenin paljastusten jälkeen on jo ehditty arvioida, että paljastusten vaikutukset amerikkalaisten pilvipalveluyritysten liiketoimintaan voisivat alakanttiin arvioitaessakin olla yhteensä yli 20 miljardin dollarin luokkaa vuosina 2014–2016.[36] Myös amerikkalaiset yritykset ovat tuoneet julkisesti esille laajamittaisen tiedustelutoiminnan paljastumisesta yrityksilleen aiheutuneita taloudellisia ja luottamukseen liittyviä haittoja.[37]

Suomella on edellytykset pärjätä hyvin kilpailussa konesali-investoinneista. Viestinnän luottamuksellisuus ja yksityisyyden suoja on meillä korkealla tasolla, olemme liittoutumaton, luotettava ja yhteiskunnallisesti ja poliittisesti vakaa maa, eikä meillä ole odotettavissa esimerkiksi palvelinkeskuksia vaarantavia geologisia järistyksiä. Viileän ilmaston lisäksi sähkön saatavuus ja hinta ovat erityisesti datakeskusten sähköveronalennuksen jälkeen hyvällä tasolla. Meillä on myös paljon osaavaa ICT:n alan työvoimaa. **Lisäksi Suomeen on parhaillaan rakentumassa suurikapasiteettinen kansainvälinen tietoliikennekaapeliyhteys Eurooppa.** Toistaiseksi kaikki kansainvälinen liikenne on reitittynyt Ruotsin kautta, mikä on ollut Suomelle epäedullista. Tämä muuttuu kun Itämeren kaapeli valmistuu vuonna 2016. Yhdessäkään palvelinkeskusten sijaintiselvityksessä ei ole ehditty ottaa huomioon tätä Suomen kilpailuasemaan merkittävästi vaikuttavaa tekijää. Itämeren kaapelin rinnalla hallitus on sitoutunut myös edistämään aktiivisesti koillisväylän arktisen merikaapelin rakentamista. Koillisväylän kaapelin rakentaminen olisi merkittävä kilpailutekijä ja sen myötä Suomi voi vahvistaa asemaansa globaalina tietoliikenteen solmukohtaa Euroopan ja Aasian välillä.

Mietinnössä on vastattu väitteeseen verkkovalvonnan Suomen korkeaa tietosuojaa heikentävästä vaikutuksesta toteamalla, että verkkovalvonta kohdistuisi Suomen rajat ylittävään tietoliikenteeseen, joka kulkee sellaisten maiden läpi, joissa on verkkovalvontaa koskevaa lainsäädäntöä. Tämä merkitsee sitä, että Suomen kansainvälisten verkkoyhteyksien kautta kulkeva tietoliikenne voi jo nyt olla valvonnan ja tiedustelun kohteena muiden kuin Suomen viranomaisten taholta. Mietinnössä esitetty pitää ainakin osittain paikkaansa. Se, että muissa maissa suoritetaan verkkovalvontaa, ei perustele sitä, että valvonta olisi Suomessa viranomaisten

[33] Gearshift Group Oy:n Liikenne- ja viestintäministeriölle tekemä selvitys aiheesta: Konesalien rakentamisen suomalaisen kilpailukyvyn kehittäminen ”Lessions learned”, 2014, s. 7.
[34] Gearshift Group Oy:n Liikenne- ja viestintäministeriölle tekemä selvitys s. 12.
[35] Ks. lisää http://kideblogi.wordpress.com/2014/09/05/datakeskusten-ekosysteemia-rakentamassa/.
[36] Information Technology and Innovation Foundation: How Much Will PRISM Cost the U.S. Cloud Computing Industry? http://www2.itif.org/2013-cloud-computing-costs.pdf . Ks. myös http://oti.newamerica.net/sites/newamerica.net/files/policydocs/Surveilance_Costs_Final.pdf .
[37] Ks. esim. ”Cisco says NSA disclosures have affected sales” http://www.cnbc.com/id/101202361 ja https://www.youtube.com/watch?v=m-P4Q-M1tW8 .

lakisääteisten tehtävien suorittamiseksi tarpeellista ja välttämätöntä. Myös muissa maissa suoritetun verkkovalvonnan teho on nykyään kyseenalaistettu koska suojausten tasoja on olennaisesti nostettu. Suomella voisi olla mahdollisuus tulla tärkeäksi, turvallisuudesta huolehtivaksi datakeskittymäksi ja profiloida itseään maana, jossa verkkovalvontaa ei suoriteta.

5. Verkkovalvonnalla rajoitetaan perusoikeuksia, erityisesti oikeutta yksityisyyteen

Tekninen pääsy kaikkeen tietoliikenteeseen rajoittaa lähtökohtaisesti jokaisen suomalaisen perustuslailla turvattua oikeutta yksityisyyteen. Nykyisen perustuslain 10 §:n sisällöstä säädettiin jo vuoden 1995 perusoikeusuudistuksen yhteydessä säätämällä hallitusmuodon 8 §, joka siirrettiin sellaisenaan perustuslakiin vuonna 2000 (10 §). Hallitusmuodon 8 §:n perusteluissa todetaan, että **yksityiselämän suojan lähtökohtana on, että yksilöllä on oikeus elää omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä.**

Yksityiselämän piirin tarkka määritteleminen on vaikeaa. Siihen kuuluu muun muassa yksilön oikeus vapaasti solmia ja ylläpitää suhteita muihin ihmisiin ja ympäristöön sekä oikeus määrätä itsestään ja ruumiistaan. Yksityisyyden suojan ulottuvuuteen liittyvää rajanvetoa tullaan tekemään lähivuosina niin kotimaassa kuin kansainvälisestikin, koska sen merkitys tulee kasvamaan digitaalisen maailman ilmiöiden myötä.[38] Ihmisistä kerääntyy kiihtyvällä vauhdilla enemmän tietoa erilaisiin järjestelmiin kuin koskaan ennen. Myös tiedon analysointi ja erilaisiin suuriin tietoaineistoihin perustuvien johtopäätöksien teko kehittyy.[39]

