Puolustusministeriö

kirjaamo@defmin.fi

Viite: Lausuntopyyntö tiedonhankintalakityöryhmän mietintöön, puolustusministeriö FI.PLM.2015-218; 909/40.02.00/2013

# Lausunto puolustusministeriölle tiedonhankintalakityöryhmän mietintöön

Tieto- ja viestintätekniikan ammattilaiset, TIVIA ry (entinen Tietotekniikan liitto ry), kiittää mahdollisuudesta kommentoida puolustusministeriön tiedonhankintalakityöryhmän mietintöä ”Suomalaisen tiedustelulainsäädännön suuntaviivoja”. Lausuntomme olemme valmistelleet yhteistyössä jäsenyhdistyksemme, HETKY ry:n kanssa.

Haluamme asiaan liittyen todeta seuraavaa:

## Yleistä

Mietinnössä on arvioitu kattavasti tiedonhankintaan liittyviä hyötyjä ja haittoja sekä tiedustelutoimintaa kokonaisuutena: sen luomia mahdollisuuksia parantaa yhteiskunnan turvallisuutta vaikuttamalla siihen kohdistuviin merkittäviin uhkiin. Tässä lausunnossa on esitetty yleisiä havaintoja ja joitakin ehdotuksia mietintöön ja sen tuloksiin - kehittämisehdotuksiin ja johtopäätöksiin - liittyen.

Jo mietinnön kuvailulehden tiivistelmässä on kattavasti todettu tiedusteluun liittyvät tarpeet ja ehdotus niiden toteuttamiseksi. On myös todettu, että tiedustelun, sen avulla saatavien tietojen keruun ja säilyttämisen sekä tietojen asianmukaisen ja oikeusperustainen käsittelyn takaamiseksi sekä lupamenettelyn että valvontajärjestelmän tulisi olla riippumaton. Tämä on olennainen seikka ja edellytys, jolla estetään valvontaviranomaisen mahdollisuus tarkkailla ja analysoida kohteita mielivaltaisesti.

Jotta tiedustelutoiminta saa kansalaisten keskuudessa hyväksynnän eikä tiedustelua tekevän viranomaisen toimintaan kohdistu aiheetonta epäluottamusta tai vastustusta, tiedustelutoiminnan raamien on oltava julkisia: yleisön täytyy olla tietoisia tiedustelun pääperiaatteista ja tietojen keruun syistä sekä siitä, mitä ja miten tietoja kerätään, miten niitä käsitellään ja miten käsittelystä tiedotetaan ainakin niille asianomaisille, joiden tietoja on aiheettomasti käsitelty. Tulisi selkeästi tuoda ilmi, että viranomaisen toiminta ei uhkaa (liike)toiminnallista ympäristöä "Suomi datan turvasatamana".

Julkisen ja avoimen keskustelun avulla tulisi panostaa kansalaisten ymmärryksen aikaansaamiseen siitä, että laki ei suinkaan lisää mahdollisuuksia viranomaisen mielivaltaan, vaan riippumattomat lupa- ja valvontamenettelyt päinvastoin vähentävät niitä. Se, että tiedustelulla ei välttämättä kyetä estämään terroritekoja, ei vähennä tiedustelun hyödyllisyyttä. Tietoisuus tiedustelusta saattaa vähentää motivaatiota terroritekoihin, ja joka tapauksessa tiedot auttavat tutkintaa ja voivat helpottaa vahinkojen minimointia ja palautumiskykyä.

Alla on esitetty vielä tarkennettuja huomioita.

