Liikenne- ja viestintävaliokunta
LiV@eduskunta.fi

Liikenne- ja viestintäministeriön kirjallinen asiantuntijalausunto (HE 202/2017 vp, HE 203/2017 vp)

Liikenne- ja viestintävaliokunta on kuullut asiantuntijoita siviili- ja sotilastiedustelua koskevista hallituksen esityksistä (HE 202/2017 ja HE 203/2017).

Asiantuntijalausunto on saatu liikenne- ja viestintäministeriön lisäksi seuraavilta tahoilta: puolustusministeriö, sisäministeriö, oikeusministeriö, valtioneuvoston kanslia, sisäministeriön rajavartio-osasto, Suojelupoliisi, Viestintävirasto, Teknologian tutkimuskeskus VTT Oy, prof. Martti Lehto (Jyväskylän yliopisto), prof. Tuomas Ojanen (Helsingin yliopisto), Google, Electronic Frontier Finland – Effi ry, FICIX ry, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, F-Secure Oyj, Suomen Erillisverkot Oy, DNA Oyj, Elisa Oyj, Telia Finland oyj, Tietosuojavaltuutetun toimisto, Elinkeinoelämän Keskusliitto EK sekä CSC-Tieteen tietotekniikan keskus Oy.

Liikenne- ja viestintäministeriö on aiemmin liikenne- ja viestintävaliokunnalle toimittamassaan lausunnossa tuonut esille ministeriön näkemyksiä ehdotuksista tiedustelua koskevaksi lainsäädännöksi. Liikenne- ja viestintäministeriö esittää seuraavassa huomionsa liikenne- ja viestintävaliokunnan saamista asiantuntijalausunnoista siltä osin kuin niillä on liityntä perustuslaissa suojattuun luottamuksellisen viestin salaisuuden suojaan taikka muutoin liikenne- ja viestintäministeriön hallinnonalalle.

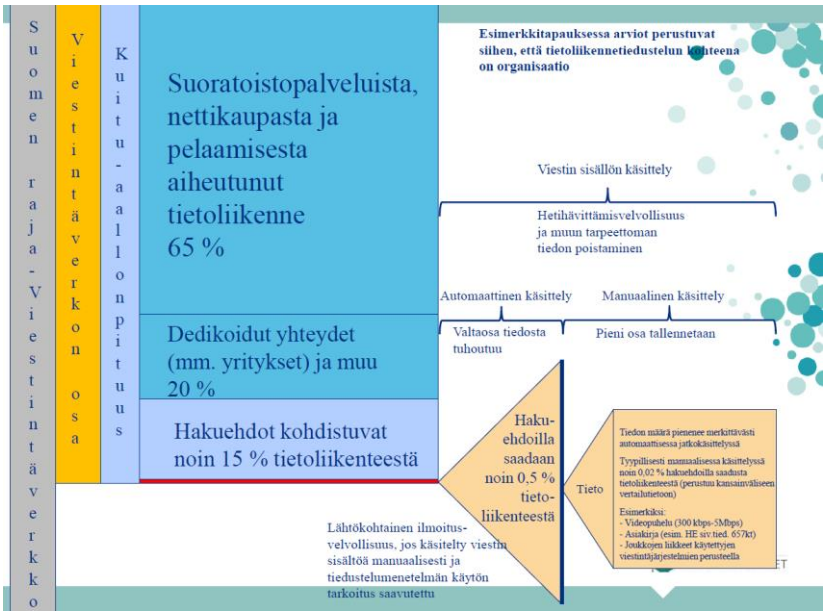
Tietoliikennetiedustelun kohdentaminen

Liikenne- ja viestintäministeriö on valiokunnalle aiemmin toimittamassaan lausunnossa tuonut esille, että ”*tietoliikennetiedustelusta on tekniseltä toteuttamistavaltaan sen kaltaista, että sen puitteissa tiedusteluviranomainen voisi saada teknisen mahdollisuuden seuloa myös hyvin monen suomalaisen luottamuksellista viestintää. Tämän vuoksi on erityisen tärkeää huolehtia riittävästä perusoikeuksien suojasta.”*

Myös useassa valiokunnalle toimitetuissa asiantuntijalausunnoissa on kiinnitetty huomiota tietoliikenne tiedustelun kohdentamiseen liittyviin kysymyksiin (Google, Tietosuojavaltuutettu, CSC-Tieteen tietotekniikan keskus Oy, Electronic Frontier Finland – Effi ry, Teknologian tutkimuskeskus VTT Oy, Prof. Ojanen).