Mietinnössä ehdotetun verkkovalvonnan arviointia suhteessa yksityisyyden suojaan voidaan hahmottaa kolmesta eri näkökulmasta:

1) Verkkovalvonta suhteessa luottamuksellisen viestinnän sisältöön
2) Verkkovalvonta suhteessa viestien tunnistamistietoihin
3) Verkkovalvonta suhteessa henkilötietojen käsittelyyn

Tiedonhankintalakityöryhmän mietinnössä on todettu, että tiedustelutarkoituksessa toteutettavasta verkkovalvonnasta ei näyttäisi olevan mahdollista säätää perustuslakia muuttamatta. Tämä johtuu siitä, ettei kansallista turvallisuutta ole mainittu perustuslain 10.3 §:ssä[40] perusteena rajoittaa viestinnän luottamuksellisuutta. **Liikenne- ja viestintäministeriö on toistuvasti esittänyt tämän myös omana näkemyksenään.**

Mietinnössä todetun lisäksi liikenne- ja viestintäministeriö haluaa erityisesti kiinnittää huomiota verkkovalvontaan suhteessa tunnistamistietoihin ja henkilötietojen käsittelyyn.

Yksityiselämän suojan kannalta merkityksellisenä voidaan pitää eduskunnan, tietoyhteiskuntakaaren säätämisen yhteydessä antamaa lausumaa. Siinä **eduskunta edellyttää, että palvelujen käyttäjien oikeuksien, kuten yksityisyyden suojan ja luottamuksellisen viestin**

[38] Näitä kuvattu esimerkiksi eriävänä mielipiteen luvussa 3.
[39] Lue lisää esim. Liikenne- ja viestintäministeriön julkaisu 20/2014: Big datan hyödyntäminen, http://www.liikenne- ja viestintäministeriö.fi/julkaisu/4417803/big-datan-hyodyntaminen .
[40] Perustuslain 10.3 §:ä ”Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana.”.

suojan säilymisestä sähköisissä palveluissa ja verkkoympäristössä huolehditaan kaikin keinoin ja muun muassa kyberturvallisuuden kehittämistyössä pyritään erityisesti ottamaan näiden oikeuksien toteutuminen huomioon.[41]

Suhtautuminen viestien tunnistamistietoihin (välitystiedot, metadata)[42] ja niiden paljastavuuteen on muuttunut. Tunnistamistietoja ovat tyypillisesti esimerkiksi tiedot siitä kuka puhuu puhelimessa kenenkin kanssa, ketkä lähettävät toisilleen sähköposti- tai tekstiviestejä tai millä internetsivustoilla kukin vierailee. Lisäksi tunnistamistietoja voivat olla myös teknisemmät tiedot kuten tiedot viestinnän reitityksestä, kestosta, ajankohdasta, siirrettävien tietojen määrästä, käytetystä protokollasta, tai tiedot lähettäjän tai vastaanottajan päätelaitteen sijainnista tietyn tukiaseman alueella. Sähköisen viestinnän monimuotoistuessa tunnistamistietojen tyhjentävä määrittely hankaloituu, mutta määritelmänsä mukaisesti ne ovat tietoja, jotka voidaan yhdistää oikeus- tai luonnolliseen henkilöön ja joita käsitellään viestin välittämiseksi.

Kuten mietinnössäkin todetaan perustuslakivaliokunnan vakiintuneen käytännön mukaan viestin tunnistamistiedot jäävät luottamuksellisen viestinnän suojaa koskevan perusoikeuden ydinalueen ulkopuolelle. Perustuslakivaliokunta on kuitenkin tietoyhteiskuntakaarta koskevassa lausunnossaan antanut viitteitä tulkintakäytännön muutoksesta:

”Käytännössä sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat kuitenkin olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen.”[43]

On siis mahdollista, että perustuslakivaliokunta voi jatkossa antaa myös tunnistamistiedoille viestinnän sisältöä vastaavaa suojaa, jos perusoikeuden rajoitus on arvioitavissa merkittäväksi. Selvää kuitenkin on, ettei tunnistamistietojen keräämistä ja erityisesti yhdistämistä muihin tietoihin, voida enää pitää kategorisesti perusoikeussuojan reuna-alueelle kohdistuvana perusoikeuden rajoituksena. **Tiedonhankintalakityöryhmä ei ole yksimielisesti pystynyt tekemään johtopäästöstä siitä, muodostavatko verkkovalvonnassa kerätyt tunnistamistiedot niin merkittävän rajoituksen perustuslain 10 §:n mukaiseen yksityiselämän suojaan, että rajoitus ulottuu perusoikeussuojan ydinalueelle ja edellyttää jo itsessään perustuslain muutosta.** Käytännössä on kyse siitä, voitaisiinko verkkovalvonta ilman perustuslain muutosta kohdistaa tunnistamistietoihin, kun viestinnän sisällön osalta tämä ei ole mahdollista.