### Tiedustelua suorittava viranomainen

Näyttäisi siltä, että puolustusvoimat olisi sopivin taho tietoliikennetiedustelua suorittavaksi viranomaiseksi olemassa olevan tehtävänsä ja asemansa, turvallisuuskulttuurinsa, osaamisensa sekä jo käytössä olevan laadukkaan teknisen toimintaympäristön osalta. Lainsäädännöllä tulisi varmistaa, että muut kansallisen turvallisuuden ylläpitämisessä toimivat viranomaiset, esimerkiksi suojelupoliisi ja keskusrikospoliisi, saavat tarvittavia valtuuksia. Toisaalta tarvittaessa myös muut viranomaiset, esimerkiksi terveydenhuollosta vastaavat viranomaiset ja lääketieteen asiantuntijat (biologisia tai epidemisiä vaikutuksia aiheuttava terroriteko) voivat toiminnassaan hyötyä tiedustelutiedosta (terroriteon maantieteellinen laajuus, käytetyt aineet ja niiden vaikutus ihmisiin, haitallisten vaikutusten torjunta ym.). Muiden viranomaisten pääsy täsmällisesti määriteltyyn tiedustelutietoon, mikäli tällaista ennalta määrätyssä tilanteessa tarvittaisiin, tulisi toteuttaa normaaleilla tai tiukennetuilla lupa- ja valvontamenettelyillä. Tiedusteluviranomaisen roolia ei tulisi luovuttaa muille viranomaisille, vaan pääsy yksityiskohtaisesti määriteltyyn dataan tulisi toteuttaa yksinomaan teknisin keinoin ja käyttämällä sovittuja pääsyn ja valtuuksien hallinnan menettelyitä.

### Vaikutus osaamiseen ja kyberturvallisuuden ammattitaitoon

TIVIA edustaa suurta määrää tietoteknisen alan ammattilaisia. Tulevaisuudessa ymmärtämyksen merkitys digitaalisisten palveluiden toteuttamisesta ja kyberympäristössä ylipäätään kasvanee voimakkaasti. Kyberturvallisuuden kehittämiseen ja ylläpitoon tähtäävä lainsäädäntö on tervetullutta ja suuntaus on oikea. On olennaisen tärkeää kehittää kokonaisvaltaista osaamista ja kattavia näkemyksiä, eikä keskittyä yhteen oljenkorteen. Tällä hetkellä pelialan on sanottu olevan "uusi Nokia". On oletettavaa, että peliala pelkästään ei kuitenkaan tarjoa riittäviä mahdollisuuksia työllistää satatuhatpäistä joukkoa tietoteknisen alan asiantuntijoita ja työntekijöitä. Viihteen lisäksi kattava joukko eri yhteiskunnan toimintoja on kyettävä toteuttamaan digitaalisesti, turvallisuuden silti vaarantumatta. On nähtävissä, että kyberturvallisuus voi toimialana olla yksi suomalaisen osaamisen ja teknologian kärkituotteita. Lainsäädännön ajantasaisuus pitää yllä Suomen kilpailukykyä toimialalla.

### Vaikutus kilpailukykyyn

Lain vaikutus Suomen kilpailukykyyn on oletettavasti positiivinen. Ei ole loogisesti perusteltavissa, että hyvin valvottu tiedustelutoiminta ja siinä käytettävien tietojen tehokas suojaaminen pienentäisi Suomen houkuttelevuutta esimerkiksi digitaalisten palveluiden tuottamisessa tarvittavien teknisten ympäristöjen (konesalikeskukset) kohteena. Päinvastoin, turvallinen ja laadukkaalla valvonnalla suojattu infrastruktuuri nostavat kynnystä kohdistaa kyberhyökkäyksiä Suomessa sijaitseviin palveluihin. On myös huomattava, että USA:an ja Isoon-Britanniaan on rakennettu huomattava määrä suurten kansainvälisten palvelutuottajien konesalitiloja, vaikka on ollut jo pitkään hyvin tiedossa, että kyseisissä maissa käytetään voimallista ja kattavaa tietoliikennetiedustelua. Se, että konesalitiloille etsitään nykyisin muita kohteita, ei johdu tiedustelusta, vaan siitä, että kyseisissä maissa on jo valtava määrä laskenta- ja tietoteknistä kapasiteettia ja lisäkapasiteettia tarvitaan esimerkiksi manner-Eurooppaan. Valtioiden vakauden, osaavan työvoiman sekä energia- ja ilmasto-olosuhteiden vuoksi myös Skandinavia on houkutteleva kohde. Toki, jos vaikkapa USA:ssa kapasiteetti loppuu, sitä lisätään kaupallisin perustein. Esimerkiksi Google on investoinut mittavan määrän rahaa merikaapeliin ja voimakkaaseen tietoliikennekapasiteetin nostamiseen USA:n ja Japanin välillä, tietäen hyvin, että kaikki kyseinen tietoliikenne altistuu USA:n (ja mahdollisesti Japanin) viranomaisen tarkkailulle. Kuten mietinnössä on todettu, Ruotsissa sen lainsäädännöstä (FRA-laki) tehty selvitys tukee kilpailua lisäävää olettamaa.

