CSC-Tieteen tietotekniikan keskus Oy

Lausunto 20.03.2018
Eduskunnan liikenne- ja viestintävaliokunta
Asia: HE 202/2017 ja HE 203/2017

Lausunto hallituksen esityksiin koskien siviili- ja sotilastiedustelulainsäädäntöä

CSC – Tieteen tietotekniikan keskus Oy (CSC) kiittää mahdollisuudesta saada lausua ehdotuksista siviili- ja sotilastiedustelua koskeviksi lainsäädännöksi. CSC on suomalainen ICT-osaamiskeskus, joka ylläpitää opetus ja kulttuuriministeriön toimeksiannosta korkeakoulujen valtakunnallista keskitettyä tietotekniikkainfrastruktuuria, ja tarjoaa sen avulla kansallisia tietotekniikkapalveluita tutkimuksen, koulutuksen, kulttuurin ja julkishallinnon tarpeisiin. CSC ylläpitää korkeakoulujen ja tutkimuksen tietoverkko Funetia. CSC:n aiemmat lausunnot siviili- ja sotilastiedustelulainsäädäntöä koskien löytyvät www-sivuiltamme[1].

Tietoliikenneoperaattorina sekä IT-palveluiden toimittajana CSC korostaa lausunnossaan seikkoja, joilla katsoo olevan merkitystä erityisesti tietoliikennetiedustelun toteuttamisessa. Jatkovalmistelussa CSC pyytää kiinnittämään huomiota seuraaviin näkökohtiin:

1) Luottamusta suomalaisiin IT-palvelutuottajiin tai yritysten palveluiden yleistä saatavuutta ei saa lainsäädännöllä heikentää.

2) Toimijoiden vastuita, velvollisuuksia ja rooleja tiedustelun toteuttamisessa tulee selkiyttää.

3) Tuloksellinen ja tehokas tiedustelu sekä sen riippumaton valvonta edellyttävät korkeaa teknistä osaamista.

4) Tiedustelun kohdentamisen haasteet on huomioitava lainsäädännön jatkovalmistelussa.

[1] https://www.csc.fi/-/siviilitiedustelulainsaadanto
https://www.csc.fi/-/sotilastiedustelulainsaadanto

1 Tiedon luottamuksellisuuden turvaaminen

CSC pitää tiedustelua koskevan lainsäädännön kehittämistä ja selkiyttämistä erittäin tärkeänä. Tuleva lainsäädäntö ei kuitenkaan saa vaarantaa kotimaisten eikä kansainvälisten toimijoiden luottamusta suomalaisten IT-palvelutuottajien kykyyn taata asiakkaidensa tietojen luottamuksellisuus ja tietoturva, sillä tiedon luottamuksellisuus liittyy vahvasti elinkeinoelämän kilpailukykyyn ja kansainvälisten investointien suuntautumiseen Suomeen. Tiedustelutoimenpiteet eivät myöskään saa heikentää yritysten palveluiden yleistä saatavuutta. Lakiehdotusten nykyisissä muodoissa riittävän uskottavat ja läpinäkyvät turvallisuuskontrollit eivät valitettavasti toteudu ja näin ollen lain toimeenpanoa tulee tämän osalta selkiyttää.

Esitysten tietoyhteiskuntavaikutusten arvioinneissa todetaan, että tiedusteluviranomaisille ei olla myöntämässä oikeutta velvoittaa yrityksiä salausavaimien luovuttamiseen. Tämä on erittäin tärkeää, koska salausavaimien luovuttamisvelvollisuudella olisi haitallisia vaikutuksia Suomen kilpailukyvylle ja suomalaisten yritysten toiminnalle.

Lisäksi luottamuksen takaamiseksi jatkovalmistelussa tulee yhtä lailla varmistaa, ettei yritysten luottamuksellisia tietoja saa tiedustelutoiminnan varjolla luovuttaa henkilöille, joilla ei lain mukaan ole yksilöityä oikeutta tietoihin, eikä myöskään kolmansille osapuolille tai muille valtiolle.

