



Puolustusministeriö  
Försvarsministeriet  
Ministry of Defence

Lainvalmistelu- ja oikeusyksikkö

30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

## Suomalaisen tiedustelulainsäädännön suuntaviivoja - lausuntoyhteenvedo tiedonhankintalakitöryhmän mietinnöstä

**Postiosoite**  
**Postadress**  
**Postal Address**  
Puolustusministeriö  
PL 31, 00131 Helsinki  
Finland

**Käyntiosoite**  
**Besökadress**  
**Street Address**  
Eteläinen Makasiinikatu 8 A  
00130 Helsinki  
Finland

**Puhelin**  
**Telefon**  
**Telephone**  
(09) 16001  
Internat. +358 9 16001

**Faksi**  
**Fax**  
**Fax**  
(09) 1608 8244  
Internat. +358 9 1608 8244

**Sähköposti, internet**  
**E-Post, internet**  
**E-Mail, internet**  
puolustusministerio@plm.vn.fi  
www.defmin.fi



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

## Sisällys

Johdanto .....	3
1 Yhteenveto.....	3
2 Viranomaisten toimivaltuuksien nykytila .....	4
3 Kansainvälinen vertailu.....	6
4 Tiedustelun menetelmät .....	7
5 Perusoikeuskysymykset .....	9
6 Toimivaltaiset viranomaiset.....	13
7 Laillisuusvalvonta ja oikeusturvakeinot .....	14
8 Erityiskysymyksiä .....	16
9 Ehdotusten vaikutukset .....	18
10 Jatkotoimenpiteet .....	21
Liite 1 .....	23



## Johdanto

Puolustusministeriö asetti 13.12.2013 työryhmän, jonka tehtävä oli lainsäädännön kehittäminen erityisesti turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi tietoverkkoympäristön vakavista uhkista. Työryhmän valmistelemassa mietinnössä Suomalaisen tiedustelulainsäädännön suuntaviivoja arvioitiin lainsäädännön kehittämistarpeita (jäljempänä mietintö). Työryhmä luovutti mietintönsä puolustusministerille 14.1.2015.

Mietinnössä esitettiin kolme ehdotusta tiedustelulainsäädännön kehittämiseksi. Mietinnön mukaan lainsäädäntöä tulisi kehittää rajat ylittävään tietoliikenteeseen kohdistuvan tiedustelun osalta siten, että tiedustelu rajattaisiin koskemaan kansallista turvallisuutta vaarantavia uhkia. Mietinnössä ehdotetaan ulkomaan tiedustelulainsäädännön kehittämistä niin, että luontaisiin sääntelyperusta ulkomaan henkilötiedustelulle ja ulkomaan tietojärjestelmätiedustelulle.

Työryhmän mietintö lähetettiin laajalle lausuntokierrokselle 9.2.2015 ja lausuntoa pyydettiin 150 eri ministeriöltä, viranomaiselta, puolueelta, järjestöltä, yritykseltä ja yhteisöltä. Lausuntopyyntö oli myös julkisesti saatavilla puolustusministeriön internet-sivuilla. Lisäksi lausunnot pyydettiin erikseen professori Martin Scheininiltä European University Institutesta, apulaisprofessori Juha Lavapuroilta Tampereen yliopistosta ja professori Tomi Voutilaiselta Itä-Suomen yliopistosta. Lausuntopyynnön jakelu ja lausunnon antaneet tahot käyvät ilmi liitteestä. Lausuntoja saatiin yhteensä 74.<sup>1</sup> Tässä yhteenvedossa käydään läpi saatua lausuntopalautetta asiakokonaisuuksittain.

## 1 Yhteenveto

Lausuntopalautteessa yhdyttiin laajasti mietinnön lähtökohtana esitettyyn arvioon toimintaympäristön muutoksesta digitalisoituvassa tietoverkkojen yhteiskunnassa. Lainsäädännön nykytilan aukollisuus katsottiin ongelmalliseksi ja säädöspohjan luomista pidettiin perusteltuna. Mietinnössä esitetyt kehittämissuositukset ja johtopäätökset jakoivat kuitenkin mielipiteitä. Ongelmallisena pidettiin viranomaisten tiedonsaantitarpeen ja yksityisyyden suojan välisen jännitteen yhteensovittamista.

Perustuslailliset ja perusoikeuksia sivuavat kysymykset nousivat esille suuressa osassa lausuntoja. Lausuntopalautteessa edellytettiin mahdollisten säädösmuutosten perustuslainmukaisuutta arvioitavan tarkasti ja kiinnitettävän erityistä huomiota luottamuksellisen viestin ja yksityisyyden suojan tarkasteluun. Myös oikeusturvaan, sananvapauteen, yksityisyyteen ja henkilötietojen suojaan liittyviä perusoikeusnäkökohtia nostettiin esille lausunnoissa. Tiedustelulainsäädännön kehittämisen keinoista, menettelyjen järjestämisestä, toimivallan rajoista, sääntelytarpeista ja vastuuviranomaisista esitettiin runsaasti erilaisia kantoja. Suurin osa lausunnoista keskittyi nimenomaan tietoliikennetiedustelua koskevien ehdotusten tarkasteluun.

Lausuntopalautteen mukaan mietintöä pidettiin pääsääntöisesti perusteellisesti laadittuna, valmisteluprosessin avoimuutta kiitettiin ja osallistumismahdollisuuksia pidettiin hyvinä. Eri sidosryhmät muista viranomaisista, liike-elämästä ja etujärjestöistä toivoivat myös jatkovalmistelulta avoimuutta ja mahdollisuutta osallistua työryhmän jäsenenä tai muuten. Erityisesti ICT-alan ja elinkeinoelämän

<sup>1</sup> Lausunnot ovat saatavilla sähköisesti osoitteessa:

[http://www.hare.vn.fi/mAsiakirjojenSelailu.asp?h\\_iid=19825&tVNo=4&sTyp=Selaus](http://www.hare.vn.fi/mAsiakirjojenSelailu.asp?h_iid=19825&tVNo=4&sTyp=Selaus).



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

asiantuntemusta tulisi käyttää jatkossa apuna, jotta sääntelyssä huomioitaisiin elinkeinoelämän tarpeet ja saataisiin laajasti asiantuntijoiden näkemyksiä teknisen toteuttamisen osalta. Myös eri viranomaisten tarpeet tulisi huomioida kokonaisuudessa.

Lausunnonantajilla oli hyvin erilaisia odotuksia, käsityksiä, uhkakuvia ja toiveita tiedusteluun liittyvistä toimivaltakysymyksistä. Jatkotyössä tulisi tehdä rajapintatarkastelu sotilas- ja siviilitiedustelusta, tiedustelusta ja rikostorjunnasta sekä tiedustelusta ja tietoturvasta. Lausuntopalautteen perusteella voidaan katsoa, että mietinnössä tiedustelusääntelylle asetetut tavoitteet ja näiden tavoitteiden suhde mietinnössä ehdotettuihin jatkotoimiin ovat jääneet jossain määrin vaikeiksi hahmottaa. Lausunnoissa käsiteltiin myös vaihtoehtoja, joita mietinnössä ei ollut esitetty.

Jatkotyössä tulisi löytää huolellisen valmistelun kautta tasapaino perusoikeuksien suojan ja tietoyhteiskuntaan liittyviltä vakavilta uhkilta suojautumisen välillä. Erityisesti tulisi huomioida oikeusvaltioperiaate, suhteellisuusperiaate, käytettävien keinojen oikeasuhtaisuus, perusoikeudet, sääntelyn tarkkarajaisuus ja korostettua luottamuksensuojaa nauttivan viestinnän erityispiirteet. Tiedustelun kestolle ja määrälle tulisi olla laissa rajat, kuten EIT edellyttää.

## 2 Viranomaisten toimivaltuuksien nykytila

Lausuntopalautteessa otettiin kantaa eri turvallisuusviranomaisten toimivaltuuksiin, sääntelykehiköön ja niiden rajoihin. Lausunnoissa pohdittiin eri viranomaisten (mm. poliisin, keskusrikospoliisin, suojelupoliisin, puolustusvoimien, tullin, rajavartiolaitoksen ja syyttäjän) toimivaltuuksia tiedusteluun ja tietoverkkoihin liittyvissä tehtävissä. Viranomaisten lausuntopalautteen perusteella laissa määriteltyjen tehtävien hoitaminen nykyisen sääntelyn puitteissa digitalisoituvassa toimintaympäristössä koettiin haasteelliseksi. Nykyisen sääntelyn aukollisuus nähtiin lausuntopalautteessa kautta linjan ongelmalliseksi. Epäsuhta puutteellisen toimivallan ja käytännön tarpeiden välillä voi johtaa oikeusturvan kannalta ongelmallisiin tilanteisiin. Lausuntopalautteen mukaan toimivaltuuksista tulee määrätä yksiselitteisesti laissa.

### Sotilastiedustelu

Lausuntopalautteessa katsottiin, ettei sääntelyn nykytila ole sotilastiedustelun osalta riittävä. Tiedusteluun liittyvillä toimivaltuuksilla voisi olla merkittävä rooli tietoverkkotilannekuvan muodostamisessa ja ylimmän valtionjohdon päätöksenteossa. Tietoverkkojen uhkien tunnistamista olisi tarpeen kehittää ja tunnistaa ne kansainväliset uhat, joita ei voida täysin torjua tai valvoa perinteisin menetelmin. Oikeusministeriö totesi lausunnoissaan, että nykyisin sotilaskurinpidosta ja rikostorjunnassa puolustusvoimissa annetun lain 9 luvun mukaan puolustusvoimilla on rajatusti oikeus käyttää salaisia tiedonhankintakeinoja rikosten ennalta estämisessä ja paljastamisessa, mitä täydentää oikeus saada poliisilta virka-apua.

Yhteiskunnan elintärkeisiin toimintoihin kohdistuva digitaalinen hyökkäys voi olla vakavuudeltaan valtioon kohdistuvaan aseelliseen hyökkäykseen rinnastettava ja sen takana voi olla vieraan valtion lisäksi ulkomailta käsin tai kotimaassa toimiva terroristiryhmä tai järjestäytyneet rikollisryhmä. Valtioneuvoston oikeuskansleri katsoi, että tiedustelutoiminta on oikeudellisen systematiikan näkökulmasta luonteeltaan eräänlaista laajennettua aluevalvontaa ja sen käyttötilannetta voidaan pitää laajennettuna poikkeusolona, joten asiassa on olennaista aluevalvontalain mukaiset keinot alueloukkausten estämiseksi ja torjumiseksi. Tietoliikennetiedustelussa olisi kysymys eräänlaisesta Suomen digitaalisen alueen koskemattomuuden valvonnasta ja turvaamisesta.

Lausuntopalautteen mukaan rajat valtakunnan ulkoisen ja sisäisen turvallisuuden välillä sekä sotilaallisten ja siviiliuhkien välillä ovat hämärtyneet. Jaottelu sotilas- ja siviilitiedusteluun koettiin hankalaksi järjestää käytännössä. Eräissä lausunnoissa katsottiin, että sotilasintressissä tehdyllä tiedonhaualla olisi vähemmän vaikutusta kansalaisten yksityisyyden suojaan, kuin poliisiviranomaisten tie-



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

dustelutoiminnalla. Tietoliikennetiedustelu katsottiin sallittavammaksi, mikäli se liittyy yksinomaan sotilaallisiin uhkiin varautumiseen.

### Siviilitiedustelu

Nykyiset tiedonhankintakeinot on sidottu rikokseen tai rikosepäilyyn. Osa lausunnonantajista katsoi, että siviili- ja sotilastiedustelulla tulee olla Suomessa valmiudet myös muuhun, kuin rikosperusteiseen tiedonhankintaan. Tiedustelun tulisi voida kohdistua myös tietoon, joka ei liity sinänsä rikollisiin tekoihin.

Esitutinnan yhteydessä käytettäviin salaisiin pakkokeinoin verrattuna osa mietinnössä tarkastelluista tiedustelutoimista olisi kuitenkin luonteeltaan nykyisiin pakkokeinoin verrattuna yksilöimätömämpää strategista valvontaa tai yleisvalvontaa. Kun vaikkapa telekuuntelulupa edellyttää yksilöityjä tietoja kuuntelun kohteesta, ehdotetut tiedustelutoimenpiteet olisivat osin luonteeltaan laajakantoisempia ja toimenpiteen kohteen kannalta sattumanvaraisempia. Toisaalta, esimerkiksi asianajajaliiton lausunnon mukaan viestinnän ollessa osin automatisoitujen selvityskeinojen kohteena jo nyt, vastaavien toimivaltuuksien myöntämistä turvallisuusviranomaisille ei tulisi pitää niin suurena muutoksena yksityisyyden suojaan kuin ensi näkemältä voidaan ajatella (vrt. tietoyhteiskuntakaari 272 §). Viestintäviraston lausunnon mukaan tietoyhteiskuntakaaren toimintamalli taas eroaa mietinnössä esitetystä toimintamallista.

Osa lausunnonantajista katsoi, että Suomen viranomaisten toimivaltuudet ovat jo nykyisin varsin laajat ja riittävät. Mikäli toimivaltuudet eivät ole enää ajan tasalla, tulisi säännökset päivittää eikä suunnitella uutta sääntelyä. Lausuntopalautteen mukaan vuoden 2014 alusta voimaan tulleet pakkokeinolain, esitutkintalain ja poliisilain muutokset takaavat poliisille laajat toimivaltuudet esimerkiksi vakoilu- ja terrorismirikosten estämiseen, selvittämiseen ja paljastamiseen. Samassa yhteydessä säädettiin salaiseksi tiedonhankintakeinoksi tekninen laitetarkkailu. Muun muassa oikeusministeriön ja tietosuojavaltuutetun toimiston mukaan kyseisten lakimuutosten riittävyys ja tehokkuus tulisi arvioida, ennen kuin uusista toimivaltuuksista ryhdytään säätämään.