### Lainsäädäntö ja tekniset yksityiskohdat

Tulisi selvittää, onko valvontaa koskevat tekniset vaatimukset syytä säätää lailla, vai voisiko niistä säätää asetustasoisesti. Varsinaiset tiedustelutoiminnan suuntaviivat, perusteet ja määrittelyt (kohteiden valintaperusteet ja -periaatteet, tietojen keräämisen, käsittelyn, seulonnan, luokittelun, lajittelun sekä analysoinnin logiikka ja toimenpiteet) sekä tietojen elinkaareen ja poistamiseen liittyvät vaatimukset voitaisiin toteuttaa ministeriön asetuksena vastaavalla tavalla kuin on toteutettu esimerkiksi potilastietojen säilytyksen vaatimukset (298/2009, Sosiaali- ja terveysministeriön asetus potilasasiakirjoista, liitteineen).

On myös huomattava, että tekninen ympäristö voi muuttua hyvinkin nopeasti. Tällöin liian tarkat vaatimukset sille, miten tiedustelua voidaan teknisesti suorittaa, voisi olla syytä säätää asetuksella, ei lailla. Esimerkiksi mikäli tietoliikennetekniset ratkaisut kehittyisivät sellaisiksi, että päätelaitteet ja/tai verkkokomponentit kykenisivät keskustelemaan keskenään ilman runkoverkon käyttöä, ei tiedustelumahdollisuus pelkkiä runkoverkon yhteyspisteitä käyttämällä tuota mitään hyötyä. Esineiden internetistä, IoT:stä (Internet of Things), käydään jo runsaasti keskustelua. On oletettu, että lähimmän vuosikymmenen aikana verkko-osoitteiden määrä moninkertaistuu. Lähes kaikki teknologiset laitteet tulevat olemaan tavalla tai toisella verkkoon kytkettyjä tai verkottuneita. Ne välittävät verkossa erilaista informaatiota, olipa tuo verkkokytkentä suoraan internetiin tai jonkun muun tyyppiseen kommunikaatioalustaan. Olennaista on säätää lailla siitä, millaista tiedustelua sallitaan (esimerkiksi Suomesta ulkomaille kohdistuva viestiliikenne), ei niinkään siitä, miten tiedustelu teknisesti toteutetaan.

Yksi seikka, joka jää mietinnössä vähälle käsittelylle, on tiedusteluviranomaiselle annettava valtuutus kehittää ja asentaa tiedonhankintaan kykeneviä sovelluksia tai muita teknisiä komponentteja jonkun sellaisen (ulkomaisen) tahon tietojärjestelmiin tai -verkkoon, joka katsotaan yhteiskunnan toiminnalle vaaralliseksi. Tulisi vähintäänkin selvittää, voisiko tällaista tiedustelutoimintaa tehdä Suomesta ulkomaille kohdistuen. Tulisi myös selvittää, voisiko näin saatavaa tiedustelutietoa kerätä ja käyttää, mikäli ulkomaalainen kohde (esimerkiksi kannettava tietokone) tuodaankin Suomen maaperälle. Viimeaikainen julkisuuteen tullut tieto (esimerkiksi tapaus Snowden) osoittaa, että ainakin joidenkin maiden tiedusteluviranomaiset käyttävät kyseisiä keinoja tiedustelutietoa hankkiessaan. Tiedustelua saatetaan kohdistaa massakeruutyyppisesti jopa sellaisiin kohteisiin, joita ei ole etukäteen todettu erityistä uhkaa aiheuttaviksi.

Tulisi myös tarkemmin selvittää viranomaisen mahdollisuudet ja edellytykset soluttautua digitaalisia välineitä käyttämällä ja osallistumalla peitetoimintatyyppisesti haitallisiksi nähtyjen organisaatioiden tai ryhmittymien toimintaan. Tämän mahdollisuuden tulisi olla yksi olennainen osa digitaalista tiedustelua ja tiedonhankintaa, kun tietoverkkoja käytetään globaalisti yhä enenevässä määrin myös rikollisiin ja haitallisiin tarkoituksiin.

