CSC - Tieteen tietotekniikan keskus Oy

Lausunto 9.4.2018
Eduskunnan puolustusvaliokunta

Asiat: HE 199/2017 vp, HE 202/2017 vp, HE 203/2017 vp

Lausunto hallituksen esityksiin koskien siviili- ja sotilastiedustelulainsäädäntöä sekä tiedustelutoiminnan valvontaa

CSC – Tieteen tietotekniikan keskus Oy (CSC) kiittää mahdollisuudesta saada lausua ehdotuksista siviili- ja sotilastiedustelua koskevaksi lainsäädännöksi sekä ehdotuksesta tiedustelutoiminnan valvonnasta. 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 ja riittävää resursointia.

4) Tiedustelun kohdentamisen haasteet on huomioitava lainsäädännön jatkovalmistelussa.

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 turvallisuus-kontrollit 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

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

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

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 ollaan 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 turvallisuus-viranomaisten 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 ja valvonnan riittävien resurssien 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 luottamuksellisuus-näkökohdat huomioiden.

Toisaalta ainoastaan teknistä tiedustelutoimintaa toteuttavien viranomaisten osaamisen varmistaminen ei ole riittävää, vaan huomiota tulee kiinnittää myös tuomioistuinten sekä tiedustelutoimintaa valvovien tahojen, tiedusteluvalvontavaliokunnan ja tiedusteluvaltuutetun, tekniseen osaamiseen. Tämä on tärkeää, jotta valvovat tahot pystyvät riippumattomasti, uskottavasti ja tosiasiallisesti arvioimaan viranomaisten tiedustelutoiminnan suhteellisuutta sekä tarkoituksenmukaisuutta. Tekninen ymmärrys on tärkeää esimerkiksi tuomioistuimessa määritettäessä hakuehtojen rajaamista, millä on oleellinen merkitys tiedustelun tehokkuudelle. Mikäli hakuehtojen määrittelyssä ei käytetä riittävän korkeaa 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 tehokkuuden varmistamiseksi on välttämätöntä, että tuomioistuinten lupapäätösmenettelyihin osallistetaan puolueettomia tietoliikenneasiantuntijoita. CSC näkee myös, että tiedustelutoimintaan liittyvät kansainväliset sertifioinnit (esim. ISO 27001 -standardi) sekä erilaisten arviointilaitosten käyttäminen toiminnan arvioinnissa toisivat läpinäkyvyyttä toimintaan ja auttaisivat valvonnassa.

CSC toteaa, 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.

CSC katsoo, että periaatteita koskien tietojen luovutusta muille toimijoilla osana tiedustelutoimintaa tulee selventää (mitä tietoja voidaan luovuttaa, kenelle ja millä perustein?). On tärkeää selventää, miten tietojen luovutuksesta voidaan raportoida kotimaassa, jotta myös tiedustelua valvovat tahot voivat suorittaa tehtävänsä tehokkaasti.

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

Tiedustelun kohteen todentaminen vaatii täsmällisyyttä sekä huolellista perustelua, mikä tulee tunnistaa tulevassa sääntelyssä. Yksi mahdollinen vaihtoehto tiedustelun kohdentamisen parantamiseksi on velvoittaa tuomioistuimen lupaa hakeva tiedusteluviranomainen ja/tai mahdollisesti myös tuomioistuin arvioimaan lupahakemuksessa mainitun hävittämistä vaativan tiedon osuus, määrittämään kerätyn

tiedon enimmäismäärä sekä kohdennetun haun ja kerätyn datan suhde tai muu vastaava mitattava raja-arvo, jota ei tule ylittää. Järjestelmä, jossa tietojen kerääminen olisi mahdollista ainoastaan tarpeen synnyttyä ja luvan saamisen jälkeen, olisi perusoikeuksien sekä yritysten luottamuksellisen tiedon turvaamisen kannalta lähtökohtaisesti parempi järjestely.

CSC katsoo, että seuraavan avoimesti saatavilla olevan tiedon kerääminen laillista ja valvottua tiedustelutoimintaa varten tulee olla sallittua lainsäädännössä:

- Avoimesti saatavilla oleva tieto julkisissa verkoissa, kuten kohde- ja lähdeosoitteet, käytetyt protokollat sekä muut otsikkotiedot ja liikennemäärät, sisältäen myös nimipalvelukyselyt.
- Salaamattoman tietoliikenteen sisältö, kuten salaamaton selainliikenne tai salaamattomat puhelut, videoneuvottelut ja sähköpostit.
- Palvelinten sekä aktiivi- ja päätelaitteiden haavoittuvuuksien havaitseminen tulee olla sallittua, ja haavoittuvuuksien tunnistetietojen kerääminen sallittua, mutta haavoittuvuuksien hyödyntämisen tulee edellyttää peitetoiminnan mukaista luvitusta.

Lakiesityksissä ehdotettu malli mahdollistaa teknisellä tasolla kaiken liikenteen, myös Suomen sisäisen liikenteen, erottelun ja analysoimisen. Tiedustelutoiminnassa ei kuitenkaan tule suorittaa massavalvontaa, jossa kaikkien lähettäjien ja vastaanottajien viestintää seurataan yleisillä hakulausekkeilla, joita ei ole kohdennettu selkeästi määriteltyihin lakiin perustuviin sekä ajantasaisiin riskitekijöihin ja -ryhmiin. Ei-hyväksyttävää massavalvontaa on:

- Yleisen tietoliikenteen salatun tietosisällön seulominen salausavaimia murtaen.
- Laajamittaiset ei-kohdennetut peiteoperaatiot salausavainten haltuunotolla.
- Tietoliikenteen ja tietosisältöjen erottelu ja analysointi muuhun kuin laillisiin tarkoituksiin.

Tiedustelutietojen turvaaminen sekä tahattomien ja tahallisten tietovuotojen estäminen on ensiarvoista tiedustelutoiminnan legitimiteetin kannalta. Tätä varten tiedusteluvaltuutetulla tulee olla riittävät resurssit valvoa toimintaa. Lisäksi tiedustelutoimintaa suorittavien tahojen tulee noudattaa varmennettuja sekä sertifioituja turvallisuuden hallintaprosesseja. Kestävälle pohjalle ja avoimien periaatteiden mukaan säädelty tiedustelutoiminta on Suomelle myös kilpailukykytekijä, jonka avulla turvataan edellytykset tietoteknisten palveluiden tarjoamiselle myös Suomessa ja suomalaisten yritysten toimesta.

Espoossa 9.4.2018

Toimitusjohtaja Kimmo Koski Tietoturvapäällikkö Urpo Kaila