Erityisesti poliisiviranomaiset olivat huolissaan, kuinka viranomaisten nykyisten resurssien puitteissa pystytään kehittämään uusia toimivaltuuksia tai uutta järjestelmää. Nykyistenkin lakisäätteisten tehtävien hoitaminen koettiin osissa lausunnoista hankalasti kiristyneen taloustilanteen vuoksi. Erityisesti poliisiviranomaisten lausunnoissa tuotiin esille kanta, että tiedustelulainsäädännön kehittämistä tulisi katsoa rikostorjunnan kokonaisuuden näkökulmasta. Tiedustelulainsäädännön suhde ja rajapinnat rikostorjuntaan, rikosten selvittämiseen ja rikosprosessiin tulisi käydä huolellisesti läpi. Tietoliikennetiedustelua ei tulisi käyttää yleisenä rikostorjunnan keinona, vaan sille tulee olla yksilöidyt perusteet laissa.

### Tietoturvaohjelman torjunnan nykytila

Viestintävirasto ohjaa ja valvoo sähköisen viestinnän ja postilainsäädännön noudattamista. HAVARO on Viestintäviraston Kyberturvallisuuskeskuksen huoltovarmuuskriittisille yrityksille ja valtionhallinnolle tarjoama vakavien tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä, joka tunnistaa erityisesti yhteisöihin suuntautuvia kehittyneitä verkkohyökkäyksiä. HAVAROn asemaa ja käyttötapoja toivottiin arvioitavan suhteessa uuteen sääntelyyn.

Erityisesti yritysten lausunnoissa muistutettiin, että vastuu tietoverkkojen uhkista kuuluu viranomaisten lisäksi lain nojalla myös tiettyä toimintaa harjoittaville yrityksille. Valtaosa viestintäverkoista ja muusta kriittisestä infrastruktuurista on suurelta osin yksityisen sektorin omistuksessa. Lainsäädäntö asettaa muun muassa teleyrityksille ja yhteisötilaajille velvoitteita toimintansa tietoturvallisesta järjestämisestä, joka toteutetaan pääasiassa tietohallinnollisen toimenpitein. Yksittäisen



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

yrittäjien on kyettävä ennakoimaan ja torjumaan toimintaansa mahdollisesti uhkaavat verkkoihin ja järjestelmien toimivuuteen liittyvät riskit.

Kaiken kaikkiaan tietoturvatyökaluita suorittavat pääasiassa viestintäverkkoja ylläpitävät teleyritykset, niille tukipalveluita tarjoavat yritykset ja eri viranomaiset. Tietoyhteiskuntakaari antaa teleyrityksille oikeudet käsitellä välittämäänsä tietoliikennettä teleyrityksen palvelulle ja sen käyttäjille haittaa aiheuttavien häiriöiden havaitsemiseksi ja estämiseksi. Lisäksi tietoyhteiskuntakaari velvoittaa teleyritykset ryhtymään välittömästi toimenpiteisiin, mikäli teleyrityksen palvelu tai siihen liitetty käyttäjä aiheuttaa vaaraa tai häiriötä palvelulle tai muille käyttäjille. Erityisesti järjestöt ja yritykset katsovat, että käytännössä kyberturvallisuus paranee viranomaisten, yksityisen sektorin ja kansalaisyhteiskunnan välisen toimivan vuorovaikutuksen kautta.

### 3 Kansainvälinen vertailu

Kansainvälisen vertailun katsottiin antavan hyvät lähtökohdat tietoliikennetiedustelulainsäädännön kehittämistarpeiden arvioinnille. Kansainväliseen vertailuun valitut maat antavat esimerkiksi ulkoasiainministeriön käsityksen mukaan hyvän kuvan oikeusjärjestelmiltään vertailukelpoisista maista, mutta esimerkiksi professori Tomi Voutilainen ja eräät järjestöt ja yritykset katsovat, että kansainvälinen vertailu olisi voinut olla laajempaa ja monipuolisempaa. Erityisesti YK:n että Euroopan parlamentin taholta esitetty kritiikki viranomaisten tietoliikenteeseen kohdistuvan valvonnan ongelmista tulisi ottaa huomioon.

Ruotsin sääntelymalli nousi esille useassa lausunnossa ja Ruotsi katsottiin lähtökohtaisesti parhaiten vertailukelpoiseksi maaksi suhteessa Suomeen. Jatkossa tulisi arvioida vielä tarkemmin, kuinka laajaa toiminta Ruotsissa on ollut, kuinka laajaan osaan viestinnästä se on kohdistunut, kuinka laajoja yksittäistapauksessa annetut valvontamandaatit ovat olleet miten tehokasta tai vaikuttavaa toiminta on ollut. Jatkotyössä olisi lausuntojen mukaan ylipäättään syytä katsoa kriittisesti ulkomaalaisia esimerkkiä ja ottaa opiksi vertailumaiden sääntelyratkaisusta. Kansainvälisesti todettuja ongelmia sääntelyssä ei ole syytä toistaa Suomessa.

Ruotsin ja Yhdysvaltojen järjestelmiä pidettiin hyvänä esimerkkinä siitä, kuinka teknologian kehittyessä ja verkkoliikenteen määrän kasvaessa valvonta vaatii jatkuvasti enemmän resursseja ja investointeja. Tiedustelulainsäädännön kokonaiskustannuksia onkin etukäteen erittäin vaikea arvioida, mutta on syytä olettaa niiden olevan kansainvälisen vertailun perusteella huomattavat. Lausuntopalautteen mukaan Ruotsin tilannetta ei voi yksiselitteisesti verrata Suomeen, vaan vaikutukset tulisi arvioida omien kansallisten lähtökohtien mukaan.

Tapaus Snowden nousi esille useissa lausunnoissa. Tiedon keräämistä viranomaisten toimesta pidettiin osissa palautteista itsessään uhkana turvallisuudelle. Yhdysvaltojen tiedusteluorganisaatio NSA:n ja Iso-Britannian GCHQ:n toimintaa arvosteltiin lausuntopalautteessa. Professori Martin Scheinin katsoi, että kansainvälisten esimerkkien valossa huolta herättää uhkakuva, jossa valtio rajoittaa ja valvoo suorasti ja epäsuorasti kaikkea toimintaa verkossa murentaen samalla kansainvälisiä velvoitteita, perusoikeuksia ja kansallista lainsäädäntöä.



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

#### 4 Tiedustelun menetelmät

##### **Mietinnössä esitettiin kolme ehdotusta tiedustelulainsäädännön kehittämiseksi:**

**Tietoliikennetiedustelulla** tarkoitetaan rajat ylittävissä tietoliikennekaapeleissa liikkuvaan tietoliikenteeseen kohdistuvaa tiedustelua. Tietoliikennetiedustelu on signaalitiedustelua. Signaalitiedustelun alalajeista se voi pitää sisällään sekä viestitiedustelua ja mittatiedustelua.

**Ulkomaan tietojärjestelmätiedustelulla** tarkoitetaan ulkomailla sijaitsevilla 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.

Lausuntopalautteessa suurin mielenkiinto kohdistui tietoliikennetiedusteluun. Mietinnön ehdotuksia pidettiin joissakin lausunnoissa nykyisten toimivaltuuksien säätämisenä ja arvioimisena, toisissa lausunnoissa taas katsottiin, että mietinnössä ehdotetaan uudentyyppisen viranomaiskoneiston luomista.

Lausunnoissa pidettiin kaikkien tiedustelukeinojen kannalta olennaisena, että lainsäädännössä olisi määritelty mahdollisimman tarkasti, mihin uhkiin tiedustelutoiminnalla olisi tarkoitus varautua. Tietoliikennetiedustelu ei saisi olla keino hankkia tietoa mistä tahansa riskistä tai uhista, vaan tiedustelulla pyrittäisiin havaitsemaan, tunnistamaan ja hankkimaan tietoa tietyistä kansallista turvallisuutta vaarantavista uhista. Mikäli kyse ei olisi samalla tavalla henkilö- ja rikossidonnaisesta toiminnasta, kuin rikostorjunnassa, niin asia tulisi perinpohjaisesti arvioida ja määritellä laissa.

Lausuntopalautteessa nostettiin esille lainvalmistelun yleisten periaatteiden noudattaminen (esim. oikeusministeriö, Suomen Asianajajaliitto, eduskunnan oikeusasiamies). Lisäksi mainittiin, että EIT:n oikeuskäytännössä ja perustuslakivaliokunnan lausunnossa on määritelty seikat, jotka pitää huomioida tiedustelulainsäädäntöä kehitettäessä.

Useissa lausunnoissa nähtiin ongelmalliseksi erottaa toisistaan tietoverkkoihin kohdistuva sotilastiedustelu ja siviilitiedustelu, koska tietoverkoissa liikkuvaa tietoakaan ei voi jakaa siviili- ja sotilastietoliikenteeseen. Ylimmän valtionjohdon päätöksenteoksi tueksi käytettävän tiedon hankkiminen nähtiin sinänsä perusoikeuksien kannalta vähemmän ongelmalliseksi, kuin rikosepäilyihin, rikostorjuntaan tai rikosprosessiin liittyvä tiedonhankinta. Käsitteitä ja määritelmiä tulisi muun muassa Viestintäviraston ja oikeusministeriön lausuntojen mukaan täsmentää.

##### Rajat ylittävään tietoliikenteeseen kohdistuva tiedustelu

Lausuntopalautteen mukaan tietoliikennetiedustelun oikeudellinen hyväksyttävyyden edellyttää, että kansallinen turvallisuus ja uhat kyettäisiin määrittelemään riittävän täsmällisesti ja tarkkarajaisesti ja että kyettäisiin luomaan järjestelmä, joka varmistaa uskottavasti, että tiedonhankinta kohdistuu ainoastaan tiettyihin kohteisiin. Eräissä lausunnoissa mietinnössä ehdotettua tietoliikennetiedustelua pidettiin luonteeltaan liikennevalvontaan tai tullivalvontaan rinnastettavana hyväksyttävänä menetelmänä, kun taas toisissa lausunnoissa tiedustelu käsitettiin rajoittamattomana kansalaisten mas-



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

savalvontana. Laajan tietojoukon käsittelyn ongelmallisuutta yksityiselämän suojan näkökulmasta voitaisiin vähentää teknisin tai organisatorisin keinoin.

Useissa lausunnoissa pidettiin ongelmallisena tietoliikennetiedustelun järjestämistä ehdotetulla tavalla. Valvonnan kohdistamista yksinomaan rajat ylittävään tietoliikenteeseen pidettiin useassa lausunnossa vaikeana järjestää. Eräissä lausunnoissa katsottiin, että kyberhyökkäyksiltä puolustautuminen valtakunnan rajoilla ei ole mahdollista, vaan suojauksen tietoverkkoja vastaan on perustuttava kohdepuolustukseen. Esimerkiksi Vihreän liiton lausunnon mukaan pitäisi pohtia perinpohjaisesti, vastaako tietoliikennetiedustelu sille asetettuja tavoitteita ylipäättään, mikäli tietoa hankitaan vain rajat ylittävistä tietoliikenteestä.

ICT-alan yritykset nostivat esille, että tietoverkossa tapahtuvalla valvonnalla on pienemmät mahdollisuudet havaita vakoilu- ja haittaohjelmia kuin hyvin toteutetulla kohteena olevan organisaation sisäverkossa tapahtuvalla haittaohjelmien käyttäytymiseen perustuvalla valvonnalla ja analyysillä. Nykyiset järjestelmät havaitsevat valtiollisia vakoilu- ja haittaohjelmia samalla tavalla kuin muitakin edistyneitä haittaohjelmia (APT, advanced persistent threat). Näiden löytäminen on yleensä työtä, jossa tarvitaan huomattava määrä tapahtumatietoa organisaation työasemista ja osaavia analytiikkoja ja tietoturvatutkijoita. Teknologia kehittyi tulevaisuudessa sääntelyä nopeammin.

Perustuslakivaliokunta on pitänyt haittaohjelmien valvontaa ja etsimistä teknisin keinoin hyväksyttävänä lausunnossaan, joka liittyi tietoyhteiskuntakaaren säätämiseen. Viestintäviraston lausunnon mukaan mietinnössä ehdotettu tietoliikennetiedustelu ei ole kuitenkaan verrannollinen tietoyhteiskuntakaaren 272 §:n tarkoittamaan teleyrityksen toimenpiteisiin, jossa on kyse lähinnä automaattisesta virus- ja verkkohyökkäystorjunnasta.

Lausuntopalautteessa huomautettiin, että on tärkeää erotella eri käsittelyperusteet toisistaan (viestintä ja viestinnän välitystiedot). Täytyy myös täsmentää, tapahtuuko tiedustelu tiedon siirron aikana, vai kohdistuuko se myös käyttäjien laitteisiin tai viestinnän osapuoliin. Eräiden kansalaisjärjestöjen mukaan toimintamalli, joka antaisi teknisesti pääsyn kaikkeen tietoliikenteeseen, aiheuttaisi se kansalaisille mielikuvan jatkuvasta valvonnasta, olisi herkkä väärinkäytöksille ja aiheuttaisi potentiaalisesti uusia uhkia.