### Uhkien torjunta

Lainsäädännön tarkoituksena on kyetä varautumaan vakaviin yhteiskuntaan kohdistuviin uhkiin. On syytä todeta erikseen, että kyberuhat ovat olennainen osa uhkatekijöitä. Tietoliikennetiedustelun hyödyntäminen kyberuhkien torjunnassa, siis miten tiedustelutietoja voitaisiin käyttää hyväksi kyberturvallisuuden ylläpidossa, on jaettavissa ainakin kolmeen eri tyyppiin. Nämä uhkat tulisi siis huomioida osana muita yhteiskunnalle vakavia uhkia.

1. Yhteiskunnan elintärkeitä toimintoja tukevien tietoteknisten ratkaisuiden ja tietoverkkojen häirintä siten, että toiminnoille aiheutuu häirinnästä vakavaa uhkaa. Esimerkkinä mainittakoon kyberhyökkäys energia- tai vesihuollon tietojärjestelmiin.

2. Tietoverkkojen ja kyberympäristöjen käyttö sellaisessa rikollisessa toiminnassa tai terrorismissa, joka voi aikaansaada vakavia haittavaikutuksia yhteiskunnan tärkeisiin palveluihin tai talouteen. Esimerkkinä mainittakoon kyberhyökkäys ja tietojen tai rahan varastaminen jonkin pankin tai viranomaisen järjestelmästä. Toinen esimerkki on yhteiskunnallisesti pahennusta aiheuttavan rikollisen toiminnan pyörittäminen, esimerkiksi ihmis- tai huumekauppa tai lapsiporno.

3. Jonkun toisen valtion tai muun tahon suorittama Suomeen kohdistuva vakoilu tai tiedustelu, jonka toteuttamisessa joko salakuunnellaan Suomessa olevia tietojärjestelmiä tai -liikennettä tai suomalaisia tietoliikenneverkkoja käytetään tietojen välittämiseen Suomen ulkopuolelle.

Uhkien torjuntakyky voi parantua myös havainnointikyvyn lisäämisellä siten, että vaikka uhkaa ei sinällään voitaisi etukäteen torjua ja vaikka vahingollinen tapahtuma jopa toteutuisi, käytettävissä olevaa tietoa voitaisiin hyödyntää sekä haittavaikutusten minimoinnissa, toipumisessa sekä jälkikäteen tehtävässä tutkinnassa. Näillä seikoilla voi myös olla merkittävä tekijän motivaatiota pienentävä vaikutus. Tästä ei tosin välttämättä ole selkeää tutkimustietoa tiedustelun osalta, mutta ihmisen käyttäytymisen tutkimus esimerkiksi liikennevalvonnan osalta osoittaa, että sääntöjen vastainen toiminta saattaa vähentyä, kun valvonnasta ollaan tietoisia (vrt. ylinopeuskamerat).

### Suojamekanismit ja tietoturva

Jotta luottamus tiedustelutoimintaan sekä sen riippumattomuuteen, laadukkuuteen ja puolueettomuuteen säilyisi, tulisi toteuttaa sellaiset tekniset suojamekanismit, että viranomaiselle tiedustelutarkoitusta varten tallennetut tiedot eivät vaarannu tai altistu sisäisille tietoturvauhkille (esimerkiksi teknisten ongelmien tai inhimillisten vahinkojen aiheuttamat vaikutukset), ulkoisille tietoturvauhkille (esimerkiksi tietojärjestelmään kohdistuvat tekniset hyökkäykset, tietoliikenteen salakuuntelu tms.) tai vastatiedustelulle (esimerkiksi viranomaisen toimintaan soluttautunut ulkopuolinen taho tai tekninen salakuuntelu). Kyseinen viranomaisen tietojärjestelmä, johon tiedustelutieto tallennetaan, järjestelmän operoinnissa ja kommunikoinnissa käytettävät tietoverkot ja kaikki tietojen käsittelyprosessit on suojattava korkeimman suojaustason mukaisesti. Tulisi myös pitäytyä luovuttamasta tietoja kyseisestä järjestelmästä muille viranomaisille tai tahoille (pois lukien mahdollinen yhteistyö kansainvälisten tiedusteluorganisaatioiden kanssa). Mikäli joku muu viranomainen tarvitsisi jotakin spesifistä tietoa järjestelmästä tiettyyn ennalta hyväksyttyyn tarkoitukseen, tämä pääsy tulisi toteuttaa asianmukaisesti tiukennetun lupa- ja valvontamenettelyn jälkeen yksittäisen pääsyoikeuden myöntämisellä, ja ainoastaan tiedusteluviranomaisen tiloista ja jatkuvassa valvonnassa.

