CSC-Tieteen tietotekniikan keskus Oy

Lausunto

16.06.2017

Asia: SMDno-2015-1509; SM047:00/2015

Ehdotus siviilitiedustelua koskevaksi lainsäädännöksi; työryhmän mietintö 8/2017

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Sisäministeriölle

Lausunto ehdotuksesta siviilitiedustelua koskevaksi lainsäädännöksi, työryhmän mietintö 8/2017

CSC – Tieteen tietotekniikan keskus Oy (CSC) kiittää mahdollisuudesta saada lausua ehdotuksesta siviilitiedustelua koskevaksi 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.

Tiivistelmä

CSC pitää tiedustelua koskevan lainsäädännön kehittämistä ja selkiyttämistä erittäin tärkeänä. Tietoliikenneoperaattorina sekä IT-palveluiden toimittajana CSC korostaa lausunnossaan seikkoja, joilla katsoo olevan merkitystä erityisesti tietoliikennetiedustelun toteuttamisessa. Kansallisen turvallisuuden näkökulmasta on ensiarvoisen tärkeää huolehtia siitä, että tietoliikennetiedustelu toteutetaan mahdollisimman kohdennetusti. Siksi tulee varmistaa, että tiedusteluntoiminnan tekninen osaaminen ja tekninen toteutus ovat riittävän korkealla tasolla, jotta tiedustelun avulla todella saadaan kansallisen turvallisuuden kannalta relevanttia ja hyödyllistä tietoa. Tietoliikennetiedustelun onnistuminen vaatii teknisen toteutustavan yksityiskohtien tarkastelua ja vaihtoehtoisten toteutustapojen vertailua sekä turvallisuus- että tietosuoja- ja

luottamuksellisuusnäkökohdat huomioiden. Mietintö herättää tältä osin joitakin keskeisiä kysymyksiä koskien esimerkiksi tiedonhankinnan kohdentamista sekä sijaintitietojen käyttöä.

Teknisen osaamisen lisäksi CSC haluaa lausunnossaan kiinnittää huomiota tietoliikennetiedustelun vaikutuksiin suomalaisten IT-toimijoiden toimintaan ja kansainväliseen kilpailukykyyn. Tältä osin keskeisiä näkökohtia ovat viranomaisten avustamisvelvollisuuksien tarkkarajaisuus, avustamisvelvollisuudesta syntyvät vastuukysymykset sekä suomalaisten IT-toimittajien uskottavuus asiakkaidensa luottamuksellisen tiedon säilyttäjänä ja tietoturvallisuuden takaajana. Työryhmän mietinnössä eri toimijoiden vastuut ja roolit tiedustelutoiminnassa herättävät kysymyksiä, joihin tulee jatkovalmistelussa kiinnittää huomioita.

Jatkovalmistelussa CSC pyytää kiinnittämään huomiota seuraaviin näkökohtiin:

1. Tiedon luottamuksellisuuden turvaaminen suomalaisissa IT-palveluissa

Tuleva siviilitiedustelulainsäädäntö ei saa vaarantaa kotimaisten eikä kansainvälisten toimijoiden luottamusta suomalaisten IT-palvelutuottajien kykyyn taata asiakkaidensa tietojen luottamuksellisuus ja tietoturva. Tiedustelutoimenpiteet eivät saa myöskään heikentää yritysten palveluiden yleistä saatavuutta. Lakiehdotuksen nykyisessä muodossa riittävän uskottavat ja läpinäkyvät turvallisuuskontrollit eivät valitettavasti toteudu. Näin ollen lain toimeenpanoa tulee tämän osalta selkiyttää. 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.

Tiedon luottamuksellisuus liittyy vahvasti elinkeinoelämän kilpailukykyyn ja kansainvälisten investointien suuntautumiseen. Ehdotetulla tietoliikennetiedustelulla voikin olla vaikutuksia yritysten sijoittautumispäätöksiin, erityisesti tiedon hyödyntämiseen perustuvassa liiketoiminnassa. Yrityssalaisuuksien ja muiden luottamuksellisten tietojen salassapito on yksi kriteeri kansainvälisten investointien kokonaisarviointia, johon vaikuttavat myös esimerkiksi sähkön hinta ja yhteiskunnallinen vakaus. Siviilitiedustelulakityöryhmän mietinnössä todetaan, että "kansantalouden ja sen osana toimivien yritysten toimintaedellytysten kannalta on tärkeää, että Suomeen luotava säädösperusta tiedusteluviranomaisten toiminnalle on selkeä". CSC kiinnittää erityishuomioita kyseiseen kohtaan ja esittää, että jatkovalmistelussa elinkeinoelämän kilpailukykynäkökulmien tulisi olla keskeisessä roolissa.