Keskustelua tunnistamistietojen paljastavuudesta suhteessa viestinnän luottamuksellisuuteen käydään tekniikan kehityksen takia yleisesti Euroopassa ja muissa länsimaissa. Asiaan on otettu kantaa esimerkiksi EU:n tietosuojaviranomaisten muodostaman **WP29:n tietosuojatyöryhmän** lausunnossa sähköisen viestinnän tarkkailusta tiedustelua ja kansalliseen turvallisuuteen liittyviä tarkoituksia varten.[44] Lausunnossa muun muassa todetaan, että valtion virkamiehet puhuvat usein metatiedon keräämisestä antaen ymmärtää, ettei se ole yhtä vakavaa kuin sisällön kerääminen. Lisäksi lausunnossa myös todetaan, että itse asiassa metatieto paljastaa tietoja helpommin kuin viestien varsinainen sisältö. Metatietoa on helppo yhdistellä ja analy-

[41] Ks. Eduskunnan vastaus 106/2014 vp: http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/ev_106_2014_p.shtml.
[42] Tietoyhteiskuntakaari (917/2014) käyttää käsitettä välitystiedot. Aiemmin sähköisen viestinnän tietosuojalaissa puhuttiin viestinnän tunnistamistiedoista ja usein kansainvälisesti puhutaan metadatasta. Välitystiedot ovat oikeus- tai luonnolliseen henkilöön yhdistettäviä tietoja, joita käsitellään viestin välittämiseksi esimerkiksi tiedot lähettäjästä ja viestin vastaanottajasta, lähetysajankohdasta ja käytetyistä osoitteista yms.
[43] PeVL 18/2014 vp, s. 6.
[44] WP29 819/14/FI, WP 215, annettu 10. huhtikuuta 2014. Erityisesti sivut 4-5. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm .

soida, koska se on jäsenneltyä. Pitkälle kehitetyillä tietoteknisillä välineillä voidaan analysoida suuria tietoaineistoja ja tunnistaa niihin sisältyviä säännönmukaisuuksia ja suhteita, kuten henkilötietoja, tottumuksia ja käyttäytymistapoja. Myös YK:n ihmisoikeuskomissaarin raportissa, yhdytään WP29-työryhmän kantaan toteamalla, että yksityisyyden suojan kannalta erottelu viestin sisällön ja sitä koskevan tiedon välillä ei ole vakuuttava.[45]

Euroopan unionin tuomioistuimen tuomio tunnistamistietojen pakkotallennusdirektiivistä[46]

Yksityisyyden suoja on ollut viime aikoina esillä myös muutamissa merkittävissä Euroopan Unionin tuomioistuimen ratkaisuissa. Näistä mietinnön kannalta keskeisin on EU-tuomioistuimen 8.4.2014 antama tuomio yhdistetyissä asioissa C-293/12 ja 594/12 Digital Rights Ireland ja Seitlinger ym., jota on käsitelty mietinnössä.[47] Tuomiossa pätemättömäksi todetun direktiivin nojalla jäsenvaltioiden on pitänyt velvoittaa teleoperaattoreita tallentamaan sähköisen viestinnän tunnistamistietoja viranomaistarpeita varten.[48] Tässä liikenne- ja viestintäministeriön eriävässä mielipiteessä ei ole tarkoitus käsitellä kyseistä tuomiota laajemmin kuin mietinnössä. Sen sijaan tarkoitus on tuoda esiin huomioita, jotka puuttuvat mietinnöstä.

EU-tuomioistuin tarkastelee tuomiossaan tunnistamistietojen pakkotallennusdirektiivin säännöksiä ja toteaa, että säilytettävät tunnistamistiedot voivat yhdessä antaa hyvin tarkkaa tietoa henkilöiden yksityiselämästä, muun muassa heidän elintavoistaan, vakituisista tai tilapäisistä oleskelupaikoistaan, päivittäisestä tai muusta liikkumisestaan, tekemisistään, sosiaalisista suhteistaan ja sosiaalisesta ympäristöstään. Vaikka direktiivissä ei sallita viestinnän sisällön säilyttämistä, tunnistamistietojen säilyttäminen voi vaikuttaa siihen, miten henkilöt käyttävät direktiivissä tarkoitettuja viestintävälineitä. Toisin sanoen, vaikka direktiivi ei edellytä tietojen hankkimista sähköisen viestinnän sisällöstä, eikä näin ollen kohdistu yksityiselämän suojaa ja henkilötietojen suojaa koskevien perusoikeuksien keskeiseen sisältöön, niin silti tietojen säilyttämisellä direktiivissä tarkoitetuin tavoin siltä varalta, että toimivaltaiset kansalliset viranomaiset haluaisivat tutustua niihin, puututaan EU-tuomioistuimen mukaan erityisen vakavasti EU:n perusoikeuskirjan 7 artiklassa tarkoitettuun yksityis- ja perhe-elämän kunnioittamiseen ja perusoikeuskirjan 8 artiklassa tarkoitettuun henkilötietojen suojaan.

Tuomioistuin myös toteaa, että tietojen säilyttäminen ja myöhempi käyttäminen ilman, että siitä ilmoitetaan henkilölle, saattaa aiheuttaa tälle tunteen yksityiselämän jatkuvasta valvonnasta.

Tunnistamistietojen pakkotallennusdirektiivissä tarkoitettu tietojen tallentaminen ja mietinnössä käsitelty verkkovalvonta eivät olisi tekniseltä toteutukseltaan täysin vastaavia toimintoja. Mietinnön mukaan verkkovalvonta ei edellyttäisi perustuslakivaliokunnan lausunnossaan esiintuomaa tunnistamistietojen laajamittaista, erittelemätöntä, pitkäaikaista ja rajoittamatonta tallentamista, vaan kyse olisi hakuehtoihin perustuvasta tietoliikenteen suodattamisesta. Verkkovalvonnassa tallennettaisiin sellaiset viestintään liittyvät tiedot, jotka vastaisivat määriteltyjä

[45] A/HRC/27/37, s. 6-7. Välitystietojen paljastamista tiedoista ks. esim. Stanfordin yliopiston jatko-opiskelijoiden tutkimus (http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/).