### Kansalaismielipide

Mietinnössä on jäänyt vähälle käsittelylle jo pelkästään selvitystyön - saati sitten lainvalmistelutyön ja lain eduskuntakäsittelyn - vaikutus julkiseen mielipiteeseen sekä mahdollisen lain valmistelun ja hyväksynnän saama voimakaskin vastarinta. Näihin voitaisiin vaikuttaa etukäteen tuomalla paremmin esiin lain positiiviset vaikutukset ja kuinka mahdolliset (vaikka eivät olisikaan todennäköisiä) negatiiviset vaikutukset, toisin sanoen lain tuomat uhkat, voidaan minimoida.

Tiedotusvälineissä on tyypillisesti käsitelty asiaa orwellilaisena isoveli valvoo -menettelynä ja urkintalainsäädäntönä, jossa viranomainen aiheuttaisi toiminnallaan vakavia uhkia kansalaisille ja heidän yksityisyytensä suojalle. Näkemys ei ole realistinen. On todettava, että tiedonhankintahan ei edellyttäisi merkittäviä teknisiä muutoksia olemassa oleviin teknologisiin ratkaisuihin, joilla tietojärjestelmät ja tietoverkot on nykyisellään toteutettu. On syytä ymmärtää, että yksityiselläkin taholla, esimerkiksi tele- tai verkko-operaattorilla, on jo nyt tekninen mahdollisuus kuunnella, tallentaa tai puuttua tietoliikenteeseen, sen laitteillahan tietoliikennettä välitetään. Isoveli valvoo -tyyppiset väärinkäytökset olisivat siis teknisesti täysin mahdollisia jo nyt eikä tekninen uhka lisääntyisi lain myötä. Uutta viranomaista ei oltaisi luomassa, vaan tiedustelu olisi yksi osa jo toimivan turvallisuusviranomaisen vastuita. Tästä syystä viranomaisen tekemien väärinkäytösten motiivikaan ei muuttuisi - jos tuollainen motiivi olisi olemassa, väärinkäytökset olisivat viranomaisen teknisesti toteutettavissa jo nykyisin. Laki ei siis lisää viranomaistoiminnan aiheuttaman mielivallan uhkaa eikä sen todennäköisyyttä - ei motiivia eikä teknistä mahdollisuutta. Päinvastoin: oikein luvitettuna, valvottuna ja suojattuna tietojen väärinkäytösmahdollisuus pienenisi nykyisestä.

Edelliset seikat huomioiden olisi syytä julkisesti käsitellä ja pyrkiä mitätöimään ne uhkakuvat ja pelot, joita mediassa on aikaansaatu ja mitä tietyt toimijat tarkoituksellisesti ylläpitävät lietsoen yleistä mielipidettä lakia vastustavaksi. Tiedonhankintalakihan määrittäisi tiedustelutoiminnalle riippumattomat lupa- ja valvontamenettelyt vastuineen ja väärinkäytössanktioineen. Viranomainen ei siis saisi käytännössä merkittäviä uusia teknisiä toimintamahdollisuuksia, mutta kuka lain määrittämä tiedusteluviranomainen olisikin, sen toimintaa valvottaisiin ja siihen voitaisiin puuttua olennaisesti nykyistä paremmin. Siksi laki päinvastoin pienentäisi, ei lisäisi, mahdollisuuksia isoveli valvoo -yhteiskunnan kehittymiselle.

Kunnioittaen

Tieto- ja viestintätekniikan ammattilaiset TIVIA ry HETKY ry

Robert Serén Tero Tammisalo

toiminnanjohtaja johtokunnan jäsen