Tietosuojavaltuutettu on lausunnossaan katsonut, että lainvalmistelun yhteydessä olisi varmistuttava siitä, että ”*toimivaltaisten viranomaisten kytkeytyessä viestintäverkkoon se tapahtuu tavalla, joka ei johda massavalvontaan.”* VTT:n lausunnon mukaan ”*voidakseen toteuttaa lakiin asetetut mahdollisuudet kerätä ja analysoida liikennettä erilaisin hakutermein ja erilaisista kanavista, täytyy luoda tekniset edellytykset valvoa kaikkea liikennettä kaikissa solmukohdissa.*” Google on lausunnossaan todennut huolensa siitä, että ”*lainkohdat sellaisena kuin ne nyt on ilmaistu, voitaisiin tulkita laajentavasti siten, että tulkinta mahdollistaisi tietojen massakeräämisen ja -tiedustelun*.” CSC:n lausunnossa on katsottu mm., että ” *lakiesityksissä ehdotettu malli mahdollistaa teknisellä tasolla kaiken, myös Suomen sisäisen, liikenteen erottelun ja analysoimisen* ” sekä että ”*tiedusteluun liittyvien hakujen kohdentamisessa tulisi hyödyntää ehdotettua tarkempaa rajausta tai rajatumpaa tekniikkaa, sillä mitä epämääräisempää tai laajempia hakutermejä tiedonhankinnassa käytetään, sitä enemmän liikennettä suodattuu jatkokäsittelyyn.”* Effi ry. on lausunnossaan katsonut, että myös julkisesti olisi pystyttävä arvioimaan, onko tiedustelu laajentunut massavalvonnan suuntaan julkaisemalla tietoja esimerkiksi ” *verkkotiedustelun osalta kuinka laajoihin henkilöryhmiin, kuinka isoon verkkoalueeseen ja data- ja viestimääriin myönnetyt tiedusteluluvat ja toisaalta toteutetut tiedustelutoimenpiteet ovat kohdistuneet.*” Prof. Tuomas Ojanen on todennut lausunnossaan, että tiedustelua koskevassa lainsäädännössä olisi syytä säätää tietoliikennetiedustelua koskien ”*tietoliikenteen yleisen, kohdentamattoman ja kaiken kattavan seurannan kiellosta tiedustelutoiminnassa.”*

Muun muassa sisäministeriö ja puolustusministeriö ovat valiokunnalle toimittamissaan lausunnoissa kuvailleet tietoliikennetiedustelun kohdentamisen edellytyksiä. Esimerkiksi sisäministeriö on esittänyt tietoliikennetiedustelun kohdentumista tietoliikenteeseen alla olevan kuvan mukaisesti:



Liikenne- ja viestintäministeriö pitää hyvänä sitä, että tietoliikennetiedustelun kohdentumista tietoliikenteeseen on hallituksen esityksissä sekä asiantuntijalausunnoissa tarkentavasti kuvattu. Teknisen toteuttamistavan tuloksellisuudesta ja kohdentumisen oikeasuhtaisuudesta jää kuitenkin edelleen avoimia kysymyksiä.

Yllä olevan kuvan perusteella syntyy käsitys, että hakuehtoja kohdennettaisiin tietoliikennetiedustelun kohteena (kuten esim. tietyn kuidun tietyssä aallonpituudessa kulkeva tietoliikenne) olevasta tietoliikenteestä käytännössä kaikkeen siihen liikenteeseen, joka voisi sisältää luottamuksellista viestintää (suodatuksen ulkopuolella jäisi viestinnän luottamuksellisuuden kannalta vähemmän merkityksellinen liikenne sisältäen esim. suoratoistopalveluista, nettikaupasta ja pelaamisesta yms. aiheutuneen liikenteen sekä ”dedikoidut yhteydet”). Tässä verkon osassa seulonta näyttäisi kohdistuvan siis kaikkien henkilöiden luottamukselliseen viestintään.

Kuvan perusteella jää myös epäselväksi, kuinka tiedusteluviranomaiset taikka esimerkiksi tuomioistuin kykenee arvioimaan, kuinka suuri osa luottamuksellista viestintää sisältävästä tietoliikenteestä suodattuisi tiedusteluviranomaiselle tarkemmin analysoitavaksi lupahakemuksessa esitettyjen hakuehtojen perustella. Tämä on kuitenkin keskeistä tiedustelutoiminnan tuloksellisuuden ja oikeasuhtaisuuden kannalta. Mitä enemmän tietoa hakuehtojen perustella suodattuu, sitä suuremmalla todennäköisyydellä mukaan päätyy myös tiedustelun kohteena olevan uhan kannalta sivullisten henkilöiden luottamuksellista viestintää. Yllä esitetystä kuvasta ei käy myöskään ilmi, miten kuvan mukaisesta kohdentumisesta on laintasolla säädetty.