Lausuntopalautteen mukaan tiedustelutoiminnan valvonnan järjestämiseen tulisi kiinnittää erityistä huomiota, kun liikutaan näin perusoikeusherkällä alueella. Valvonnan tulisi olla tehokasta ja läpinäkyvää. Valvovalla viranomaisella tulisi olla riittävä asiantuntemus ja resurssit tehtävänsä hoitamiseen asian kansainvälinen herkkyys huomioiden.

#### Ulkomaan tietojärjestelmätiedustelu

Ulkomaan tietojärjestelmätiedustelun osalta lausunnoissa esitettiin samantyyppistä kysymyksenasettelua, kuin tietoliikennetiedustelun kohdalla. Mietinnössä esitetty kanta ulkomaan tiedustelun perustuslainmukaisuudesta kyseenalaistettiin tietyin osin. Lausuntojen mukaan PL 10 §:n turvaama viestintäsalaisuuden suoja koskee yhtä lailla Suomessa kuin ulkomaillaakin oleskelevia henkilöitä. Perusoikeussuojan kannalta ei ole merkitystä sillä, ovatko viestinnän osapuolet tai edes toinen heistä ulkomailla, vaan sama suoja koskee kaikkia Suomen oikeudenkäytön piirissä olevia henkilöitä. On myös syytä huomata, että kaikki Suomen rajanaapurit ovat Euroopan ihmisoikeussopimuksen osapuolia ja heidän kansalaisensa saavat suojaa myös sitä kautta. Ulkomaan kansalaisen oikeutta ei voida rajoittaa vain hänen kansalaisuutensa perusteella. Ihmisten asettaminen kansalaisuuden perusteella eriarvoiseen asemaan loukkaisi ihmisarvoa.

Oikeusasiamiehen lausunnossa pidettiin erityisen tarkkaa harkintaa edellyttävänä ja uutena keinona, että Suomen viranomaisille annettaisiin toimivaltaa toimia kohdemaassa niin, että toiminnassa syy-





30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

listyttäisiin tuon maan lainsäädännön mukaiseen rikokseen. Jatkotyössä tulisi kiinnittää huomiota muiden maiden lainsäädännön sisältöön myös oikeusoppineiden lausuntojen mukaan.

Ulkoministeriö katsoo, että selkeän lainsäädännön luominen parantaisi Suomen ylimmän valtionjohdon ulko- ja turvallisuuspoliittisen päätöksenteon edellytyksiä ja voisi torjua Suomeen kohdistuvia vakavia ulkoisia turvallisuusuhkia, kuten esimerkiksi kansainvälistä terrorismia, Suomeen kohdistuvaa ulkovaltojen tiedustelutoimintaa tai yhteiskunnan elintärkeisiin toimintoihin kohdistuvia uhkia (mm. kohdennetut kyberiskut kriittistä infrastruktuuria kohtaan). Elinkeinoelämän ja yritysten edustajat pitivät erityisen tärkeänä, ettei ulkomaan tietojärjestelmätiedustelu kohdistuisi kansainvälisiin yrityksiin tai organisaatioiden sisäisiin tietoverkkoihin. Ulkomaan tiedustelun kohteena eivät saisi olla suomalaisten yritysten ulkomailla omistamat tietojärjestelmät.

Jatkossa tulisi lisäksi selvittää, voidaanko tiedusteluviranomaiselle antaa valtuus kehittää ja asentaa tiedonhankintaan kykeneviä sovelluksia tai muita teknisiä komponentteja vaaralliseksi katsotun ulkomaisen tahon tietojärjestelmään tai verkkoon. Kansainvälisten esimerkkien valossa on syytä arvioida myös tilannetta, jossa ulkomailla tuodaan esimerkiksi tietokone analysoitavaksi Suomeen. Tullee arvioida, voiko viranomaisen soluttautua digitaalista toimintaympäristöä käyttäen tietyn uhkavan ryhmän toimintaan. Lausunnoissa huomautettiin, että suomalaisiin tietoverkkoihin ja yrityksiin kohdistuu jatkuvasti vieraiden valtioiden tiedusteluelinten ja muiden ulkomaalaisten toimijoiden taholta oikeudettomia toimia. Tietojenvaihto toisten valtojen kanssa tulisi käydä yksityiskohtaisesti läpi jatkossa.

#### Ulkomaan henkilötiedustelu

Lausuntopalautteen mukaan henkilötiedustelu kykenee tuottamaan sellaista yksityiskohtaista ja syvää korkeimman suojaustason tietoa, jota ei muilla tiedustelulajeilla ole mahdollista tuottaa. Henkilötiedustelun avulla luodaan mahdollisuuksia myös muiden tiedustelulajien tehokkaalle hyödyntämiselle. Käytännössä tiedustelun ja yhteystoiminnan toimintamalleissa on paljon samoja elementtejä. Periaatteessa toiminta pitää sisällään sen, että tiedustelevalle valtion ulkomaille lähettämä henkilöstö tekee asemaansa perustuen yleisiä havaintoja kyseisen valtion oloista ja käy keskusteluja valtion edustajien ja kansalaisten kanssa.

Ulkomaan henkilötiedusteluun ei liity nimenomaista lainsäädäntöä. Vaikka kyse ei olisi virallisesti sovitusta tiedonvaihdosta, toiminta tapahtuu usein hiljaisen hyväksynnän turvin. Lausuntopalautteen mukaan säädösperusta olisi perusteltua luoda myös ulkomaan toiminnalle. Ulkomaan tiedustelujärjestelmää kehittäessä tulisi miettiä muiden valtioiden lainsäädännön noudattamisen kannalta ja ovatko ehdotukset kansainvälisen oikeuden näkökulmasta hyväksyttävissä. Lausuntopalautteen mukaan henkilötiedustelua voisi suorittaa osana kriisinhallintaoperaatiota tai muuten tarpeen vaatiessa. Lausuntopalautteessa todettiin, että henkilötiedustelu on rinnastettavissa poliisi- ja pakkokeinolaissa säädeltyyn tietolähdetoimintaan (ohjattu tietolähteen käyttö).

Suojelupoliisin lausunnon mukaan suojelupoliisin hallinnollista asemaa ja tulohajasta sekä valvonnan kehittämistä selvittäneen työryhmän loppuraportissa oli maininta, jonka mukaan ulkomaantoinmivaltuudet ovat jossain määrin tarpeen. Rauhanturvaajaliiton lausunnon mukaan tiedonhankintaan osallistuvien virkamiesten ja sotilaiden turvallisuus ja oikeusturva on taattava, myös palvelussuhteen päättymisen jälkeen.

## **5 Perusoikeuskysymykset**

Lausuntopalautteessa pidettiin tiedustelulainsäädännön kehittämistä perusoikeusherkkänä alueena. Keskeisimmät lausuntopalautteessa esille nousseet perusoikeuskysymykset liittyivät yksityisyyden tai yksityiselämän suojaan ja henkilötietojen suojaan. Nämä oikeudet on turvattu mm. Suomen Perustuslain 10 §:ssä, Euroopan ihmisoikeussopimuksen 8 artiklassa, YK:n kansalaisoikeuksia ja poliit-



30.6.2015

Lainvalmistelu- ja oikeusyksikkö

tisia oikeuksia koskevan yleissopimuksen 17 artiklassa sekä Euroopan Unionin perusoikeuskirjan 7 ja 8 artikloissa. Tiedustelulla saattaa olla vaikutuksia myös muihin perus- ja ihmisoikeuksiin ja niihin kiinteästi liittyviin oikeuksiin, kuten sananvapaus, yhdistymisvapaus, kokoontumisvapaus, uskonnonvapaus, yhdenvertaisuus ja syrjinnän kieltö, liikkumisvapaus, omaisuuden suoja, elinkeinotoiminnan vapaus ja oikeus työhön. Hyvän hallinnon ja viranomaisten lakisääteisten tehtävien hoitamiseen liittyvät perusoikeuskysymykset nousivat myös esille.

Lausuntopalautteen mukaan suunnitteilla oleva sääntely tulisi pystyä toteuttamaan ensisijaisesti nykyisen perustuslain puitteissa. Mietinnössä ehdotetuista keinoista tietoliikennetiedustelun perusoikeuslottuvuus nousi eniten esille. Myös perusoikeuksien rajoittamisen ja perustuslain muuttamisen perusteita arvioitiin lausuntopalautteessa. Muun muassa oikeusministeriö ja eduskunnan oikeusasiamies kiinnittivät huomiota perustuslakivaliokunnan kannanottoihin perustuslain muutostarpeiden arvioinnin yleisistä lähtökohdista. Valiokunnan kannanottojen mukaan perustuslain muutostarpeita tulee arvioida huolellisesti ja välttämättömiksi arvioidut muutokset tehdä perusteellisen valmistelun sekä siihen liittyvän laajapohjaisen keskustelun ja yhteisymmärryksen pohjalta.

#### Yksityisyyden suoja

Keskeisimmäksi perusoikeudeksi lausuntopalautteessa katsottiin yksityisyyden suoja ja sen liitännäisperusoikeudet, eli luottamuksellisen viestin suoja, yksityiselämän suoja ja henkilötietojen suoja. Myös journalistin lähdesuojaan liittyviin erityiskysymyksiin kiinnitettiin Journalistiliiton lausunnossa huomioita. Lausuntopalautteen mukaan tiedustelulainsäädännön kehittämistä arvioitaessa tulisi arvioida tarkkaan, millä edellytyksellä poikkeuksia yksityisyyden suojaan voidaan tehdä. Asianajajaliitto toteaa, että myös Euroopan ihmisoikeustuomioistuin (EIT) on arvioinut tiedustelutoiminnan edellytyksiä ratkaisussa Weber ja Saravia vs Saksa.

Professori Martin Scheinin kiinnitti lausunnossaan huomiota siihen, että perustuslakivaliokunta on katsonut EUTI:n Data retention -ratkaisua arvioituaan, että käytännössä sähköisen viestinnän käyttöön liittyvät tunnistetiedot, sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen, voivat 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. Apulaisprofessori Juha Lavapuron mukaan Data retention -ratkaisu tulisi ottaa jatkotyössä lähempään tarkasteluun, koska kyse on tämän hetken merkittävimmästä auktoritatiivisista tulkintakannanotoista siihen, millaisia rajoituksia yksityiselämän suoja asettaa mietinnössä ehdotetulle toiminnalle.

#### Luottamuksellisen viestin suoja

Lausuntopalautteen perusteella erityisesti tietoliikennetiedustelua pidettiin luottamuksellisen viestin suojan kannalta keskeisenä perusoikeuskysymyksenä. Tietoliikenneanalyysi, jossa etsitään ja seurataan viestinnällisiä ja muita toimintamalleja, säännönmukaisuuksia ja poikkeamia, edellyttää viestinnän seulontaa, katsottiin perusoikeuskysymykseksi esimerkiksi apulaisprofessori Juha Lavapuron lausunnossa. Toisissa lausunnoissa katsottiin, että perusoikeuskysymykset aktualisoituvat vasta sitten, kun tietoja ryhdytään manuaalisesti käsittelemään.

Viestintävirasto totesi, että perustuslain esitöiden mukaan perustuslain 10 §:n 2 ja 3 momentin luottamuksellisen viestin salaisuutta koskevan sääntelyn ensisijaisena tarkoituksena on suojata luottamukselliseksi tarkoitettujen viestin sisältö ulkopuolisilta. Sääntely turvaa jokaiselle oikeuden luottamukselliseen viestintään ilman, että ulkopuoliset saavat oikeudettomasti tiedon hänen lähettämiensä tai hänelle osoitettujen luottamuksellisten viestien sisällöstä. Säännös ei suojaa vain viestin lähettäjä, vaan kyseessä on molempien viestinnän osapuolten perusoikeus.

Luottamuksellisen viestin suojan osalta nostettiin lausuntopalautteessa esille jaottelu suojan ydinalueeseen ja sen ulkopuolelle jääviin tietoihin. Perustuslakivaliokunnan aikaisemman tulkintakäytän-



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

## Lainvalmistelu- ja oikeusyksikkö

nön mukaan ydinalueen ulkopuolelle jääviä tietoja voidaan katsoa olevan tunnistamistiedot, joihin kohdistuvia rajoitustoimia ei arvioitu samanlaisin tiukoin kriteerein kuin oikeuden ydinalueelle puuttuvia rajoituksia. Aikaisemmin perustuslakivaliokunta on esimerkiksi pitänyt mahdollisena, että tunnistamistietojen saaminen jätetään sitomatta tiettyihin perustuslain 10 §:n 3 momentissa mainittuihin rikostyyppeihin, jos sääntely muutoin täyttää perusoikeuksien yleiset rajoitusedellytykset. Nykyisin jako ydinalueeseen ja sen ulkopuolelle ei ole yhtä suoraviivainen.

Oikeusministeriön mukaan perustuslaki ei tunnista kansallista turvallisuutta viestin luottamuksellisuuden rajoittamisen perusteena, ellei rajoitusperuste kytkeydy konkreettiseen ja yksilöityyn rikosepäilyyn perustuslakivaliokunnan tulkintakäytännön edellyttämällä tavalla. Perustuslain 10.3 § mukaan luottamuksellisen viestin suojasta voidaan poiketa lailla ainoastaan rikostutkintaan, oikeudenkäyntiin, turvallisuustarkastukseen ja vapaudenmenetyksiin liittyvillä perusteilla. Oikeusministeriö ehdotti, että jatkotyössä voitaisiin pohtia, voitaisiinko tehokasta tietoliikennetiedustelua toteuttaa ensi vaiheessa rajoitetummin, esimerkiksi kohdistamalla se tunnistetietoihin. Lisäksi huomautettiin, että Euroopan ihmisoikeussopimuksen 8 artikla mahdollistaa kansallisen turvallisuuden mahdollisena perusoikeuksien rajoitusperusteena.