[46] Tiedonhankintalakityöryhmän mietinnössä käytetään direktiivistä nimeä Data Retention -direktiivi, tässä eriävässä mielipiteessä puhutaan tunnistamistietojen pakkotallennusdirektiivistä. Direktiivin täydellinen nimi on ”Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta 15.3.2006 annettu Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY”. Tuomio saatavilla: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d594b5070ed47541ce9786bce364f3cac9.e34KaxiLc3eQc40LaxqMbN4Obh8Re0?text=&docid=150642&pageIndex=0&doclang=FI&mode=req&dir=&occ=first&part=1&cid=8134.

[47] Luvussa 6.1.2.3.

[48] Suomen kansalliset säännökset sisältyvät 1.1.2015 voimaan tulevaan tietoyhteiskuntakaareen (917/2014).

hakuehtoja. Riippuen toimeksiannosta ja hakutermeistä, tallennettaisiin siis käsittelyä varten tietty tietoliikenne ja sen tunnistamistiedot.

Käytännössä, jotta verkkovalvontaa voitaisiin suorittaa, tarkoittaisi tämä sitä, että viranomaisilla olisi pääsy kaikkeen tietoliikenteeseen, josta aina tietty osa otettaisiin talteen hakutermien perusteella. Siinä mielessä tunnistamistietojen pakkotallennusdirektiivin mukaisten tietojen ja verkkovalvonnan välillä ei olisi merkittävää eroa, että molemmissa viranomaisella olisi tiettyjen reunaehtojen täyttyessä pääsy viestintää koskeviin tunnistamistietoihin. Verkkovalvonnassa käytettyjen hakutermien merkitys kasvaa kuitenkin suureksi. Mitä epämääräisempää tai laajempaa hakutermiä käytettäisiin, sitä enemmän liikennettä suodattuisi jatkokäsittelyyn. Tunnistamistietojen pakkotallennusdirektiivin mukaisia tietoja taas voidaan saada rikosten tutkimiseksi ja syyteharkintaan saattamiseksi käyttöön vain yksilöidyissä tapauksissa.

EU-tuomioistuimen tunnistamistietojen pakkotallennusdirektiiviä koskeva tuomio ja siinä esitetty suhteellisuusperiaatteen arviointi on otettava lähtökohdaksi, jos edes harkitaan sääntelyä verkkovalvonnasta. **Erityisesti on huomioitava se, että tuomion perusteella avoimeksi jää, kuten perustuslakivaliokuntakin totesi, merkitseekö viranomaistarpeita varten säädetyn säilyttämisvelvollisuuden ulottuminen käytännössä kaikkien sähköisiä viestimiä käyttävien ihmisten tietoihin jo yksinään oikeasuhtaisuusvaatimuksen loukkausta.** Jos näin arvioidaan, ei myöskään viranomaisten pääsyä kaikkeen tietoliikenteeseen, voida pitää oikeasuhtaisena.

Henkilötietojen suoja

Perustuslain 10.1 §:ssä, todetaan, että henkilötietojen suojasta säädetään tarkemmin lailla. Hallituksen esityksen mukaan säännös viittaa tarpeeseen lainsäädännöllisesti turvata yksilön oikeusturva ja yksityisyyden suoja henkilötietojen käsittelyssä, rekisteröinnissä ja käyttämisessä.[49] Säännöksellä myös edellytetään lainsäädännöllisiä järjestelyjä henkilötietojen suojasta.

On olennaista huomata, että tunnistamistietojen pakkotallennusdirektiiviä koskevassa tuomiossa EU-tuomioistuin katsoi, että tunnistamistietojen säilyttämisellä loukattiin myös EU perusoikeuskirjan 8 artiklassa tarkoitettua henkilötietojen suojaa. Vaikka tunnistamistiedot eivät aina välttämättä ole henkilötietoja, edellyttää tunnistamistietojen tallentaminen kuitenkin yleensä myös henkilötietojen käsittelyä. EU-tuomioistuin totesikin, että tunnistamistietojen tallentamisen tulee täyttää myös kaikki henkilötietojen suojaan liitetyt vaatimukset.

Mietinnössä on käsitelty henkilötietojen suojaa Euroopan unionin perusoikeuskirjan näkökulmasta, mutta ei Suomen perustuslain. Verkkovalvonnassa väistämättä käsiteltäisiin henkilötietoja, joten tällöin tulisi noudattaa perustuslakivaliokunnan kannanottoja henkilötietojen käsittelystä säätämisestä.

Verkkovalvontaa koskeva sääntely olisi merkityksellistä yksityiselämän ja henkilötietojen suojaa koskevan perustuslain 10 §:n kannalta. Sen 1 momentin mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslakivaliokunnan vakiintuneen käytännön mukaan lainsäätäjän liikkumavaraa rajoittaa tämän säännöksen lisäksi myös se, että henkilötietojen suoja osittain sisältyy samassa momentissa turvatun yksityiselämän suojan piiriin. Kysymys on kaiken kaikkiaan siitä, että lainsäätäjän tulee turvata tämä oikeus tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa. Perustuslakivaliokunta on käytännös-

[49] HE 309/1993 vp. 8 §:n yksityiskohtaiset perustelut.

sään pitänyt henkilötietojen suojan kannalta tärkeinä sääntelykohteina ainakin rekisteröinnin tavoitetta, rekisteröitävien henkilötietojen sisältöä, niiden sallittuja käyttötarkoituksia mukaan luettuna tietojen luovutettavuus sekä tietojen säilytysaikaa henkilörekisterissä ja rekisteröidyn oikeusturvaa. Näiden seikkojen sääntelyn lain tasolla tulee lisäksi olla kattavaa ja yksityiskohtaista.[50]

Liikenne- ja viestintäministeriö katsoo, että mietintö on henkilötietojen käsittelyn osalta puutteellinen.