2 Vastuiden, velvollisuuksien ja roolien selkiyttäminen

CSC toteaa, että tiedustelulainsäädännön jatkovalmistelussa tulee kiinnittää huomioita eri toimijoiden välisiin rooleihin ja velvollisuuksiin sekä pyrkiä selkeyteen ja yksiselitteisyyteen. Kiirehtimisen sijaan valmistelussa tulee tehdä sisällöllisesti huolellista työtä, jotta tulevasta lainsäädännöstä on todellista hyötyä kansalliselle turvallisuudelle.

Selkeä tiedustelulainsäädäntö on tärkeä myös yrityksille, ja tarkasti määritellyt velvoitteet takaavat viranomaisyhteistyön toimivuuden. Lainsäädännössä on selkeästi rajattava, mitä toimia yritys on velvollinen tekemään osana tiedusteluviranomaisten avustamista. Lisäksi tiedusteluviranomaisten avustamisesta syntyviä yritysvaikutuksia tulee arvioida jatkovalmistelussa kokonaisvaltaisesti sisältäen yksityiskohtaista arviointia esimerkiksi yrityksissä tarvittavan uuden osaamisen ja tekniikan vaatimista lisäresursointitarpeista.

Vastuun yrityksen palvelutuotantoon vaikuttavista tiedustelutoimenpiteistä tulee olla yrityksen johdolla, kuten toimitusjohtajalla tai turvallisuusjohtajalla. Vastuuttamisen pitää tapahtua kirjallisessa muodossa salassapitovelvoitteet huomioiden. Tiedustelutoimintaan kuuluvien toimenpiteiden teettäminen yksittäisellä työntekijällä olisi laillisuusperiaatteiden vastaista ja aiheuttaisi yrityksen toimintaan merkittäviä häiriöitä, kuten ongelmia työntekijäresurssien allokoinnissa ja työnjohtovelvollisuuden toteuttamisessa.

Molemmissa lakiesityksissä oltaisiin antamassa viranomaisille oikeus teknisen laitteen, menetelmän tai ohjelmiston asentamiseksi, käyttöön ottamiseksi ja poistamiseksi salaa mennä

erilaisiin kohteisiin tai tietojärjestelmiin sekä kiertää, purkaa tai muulla vastaavalla tavalla tilapäisesti ohittaa kohteen tai tietojärjestelmän suojaus tai haitata sitä. CSC:n näkemyksen mukaan puolustusvoimien tai turvallisuusviranomaisten henkilöstöllä ei missään olosuhteissa tule olla oikeutta omatoimisesti manipuloida yritysten palvelutuotantoon liittyvää tietoliikennettä tai tietojärjestelmiä, vaan mahdollisesta seurannasta ja muutoksista tulee aina sopia yrityksen johdon kanssa etukäteen laillisin perustein. Yleensäkin viranomaisten ja yritysten yhteistyö on CSC:n mielestä paras lähtökohta onnistuneelle tiedustelutoiminnalle.

Lisäksi jatkovalmistelussa tulee pohtia yritysten henkilöstön vastuu- ja oikeusturvanäkökulmaa avunantotapauksissa. Mikä on yritysten henkilöstön oikeudellinen vastuu esimerkiksi tapauksissa, joissa joudutaan avaamaan asiakkaiden luottamuksellista tietoliikennettä?

3 Korkean teknisen osaamisen vaatimus

CSC katsoo, että tiedustelutoiminnassa tulee varmistaa tiedusteluviranomaisten riittävän korkea tekninen osaaminen, jotta tiedustelun avulla todella saadaan kansallisen turvallisuuden kannalta oleellista ja hyödyllistä tietoa. Tietoliikennetiedustelun onnistuminen vaatii teknisen toteutustavan yksityiskohtien tarkastelua sekä vaihtoehtoisten toteutustapojen vertailua turvallisuus-, tietosuoja- ja luottamuksellisuusnäkökohdat huomioiden.