Useat yritykset ja elinkeino-elämän edustajat kiinnittivät erityistä huomiota yritysten luottamuksellisen viestinnän suojaan. Luottamuksellisen viestin suojan kohteena voi olla myös oikeushenkilö, jolla on suojattavia liike- ja ammattisalaisuuksia. Oikeushenkilöillä voi olla myös eräissä tilanteissa velvollisuus suojata viestinnän sisältö ja henkilötiedot. Lausuntopalautteessa huomautettiin, että luottamuksellisen viestin suoja koskee sekä lähettäjä, että vastaanottajaa.

### Henkilötietojen suoja

Tietosuojavaltuutetun ja rajavartiolaitoksen lausuntojen mukaan mietinnössä ei ole käsitelty tiedustelun suhdetta henkilötietolainsäädäntöön. Jatkossa tulisi selvittää, miltä osin tiedustelu käsittäisi henkilötietoja ja miten henkilötietojen suoja järjestettäisiin. Mietinnöstä käy ilmi, että toiminnassa välttämättä olisi kyse myös henkilötietojen käsittelystä, vaikkei se olisikaan tiedustelun ensisijainen tarkoitus. Perustuslakivaliokunnan ja hallintovaliokunnan lausuntokäytännössä on muodostunut vaikiintuneita periaatteita henkilötietojen käsittelystä.

### Sananvapaus ja lähdesuoja

Journalistiliiton ja EFFI ry:n mukaan tiedustelulainsäädännöllä voi olla vaikutusta sananvapauteen, mikäli eri toimijoilla on syytä olettaa viestintää valvottavan. Eräissä lausunnoissa nostettiin esille, että tietoisuus viranomaisvalvonnasta on yhdysvaltalaisuuskimpuksissa todettu vaikuttavan kansalaisten käyttäytymiseen esimerkiksi sosiaalisessa mediassa. Viestintään puuttuminen heikentäisi sananvapauden toteuttamismahdollisuuksia ja vähentäisi uskallusta tuoda yhteiskunnallisia epäkohtia julkiseen keskusteluun.

### Tiedolliset perusoikeudet

Tiedolliset perusoikeudet ovat yhteydessä muun muassa tietoturvaan. Tietoturvan tehtävä on turvata tiedollisten perusoikeuksien toteutumista. Tiedustelua pohdittaessa tulisi kiinnittää suhteellisuusperiaatteen nojalla huomiota muihin mahdollisiin kyseeseen tuleviin keinoihin. Pohtia tulisi tiedustelutoimivaltuuksien vaikutusta salausten käyttöön ottoon ja yleisen tietoturvalain tarpeelle. Teknologian ja uusien innovaatioiden kehitys riippuu siitä, että käyttäjät luottavat tietoyhteiskunnan palveluihin ja että niissä suojataan käyttäjien perusoikeudet.

### Oikeusturva

Lausuntopalautteessa huomautettiin, että oikeusturvasta säädetään perustuslain lisäksi sitovasti Euroopan ihmisoikeussopimuksessa. Oikeusturvan toteutumisen kannalta on perusteltua, että tiedusteluasioita tulisi käsitellä riippumattomassa tuomioistuimessa tai muussa elimessä, missä varmistettaisiin, että yksittäinen tehtävä ja siihen liittyvät keinot ovat lainmukaisia ja perusteltuja. Oikeusturvan



30.6.2015

Lainvalmistelu- ja oikeusyksikkö

kannalta on tärkeää, että tiedustelulainsäädäntöä kehitettäessä määritellään valitustie ja mahdollisuus päätösten alistamiseen oikeuskäsittelylle. Tiedustelun kohteilla tulisi olla oikeus saada lainvalvontaviranomaisen apua oikeuksiensa toteuttamisessa.

Lausuntopalautteen mukaan lainvalvontakysymys kaipaa kaikkinsa lisäselvitystä, että se täyttäisi mm. EU:n perusoikeuskirjan vaatimukset. Tietojen tarkastamista, hyödyntämistä, säilyttämistä, luovuttamista ja tuhoamista tulisi olla menettelytapasäännökset. Tiedustelutoiminnan tulisi olla kattavan parlamentaarisen ja oikeudellisen valvonnan kohteena. Toimintaa suoritettaisiin virkavastuulla ja siihen tulisi liittyä myös rikosoikeudellinen vastuu. Elinkeinoelämän edustajien lausuntopalautteessa oltiin huolissaan myös yritysten oikeusturvasta, mikäli sääntely tulisi kohdistumaan myös niiden toimintaan.

#### Perusoikeuksien turvaaminen

Perustuslain 22 § mukaan julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteuttaminen. Perusoikeuksien toteuttaminen velvoittaa viranomaisia yhtäältä olemaan puuttumatta perusoikeuksiin ja toisaalta taas ryhtymään niihin toimiin, jotka ovat perusoikeuksien toteutumisen kannalta tarpeen. Viranomaisten tehtäviin kuuluu mm. vapauden, hyvinvoinnin, turvallisuuden ja laillisten oikeuksien takaaminen. Laillisuusvalvonnassa on toistuvasti todettu, että viranomaisten on huolehdittava lakisääteisten tehtäviensä hoitamisesta myös poikkeusoloissa, kuten tietojärjestelmien toimintahäiriöissä. Tiedustelulainsäädännön puuttuminen asettaa viranomaisten lausuntopalautteen mukaan Suomen turvallisuusviranomaiset lakisääteisten perustehtäviensä hoitamisen kannalta vaikeaan tilanteeseen. Professori Tomi Voutilainen toteaa lausunnossaan, että sähköisissä tietovarannoissa olevien tietojen avulla toteutetaan osaltaan yksilön perusoikeuksia välttämättömään toimeentuloon ja huolenpitoon, sekä riittäviin sosiaali- ja terveyspalveluihin perustuslain 19 §:n mukaisesti.

Laillisuusvalvonnassa on vakiintuneesti katsottu, ettei tietojärjestelmiin liittyvillä syillä voida perustella poikkeamista hyvän hallinnon ja oikeusturvan viranomaismenettelylle asettamista vaatimuksista. Viranomaisten tulisikin tietojärjestelmiä kehittäessään ja käyttäessään kiinnittää huomiota myös siihen, että järjestelmät mahdollistavat hyvän hallinnon turvaavat toimintatavat.

#### Ulkomaantiedusteluun liittyvät erityiskysymykset

Tiedustelutoiminnassa saatu tieto muodostaa myös modernin ulko- ja turvallisuuspoliittisen päätöksenteon perustan. Perusoikeusnäkökulma tulee ratkaista mietinnössä esitetyllä tavalla niin, että turvallisuuteen ja luottamuksellisen viestin suojaan liittyvät näkökohdat tulevat huomioituiksi tasapainoisella tavalla. Tiedustelulainsäädäntöä on voimassa monissa länsimaisissa demokratioissa ja Suomen ei ole perusteltua jättäytyä kehityksestä, koska ehdotetut sääntelykeinot ovat EIT:n ja ihmisoikeusveloitteiden kanssa sopusoinnussa.

Ulkomaantiedustelu voi olla perusoikeuksien kannalta hyväksyttävämpää, koska tiedonhankintatoimenpiteillä ei olisi samanlaisia välittömiä oikeusvaikutuksia yksilöiden oikeuksiin ja velvollisuuksiin, kuin lainvalvonta- ja oikeusviranomaisten rikosprosessiin liittyvillä tiedonhankintatoimenpiteillä. Ulkomaan sääntelykenttään kuuluu lähettäjävaltion lainsäädäntö, vastaanottajavaltion lainsäädäntö ja kansainväliset sopimukset ja siihen liittyviä oikeusturvajärjestelyjä tulisi miettiä kokonaisuutena.

Lausuntopalautteen mukaan valtioiden välistä "hiljaista hyväksyntää" siihen kohdistuvaan tiedusteluun ei pidetty kestäväenä pitkällä aikavälillä. Suomi voisikin olla aloitteellinen kansainvälisesti vahvistamaan sopimuksia ja käytäntöjä, joilla vahvistettaisiin kansalaisten oikeushyvien turvaamista kestäväällä tavalla. Myös tiedustelutietojen luovuttaminen ulkomaille on myös herkästi perusoikeuskysymys, joka vaatii erityistä tarkastelua.

Professori Martin Scheinin totesi lausunnossaan, että Suomen ei tule sivuuttaa YK:n KP-sopimuksen täysin vakiintunutta tulkintalinjaa, jonka mukaan valtio on ihmisoikeusveloitteidensa sitoma myös



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

suhteessa ulkomailla sijaitseviin ei-kansalaisiin. Toiminnan oikeuttamisen lähtökohtana ei voi olla, ettei vakoilu kohdistu omiin kansalaisiin, vaan ulkomaalaisiin. Yksityiselämän suojan ulottuvuutta suhteessa ulkomaalaisiin tulee tulkita vähintään yhdenmukaisesti Euroopan ihmisoikeussopimuksen 8 artiklan ja sen oikeuskäytännön kanssa.

## 6 Toimivaltaiset viranomaiset

### Tiedusteluviranomainen

Tiedusteluviranomaisen ja sille asetettavien toimivaltuuksien tulisi lausuntopalautteen mukaan täyttää tietyt edellytykset. Viranomaisen tulisi olla valvottu, lailla tehtävään määrätty, riippumaton ja asiantunteva. Viranomaisten lausuntopalautteessa katsottiin perustelluksi, että resurssien tehokkaan käytön, asiantuntemuksen keskittämisen ja valvonnan järjestämisen vuoksi tietoliikennetiedustelua toteuttaisi vain yksi viranomainen. Tietoliikennetiedustelua toteuttavan viranomaisen tulisi olla ensinnäkin riippumaton ja sen toiminnan tulisi olla valvottua. Viranomaiselle tulisi varata riittävät resurssit ja asiantuntemus tehtävän hoitamiseen. Lisäksi tiedustelutiedon tulee olla analysoitua. Erityisesti tietoliikennetiedustelutieto on luonteeltaan sellaista, että sen tulee olla prosessoitua ollakseen ymmärrettävää.

Lausuntopalautteen mukaan tiedustelua suorittavaksi viranomaiseksi ehdotettiin muun muassa suojelupoliisia, puolustusvoimia, puolustusvoimien tiedustelulaitosta ja erikseen perustettavaa uutta viranomaista. Eräissä lausunnoissa katsottiin, että teleyritys voisi toimittaa pyynnöstä tiedot viranomaiselle tapauskohtaisesti rajatuin perustein, kuten nykyisten telepakkokeinojen osalta. Lausunnoissa esitettiin myös, että siviiliviranomaisten tiedustelu ja sotilasviranomaistiedustelu järjestettäisiin erikseen, koska niiden tarpeet ovat niin erilaiset. Poliisiviranomaisten lausuntojen mukaan siviili- ja sotilastietoliikenteen erottaminen on käytännössä lähes mahdotonta.

Useissa lausuntopalautteissa kiinnitettiin huomiota tapaukseen *Snowden* ja tietoliikennetiedustelua suorittavan viranomaisen haavoittuvuuteen, sekä tästä aiheutuviin uhkiin. Tietoliikennetiedustelua suorittavien viranomaisten mahdollisuuksiin käyttää väärin toimivaltuuksiaan arvioitiin eräiden järjestöjen lausunnoissa huomionarvoiseksi kysymykseksi.

### Toimeksiantajaviranomainen

Lausuntopalautteen mukaan toimeksiantajaviranomaisten tulisi olla täsmällisesti rajattu joukko, jonka valtuuksien pitäisi perustua yksiselitteisesti lakiin. Lausuntopalautteessa esitettiin toimeksiantajaviranomaiseksi useita turvallisuusviranomaisia, joilla on hyvin erilaisia intressejä tiedustelutietoa kohtaan. Ulkomaan tiedustelua koskevassa päätöksenteossa olisi otettava huomioon erityisesti ylimmän valtionjohdon linjaukset. Myös poliisilla, keskusrikospoliisilla ja suojelupoliisilla on selkeä tarve tehtäviensä hoitamisen kannalta tiedustelutietoon.

### Tietoon oikeutettu viranomainen

Tiedustelutiedon käyttäminen ja tietoon oikeutettujen tahojen piirin määrittäminen nousi myös lausuntopalautteessa esille. Lausuntopalautteen perusteella on tärkeää, että tiedustelutiedon käytämisestä on tarkat säännökset. Toimeksiantajaviranomaisen lisäksi muillakin viranomaisilla voi olla tarve hankittuun tiedustelutietoon. Useat viranomaiset toivat esille, että rajallisten resurssien ja tiedon tehokkaan hyödyntämisen vuoksi olisi perusteltua, että tiedot olisivat usean viranomaisen käytettävissä. Viranomaisten tietojenvaihdon ja tietojenvälittämisen tarpeet tulisi huomioida jatkotyössä.

Viranomaislausunnoissa katsottiin pitkälti, että päätöksenteon kannalta olennaisen tiedon tulisi olla päätöksentekijöiden ja päätösten valmistelijoiden käytettävissä. Hakuheitojen kautta rajattua tietomassaa tulisi voida edelleen analysoida ja käyttää, myös rikksentorjuntatehtävissä. Lausuntopalautteessa esitettiin, että esimerkiksi valmisteilla olevasta rikoksesta tulisi voida ilmoittaa, yrityksille



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

tulisi ilmoittaa niihin kohdistuvasta hyökkäyksestä ja muille viranomaisille tulisi välittää niiden tarvitsemat tiedot.