Tietoyhteiskuntakaaren 272 §[51]

Tietoyhteiskuntakaaren 272 §:ä ja sen mahdollistama tietoliikenteen seulonta tietoturvasta huolehtimiseksi on mietinnössä rinnastettu verkkovalvontaan. **Liikenne- ja viestintäministeriö katsoo, ettei tietoyhteiskuntakaaren 272 §:n käsittely verkkovalvonnan yhteydessä ole tarkoituksenmukaista.** Vaikka tietoyhteiskuntakaaren 272 §:ssä tarkoitetut toimenpiteet saattavat teknisesti olla lähellä verkkovalvontaa, ei kyseistä sääntelyä voi muilta osin verrata verkkovalvonnasta säätämiseen.

Tietoyhteiskuntakaaren 272 §:n mukaiset tietoturvatoimenpiteet ja tiedustelutarkoituksessa toteutettava verkkovalvonta olisivat sekä yksityisyydensuojaan puuttumisen että toimenpiteiden kohteeksi joutuvien organisaatioiden näkökannalta täysin erilaisia toimia. Yksityisyydensuojan osalta tietoturvatoimenpiteillä pyritään ainoastaan tietoturvaongelman selvittämiseen. Tietoa ei voida käyttää muihin tarkoituksiin. Organisaatiot arvioivat itse toimenpiteiden laajuuden ja tarpeellisuuden. Toimenpiteet käsitellään henkilöstön kanssa yhteistoimintamenettelyssä.

Perustuslain 22 §:n mukaan julkisen vallan tehtävänä on turvata perusoikeuksien ja ihmisoikeuksien toteutuminen. Yksityiselämän suojan takaamiseksi valtiolta on sen lisäksi, että se itse pidättäytyy loukkaamasta kansalaisten yksityiselämää, edellytetty aktiivisia toimenpiteitä yksityiselämän suojaamiseksi toisen yksilöiden loukkauksia vastaan. Perustuslain esitöiden mukaan myös viestinnän luottamuksellisuuden suoja edellyttää toteutuakseen lainsäädäntöä, joka tehokkaasti turvaa luottamuksellista viestintää sekä viranomaisten että muiden ulkopuolisten loukkauksilta.[52] **Tietoyhteiskuntakaaren 272 §:ssä on kyse tällaisesta aktiivisesta toimenpiteestä luottamuksellisen viestinnän suojaamiseksi.** Sen sijaan verkkovalvontaa koskeva sääntely ei ole perusteltavissa luottamuksellisen viestinnän suojaamisella, eikä siinä siten ole samalla tavalla kyse perusoikeuden toteutumista turvaavasta välttämättömästä sääntelystä kuin tietoyhteiskuntakaaren 272 §:ssä. Sen tarkoitus on päinvastaisesti tiedon luottamuksellisuuden murtaminen.

[50] Ks. koko kappaleen osalta esim. PeVL 14/2009 vp , s. 2, PeVL 11/2008 vp , s. 3/I ja PeVL 51/2002 vp , s. 1-2, PeVL 14/2002 vp , s. 2/II.
[51] Tietoyhteiskuntakaari (917/2014) tulee voimaan 1.1.2015, 272 § vastaa sisällöltään sähköisen viestinnän tietosuojalain (516/2004) 20 §:ää.
[52] HE 209/1993 vp.

6. Verkkovalvonta ei parantaisi tietoturvaa, vaan heikentäisi sitä

Tietoturvallisuudella tarkoitetaan vakiintuneesti toimenpiteitä, joilla turvataan jonkin tiedon luottamuksellisuus, eheys ja käytettävyys.[53] Työryhmän tarkastelemilla tiedustelukeinoilla pyrittäisiin ohittamaan tai murtamaan tiedonhankinnan kohteena olevan henkilön tai hänen käyttämänsä tietojärjestelmän tietoturvallisuutta varmistavat suojaukset ja hankkimaan tiedonhankintaa suorittavalle viranomaiselle sellaista tietoa, johon kohde ei ole oikeuttanut ulkopuolisia pääsemään käsiksi. **On selvää, että mietinnössä tarkasteltu verkkovalvonta heikentäisi kaikkien niiden henkilöiden tietoturvallisuutta, joiden viestejä välitettäisiin verkkovalvonnan kohteena olevissa viestintäverkoissa.**

Liikenne- ja viestintäministeriö katsoo, että sen perustuslaista johtuvana tehtävänä on nimenomaisesti edistää yksityisyyden suojan ja viestinnän luottamuksellisuuden toteutumisesta tietoturvallisesti sähköisessä viestinnässä.[54] Perusoikeuksien toteutumisen turvaamiseksi on tärkeää, että kansalaisten, yritysten ja muiden yhteisöjen käytettävissä on korkealaatuisia, luotettavia ja tietoturvallisia viestintäpalveluja.[55] Ministeriö pyrkii ohjauskeinoillaan edistämään viestintäpalvelujen luotettavuutta ja turvallisuutta sekä viestintäpalveluja käyttävien kansalaisten ja yhteisöjen kykyä huolehtia omien verkkoon liitettyjen tietojärjestelmiensä tietoturvasta.

