

Eduskunnan liikenne- ja viestintävaliokunnalle

HALLITUKSEN ESITYS EDUSKUNNALLE LAIKSI SOTILATIEDUSTELUSTA SEKÄ ERÄIKSI SIIHEN LIITTYVIKSI LAEIKSI

Tässä vastineessa käsitellään lausunnonantajien huomiot, jotka liittyvät ennen kaikkea eduskunnan liikenne- ja viestintävaliokunnan toimialaan.

Useat lausunnoissa on tuotu esiin seikkoja, jotka ovat puolustusministeriön näkemyksen mukaan pyritty ottamaan hallituksen esityksessä huomioon valmisteluvaiheessa. Esimerkiksi Euroopan unionin oikeuden asettamat reunaehdot on pystytty ottamaan hyvin huomioon hallituksen esityksessä.

Vastineessa käsitellään Rajavartiolaitoksen lausunnossaan esittämiä huomioita tarkemmin. Rajavartiolaitos on merkittävä yhteistyökumppani Puolustusvoimille maanpuolustuksen alalla, ja hyvän yhteistyön jatkuminen on tärkeää.

Pyydettyinä vastineena asiantuntijalausunnoista puolustusministeriö esittää asiakohtaisesti, siltä osin kuin lausunto on edellyttänyt vastaamista, seuraavaa:

1. Sotilastiedustelutoiminnasta tiedottaminen

Effi ry ja VTT ovat lausunnoissaan esittäneet, että tiedustelutoiminnasta tulisi kertoa mahdollisimman avoimesti. Lausunnoissa on esitetty, että julkisissa esityksissä voitaisiin ilmoittaa määrällisiä tietoja muun muassa tietoliikennetiedustelun osalta, kuinka laajoihin henkilöryhmiin, kuinka isoon verkkoalueeseen ja data- ja viestimääriin myönnetyt tiedusteluluvat ja toisaalta toteutetut tiedustelutoimenpiteet ovat kohdistuneet. Lisäksi lausunnoissa esitetään, että julkisiin esityksiin voitaisiin lisätä tilastoja siitä, paljonko ja kuin monta eri henkilöä koskevia tietoja tiedusteluviranomaiset ovat saaneet muiden viranomaisten rekistereistä.

Tiedustelutoiminnan yhteiskunnallisen hyväksyttävyyden näkökulmasta lausunnoissa esitettyä voidaan pitää periaatteellisesti kannatettavana ja mahdollisuuksien mukaan salassapitosäännökset huomioon ottaen toiminnasta voitaneen laatia myös julkisia lausunnossa tarkoitettuja tilastoja. Viestintää varten hallituksen esityksessä on esitetty Puolustusvoimille kahta uutta virkaa (2 htv), joissa nimenomaisena tehtävänä olisi saattaa sotilastiedusteluviranomaisen analysoimaa tietoa mahdollisimman julkiseen muotoon.

Kattavin kuva edellä tarkoitetuista tiedoista koko tiedustelutoiminnassa, sotilas- ja siviilitiedustelussa, olisi tiedusteluvaltuutetulla. Uusi perustettava parlamentaarinen valvonta parantaa tiedustelun valvonnan tilannekuvaa. Julkaistavat tiedot ja tilastot tulee kuitenkin

käydä tarkasti läpi tiedusteluviranomaisten ja tiedusteluvaltuutetun kanssa, jottei tiedustelun tarkoitus vaarannu. Päätös tietojen julkistamisesta tulisi olla aina viime kädessä sotilastiedustelupuolella sotilastiedusteluviranomaisella.

2. Kaiken tietoliikenteen kattava tiedustelu

VTT, BaseN ja CSC toteavat lausunnoissaan, että sotilastiedusteluviranomaiselle luotaisiin teknisten edellytykset valvoa kaikkea tietoliikennettä kaikissa tietoliikenteen solmukohtissa. Lisäksi lausunnoissa todetaan, että myös Suomen sisäinen liikenne saattaa joutua tietoliikennetiedustelun piiriin.

Tietosuojavaltuutetun toimisto toteaa, että tiedusteluviranomaisen kytkeytyessä viestintäverkkoon, olisi se toteutettava tavalla, joka ei johda massavalvontaan.

CSC toteaa myös, että järjestelmä, jossa tietojen kerääminen olisi mahdollista ainoastaan tarpeen synnyttä ja luvan saamisen jälkeen, olisi perusoikeuksien kannalta lähtökohtaisesti parempi.