Lausuntopalautteen mukaan tietoon oikeutettuja viranomaisia voisivat olla turvallisuusviranomaisten ohella esitutkintaviranomaiset ja tietyissä tapauksissa syyttäjät. Lisäksi rajavartiolaitos ja tullit katsovat, että niiden toimialueeseen kuuluu mietinnössä mainittujen uhkien kannalta keskeisiä tehtäviä ja näin ollen perusteltu intressi tiedustelutietoon. PTR-yhteistoiminnan katsottiin jääneen lausunnossa vaille tarkastelua (poliisin, tullin ja rajavartiolaitoksen yhteistyö). Valtionvarainministeriön mukaan sen Julkisen hallinnon ICT-toiminto tarvitsee lakisääteisten tehtäviensä hoitamiseksi ajantasaista ja ennakoivaa tilanneymmärrystä julkisen hallinnon viranomaisten tiedonkäsittelystä, sähköisistä palveluista, tietoliikenteestä ja tietoturvasta sekä näihin kohdistuvista uhkista ja niiden analyyseistä. Valtioneuvoston kansliassa toimivan valtioneuvoston tilannekeskuksen keskeisten tehtävien kannalta tiedustelutiedolla on merkitystä. Professori Tomi Voutilaisen lausunnon mukaan turvallisuusviranomaisten hallintorakenteen laajuuden vuoksi jatkovalmistelussa olisi syytä linjata suppeasti ne viranomaiset, jotka voivat hyödyntää tiedustelutietoa.

Lausuntopalautteessa pidettiin epäselvänä, millaisin edellytyksin tiedustelutietoa voitaisiin luovuttaa ulkomaille. Laissa tulisi rajata millä perusteilla tiedustelutiedot voitaisiin luovuttaa ulkomaalaisille yhteistyötahoille. Lausuntopalautteessa suhtauduttiin osin kielteisesti tiedustelutiedon luovuttamiseen ulkomaisille tahoille ylipäätään. Järjestelmän läpinäkyvyyteen tulisi kiinnittää huomioita.

## 7 Laillisuusvalvonta ja oikeusturvakeinot

Laillisuusvalvonnan ja oikeusturvakeinojen tulisi olla lainsäädäntöön sisäänrakennettuja niin, että tiedustelussa mahdollisuus väärinkäyttöihin jäisi mahdollisimman pieneksi, yksilöllä olisi tehokkaat oikeusturvakeinot käytössään ja järjestelmä olisi mahdollisimman läpinäkyvä. Valvonnan tulisi olla tiedustelujärjestelmään sisäänrakennettu elementti. Lausuntojen mukaan valvonta ei saa olla pinta-puolista ja yleistä.

Lausuntopalautteen mukaan oikeusturvakeinot ovat kohteen kannalta salaisten tiedustelutoimien erityisluonteesta johtuen korostetun tärkeitä. Oikeusturvakeinojen asianmukainen järjestäminen liittyy koko oikeudellisen järjestelmän uskottavuuteen. Tiedustelukeinojen käyttöön liittyvä salassapito altistaa toiminnan myös epäilyille sen lainmukaisuudesta, olipa siihen aihetta tai ei. Eduskunnan oikeusasiamiehen mukaan oikeussuojajärjestelmän keskeisiä osia ovat tuomioistuimen lupamenettely, viranomaisten sisäinen valvonta ja oikeusasiamiehen laillisuusvalvonta.

### Lupamenettely

Lausuntopalautteessa puollettiin vahvasti sitä, että riippumattoman tuomioistuimen tai muun elimen myöntämä lupa tiedonhankintakeinon käytön edellytyksenä varmistaisi objektiivisen arvion sille, että lainmukaiset edellytykset keinoon käytölle ovat olemassa. Erityisesti punninta keinoon oikeasuhtaisuudesta edellyttää ulkopuolista arviota. Sekä luvan hakijalta että sen myöntäjältä edellytetään riittävä perusteleminen, jotta niiden toiminta on uskottavaa ja jälkikäteinen arviointi mahdollista. Toiminnan raamien avoimuus ja valvonnan läpinäkyvyys nähtiin myös oikeusturvan kannalta tärkeinä elementteinä.

Lausuntopalautteessa arvioitiin, missä vaiheessa prosessia lupaa tulisi hakea. Esimerkiksi sosiaali- ja terveysministeriön mukaan tiedusteluviranomaisen tulisi hakea lupaa siinä vaiheessa, kun automaattikalla kerätyn tiedon perusteella halutaan tutkia tarkemmin tietoliikenteen sisältöä. Eräissä lausunnoissa kannatettiin hakuehtojen hyväksyttämistä lupamenettelyssä. Luvan antavan tahon tulisi voida lain tasolla määritetyn luettelon perusteella arvioida, onko luvan antamiselle perusteita. Mikäli tietoliikennetiedustelun perusteella yksilöidään henkilö, johon tarkempaa tiedustelua kohdistetaan, tarvitaan kohdennettuun tiedonhankintaan oma erillinen toimivaltuutus.



30.6.2015

Lainvalmistelu- ja oikeusyksikkö

Tiedonhankintaa koskevat lupa-asiat olisi poliisihallituksen lausunnon mukaan ohjattava Helsingin käräjäoikeuteen, jonne on jo keskitetty tiettyjen salaisten tiedonhankintakeinojen lupaharkinta. Kyseisellä tuomioistuimella on jo asian edellyttämää vastaavaa kokemusta. Myös mahdollisuus erityistuomioistuimen tai -viranomaisen perustamiseen on tarkoin harkittava. Tiedustelulainsäädännössä olisi myös huomioitava mahdollinen tiedustelutiedolla saatava ylimääräinen tieto. Ylimääräisellä tiedolla tarkoitetaan tässä yhteydessä tietoa, joka voi olla viranomaistoiminnan kannalta merkityksellistä, mutta jonka hankkimiseen tiedustelutoimeen oikeuttanutta lupaa ei ole haettu.

#### Valvonta

Lausunnoissa otettiin enemmän kantaa siihen, millaista valvonnan tulisi olla kuin siihen, mikä valvontaa suorittava taho olisi. Valvonnan tulisi olla riittävän asiantuntevaa, riippumatonta ja tehokasta. Valvojalla tulisi olla pääsy kaikkeen asiaan liittyvään materiaaliin. Viranomaisen sisäinen valvonta ja esimiestyö ovat salaisen tiedonhankinnan kohdalla keskeistä toiminnan lainmukaisuuden takaamisessa. Mitä lähempänä toimintaa valvonta on, sitä tehokkaammin se voi havaita ja välittömästi puuttua vähäisiinkin ongelmiin. Valvontatoimilla tulisi olla oikeudellisesti velvoittava vaikutus suhteessa valvottaviin.

Salaisella toimintakentällä vastuullisuus edellyttää tilivelvollisuutta ja toimintojen kirjaamista eli selkeitä vastuu-asemia, kattavaa dokumentointia ja valvontaa. Rekisterinpitäjän on kyettävä osoittamaan rekisteröinnin laillisuus. Tiedusteluviranomainen on auktorisoidun tahon kysyessä velvollinen esittämään täydellisen selvityksen toiminnastaan. Järjestelmässä voisi olla myös sisäänrakennettu automaattinen leikkuri, joka lopettaa tietoliikenteen seurannan ja talletuksen, jos se kasvaa lupaehdoista suuremmaksi.

Lausuntopalautteessa kiinnitettiin huomiota myös hallintovaliokunnan lausuntoon, jonka mukaan vastuullisuus ja tilivelvollisuus korostuvat toimintakentällä, joka ei ole julkinen tai läpinäkyvä. Lausunnoissa mainittiin myös kansallisia esimerkkejä julkisuudessa olleista tapauksista, joissa viranomainen on katsellut luvatta kansalaisten tietoja rekistereistä.

Oikeusasiamiehen ulkoinen laillisuusvalvonta painottuu sisäisen valvonnan valvontaan. Oikeusasiamiehen lausunnon mukaan sen suorittama laillisuusvalvonta on jälkikäteistä ja parhaimmillaankin varsin yleiskatsauksellista. Oikeusasiamies on kaukana itse toiminnasta, eikä hän voi ryhtyä ohjaamaan viranomaisten toimintaa tai muutoinkaan olla keskeinen rajojen asettaja, joka korjaisi lainsäädännön heikkoudet.

Valvontaa suorittavaksi tahoksi ehdotettiin muun muassa viestintävirastoa, eduskunnan oikeusasiamiestä, sisäistä valvontaa ja uutta tehtävää varten nimenomaan perustettavaa elintä. Riippumaton ja eettisiin kysymyksiin huomiota kiinnittävä valvontaelin voisi koostua esimerkiksi oikeuslaitoksen, poliittisen edustuksen ja tietosuojavaltuutetun muodostamasta ryhmästä. Myös eduskunnan kautta tapahtuva parlamentaarinen valvonta nostettiin lausunnoissa esille.

Lausuntopalautteen mukaan tiedustelusta tulisi julkistaa yksityiskohtaista tilastotietoa, julkilausumia ja seurata sen tosiasiallista tehokkuutta. Tilastot mahdollistaisivat julkisen keskustelun. Tilastojen tulisi sisältää lupien määrä tilastointiväliä kohden, kuinka suureen verkkoalueeseen, datamäärään, henkilömäärään ja ajanjaksoon kullakin luvalla suoritettu tietoliikennetiedustelu on kohdistunut, sekä miten pitkäksi määräajaksi luvat on myönnetty. Valvontaorganisaation tulisi tarkistaa tilastojen oikeellisuus. Valvontaorganisaation tulisi tehdä tilastojen ja muun valvonnan perusteella vuosittainen julkilausuma.

Ulkomaan tiedustelun osalta merkillepantavaa on, että huomioiden tiedustelutoimien tehokkuuden edellyttävän toimien pysymistä niiden kohteelta salassa ja huomioitaessa, että määrättyihin tiedus-



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

telutoimiin ryhtyminen voi olla omiaan vaarantamaan Suomen suhteet vieraisiin valtioihin, tavanomainen vastavuoroinen oikeudenvälitys ei liene tiedustelutoimien osalta mahdollista. Tiedustelutoimintaan liittyvä tiedonvaihto toisen maan kanssa tulisi säännellä ja valvoa, ettei esimerkiksi voitaisi ulkoistaa oman maan kansalaisten valvontaa ulkomaille. Tiedustelulla saadun tiedon luovutus ulkomaille tulisi altistaa parlamentaariseen ohjaukseen ja valvontaan, jotta poliittinen riski voidaan arvioida demokraattisella menettelyllä.

#### Tietojen käsittely

Oikeusturvan näkökulmasta on myös olennaista, että laissa olisi määritelty kuinka kauan tiedustelutietoja säilytetään ja miten niitä säilytetään. Esimerkiksi Data retention -ratkaisussa tulkittiin laajamittainen tietojen tallentamisvelvollisuus perusoikeuskirjan 7 ja 8 artiklan vastaiseksi. Data Retention-tuomion perusteella perustuslakivaliokunta on katsonut, ettei tuomiosta aiheudu suoranaista estettä tällaiselle sääntelylle, jos oikeasuhtaisuuden vaatimukset toteutetaan muilla tavoin, kuten rajaamalla säilytettävät tiedot vain siihen, mitä pidetään välttämättömänä sääntelyn taustalla olevan tarkoituksen, eli esimerkiksi vakavien rikosten tutkinnan, selvittämisen ja syyteharkintaan asettamisen kannalta.

Valtionhallinnon tieto- ja kyberturvallisuuden hajautunut hallinnointi- ja ohjausjärjestelmä hankaloitavat erilaisten tieto- ja kyberturvallisuustoimenpiteiden toteuttamista. Hajautuneesta mallista johdun tieto- ja kyberturvallisuutta koskevia erityisen korkean suojaustason tietoja voidaan joutua käsittelemään usean ministeriön hallinnonalalla, joka lisää riskiä näiden tietojen paljastumisesta.

Käytännössä tiedustelussa saadaan myös muita tietoja, kuin mihin tiedustelu alun perin kohdistettiin (ylimääräinen tieto). Esimerkiksi tietoverkkokorjauksen esitutkinnassa on havaittu, että joissain tapauksissa esim. verkkolaitteiden ohjaustietojen virheelliset päivitykset ovat generoineet hyökkäykseksi tulkittua verkkoliikennettä tai asianomistajaorganisaatiot eivät ole pystyneet tunnistamaan kaikkea organisaationsa eri liitännäisosien tuottamaa verkkoliikennettä. Näiden kokemusten perusteella voidaan arvioida, että tietoliikennetiedustelun kohteeksi voi joutua aiheettomasti. Professori Martin Scheinin arvioi lausunnossaan tämän olevan erittäin merkittävä kysymys tietoliikennetiedustelun oikeudellisen sallittavuuden kannalta.

## **8 Erityiskysymyksiä**

Erityiskysymyksenä lausuntopalautteessa nousi esiin tietyt asiakokonaisuudet, joihin liittyy erityisen arkaluonteista ja erityistä suojattua asemaa nauttivaa tietoa. Tällaista sähköistä tietoverkoissa liikkuva tietoa Asianajajaliiton, Journalistiliiton ja Viestinnän keskusliiton lausuntojen mukaan ovat erityisesti terveystieto, oikeudenkäyntiavustajan ja asiakkaan välinen tiedonvaihto sekä journalistin lähdesuoja. Lausunnoissa mainittiin myös papin, sairaanhoitajan, psykologin, sosiaalityöntekijän ja lääkärin kanssa käytyjen keskustelujen erityisluonteesta. Näiden tahojen kanssa käytävään keskusteluun ei voi edes pakkokeinolin mukaisella tuomioistuimen luvalla kohdentaa toimia.