Suomessa on liikenne- ja viestintäministeriön arvion mukaan kansainvälisesti vertaillen erittäin hyvin ja kattavasti toimiva yhteistoimintamalli tietoturvaloukkausten havaitsemiseksi, estämiseksi ja selvittämiseksi. Kaikilla viestintäverkkojen ja palveluiden suunnittelijoilla, rakentajilla ja ylläpitäjillä on 1.1.2015 voimaan tulevan tietoyhteiskuntakaaren mukaan oikeus ja velvollisuus huolehtia verkkojensa ja palveluidensa laadusta ja turvallisuudesta sekä velvollisuus huolehtia muun muassa siitä, että verkkoihin ja palveluihin kohdistuvat tietoturvaloukkaukset ja niiden uhkat voidaan havaita. Valtaosa tietoturvallisuutta edistävistä toimenpiteistä voidaan tehdä ilman erityisiä toimivaltuuksia, mutta teleyrityksille, yhteisötilaajille ja lisäarvopalvelun tarjoajille on säädetty eduskunnan lokakuussa 2014 hyväksymässä tietoyhteiskuntakaaressa erityisiä oikeuksia ryhtyä välttämättömiin toimenpiteisiin tietoturvasta huolehtimiseksi.[56]

Viestintäverkkojen suunnittelevat, rakentavat tai ylläpitävät tahot tai niiden käyttäjinä toimivat asiakasyhteisöt eivät millään tavalla nostaneet esiin tarvetta parantaa tietoturvaa verkkovalvonnan tai muidenkaan tiedusteluvaltuuksien keinoin tietoyhteiskuntakaaren erittäin laajaalaisen ja avoimen valmistelun tai eduskuntakäsittelyn yhteydessä. **Liikenne- ja viestintäministeriö huomauttaa, ettei mietinnössä ole konkreettisesti esitetty, missä mielessä tai minkälaisella toimintamallilla yrityksille voisi olla hyötyä verkkovalvonnasta.**

---

[53] 1.1.2015 voimaan tulevassa tietoyhteiskuntakaaren (917/2014) 3 §:ssä tietoturvallisuudella tarkoitetaan *toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä.* Tietoturvallisuuden oikeudellisesta määritelmästä tarkemmin esim. Saarenpää (toim): Tietoturvallisuus ja laki, 1997.

[54] Perustuslain 23 § ja Valtioneuvoston ohjesäännön 20 §.

[55] Tietoyhteiskuntakaaren 1 § ja HE 221/2013 vp.

[56] Kyseistä tietoyhteiskuntakaaren säännöstä on käytetty mietinnössä ikään kuin perusteluna sille, ettei verkkovalvonnasta säädettäessä tarvitsisi muuttaa perustuslakia. Liikenne- ja viestintäministeriö katsoo, ettei tietoyhteiskuntakaaren 272 §:n käsittely tässä tarkoituksessa ole ymmärrettävää. Tietoyhteiskuntakaaren 272 §:ssä on kyse perustuslain 23 §:n mukaisesta aktiivisesta lainsäädäntötoimesta, jolla nimenomaisesti pyritään edistämään kansalaisten luottamuksellisen viestinnän suojaa. Sen sijaan verkkovalvontaa koskevaa sääntely ei ole perusteltavissa luottamuksellisen viestinnän suojaamisella, eikä siinä olisi kyse perusoikeuden toteutumista turvaavasta välttämättömästä sääntelystä.

Työryhmän mietinnössä tiedustelun tarvetta on perusteltu muun muassa tarpeella parantaa tietoturvallisuutta. Liikenne- ja viestintäministeriö on kuullut laaja-alaisesti viestintäpalvelujen tarjoajia, ja tullut mietinnöstä poiketen siihen käsitykseen, ettei poliisin tai puolustusvoimien tiedustelutoimivaltuuksien tarvetta voida perustella yleisten viestintäverkkojen tai niiden käyttäjien tietoturvan parantamisen tarpeella. **Liikenne- ja viestintäministeriö katsoo, että niin julkisten kuin yksityistenkin yhteisöjen tietoturvallisuuden kehittämiseen on huomattavasti tarpeellisempia, tehokkaampia ja oikeasuhtaisempia keinoja kuin mitä poliisin tai puolustusvoimien tiedustelutoimivaltuuksia lisäämällä voitaisiin saavuttaa.**

Mietinnössä on viitattu Kyberturvallisuuskeskuksen raporttiin[57], jossa todetaan että myös suomalaisiin sekä myös muihin länsimaalaisiin verkkoihin kohdistuu kybervakoilutapauksia, joissa teknisenä apukeinona on käytetty muun muassa kohdistettuja haittaohjelmia. Viittauksella raporttiin on pyritty kyseenalaistamaan väitettä suomalaisten tietoverkkojen puhtaudesta. Vain se, että uhka vakoilusta kohdistuu myös Suomeen, ei vielä kerro Suomen verkkojen puhtaudesta. Suomi on nimenomaan pärjännyt hyvin esimerkiksi Microsoftin tekemissä vertailuissa verkkojen puhtaudesta.[58]

7. Suomen toimenpiteitä tietoturvan kehittämiseksi

Suomen sähköisen viestinnän tietoturvaa koskevia säännöksiä on vastikään uudistettu vuoden 2015 alusta voimaan tulevassa tietoyhteiskuntakaaressa (917/2014). Viestinnän välittäjän on tietoyhteiskuntakaaren 247 §:n mukaan viestejä välittäessään huolehdittava palvelujensa, viestien, välitystietojen ja lisäarvopalvelujen tietoturvasta. Lisäksi tietoyhteiskuntakaaren 243 §:n mukaan kaikki viestintäverkot ja viestintäpalvelut on Suomessa lain mukaan suunniteltava, rakennettava ja ylläpidettävä siten, että sähköinen viestintä on tietoturvallista eikä kenenkään tietosuoja, tietoturva tai muut oikeudet vaarannu. Verkot ja palvelut on niin ikään suunniteltava, rakennettava ja ylläpidettävä siten, että niihin kohdistuvat merkittävät tietoturvaloukkaukset ja tietoturvauhat sekä niiden toimivuutta merkittävästi häiritsevät viat ja häiriöt voidaan havaita.