Toisaalta ainoastaan teknistä tiedustelutoimintaa toteuttavien viranomaisten osaamisen varmistaminen ei ole riittävää, vaan huomiota tulee kiinnittää myös tuomioistuinten sekä tiedustelutoimintaa valvovien tahojen tekniseen osaamiseen. Tämä on tärkeää, jotta valvovat tahot pystyvät riippumattomasti, uskottavasti ja tosiasiallisesti arvioimaan viranomaisten tiedustelutoiminnan suhteellisuutta sekä lupapyyntöjen tarkoituksenmukaisuutta. Tekninen ymmärrys on tärkeää esimerkiksi määritettäessä hakuehtojen rajaamista, jolla on oleellinen merkitys tiedustelun tehokkuudelle. Mikäli hakuehtojen määrittelyssä ei käytetä teknistä asiantuntemusta, ei tiedustelu välttämättä ole riittävän tehokasta – toisin sanoen kansallinen turvallisuus voi vaarantua. Lisäksi resurssien riittävyys suhteessa tiedonhankinnalla kerättyyn datamassaan ja sen tehokkaaseen analysointiin voi synnyttää haasteita, mikä tulee tiedostaa jatkovalmistelussa ja -suunnittelussa. Tiedustelun laadun ja kustannustehokkuuden varmistamiseksi on välttämätöntä, että tuomioistuinten lupapäätösmenettelyihin osallistetaan puolueettomia tietoliikenneasiantuntijoita.

CSC näkee, että eri osapuolten korkea tekninen osaaminen vähentää myös tiedustelutoiminnan väärinkäytösriskejä. Keskeisenä tekijänä väärinkäytösten ehkäisemisessä valvonnan ohella on tiedustelussa käytettävien järjestelmien riittävän kattavat lokitusmekanismit, joiden avulla tiedusteluviranomaisten toimintaa on mahdollista seurata ja mahdolliset väärinkäytökset voidaan todentaa luotettavasti.

4 Tiedustelun kohdentamisen haasteet

Kansallisen turvallisuuden näkökulmasta on ensiarvoisen tärkeää huolehtia siitä, että tietoliikennetiedustelu toteutetaan mahdollisimman kohdennetusti. Kuten lainsäädäntövalmisteluissa on jo todettu, ei kaikkeen tietoliikenteeseen kohdistuvaa tiedustelua voi pitää hyväksyttävänä kansainvälisen oikeuskäytännön nojalla. CSC katsoo, 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. Liian suurten datamassojen analysointi ei ole myöskään tiedustelutoiminnan tehokkuuden ja siten tiedustelutoiminnalle asetettujen tavoitteiden saavuttamisen kannalta tarkoituksenmukaista.

Hakujen ja suodatusten kohdentamisen käytänteet tulisi määritellä etukäteen sekä tiedusteluintressit että yritysten luottamuksellisuuden ja kansalaisten yksityisyyden turvaaminen huomioon ottaen. Haut ja suodatukset olisi syytä asettaa valvovien tahojen saataville. Lisäksi hakutuloksille tulisi määritellä enimmäismäärät dataa, jotka tietyllä haulla voi seuloa, kuitenkin huomioon ottaen, että myös tiedustelutekniikat ovat jatkuvan kehityksen alla.

Tiedustelun kohteen todentaminen vaatii suurta huolellisuutta ja tämä tulee tunnistaa tulevassa sääntelyssä. Yksi mahdollinen vaihtoehto tiedustelun kohdentamisen parantamiseksi olisi velvoittaa tuomioistuimen lupaa hakeva tiedusteluviranomainen ja/tai mahdollisesti myös tuomioistuin arvioimaan luvassa mainitun hävittämistä vaativan tiedon osuus ja määritettävä jokin kerätyn tiedon määrä, kohdennetun haun ja kerätyn datan suhde tai jokin muu mitattava raja-arvo, jota ei saa ylittää. Järjestelmä, jossa tietojen kerääminen olisi mahdollista ainoastaan tarpeen synnyttyä ja luvan saamisen jälkeen, olisi perusoikeuksien kannalta lähtökohtaisesti parempi.

Lakiesityksissä ehdotettu malli mahdollistaa teknisellä tasolla kaiken, myös Suomen sisäisen, liikenteen erottelun ja analysoimisen, jolloin myös tällaisten tietojen vuotaminen on mahdollista. Tällaisen vuodon mahdollisuutta tai vaikutuksia ei ole arvioitu nykymuotoisessa esityksessä riittävästi, ja onkin toivottavaa, että jatkovalmistelussa arvioidaan tällaisen vuodon riskiä.

Toimitusjohtaja Kimmo Koski Tietoturvapäällikkö Urpo Kaila