2. Vastuiden, velvollisuuksien ja roolien selkiyttäminen

CSC toteaa, että 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.

Ehdotuksessa poliisilain muuttamisesta 5 a luvun 15 §:n mukaan "suojelupoliisin palveluksessa olevalla virkamiehellä on tällöin oikeus laitteen, menetelmän tai ohjelmiston asentamiseksi, käyttöön ottamiseksi ja poistamiseksi salaa mennä edellä mainittuihin kohteisiin tai tietojärjestelmään 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 voida omatoimisesti manipuloida yritysten palvelutuotantoon liittyvää tietoliikennettä tai tietojärjestelmiä, vaan mahdollisesta seurannasta ja muutoksista tulee aina sopia yrityksen johdon kanssa etukäteen laillisin perustein. Tämä edellyttää jatkovalmistelussa tiedusteluviranomaisten avustamistehtävissä yritykseltä vaadittavien osaamisen, valmiuksien ja velvollisuuksien tarkempaa määrittelemistä. Lisäksi jatkovalmistelussa on selkeästi rajattava, mitä toimia yritys on velvollinen tekemään osana tiedusteluviranomaisten avustamista. Selkeä tiedustelulainsäädäntö on tärkeä myös yrityksille ja tarkasti määritellyt velvoitteet takaavat viranomaisyhteistyön toimivuuden.

Siviilitiedustelulainsäädännön jatkovalmistelussa tulisi kiinnittää yleisestikin huomioita eri toimijoiden välisiin rooleihin ja velvollisuuksiin ja pyrkiä selkeyteen ja yksiselitteisyyteen. Esimerkiksi Helsingin käräjäoikeuden tiedusteluun liittyvää päätöksentekomekanismia sekä esittelyperiaatteita tulee entisestään selkeyttää ja saattaa läpinäkyvämmäksi. Myös tiedusteluviranomaisten valtuudet ja vastuut tulee määritellä tarkoin ja eksplisiittisesti.

Tiedusteluviranomaisten avustamisesta syntyviä yritysvaikutuksia tulee arvioida jatkovalmistelussa kokonaisvaltaisesti sisältäen yksityiskohtaista arviointia esimerkiksi yrityksissä tarvittavan uuden osaamisen ja tekniikan vaatimista lisäresursointitarpeista. Tiedustelutoiminnan menestyksellinen toteuttaminen vaatii korkeaa teknistä osaamistasoa, mikä tulee huomioida lainsäädännön jatkovalmistelussa.

3. Tiedustelun kohdentamisen haasteet

Kuten mietinnössä todetaan, ei kaikkeen tietoliikenteeseen kohdistuvaa tiedustelua voi pitää hyväksyttävänä kansainvälisen oikeuskäytännön nojalla. Mietinnössä korostetaan myös tarvetta toteuttaa tiedustelu tietoliikennettä häiritsemättä, tarpeettomasti yksityisyyttä loukkaamatta ja teloperaattorineutraalisti. Esitetyssä teknisessä toteuttamisvaihtoehdossa tiedustelu kuitenkin käytännössä kohdistuu kaikkeen tuomioistuimen luvassa mainitun rajanylityspisteen kautta kulkevaan liikenteeseen. Ongelma on mietinnössä tunnistettu ja ratkaisuksi esitetään tiedon hävittämisvelvollisuutta (ehdotus laiksi tietoliikennetiedustelusta siviilitiedustelussa, 15 §).

Tämä ei kuitenkaan poista tiedustelun tosiasiallista massavalvontatekniikkaa eikä kerättyä tietoa voida hävittää esimerkiksi erottelua suorittavien tiedusteluviranomaisten muistista. Haun kohdentamisessa tulisi hyödyntää ehdotettua tarkempaa rajausta tai rajatumpaa tekniikkaa, sillä

mitä epämääräisempää tai laajempaa hakutermiä tiedonhankinnassa käytettäisiin, sitä enemmän liikennettä suodattuisi jatkokäsittelyyn. Liian suurten datamassojen analysointi ei ole myöskään tiedustelutoiminnan tehokkuuden ja siten tiedustelutoiminnalle asetettujen tavoitteiden saavuttamisen kannalta tarkoituksenmukaista. Ehdotettu malli mahdollistaakin 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.

Esityksessä sijaintitieto luokitellaan välitystiedoksi, jos sitä käytetään esimerkiksi viestin välittämisessä. Näin ollen viranomaisella on oikeus kerätä sijaintitietoja (esim. päätelaitteen paikkatieto), mikäli sijaintitietoja on käytetty viestin välittämisessä ja tuomioistuimen päätös antaa luvan välitystietojen hyödyntämiseen. Sijaintitietoja on nykytekniikalla kuitenkin suhteellisen helppo väärentää. Tämä saattaa johtaa viranomaisten virheellisiin tulkintoihin ja epäilyihin, mikäli asiaa ei osata huomioida erikseen tiedustelutoiminnassa. 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.