Lausuntopalautteen mukaan lainsäädäntöä tulisi kehittää niin, ettei erityissuojaa nauttiviin tietoihin lainkaan kajottaisi. Asia voitaisiin myös mahdollisesti järjestää samalla tavalla, kuin pakkokeinolisissa. Mikäli ilmenee, että kyseessä on viesti, jonka kuuntelu tai katselu ei ole sallittu, toimenpide on keskeytettävä ja sillä saadut tallenteet ja tiedot koskevat muistiinpanot on heti hävitettävä.

Toisena erityiskysymyksenä esiin nousi useissa lausunnoissa rikosperusteiseen tiedusteluun liittyvät kysymykset. Rikostorjunnan ja sotilastiedustelun tavoitteiden välinen rajanveto oli lausuntopalautteen perusteella vaikea hahmottaa.

#### Journalistin lähdesuoja

**Postiosoite**  
**Postadress**  
**Postal Address**  
Puolustusministeriö  
PL 31  
FI-00131 Helsinki  
Finland

**Käyntiosoite**  
**Besöksadress**  
**Office**  
Eteläinen Makasiinikatu 8  
00130 Helsinki  
Finland

**Puhelin**  
**Telefon**  
**Telephone**  
0295 16001  
Internat. +358 295 16001

**Faksi**  
**Fax**  
**Fax**  
(09) 160 88244  
Internat. +358 9 160 88244

**s-posti, internet**  
**e-post, internet**  
**e-mail, internet**  
kirjaamo@defmin.fi  
www.defmin.fi





30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

Lausuntopalautteen mukaan mietintö ei sisällä tarkastelua sananvapauteen (EIS 10 artikla, PL 12 §) sisältyvän tiedotusvälineiden lähdesuojan osalta. Euroopan ihmisoikeussopimuksen tulkinnassa lähdesuojan on katsottu sisältyvän nimenomaan 10 artiklan sananvapaussäännöksen soveltamisalaan. Lähdesuojassa on kyse mahdollisuudesta tuoda tietoa ja osallistua julkiseen keskusteluun. Lausuntopalautteen mukaan valtion tulee pidättäytyä sääntelystä, joka tekisi lähdesuojan käytännössä tehottomaksi ja toisaalta valtiolta odotetaan positiivisia toimenpiteitä oikeuksien turvaamiseksi.

Viestinnän keskusliiton lausunnon mukaan journalistin verkkoyhteyksiin kohdistuva tiedustelu vastaa nykyisessä teknisessä ympäristössä pääsyä kaikkiin journalistin tallenteisiin, asiakirjoihin ja viesteihin, jotka aikaisemmin olivat hänen työpöydällään. Tiedonhankintalain vaarana on mahdollisuus, että tiedonantajan tiedot tulevat myös viranomaisten tietoon, mikä vaikuttaisi negatiivisesti yhteiskunnalliseen keskusteluun ja tiedotusvälineisiin. Lausunnossa mainittiin, että joissakin maissa tiedustelutoiminta on tosiasiallisesti kohdistunut journalisteihin. Lähdesuoja turvaa välillisesti kansalaisen oikeuden tiedonsaantiin ja oikeuden muodostaa käsityksensä yhteiskunnallisista asioista. Tyypillisesti kyseessä on yhteiskunnallisen epäkohdan paljastaminen, eikä lähde kertoisi viranomaisille tiedoistaan. Lähdesuojaan vaikuttaa myös se, kuinka vahvaksi se käytännössä mielletään ja luottamus lähdesuojan pitävyyteen.

Lausunnossa ehdotetaan tiedustelulakiin otettavaksi tietoyhteiskuntakaaren 151 § 1 momenttia vastaavaa säännös, jolla kielletäisiin tiedonhaku median toimitukselliseen sisältöön. Lisäksi tiedustelulaissa tulisi olla säännös, jonka mukaan viranomainen on velvollinen poistamaan journalistista sisältöä koskevan viestin, joka voi johtaa lähdesuojan murtumiseen. Lisäksi laissa tulisi olla riittävät rangaistukset edellä mainittujen sääntöjen rikkomisesta.

#### Terveystieteen liittyvät tiedot

Sosiaali- ja terveysministeriö korosti lausunnossaan terveystietojen erityisluonteen huomioimisen tärkeyttä. Sosiaali- ja terveysministeriön hallinnonalan vastuulla on useita yhteiskunnan turvallisuusstrategiassa määriteltyjä elintärkeitä toimintoja. Lausunnon mukaan terveystietoja on siirretty enenevässä määrin sähköisiin järjestelmiin, niitä välitetään sähköisesti ja myös kansallisten rajojen ulkopuolelta. Tietoja liikkuu sähköisesti myös asiakkaiden ja viranomaisten välillä, joten salaus ei ole usein kovin tehokasta. Sosiaali- ja terveydenhuollossa ja sen tietoverkoissa käsitellään arkaluonteisia tietoja, joista viestin sisällön lisäksi arkaluonteista ovat viestin metatiedot ja itse viestin olemassaolo.

Sosiaali- ja terveysministeriön lausunnon mukaan palvelujen sähköistäminen ja tehostaminen on ensiarvoisen tärkeää, eikä pelko tietojen seurannasta saa vaarantaa tätä kehitystä. Jatkotyössä tulisi huomioida eri viranomaisten erityispiirteet ja erityisesti se, että terveystietoja liikkuu myös yli rajojen sekä yksityisten palveluntarjoajien palveluissa. EU/ETA-maihin on suhtauduttava tältä osin kuin kotimaiseen tietoliikenteeseen, koska näihin maihin voidaan siirtää sosiaali- ja terveydenhuollon toimintoja.

#### Rikosperusteiseen tietoliikennetiedusteluun liittyvät kysymykset

Rikostorjuntaan liittyvän siviilitiedustelun ja sotilastiedustelun erottamista omiksi erityisalueikseen pohdittiin monissa lausunnoissa. Useissa lausunnoissa käsiteltiin nimenomaisesti poliisin valtuuksiin tai ehdotettujen tiedustelumenetelmien suhdetta rikosprosessiin. Useissa lausunnoissa nähtiin epäselväksi rajanveto puolustuksellisten uhkien ja muiden uhkien välillä. Tietyissä lausunnoissa pidettiin tärkeänä oikeusvaltioperiaatteen kannalta, että poliisin toimivaltuuksien tulee perustua yksinomaan rikosperusteiseen tiedonhankintaan ja sotilastiedustelu tulee pitää tästä erillään. Erityisesti poliisiviranomaiset kuitenkin katsoivat tiedustelutiedon hyödyntämisen moniviranomaismallin mukaisesti tarkoituksenmukaisimmaksi sääntelykeinoksi, koska uhkien torjumiseen ja tutkimiseen liittyviä toimivaltuuksia on vaikea osoittaa puolustusvoimien tehtävälueelle.



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

Lausunnoissa todettiin, että tiedustelu on yksi osa rikostorjunnan kokonaisuutta. Yhteiskunnan turvallisuuden kokonaistilannekuvan kannalta merkittävää tietoa tulee jatkuvasti poliisin ja muiden lainvalvontaviranomaisten tietoon. Mahdollisimman täydellisen tilannekuvan saavuttamiseksi sekä mietinnössä tarkoitettulla tiedustelulla että normaalilla poliisitoiminnalla saadut tiedot tulee voida tiedusteluprosessin analyysivaiheessa yhdistää. Sotilastiedustelutieto tulisi joka tapauksessa antaa poliisin käyttöön niissä tapauksissa, joissa on kyse vakavan rikoksen valmistelusta, josta ilmoittamatta jättäminen on rikoslain mukaan rangaistavaa. Olisi myös asianomistajan kannalta ongelmallista, ettei viranomaisten tietoja voisi käyttää oikeusprosessissa, vaikka tiedot rikoksesta ja sen tekijästä olisivat olemassa. Omana kysymyksenä tulisi tarkastella perinteisten virka- ja oikeusapumenettelyjen ulottuvuuksia.

Eräiden lausuntojen mukaan sotilas- ja siviilitiedustelu tulisi voida erottaa niin, ettei rikostutkinnallisenä menetelmänä käytettäisi ehdotettua tietoliikennetiedustelua. Lausuntopalautteen perusteella jäi ilmeisen epäselväksi, mitkä olisivat tiedustelun oikeusvaikutukset. Tiedonhankinnan jälkeen tapahtuvat, tiedon käyttämiseen liittyvät seikat herättivät erityisesti kysymyksiä.

## 9 Ehdotusten vaikutukset

Lausunnoissa arvioitiin ensinnäkin ehdotusten toteuttamisen mahdollisia vaikutuksia ja kuinka ehdotukset toteutettaisiin niin, että niillä olisi mahdollisimman vähän tai ei ollenkaan negatiivisia vaikutuksia toimintakenttään. Lisäksi arvioitiin, mikä olisivat ns. nollavaihtoehdon vaikutukset, mikäli tiedustelulainsäädäntöä ei lähdetäisiin kehittämään ollenkaan.

Tiedustelujen etujen ja haittojen arviointia pidettiin lähtökohtana sille, tuleeko tiedustelulainsäädäntöä ylipäättään kehittää. Edut tulisi esittää konkreettisesti. Tiedonhankinta olisi yksi keinoista tietoa ja kyberturvallisuuden edistämiseksi, jonka lisäksi tarvitaan turvallisuus- ja varautumisvaatimuksia täyttävää osaamista, toimintaprosesseja ja teknisiä ratkaisuja. Ehdotusten vaikutuksia ei tulisi arvioida irrallisesti, vaan osana kokonaisuutta.

### Vaikutukset yrityksiin

Lausuntopalautteessa erityisesti mielenkiintoa herättivät vaikutukset yrityssalaisuuksiin sekä yritysten ja niiden asiakkaiden luottamuksellisiin viesteihin ja tietoihin. Lausuntopalautteen mukaan yrityksille ei tule esittää velvoitteita suomalaisten tuotteiden tai palveluiden tietoturvan heikentämiseen, esim. asentamaan takaportteja tai luovuttamaan salausavaimia. Suomalaisten yritysten on voitava profiloitua koostetusti tietoturvallisten tuotteiden kehittäjinä ja tuottajina. Olisi asiakassuhdeiden kannalta ongelmallista, mikäli viranomaiset edellyttäisivät yrityksiltä yhteistyötä tietojen luottamuksellisuuden murtamiseksi.

Tiedonhankintamenetelmien kehittämisessä kotimaisella teollisuudella tulisi olla lausuntopalautteen mukaan merkittävä rooli, koska Suomessa on tämän alan korkeatasoista osaamista. Ehdotetusta viranomaistoiminnasta olisi hyötyä myös elinkeinoelämälle, koska on todennäköistä, että teollisuus kehittää, toteuttaa, integroi ja ylläpitää ehdotuksissa kuvattujen toimien edellyttämät järjestelmät. Tiedustelussa havaituista tietomurroista tulee tiedottaa kyseisiä yrityksiä, jos tiedustelun tarkoitus ei vaarannu. Yrityssalaisuuksia ei saa paljastaa kansainvälisten organisaatioiden välisessä tiedonvaihdossa, jos salaisuudet voivat päästä toisten yritysten tietoisuuteen.

Elinkeinoelämän kannalta turvallinen, selkeä ja ennustettava toimintaympäristö, sekä yrityssalaisuuksien ja uusien innovaatioiden säilyminen ovat perusedellytyksiä, jotka tulee asian valmistelussa huomioida. Vastuullisesti toteutettu sääntely voi toimia kilpailuetuna Suomelle. Turvallisuus tulevaisuudessa varmistetaan kunkin toimijan itsensä toimesta myös tulevaisuudessa ja toimijoilla on oltava tähän riittävät valtuudet. Jos verkkoa yritetään säännellä ja sen sisältöä kuunnella yksilönsuojan tai avoimuuden kustannuksella, voi mielenkiinto tietoturvan kehittämiseen kääntyä viranomaisvastai-



30.6.2015

Lainvalmistelu- ja oikeusyksikkö

seksi. Sääntely voi lisätä sellaisten toimijoiden aktiivisuutta, joiden tavoitteena on verkon vahingoittaminen. Suomalainen käytäntö, jossa viestin salaisuutta vaalitaan ja asiakas voi luottaa viestinnän suojaan, on kilpailuetu.

Ehdotuksilla olisi vaikutuksia erityisesti tietoverkkoja ylläpitäviin ja hallinnoiviin tahoihin. Kriittinen infrastruktuuri on yksityisten yritysten hallussa ja tiedustelun tekninen toteuttaminen tulisi ainakin osittain yritysten tehtäväksi. Jatkotyössä tulee ottaa huomioon tietoverkkopalvelualan yrityksiin kohdistuvat oikeusvaikutukset, kustannukset ja muut vaikutukset. Mikäli tietoliikennetiedustelu toteutettaisiin ja asetettaisiin kaikille relevanteille toimijoille velvollisuus osoittaa liityntäpisteet omistamistaan tietoliikenneverkosta, aiheuttaisi se näille toimijoille ylimääräisiä investointikustannuksia ja tämän lisäksi todennäköisesti korkeampia ko. infrastruktuurin ylläpito- ja huoltokuluja. Tähän järjestelmään rakennettavat liityntäpisteet olisivat jo itsessään mm. tietoturvaan ja jatkuvuussuunnitteluun vaikuttava riskikokonaisuus, jonka suojaamiseen liittyisi oma pysyvä investointi- ja kulutaakansa.