Tiedustelutoiminnan tehokkuus ja tuloksellisuus voivat mahdollisesti myös heiketä, mikäli viranomaisille kertyy enemmän tietoa, kuin resurssien puitteissa on mahdollista analysoida. Tietoverkoissamme kulkee valtavia määriä tietoliikennettä. Tämän johdosta vain 0,5 % kuidun aallonpituuden tietoliikenteestä saattaa jo tarkoittaa suurtakin tietomassaa.

Liikenne- ja viestintäministeriö on aiemmin valiokunnalle toimittamassaan lausunnossa todennut, että ”*perusoikeussuojan toteutumisen kannalta laissa on keskeistä säätää riittävistä vaatimuksista tiedustelun kohdentamiselle sekä tiedustelumenetelmällä kerätyn luottamuksellisen viestin salaisuuden suojan alaisen tiedon käsittelylle. Lisäksi on huolehdittava siitä, että tiedustelu voidaan tosiasiassa teknisesti toteuttaa laissa säädettyjen perusoikeuksia suojaavien vaatimusten mukaisesti*.” Liikenne- ja viestintäministeriö pitää tiedustelulakien säätämisen edellytyksenä sitä, ettei tiedustelulainsäädännön perusteella ole mahdollista harjoittaa tietoliikenteen yleistä, kohdentamatonta ja kaiken kattavaa seurantaa. Liikenne- ja viestintäministeriö pitää myös tärkeänä, että sähköiseen viestintään kohdistuvien viestintämenetelmien oikeasuhtaista kohdentamista pystytään tehokkaasti ja läpinäkyvästi valvomaan sekä etu- että jälkikäteisesti.

Tiedon luovuttaminen muille toimijoille

Lausunnoissa on nostettu esiin myös huoli tiedusteluviranomaisten oikeudesta luovuttaa tiedustelumenetelmin kerättyä tietoa muille toimijoille sekä siitä, että tästä säädettäisiin henkilötietojen käsittelyä koskevassa lainsäädännössä, jota ei ole vielä annettu.

Liikenne- ja viestintäministeriö katsoo, että tiedusteluviranomaisten tietojen käsittelyä koskevan lainsäädännön käsittelyssä on keskeistä arvioida henkilötietojen käsittelyn suojatoimia ja henkilötietojen luovuttamista koskevan sääntelyn merkitystä luottamuksellisen viestin salaisuuden suojalle erityisesti silloin, kuin henkilötiedot voivat sisältää sähköisen viestinnän luottamuksellisuuden kannalta merkityksellisiä tietoja (kuten viestinnän sisältöä taikka sähköisen viestinnän välitystietoja). On tärkeää varmistaa, että tiedustelumenetelmin kerättyjä tietoja käsitellään (myös niiden tahojen osalta, joille tietoja luovutetaan) turvallisesti ja huolellisesti sekä hyväksyttäviin tarkoituksiin.

Sähköisen viestinnän välitystietojen säilytysvelvollisuus

Prof. Tuomas Ojanen on lausunnossaan kiinnittänyt huomiota sähköisen viestinnän välitystietojen säilytysvelvollisuuteen ja viranomaisten pääsyä näihin tietoihin koskevaan Euroopan Unionin tuomioistuimen oikeuskäytäntöön (*Digital Rights Ireland, Tele2 ja Watson*). Ojanen toteaa lausunnossaan seuraavaa:

> *Käsillä olevissa hallituksen esityksissä olisi tarkoitus sallia tiedustelu, joka kohdistuu sellaiseenkin toimintaan, joka käytännön toimenpiteisiin edetessään olisi rikos, mutta johon ei vielä voida kohdistaa konkreettista ja yksilöityä rikosepäilyä. Samoin tiedustelun kohteena voisi olla toiminta, joka ei lähtökohtaisesti ole Suomen lain mukaan rikos tai joka ei edetessäänkään voisi kehittyä rikokseksi, kuten ulkomaisten tiedustelupalvelujen laillinen toiminta Suomessa. Näistä syistä asioissa Tele2 ja Watson annetussa ratkaisussa on myös huomionarvoista se linjaus, jonka mukaan toimivaltaisille kansallisille viranomaisille annettava oikeus saada tilaajien tai rekisteröityjen käyttäjien tietoja ”voidaan lähtökohtaisesti myöntää rikollisuuden torjumisen tavoitteen yhteydessä vain sellaisten henkilöiden tietoihin, joiden epäillään suunnittelevan, tekevän tai tehneen vakavan rikoksen tai olevan jollakin tavalla mukana tällaisessa rikoksessa.” (kohta 119). Tämän jälkeen EU-tuomioistuin kuitenkin toteaa, että ”(e)rityisissä tilanteissa, kuten niissä, joissa kansallisen turvallisuuden, maanpuolustuksen tai yleisen turvallisuuden elintärkeitä intressejä uhkaa terrorismi, oikeus saada muiden henkilöiden tietoja voidaan kuitenkin myöntää myös, jos olemassa on objektiivisia seikkoja, joiden perusteella voidaan katsoa, että näillä tiedoilla voidaan konkreettisessa tapauksessa tosiasiallisesti myötävaikuttaa tällaisen toiminnan torjumiseen.” (kohta 119) Näin ollen on EU-oikeus sallii sen, että viranomaisilla on oikeus tietyin edellytyksin oikeus saada tilaajien tai rekisteröityjen käyttäjien tietoja myös tilanteissa, johon ei vielä voida kohdistaa konkreettista ja yksilöityä rikosepäilyä, jos on ”olemassa on objektiivisia seikkoja, joiden perusteella voidaan katsoa, että näillä tiedoilla voidaan konkreettisessa tapauksessa tosiasiallisesti myötävaikuttaa tällaisen toiminnan torjumiseen”.*

Liikenne- ja viestintäministeriö huomauttaa, että kansallisesti teleyritysten velvollisuudesta säilyttää eräitä sähköisen viestinnän välitystietoja viranomaistarkoituksiin on säädetty sähköisen viestinnän palveluista annetussa laissa (157 §). Lain mukaan säilytettäviä tietoja saa käyttää ainoastaan pakkokeinolain (806/2011) 10 luvun 6 §:n 2 momentissa tarkoitettujen rikosten selvittämiseksi ja syyteharkintaan saattamiseksi. Liikenne- ja viestintäministeriö asettama työryhmä on arvioinut kansallista lainsäädäntöä. Työryhmän tehtävänä oli antaa kattava selvitys: 1) välitystietojen säilytysvelvollisuutta ja viranomaisten pääsyä tietoihin koskevan lainsäädännön nykytilasta, 2) viranomaisten tarpeista saada sähköisen viestinnän tietoja vakavan rikollisuuden torjumiseksi, 3) toimintaympäristön muutoksen aiheuttamista vaikutuksista sähköisen viestinnän palveluihin, 4) viestinnän välitystietojen säilyttämisen nykykäytännöistä, sekä

5) viestinnän luottamuksellisuuden, yksityisyyden suojan ja muiden asiaan liittyvien perusoikeuksien sisällöstä ja reunaehdoista. Työryhmä ei havainnut välittömiä tietoyhteiskuntakaaressa säädettyä säilytysvelvollisuutta koskevia muutostarpeita (Selvitys sähköisen viestinnän välitystietojen säilytysvelvollisuudesta, liikenne- ja viestintäministeriön raportit ja selvitykset 9/2017, http://julkaisut.valtioneuvosto.fi/handle/10024/80111).

Sotilastiedustelua (100 §) sekä siviilitiedustelua (53 §) koskevissa ehdotuksissa säädetään sähköisen viestinnän palveluista annetun lain 157 §:ssä tarkoitettujen tietojen käyttämisestä tietojen hankkimiseksi sotilas- ja siviilitiedustelun kohteena olevasta toiminnasta. ***Liikenne- ja viestintäministeriö huomauttaa, että hallituksen esityksissä ei ole arvioitu näiden säännösten EU-oikeuden mukaisuutta ottaen huomioon erityisesti Tele2 ja Watson -tapauksen mukaiset edellytykset sähköisen viestinnän välitystietojen säilytykselle ja viranomaisten pääsyyn näihin tietoihin.***

Teleyritysten korvaukset

EK, FiCom ry, FICIX ry sekä teleyritykset ovat lausunnoissaan katsoneet, että yrityksille tulisi olla aina oikeus täysimääräiseen korvaukseen viranomaisten avustamisesta aiheutuneista kustannuksista. FiCom ry ja teleyritykset ovat tämän osalta katsoneet, että tietoyhteiskuntakaaren teleyritysten kustannusten korvaamista koskevaa lainsäädäntöä tulisi muuttaa.