Lisäksi tietoturvan kehittämiseksi on viime vuosina tehty useita toimenpiteitä. Niistä keskeisimmät käydään seuraavaksi lyhyesti läpi.

Tietoturvastrategiat

Ensimmäinen poikkiyhteiskunnallinen **kansallinen tietoturvastrategia** hyväksyttiin valtioneuvoston periaatepäätöksenä 4.9.2003. Strategia oli Euroopassa ja ilmeisesti maailmassakin ensimmäinen laatuaan. Julkinen ja yksityinen sektori laativat yhdessä strategian, jonka valmistelun ja toimeenpanon koordinoinnista vastasi liikenne- ja viestintäministeriö. Strategiassa todettiin, että kansalaisten ja yritysten luottamusta tietoyhteiskuntaan voidaan lisätä erityisesti tietoturvallisuutta ja yksityisyyden suojaa parantamalla. Strategialla pyrittiin torjumaan tietoturvallisuuden uhkia sekä toisaalta hyödyntämään korkeatasoisen tietoturvallisuuden tarjoamia mahdollisuuksia.

[57] Kohdistettujen haittaohjelmahyökkäyksien uhka on otettava vakavasti. Viestintäviraston Kyberturvallisuuskeskuksen raportti. Syksy 2014: https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2014/08/ttn201408281226.html .

[58] Väitettä verkkojen puhtaudesta tukee mm. Microsoftin SIR-raportti nro 17, 2014. http://www.microsoft.com/en-us/download/confirmation.aspx?id=44937.

Tietoyhteiskuntaohjelman osana **toinen kansallinen tietoturvastrategia** hyväksyttiin valtioneuvoston periaatepäätöksenä 4.12.2008. Strategian visiona on, että kansalaiset ja yritykset voivat luottaa tietojensa turvallisuuteen sekä tieto- ja viestintäverkoissa että niihin liittyvissä palveluissa. Strategialla on kolme painopistealuetta. Näitä olivat perustaidot arjen tietoyhteiskunnassa, tietoihin liittyvien riskien hallinta ja toimintavarmuus sekä kilpailukyky ja kansainvälinen verkostoyhteistyö. Liikenne- ja viestintäministeriö koordinoi strategian valmistelua ja toteuttamista eri hallinnonaloilla. Toisen tietoturvastrategian tavoitteiden toteuttamiseksi laadittiin vuonna 2009 yhteensä yhdeksän erillistä hanketta käynnistänyt toimenpideohjelma, joka hyväksyttiin valtioneuvoston periaatepäätöksenä.

Vuonna 2013 laadittiin valtioneuvoston periaatepäätöksenä hyväksytty **kansallinen kyberturvallisuusstrategia**, jonka visiona on, että 1) Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan; 2) kansalaisilla viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti ja että 3) vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallitsemisessa. Strategian toimeenpanemiseksi laadittiin virkamiestasolla toimeenpano-ohjelma.

Esimerkkejä kansainvälisen tiedustelun kansallisesta käsittelystä

Vuonna 2008 liikenne- ja viestintäministeriössä arvioitiin Ruotsin signaalitiedustelulain (FRA) vaikutuksia suomalaisten viestintäpalvelujen tietoturvaan. Viestintävirasto laati ja julkaisi ohjeistuksen viestinnän salaamisesta vuonna 2009.

Valtioneuvosto käsitteli 19.6.2013 verkkovakoilua ja massatiedustelua koskeneita uutisia Edward Snowdenin paljastuksista sekä niitä toimenpiteitä, joihin tapauksen johdosta ryhdyttiin kansallisesti ja kansainvälisissä yhteyksissä.

Kesäkuussa 2014 Viestintävirasto julkaisi ohjeita ja suosituksia siitä, kuinka suomalaisten tulisi suojautua joutumasta ulkomaisten tiedusteluorganisaatioiden harjoittaman verkkovalvonnan kohteeksi.[59]

Viestintäviraston kyberturvallisuuskeskus

Viestintävirastoon perustettiin vuoden 2014 alussa kyberturvallisuuskeskus valtioneuvoston periaatepäätöksellä. Kyberturvallisuuskeskuksen kautta Viestintävirasto tuottaa tietoturvapalveluita koko yhteiskunnalle ja edistää Suomen varautumista kyberuhkiin ja niiden aiheuttamien häiriötilanteiden hallintaan. Kyberturvallisuuskeskuksen tehtäviin kuuluu tietoturvauhkien- ja loukkausten havainnointi ja selvittäminen sekä kyberturvallisuuden tilannekuvan ylläpito.

Tammikuussa 2014 Viestintävirasto ja valtiovarainministeriö sopivat, että Viestintävirasto tuottaa tietoturvaloukkausten ennaltaehkäisyyn, havainnointiin ja ratkaisuun tähtääviä palveluita[60] valtiovarainministeriölle osana valtiovarainministeriön ympärivuorokautisen tietoturvatoiminnan kehittämishanketta.

NIS-direktiivi

[59] Viestintäviraston suositus 205/2014 S.
[60] ns. GovCERT- ja GovHAVARO-palvelut (lyhenteet tulevat sanoista Governmental Computer Emergency Response Team ja Tietoturvaloukkausten HAvainnointi ja VAROitusjärjestelmä).