Elinkeinoelämän edustajien lausuntojen mukaan yrityksille aiheutuvat välilliset sekä välittömät kustannukset tulisi korvata täysimääräisesti. Kuluja aiheutuisi henkilöstökuluista, raportoinnista, vikailoista, viranomaisten avustamisesta, hallinnoinnista, päivityksistä ja tarvittavista investoinneista. Viranomaisten toiminta tietoverkoissa voisi aiheuttaa häiriöitä ja verkon kuormittumista. Mietinnössä olisi tullut ottaa enemmän kantaa arvioituihin kustannusvaikutuksiin.

#### Vaikutukset Suomen kilpailukykyyn, investointeihin ja elinkeinoelämään

Elinkeinopoliittiset vaikutukset tulisi arvioida esim. toiminnan välittömiä ja pitkän aikavälin kustannuksia sekä elinkeinotoimintaan, investointeihin ja kilpailukykyyn liittyviä seikkoja. Jatkossa tulisi selvittää tarkemmin tietoturvaan ja kyberrikollisuuteen liittyviä kysymyksiä, sekä vakoilun havaitsemista ja torjuntaa. Valtionlaista alkuperää olevien haittaohjelmien torjuntakyvyn parantaminen on elinkeinoelämän näkökulmasta tarpeellista. Turvallisella ja laadukkaalla valvonnalla suojattu infrastruktuuri nostaa kynnystä kohdistaa kyberhyökkäyksiä Suomessa sijaitseviin palveluihin. Elinkeinoelämän edustajien lausuntojen mukaan viranomaisten tulisi selkeästi tuoda ilmi, ettei sääntely uhkaa liiketoiminnallista ympäristöä ja Suomen mainetta datan turvasatamana.

Eräissä lausunnoissa katsottiin, että tiedustelulainsäädännön kehitykseen liittyvän epävarmuuden jatkuminen vahingoittaa kansantaloutta. Lainsäädäntöehdotuksilla voisi olla negatiivisia vaikutuksia yritystoimintaan, jotka tulee ehdotusten täsmentyessä arvioida. Voimakkaasti vieniin nojaavien kotimaisten tietoturva- ja tietotekniikkayritysten kilpailuedun poistuessa ja viennin vaikeutuessa toimintaedellytykset vaarantuvat, mikä lisää Suomen riippuvuutta ulkomaisesta teknologiasta. Tällä hetkellä Suomi nauttii vielä ainutlaatuista ja merkittävää kilpailuetua.

Kansainvälisen vertailun osalta tulee huomioida, että toteutumatta jääneiden investointien ja käytämättömien mahdollisuuksien vaikutusta kokonaistalouteen on lähes mahdotonta arvioida. Jos sääntelyllä päädytään asettamaan yrityksille velvoitteita (esimerkiksi liityntäpisteiden osoittaminen), on erittäin tärkeää tunnistaa kaikki relevantit toimijat tietoliikennemarkkinoilla. Suomalaisten teleyritysten lisäksi markkinoilla toimii mm. useita kansainvälisiä teleyrityksiä ja toimijoita.

Valmisteluprosessi on saatava vahvistamaan Suomen kiinnostavuutta investointien ja digiteollisuuden sijaintimaana. Elinkeinoelämään liittyvät näkökohdat tulee huomioida jatkotyössä, eli luottamusta suomalaiseen ICT-alaan tai Suomeen investointikohteena ei saa vaarantaa, salausavaimia tai takaportteja ei anneta viranomaisten käyttöön ja tiedustelusta aiheutuvat kustannukset tulee suunnata viranomaisten maksettavaksi.

#### Yhteiskunnalliset vaikutukset

**Postiosoite**  
**Postadress**  
**Postal Address**  
Puolustusministeriö  
PL 31  
FI-00131 Helsinki  
Finland

**Käyntiosoite**  
**Besöksadress**  
**Office**  
Eteläinen Makasiinikatu 8  
00130 Helsinki  
Finland

**Puhelin**  
**Telefon**  
**Telephone**  
0295 16001  
Internat. +358 295 16001

**Faksi**  
**Fax**  
**Fax**  
(09) 160 88244  
Internat. +358 9 160 88244

**s-posti, internet**  
**e-post, internet**  
**e-mail, internet**  
kirjaamo@defmin.fi  
www.defmin.fi



30.6.2015

Lainvalmistelu- ja oikeusyksikkö

Lisääntyvää valvontaa yhteiskunnallisena ja yleismaailmallisena ilmiönä, sekä sen vaikutuksia käsiteltiin useissa lausunnoissa. Eräissä lausunnoissa katsottiin, että tietoverkkojen valvontamahdollisuuksien laajentuessa luottamus valtioon vähenee, millä on vaikutusta yhteiskunnan vakauden, taloudelliseen kehitykseen ja yleisen luottamustason kannalta. Tietoliikenteeseen kohdistuva tiedustelu nähtiin monissa lausunnoissa negatiivisena asiana ja sen yhteiskunnallisista vaikutuksista oltiin huolissaan. Lausuntopalautteen mukaan internetin avoimuus on ollut perustana sen menestykselle, eikä sääntelyllä tulisi rajoittaa avoimuudesta kumpuavaa innovatiivisuutta.

Lausuntopalautteessa todettiin, että kansalaiset ovat hyvin riippuvaisia tietoyhteiskunnan palveluista, kuten vesi- ja energiahuollosta, mitkä tulee voida turvata muuttuvassa toimintaympäristössäkin. Lausuntopalautteen mukaan kansalaisten ja yritysten luottamusta digitaalista asiointia ja verkkopalveluja kohtaan on lisättävä, mikä myös lisää toimijoiden halua investoida verkkoon ja palveluihin. Lausuntopalautteen mukaan internetin suojaukseen panostavia toimijoita on paljon ja elinkeinoelämän edustajat suhtautuivat epäilevästi siihen, että sääntely parantaisi verkkojen turvallisuutta. Toisaalta lausuntopalautteen perusteella on selvää, ettei sääntelyn toteuttamatta jättäminen myöskään varjele tietoverkkojen puhtautta tai korkeaa tietosuojaa.

Eräissä lausunnoissa viitattiin tutkimuksiin, jossa on todettu, että Yhdysvaltojen kansalaiset ovat muuttaneet käyttäytymistään tietoverkoissa suojataksaan tietojansa valtiolta. Kansalaiset ovat muun muassa rajoittaneet sosiaalisen median käyttöä, muuttaneet matkapuhelimenkäyttötapojaan ja tehneet suojaustoimenpiteitä. Ilmiö ei ole toivottava valtioon kohdistuvan luottamuksen, yhteiskuntauhan tai kansantalouden kannalta. Asiassa tulisi huomioida myös valmistelun aikaiset vaikutukset. Valmistelussa tulee suorittaa aktiivista ja ymmärrettävää viestintää ulospäin. Lausuntopalautteen mukaan yleinen mielipide on huomioitava valmistelussa.

#### Kustannusvaikutukset

Lausuntopalautteessa edellytettiin kustannusten huolellista arvioimista jatkossa. Lausuntojen antajat olivat tyytymättömiä mietinnön kustannusvaikutusten arviointiin. Tarvittavan teknologian arvioitiin olevan arvokasta ja vanhentuvan nopeasti. Lausuntopalautteessa kritisoitiin Ruotsin ja USA:n tiedustelutoiminnan kasvavaa kulurakennetta.

Eryteisesti viranomaiset olivat huolissaan siitä, onko uuden sääntelyn toteuttaminen rajallisten resurssien puitteissa mahdollista. Yksityiset tahot olivat taas huolissaan siitä, rakennetaanko kallis ja raskas valvontakoneisto ilman takeita sen tehokkuudesta ja toimivuudesta. Mietinnössä esitetty toimintamalli olisi lausuntopalautteen mukaan toteutettava resurssitehokkaasti. Tiedustelutoiminta on toteutettava niin, että malli on yhteensopiva sekä HAVARO-palvelun, että muiden toteutuneiden tai toteutettavien Kyberturvallisuuskeskuksen huoltovarmuuskriittisille yrityksille kohdentamien palveluiden kanssa.

Kustannusten kannalta ongelmallisena nähtiin tarvittavan tiedusteluteknologian kehittäminen ja sen ajan tasalla pitäminen. Tiedustelun kohteeksi valikoituvat toimijat eivät tule käyttämään sellaista teknologiaa, joka olisi helposti murrettavissa. Jatkotyössä on otettava huomioon, että salausteknologia kehittyy tiedustelua nopeammin. Viestien sisällön ja metadatan kerääminen tulee olemaan vaikeaa tulevaisuudessa. Ulkomailla kehitetyn teknologian tietoturva-aukkoja olisi mahdotonta havaita etukäteen, joten järjestelmä tulisi kehittää kotimaassa. Suomen sijainti verkkotopologisesti ja kauttakulkuliikenteen kannalta ei ole edullinen tiedustelun näkökulmasta.

Tiedustelutoiminnan avulla löydettäisiin tietoja, joiden perusteella viranomaisten olisi ryhdyttävä erilaisiin toimenpiteisiin. Näiden toimien käsittely ja prosessaaminen toisi myös kustannuksia. Toimintakokonaisuudelle on varattava riittävät resurssit.

#### Vaikutus turvallisuuteen

**Postiosoite**  
**Postadress**  
**Postal Address**  
Puolustusministeriö  
PL 31  
FI-00131 Helsinki  
Finland

**Käyntiosoite**  
**Besöksadress**  
**Office**  
Eteläinen Makasiinikatu 8  
00130 Helsinki  
Finland

**Puhelin**  
**Telefon**  
**Telephone**  
0295 16001  
Internat. +358 295 16001

**Faksi**  
**Fax**  
**Fax**  
(09) 160 88244  
Internat. +358 9 160 88244

**s-posti, internet**  
**e-post, internet**  
**e-mail, internet**  
kirjaamo@defmin.fi  
www.defmin.fi



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

Lausuntopalautteen mukaan tiedustelulainsäädännön vaikutukset turvallisuuteen tulisi arvioida kokonaisuutena. Jatkovalmistelussa täytyy tarkastella kriittisesti, voidaanko valvonnalla vaikuttaa tehokkaasti yhteiskunnan turvallisuuteen. Asiassa tulee huomioida yhteiskunnan, kriittisen infrastruktuurin ja tietoverkkojen turvallisuus, mutta myös yksittäisen kansalaisen näkökulma. Sotilaallisen tason turvallisuusseikat tulee myös asianmukaisesti arvioida ja Suomen kansallinen turvallisuus on pystyttävä takaamaan.

Useassa lausunnossa todettiin, että tietovuotojen riskit vaikutuksineen olisi myös arvioitava. Tietovuodoilla voi olla hyvin suuri vaikutus Suomen kansainvälisiin suhteisiin, maineeseen ja asemaan. Myös itse järjestelmän muodostama riski turvallisuudelle on otettava huomioon. Tietojen kerääminen kasvattaa sinänsä uhkaa niiden paljastumisriskin takia ja itse järjestelmä voidaan valjastaa päinvastaiseen käyttötarkoitukseen. Arkaluontoisten ulkovaltoja koskevan tiedon säilyttämiseen ja salassapitoon liittyy erityisen suuria riskejä, mikä voi vaikuttaa koko valtion turvallisuuteen. Viranomaisten ja elinkeinoelämän yhteistyöllä voitaisiin pitää yllä kattavaa verkkoturvallisuuden tilannekuvaa. Vaikka tiedustelulla ei pystyttäisi estämään terroritekoja, se voisi vähentää motivaatiota niihin, auttaa tutkintaa, helpottaa vahinkojen minimointia ja palautumiskykyä. Turvalliset verkot ja verkkopalvelut lisäävät kaikkien osapuolten luottamusta toisiinsa, millä olisi positiivinen vaikutus toimintakentällä.

## 10 Jatkotoimenpiteet

Useimmissa lausunnoissa tuettiin lainsäädännön kehittämistä ja selkeiden pelisääntöjen luomista. Keskeistä sääntelyn kannalta on, että luottamuksellisten tietojen suoja ja viestinnän salaisuus turvattaisiin niin kansalaisten, kuin yritystenkin osalta. Perustuslainmukaisuutta on pohdittava jatkovalmistelussa. Hyvin toteutetun sääntelyn tuloksena voisi olla turvallinen toimintaympäristö myös digitaaliselle yritystoiminnalle ja kilpailuetu Suomelle. Suomella on hyvä maine vakaana ja laillisena yhteiskuntana, jossa viranomaisten valtuudet ovat tarkkaan rajattu, mikä on kansallinen etu toimittaessa globaalisti digitaalisia palveluita. Lausuntopalautteen mukaan suomalaisilla yrityksillä ja kansalaisilla on vahva pyrkimys tukea laillista yhteiskuntajärjestystä ja maanpuolustusta, mitä voisi hyödyntää viranomaistoiminnassa. Muun muassa tietosuojavaltuutetun lausunnossa esitettiin pohdittavaksi vaihtoehtoja vapaaehtoiselle yhteistyölle ja kehittämiselle yksityisen ja julkisen sektorin välillä.