Liikenne- ja viestintäministeriö toteaa, että sähköisen viestinnän palveluista annetun lain mukaista sääntelyä teleyritysten kustannusten korvaamisesta on kattavasti arvioitu lain antamisen yhteydessä (HE 221/2013 vp). Liikenne- ja viestintäministeriö katsoo, ettei tiedustelua koskevassa lainsäädännössä tulisi säätää teleyrityksille tai muille yrityksille ei-korvattavia velvoitteita, joiden toteuttamisesta voisi syntyä kohtuuttomia tai arvaamattomia kustannuksia.

Tietoturvallisuudesta huolehtiminen

Useissa liikenne- ja viestintävaliokunnalle toimitetuissa lausunnoissa on kiinnitetty huomiota siihen, ettei lakiehdotukset velvoita yrityksiä heikentämään tuotteiden ja palveluiden luotettavuuden tasoa esimerkiksi luovuttamalla salausavaimia, asentamalla salaamisteknologian takaovia tai rajoittamalla salaustuotteiden käyttöä. FiCom ja eräät teleyritykset ovat korostaneet, ettei tiedustelutoiminnalla tule vaarantaa viestintäverkkojen ja -palveluiden laatua tai häiriöttömyyttä.

Liikenne- ja viestintäministeriö pitää tärkeänä, ettei tiedustelutoiminnalla heikennetä sähköisten viestintäpalvelujen laatua, turvallisuutta tai saatavuutta. Tietoturvallisuuden kasvattamisen kannalta on myös keskeistä, että digitaalisten palveluiden käyttäjillä on saatavilla tarpeidensa mukaisia viestinnän salaus- ja suojausteknologioita ja näitä hyödyntäviä palveluita. Tämän takaamiseksi on tärkeää, ettei yrityksiä velvoiteta heikentämään tuotteidensa tietoturvallisuutta esimerkiksi rajoittamalla salaustuotteiden käyttöä taikka vaatimalla takaportteja salaamisteknologioihin.

Olisi tärkeää myös vaikuttaa kansainvälisellä ja EU-tasolla niin, ettei tällaisiin toimenpiteisiin jatkossakaan ryhdyttäisi.

Lisäksi lausunnoissa on nostettu esille tiedustelutoiminnan merkitystä kyberturvallisuuden edistämiseksi. Tiedustelutoimivaltuudet eivät kuitenkaan yksinään kykene turvaamaan digitaalisen yhteiskunnan korkeatasoista luotettavuutta. Tietoturvallisuuden kasvattamiseksi voidaan ryhtyä useisiin erilaisiin toimenpiteisiin, joita on kuvattu liikenne- ja viestintäministerin antamassa kansallisessa tietoturvastrategiassa (http://julkaisut.valtioneuvosto.fi/handle/10024/78106).

Yhteiskunnan kyberturvallisuuden johdonmukaiseksi kasvattamiseksi on tärkeää, että viranomaiset auttavat yrityksiä tietoturvallisuuden kasvattamisessa. Useat yhteiskunnan toiminnan kannalta keskeiset palvelut ovat yritysten tuottamia. Viestintäviraston tehtäviin kuuluu kerätä ja jakaa tietoa tietoturvaloukkauksista sekä niiden uhkista. Virasto saa valtaosan näistä tiedoista vapaaehtoisina ilmoituksina ja tiedon vaihtaminen perustuu molemminpuoliseen hyötyyn sekä luottamukseen. Lisäksi Viestintävirasto tiedottaa myös tietoturvauhkista ja ohjelmistohaavoittuvuuksista sekä avustaa kansalaisia ja yrityksiä tietoturvallisuuden kasvattamisessa esimerkiksi julkaisemalla varoituksia ja ohjeistusta tietoturvauhkiin varautumiseksi. Kyberturvallisuuskeskuksen toiminnalla on ollut erittäin keskeinen rooli siinä, että useissa kansainvälisissä haittaohjelmatapauksissa ja palvelunestohyökkäyksissä haitallisia vaikutuksia ollaan Suomessa pystytty tehokkaasti rajoittamaan. **Viestintäviraston Kyberturvallisuuskeskuksella onkin keskeinen asema koko yhteiskunnan tietoturvallisuuden varmistamisessa.**

Maija Rönkä
Ylitarkastaja