EU:n komissio on vuonna 2013 antanut ehdotuksen direktiiviksi verkko- ja tietoturvan korkean tason varmistamiseksi EU:n alueella (**EU:n verkko- ja tietoturvadirektiivi**), jota käsitellään parhaillaan Euroopan parlamentissa ja neuvostossa. Direktiiviehdotuksella luotaisiin yhtäältä velvoitteita verkko- ja tietoturvan parantamisesta jäsenvaltioissa sekä toisaalta jäsenvaltioiden välinen yhteistyömekanismi tietoturvapoikkeamiin liittyvän tiedonvaihdon ja muun yhteistoiminnan järjestämiseksi. Kolmanneksi direktiivi velvoittaisi eräiden soveltamisalaan kuuluvien yhteiskunnan keskeisten alojen (rahoituspalvelut, liikenne, energia, terveys) kriittisten infrastruktuurien ylläpitäjät sekä keskeisimmät tietoyhteiskunnan internetpalveluiden tarjoajat ja julkishallinnot ottamaan käyttöön riskinhallintakäytänteitä ja raportoimaan ylläpitämiinsä keskeisiin palveluihin kohdistuvista merkittävistä tietoturvapoikkeamista.

8. Kansalaisten luottamusta tietoyhteiskuntaan ja internetiin kannattaa vahvistaa

Päätöksenteossa on tärkeä huomioida, ettei toimivia ja kilpailukykyisiä digitaalisia palveluita pystytä nykypäivänä rakentamaan ilman luottamusta. Luottamuksen merkitys näyttäisi jatkuvasti vahvistuvan kansalaisten verkkovalvontaan ja tietoturvauhkiin liittyvien uutisten paljastuessa.

Perinteisissä palveluissa luottamuksen merkitys on itsestään selvää. Harvat haluavat astua turvattomaan lentokoneeseen, antaa rahojaan epäluotettavalle pankille tai laittaa kirjeitään epäluotettavan kuriirin matkaan. Myös digitaalisissa palveluissa käyttäjien luottamus palveluun tulee käyttökokemuksen ohella yhä useammin ratkaisemaan palvelun elinkelpoisuuden ja menestyksen. Jos palveluja tuottavat yritykset haluavat pärjätä kilpailussa, on niiden annettava asiakaslupauksia palveluidensa korkeasta luotettavuudesta.

Suomella on nyt tilaisuus profiloitua maana, jossa valtio pitää osaltaan huolen siitä, ettei asiakkaiden luottamusta ja yritysten kykyä pitää asiakaslupauksensa vaaranneta. Samalla Suomella on yleisemmälläkin tasolla erinomaiset edellytykset kehittyä maailman osaavimmaksi ja luotettavimmaksi maaksi internetissä. Tämän päämäärän voimme saavuttaa, jos pidämme huolta siitä, että yksityisyyden ja luottamuksellisen viestinnän suojaa vaaliva lainsäädäntömme pysyy jatkossakin korkealla tasolla.

Jos Suomi haluaa lunastaa digitalisaation ja internet-talouden avaamat mahdollisuudet, sen tulee kiinnittää erityistä huomiota ainakin seuraaviin seikkoihin:

1. Tieto- ja viestintäteknisten hyödykkeiden käyttäjillä on oltava riittävät valmiudet ja nykyistä parempi ymmärrys tuotteiden käyttöön liittyvistä mahdollisuuksista ja riskeistä. Tuotteiden turvallisuus- ja suojausominaisuuksien sekä käyttöehtojen tulee olla nykyistä läpinäkyvämpiä siten, että asiakas voi verrata eri tuotteiden luotettavuutta ja käyttää halutessaan apuna ulkopuolisia arvioitsijoita. Viranomaisilla ja arviointilaitoksilla voisi olla merkittävä rooli sen todentamisessa, että kuluttajien käyttämät laitteet ja palvelut vastaavat suomalaisia tai eurooppalaisia tietoturvavaatimuksia.

2. Tutkimus-, kehitys- ja opetustyöhön tulee kiinnittää nykyistä enemmän huomiota. Riittävän tutkimus- ja kehitystyön avulla tietoturvallisten tuotteiden ja palveluiden markkinoita on mahdollista kehittää siten, että tieto- ja viestintäteknologiset hyödykkeet vas-

taisivat entistä paremmin käyttäjien tarpeita ja odotuksia erityisesti palveluiden luotettavuuden osalta. Hyviä kehitystyön kohteita ovat esimeriksi ohjelmointi, data-analyysi ja erilaiset salausmenetelmät.

3. Markkinoille täytyy saada uusia, eurooppalaisista lähtökohdista tuotettua palveluita. Markkinoilla on tilausta erityisesti erilaisille ”internetin päällä” toimiville palveluille (ns. Over The Top -palvelut), joilla tarkoitetaan muun muassa viestintäohjelmistoja, selaimia, hakukoneita, tallennuspalveluita ja sosiaalisen median alustoja. Nämä palvelut ovat arvonmuodostuksen kannalta olennaisia liiketoiminnan alueita, sillä monessa tapauksessa ne pystyvät kerryttämään tuloa myös niiden päälle luotujen palveluiden tarjonnasta (esimerkiksi Google Mapsin perustalle luodut palvelut).

IV. Lopuksi

Liikenne- ja viestintäministeriö haluaa kiittää mahdollisuudesta osallistua tiedonhankintalakityöryhmän työskentelyyn. Eriävästä mielipiteestä huolimatta ministeriö katsoo, että työryhmässä on pyritty tekemään työtä entistä paremman ja turvallisemman tulevaisuuden puolesta. Kuten edellä on käynyt ilmi, ministeriö suhtautuu erittäin vakavasti niihin huoliin, joita poliisi ja puolustusvoimat ovat esittäneet toimivaltuuksiensa riittämättömyydestä muuttuvassa maailmassa. Tästä huolimatta ministeriö katsoo, ettei verkkovalvonta ole oikea keino vastata näihin huoliin.

Päivi Antikainen
viestintäneuvos, internetpalvelut -yksikön päällikkö

Laura Tarhonen
neuvotteleva virkamies