Mahdollisten säädösmuutosten perustana on oltava kansalliset tarpeet. Eräissä lausunnoissa katsottiin, että ensisijaisesti tulisi selvittää nykyisen lainsäädännön mahdollisuuksia ja mitä voidaan saavuttaa olemassa olevaa lainsäädäntöä ja käytäntöjä kehittämällä. Toisaalta, muun muassa valtioneuvoston kanslia lausui, että ensin tulisi säätää yleislaki tiedustelusta. Yleislain pohjalta voitaisiin sen jälkeen laatia erityissääntelyä koskien siviili- ja sotilastiedustelua, sekä eri tiedustelumenetelmiä. Tietyissä lausunnoissa toisaalta katsottiin, ettei jatkovalmistelua tulisi aloittaa ollenkaan, koska tiedustelulainsäädäntelyn kehittämisen katsottiin vahingoittavan yksilöiden perusoikeuksia, Suomen kilpailukykyä, yritysten liiketoimintamahdollisuuksia, luottamuksellisen viestin suojaa ja verkon vapautta.

Toimivaltuuksia säädettäessä on kiinnitettävä huomiota erityisesti uskottavan ja mahdollisimman läpinäkyvän valvontamekanismin rakentamiseen. Suomen neutraali ja luottamusta herättävä asema tietoliikenteen kansainvälisenä solmukohtana ei saa vaarantua. Lausunnoissa esitettiin vaihtelevia arvioita siitä, millaisia ehdotusten vaikutukset suhteessa Suomen kilpailukykyyn, investointeihin ja elinkeinoelämään olisivat. Suomi voisi toimia kansainvälisillä foorumeilla edelläkävijänä tietojärjestelmien turvallisuudessa ja digitaalisen toimintaympäristön oikeushyvien turvaamisessa. Valtioiden välillä on pyrittävä ratkaisemaan lainsäädäntöriidit ja vahvistamaan virka-apusopimukset.



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

Tietoliikennetiedustelua koskevan sääntelyn lähtökohdaksi tulee asettaa nykyisen perustuslain puitteissa pysyminen. Apulaisprofessori Juha Lavapuron mukaan erityisesti tulisi kiinnittää huomiota päällekkäisten oikeussuojajärjestelmien keskinäissuhteisiin ja perusoikeuksien muodostamaan kokonaisuuteen. Perusoikeuksien vähimmäissisältöä tulisi katsoa perusoikeusmyönteisestä näkökulmasta, kansallista ja kansainvälistä perusoikeuksien tulkintakäytäntöä kunnioittaen.

Lausuntopalautteessa oli pohdittu sisäministeriön hallinnonalaan kuuluvan siviilitiedustelun ja puolustusministeriön hallinnonalaan kuuluvan sotilastiedustelun suhdetta ja tulisiko lainsäädäntöä kehittää hallinnonalakohtaisesti vai yhdessä. Lausuntopalautteen mukaan siviili- ja sotilastiedustelulla on erilaisia tarpeita ja erityispiirteitä, mutta molempien osalta arvioitaviksi tulevat samantyyppiset peruskysymykset. Siviilitiedustelun ja sotilastiedustelun tehtävien ja toimivaltuuksien sääntelyn, ohjauksen ja valvonnan kehittämisen tulisi olla oikeudellisista johdonmukaisuussyistä sekä tältä osin että muutoinkin keskenään yhteen sovitettua. Raja-aitojen tarpeetonta pystyttämistä tiedustelun, perinteisen poliisitoiminnan ja muun viranomaistoiminnan välille on vältettävä. Erityisesti poliisiviranomaisten lausuntopalautteessa nähtiin resurssitehokkaimmaksi vaihtoehdoksi hoitaa jatkovalmistelu yhdessä työryhmässä, ettei tehtäisi päällekkäistä työtä tai luotaisi päällekkäistä sääntelyä. Viranomaistoimivaltuudet ja asiantuntemus tulisi keskittää tehokkaasti.

Valtiovarainministeriön lausunnon mukaan tiedustelulainsäädännön kehittämisessä tarvitaan lisää strategista ja taloustieteellistä tutkimusta tieto- ja kyberturvallisuuden merkityksestä, jotta voidaan ennakoida ja johtaa digitalisaation vaatimia muutoksia hallinnossa ja säädöksissä. Lausuntopalautteen mukaan kansallinen tiedustelulainsäädäntö on laadittava huomioiden toteutettavuus, hyödyt ja haitat, muutokset toimintaympäristössä, muutostahti, internet-integriteetti maabrändissä, merikaa- peliyhteydet ja ulkomaisten pilvipalvelujen lausunnot. Tietoliikennetiedusteluun liittyvä sääntely tulisi laatia alan toimijoiden kanssa yhteistyössä, jotta vaikutukset tulisivat perusteellisesti arvioiduiksi ja eräät mietinnön virheelliset näkemykset saataisiin oikaistua. Jatkovalmisteluun tulisi ottaa elinkeinoelämän edustusta ja ICT-alan asiantuntemusta.

Jatkotyössä toivottiin kiinnitettävän huomiota EU-parlamentin raporttiin *Report on the US NSA surveillance programme, surveillance bodies in various member states and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*. Lisäksi useassa lausunnossa viitattiin merkittävien internet toimijoiden yhdessä laatimiin periaatteisiin, jotka tulisi ottaa käyttöön kansallisen turvallisuuden turvaamiseen tarkoitettuja viranomaistoimivaltuuksia käytettäessä ja suunniteltaessa ([www.reformgovernmentsurveillance.com](http://www.reformgovernmentsurveillance.com)). Lausunnoissa myös viitattiin myös yhdysvaltojen NSA:n valvontaelimen raporttiin *Report on the Telephone Records Program Conducted under section 215 of the USA Patriot Act and the operations of the Foreign Intelligence Surveillance Court*. SURVEILLE-tutkimushankkeessa on tuotettu asiaan liittyvää arvokasta tietoa, joka tulisi ottaa huomioon.

Jatkovalmistelun aikataulun osalta katsottiin pääsääntöisesti, että sääntelyn kehittämisellä on kiire. Asian kiireellisyyttä korostaa kansainvälisen turvallisuustilanteen heikentyminen ja sen vastaisuudessa todennäköisesti entisestään lisääntyvä arvaamattomuus. Jatkovalmistelussa on kuitenkin ennen kaikkea kiinnitettävä edelleen huomiota avoimuuteen ja kuulemisiin, sekä perusteelliseen lainvalmisteluun.



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

## Liite 1

Mietinnöstä Suomalaisen tiedustelulainsäädännön suuntaviivoiksi pyydettiin lausuntoa alla listatuilta tahoilta. Näiden lisäksi lausuntoa pyydettiin erikseen oikeudellisilta asiantuntijoilta. Nimen jälkeen on merkitty \*-symboli, jos lausuntoa ei annettu.

Kansallinen kokoomus r.p.\*  
Suomen Sosiaalidemokraattinen Puolue r.p.  
Perussuomalaiset r.p.\*  
Suomen Keskusta r.p.  
Vasemmistoliitto r.p.  
Suomen ruotsalainen kansanpuolue r.p.  
Vihreä liitto r.p.  
Suomen Kristillisdemokraatit r.p.  
Tasavallan presidentin kanslia\*  
Valtioneuvoston kanslia  
Ulkoasiainministeriö  
Oikeusministeriö  
Sisäministeriö  
Puolustusministeriö  
Valtiovarainministeriö  
Opetus- ja kulttuuriministeriö  
Maa- ja metsätalousministeriö  
Liikenne- ja viestintäministeriö  
Työ- ja elinkeinoministeriö\*  
Sosiaali- ja terveysministeriö  
Ympäristöministeriö\*  
Oikeuskanslerinvirasto  
Eduskunnan oikeusasiamiehen kanslia  
Tietosuojavaltuutetun toimisto  
Turvallisuuskomitean sihteeristö  
Huoltovarmuuskeskus  
Viestintävirasto  
Poliisihallitus  
Keskusrikospoliisi  
Suojelupoliisi  
Tullihallitus  
Valtakunnansyyttäjänvirasto  
Poliisiammattikorkeakoulu  
Pääesikunta  
Rajavartiolaitoksen esikunta  
Accenture\*  
ABB Oy\*  
AinaCom Oy\*  
Anvia Oyj\*  
Appelsiini Finland Oyj\*  
Avaus Consulting Oy\*  
BaseN Oy  
BusinessOulu\*  
Patria  
Capgemini Finland Oy\*  
Cassidian\*



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

CGI Suomi\*  
Cisco Systems\*  
Codenomicon Oy\*  
Combitech Oy\*  
Cinia Oy (ent. Corenet Oy)  
Cygate Oy\*  
Digialist Oy\*  
DIGILE\*  
Digita Oy\*  
DNA Oyj  
Elisa Oyj\*  
Enfo Oyj\*  
Ericsson\*  
F-Secure Oyj\*  
Flexim Security Oy\*  
Fujitsu Finland Oy  
Google\*  
Idean\*  
Insta Group Oy\*  
Intel Security\*  
Itella\*  
ITS Finland\*  
Ivorio Oy\*  
Juniper\*  
Kaisanet Oy\*  
LPOnet Oy Ab\*  
MavaCom Oy\*  
Microsoft Oy  
MobileMonday Finland\*  
Navicre Oy\*  
Nets Group\*  
Netum oy\*  
Nixu Oy  
Nokia Oyj  
Oy International Business Machines Ab\*  
Pohjois-Karjalan Tietotekniikkakeskus Oy\*  
Prof-Tel Oy  
Pöyry Oy\*  
Relacom Finland Oy\*  
Saab Oy\*  
Samlink\*  
Soprano Commerce Oy\*  
SSH Secure Communications Oyj  
Startup Sauna\*  
Stonesoft Oy\*  
Sunduka Oy\*  
Suomen Erillisverkot Oy  
T G Sarkkinen Oy\*  
TDC Oy\*  
TDF Nordic Oy\*  
TeliaSonera Finland Oyj\*  
Telemast Nordic Oy\*

**Postiosoite**  
**Postadress**  
**Postal Address**  
Puolustusministeriö  
PL 31  
FI-00131 Helsinki  
Finland

**Käyntiosoite**  
**Besöksadress**  
**Office**  
Eteläinen Makasiinikatu 8  
00130 Helsinki  
Finland

**Puhelin**  
**Telefon**  
**Telephone**  
0295 16001  
Internat. +358 295 16001

**Faksi**  
**Fax**  
**Fax**  
(09) 160 88244  
Internat. +358 9 160 88244

**s-posti, internet**  
**e-post, internet**  
**e-mail, internet**  
kirjaamo@defmin.fi  
www.defmin.fi





30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

Tieteen tietotekniikan Keskus Oy (CSC)  
Tieto Finland Oyj  
Ubisecure Solutions Oy\*  
Unisyns\*  
Ymon Oy\*  
American Chamber of Commerce in Finland  
ASML\*  
Electronic Frontier Finland ry EFFI  
Elinkeinoelämän keskusliitto EK  
Euroopan komission Suomen edustusto\*  
FiCix ry  
Finnet-liitto ry  
Finnvera  
FISC  
Internet-käyttäjät ikuisesti IKI ry  
Invest in Finland, Finpro ry\*  
Julkisen sanan neuvosto\*  
Keskuskauppakamari  
Ohjelmistoyrittäjät ry  
Suomen puolustus- ja ilmailuteollisuus PIA ry  
Sähkö- ja teleurakoitsijaliitto STUL ry\*  
Start-up säätiö\*  
Suomen Asianajajaliitto  
Suomen Internet-yhdistys\*  
Suomen Journalistiliitto  
Suomen Sadankomitea ry  
Teknologiateollisuus ry  
Teleforum ry\*  
Tieto- ja viestintätekniikan ammattilaiset TIVIA ry  
Tietoliikenteen ja tietotekniikan keskusliitto FiCom  
Tietoyhteiskunnan kehittämiskeskus ry TIEKE  
Viestinnän keskusliitto  
Maanpuolustuskouluyhdistys  
Kadettitoverikunta ry\*  
Maanpuolustuskiltojen liitto ry\*  
Maanpuolustusnaisten liitto ry\*  
Naisten Valmiusliitto ry\*  
Reserviläisliitto ry\*  
Sininen reservi ry\*  
Suomen Rauhanturvaajaliitto ry  
Suomen reserviupseeriliitto ry\*  
Maanpuolustuksen tuki ry\*  
Varusmiesliitto ry\*  
Julkisalan koulutettujen neuvottelujärjestö JUKO ry\*  
Palkansaajajärjestö Pardia ry  
Julkisten ja hyvinvointialojen liitto JHL ry\*  
Upseeriliitto\*  
Päällystöliitto ry\*  
Aliupseeriliitto ry\*  
Maanpuolustuksen henkilökuntaliitto MPHL ry\*  
Maanpuolustuksen teknisten toimihenkilöiden liitto MTTL ry\*  
Puolustusvoimien Diplomi-insinöörit ry



30.6.2015

FI.PLM.2015-3439  
909/40.02.00/2013

Lainvalmistelu- ja oikeusyksikkö

Maanpuolustuksen insinöörit MPI ry

Professori Martin Scheinin, European University Institute  
Apulaisprofessori Juha Lavapuro, Tampereen yliopisto  
Professori Tomi Voutilainen, Itä-Suomen yliopisto

Piraattipuolue r.p.  
IAMCP Finland

**Postiosoite**  
**Postadress**  
**Postal Address**  
Puolustusministeriö  
PL 31  
FI-00131 Helsinki  
Finland

**Käyntiosoite**  
**Besöksadress**  
**Office**  
Eteläinen Makasiinikatu 8  
00130 Helsinki  
Finland

**Puhelin**  
**Telefon**  
**Telephone**  
0295 16001  
Internat. +358 295 16001

**Faksi**  
**Fax**  
**Fax**  
(09) 160 88244  
Internat. +358 9 160 88244

**s-posti, internet**  
**e-post, internet**  
**e-mail, internet**  
kirjaamo@defmin.fi  
www.defmin.fi