4. Korkean teknisen osaamisen vaatimus

Sikäli kun tulevan lainsäädännön tavoitteena on tuloksellinen ja tehokas tiedustelutoiminta, tiedustelua toteuttavien viranomaisten tekniseen osaamiseen ja asiantuntijuuteen tulee kiinnittää erityistä huomioita. Tietoliikenteen salaamisen lisääntyminen vaikeuttaa käytännössä tiedonhankintaa tietoliikennetiedustelulla, koska salatun tietoliikenteen analysoiminen vaatii joko salauksen murtamista tai salausavaimien hallintaa. Mietinnön tietoyhteiskuntavaikutusten arvioinnissa todetaan, että tiedusteluviranomaisille ei olla tietoliikennetiedustelua koskevassa sääntelyssä myöntämässä oikeutta velvoittaa yrityksiä salausvaimien luovuttamiseen. Tämä on erittäin tärkeää, koska kuten työryhmän mietinnössä todetaan, salausavaimien luovuttamisvelvollisuudella olisi haitallisia vaikutuksia Suomen kilpailukyvylle ja suomalaisten yritysten toiminnalle.

Ehdotuksessa laiksi tietoliikennetiedustelusta siviilitiedustelussa 2 §:ssä määritellään tietoliikennetiedustelu Suomen rajan viestintäverkossa ylittäväksi tietoliikenteeseen kohdistuvaksi, tietoliikenteen automatisoituun erotteluun perustuvaksi tekniseksi tiedonhankinnaksi sekä hankitun tiedon käsittelyksi. Lisäksi ehdotetun lain 15 §:ssä esitetään, että "tietoliikennetiedustelulla saatu tieto on hävitettävä viipymättä, jos käy ilmi, että viestinnän molemmat osapuolet olivat Suomessa silloin, kun viestintä tapahtui". Esimerkiksi pilvipalveluita käytettäessä tietoa tallentuu useammalle palvelimelle, jotka voivat sijaita eri puolilla maailmaa eikä näin ollen Suomen sisäistä ja rajat ylittävää tietoliikennettä voida yksinkertaisesti erottaa toisistaan. Tietoliikenne onkin yhä enenevässä määrin

valtioiden rajat ylittävää, vaikka se olisikin tarkoitettu liikkumaan vain Suomen sisällä lähettäjältä vastaanottajalle. CSC esittää, että jatkovalmistelussa tulisi pohtia, miten geolokaation manipulointimahdollisuus vaikuttaa saatavilla olevaan tiedustelutietoon ja miten tähän voidaan tehokkaasti vastata ehdotetussa siviilitiedustelulainsäädännössä.

5. Väärinkäytösriskien minimoiminen

Keskeisenä tekijänä väärinkäytösten ehkäisemisessä on varmistaa tiedustelussa käytettävien järjestelmien riittävän kattavat lokitusmekanismit, jotta tiedusteluviranomaisten toimintaa on mahdollista seurata ja mahdolliset väärinkäytökset voidaan todentaa luotettavasti. Lokitusmekanismeilla on merkittävä rooli väärinkäytösten ennaltaehkäisyssä, jonka lisäksi ne ovat keskeisiä työvälineitä tiedustelua valvoville tahoille. Jotta siviilitiedusteluun kohdistuva luottamus säilyy, tarvitaan riippumaton ja uskottava taho valvomaan tiedustelutoimintaa. Ns. valvojien valvominen tuleekin toteuttaa läpinäkyvästi ja selkeästi.

Riippumattomuuden ja uskottavuuden takaamiseksi tulee varmistaa, että valvovalla taholla on riittävä tekninen osaaminen ja resurssit, jotta tämä pystyy tosiasiallisesti arvioimaan viranomaisten tiedustelutoiminnan suhteellisuutta ja viranomaisten lupapyyntöjen tarkoituksenmukaisuutta. Tekninen ymmärrys on tärkeää esimerkiksi valvottaessa hakuehtojen riittävän tarkkaa rajaamista, jolla on merkitystä myös siviilitiedustelun tehokkuudelle. Resurssien riittävyys suhteessa tiedonhankinnalla kerättyyn datamassaan ja sen tehokkaaseen analysointiin voi synnyttää haasteita, mikä olisi hyvä tiedostaa jatkovalmistelussa ja -suunnittelussa.

Toimitusjohtaja Kimmo Koski Tietoturvapäällikkö Urpo Kaila

Kaila Urpo
CSC-Tieteen tietotekniikan keskus Oy