Osana tietoliikennetiedustelun rakentamista kartoitetaan ne yhteydet, joissa on sotilastiedustelun kannalta kiinnostavaa liikenne. Nämä yhteydet voivat vaihdella ja muutoksiin reagoidaan. Toiminnassa ei ole tarkoituksenmukaista eikä tarvetta rakentaa jatkuvaa seuranta kaikkii tietoliikennesyhteyksiin tai tietoliikenteen solmukohtiin. Sotilastiedustelu tuntee jo tietyllä tasolla ja hankkii aktiivisesti tietoa kohteistaan, jolloin liityntäpisteiden rakentaminen ei tapahdu sattumanvaraisesti.

Tietoliikennetiedustelu ei olisi mahdollista, ellei tiedustelua voitaisi kohdistaa niihin tietoliikennesyhteyksiin, joissa kulkee tiedustelun kannalta merkittävää tietoliikennettä. Tämä ei kuitenkaan tarkoita sitä, että kyseisen tietoliikennesyhteyden kaikkea tietoliikennettä valvottaisiin. Jotta tietoliikennetiedustelua voitaisiin käyttää, tarvittaisiin käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen mukaan aina tuomioistuimen lupa, jossa olisi ilmoitettava 1) tiedustelutehtävä, 2) se viestintäverkon osa (kuten kuitu tai aallonpituus) johon tietoliikennetiedustelua kohdennettaisiin, 3) hakuehdot, joilla tiedustelutehtävän kannalta merkityksellistä tietoa saataisiin sekä 4) luvan voimassa oloaika. Jos tuomioistuin myöntää luvan sotilastiedusteluviranomaiselle, tietoliikennetiedustelun käytön aloittaminen edellyttää ulkopuolisen kytkennän suorittajan suorittamaa kytkentää tuomioistuimen myöntämän luvan tarkoittamaan viestintäverkon osaan. Sotilastiedusteluviranomaisella ei ole suoraa pääsyä kaikkeen tietoliikenteeseen.

Lisäksi on huomattava, että kaiken tietoliikenteen kattava tietoliikenteen tiedustelu vaatii huomattavia resursseja. Resurssien huomattava lisääminen tietoliikennetiedusteluun vaatii normaaliin tapaan talousarvioehdotuksen mukaisen resurssien lisäyksen ja sen mukaisen käsittelyn eduskunnassa.

Käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksessa on säädetty myös hetihävittämisvelvollisuuksia muun muassa Suomen sisäisen liikenteen osalta. Käytännössä tämä tapahtuu jo tietoliikenteen käsittelyn automatisoidun käsittelyn vaiheessa. Jos Suomen sisäinen tietoliikenne päättyisi edelleen manuaalisen käsittelyn vaiheeseen, sitoo hetihävittämisvelvollisuus edelleen tietoliikennettä käsittelevää virkamiestä. Mikäli näin ei toimita, sotilastiedusteluviranomainen ei toimi lainmukaisesti ja tällaiseen toimintaan olisi puututtava.

Vaikka tiedusteluviranomaisella olisikin tekninen mahdollisuus kaiken tietoliikenteen kattavaan tiedusteluun, tätä rajoittaa laissa esitetyt oikeudelliset reunaehdot, edellytyksenä oleva tuomioistuimen lupa, ulkopuolinen kytkennän suorittaja, tietoliikennetiedustelujärjestelmään rakennettavat tekniset ja toiminnalliset rajoitteet sekä resurssinäkökohdat. Edellä todetut seikat johtavat siihen, ettei tiedusteluviranomaisella ole tosiasiallisesti mahdollisuutta kaiken tietoliikenteen kattavaan tiedusteluun.

3. Tietoliikennetiedustelun yleisen, kohdentamattoman ja kaiken kattavan seurannan kieltö

Professori Tuomas Ojanen toteaa lausunnossaan, että laissa olisi syytä säätää tietoliikenteen yleisen, kohdentamattoman ja kaiken kattavan seurannan kiellosta tiedustelutoiminnassa nimenomaisesti sotilastiedustelu- ja siviilitiedustelulaeissa siltä osin kuin niissä säädetään tiedonhankinnasta tietoliikenteestä. Tämä loisi osaltaan takeita niiden sääntelyn sopusoinnulle EU-oikeuden (samoin kuin Euroopan ihmisoikeussopimuksen) kanssa. Professori Ojanen ei ota tässä vaiheessa yksityiskohtaisemmin kantaa kielto­säännöksen muotoiluun, vaan painottaa tarvetta tällaiselle kielto­säännökselle Euroopan ihmisoikeussopimuksen ja EU-oikeuden kannalta.

Puolustusministeriön näkemyksen mukaan esitetty kanta on huomioitu jo perustuslain 10 §:n muutosta koskevassa hallituksen esityksessä (HE 198/2017 vp.). Sen yksityiskohtaisissa perusteluissa todetaan, että: ”[Perustuslain] Säännöksessä mainittavasta ja perusoikeuksien yleisiin rajoitusedellytyksiinkin kuuluvasta välttämättömyysvaatimuksesta ja vaatimuksesta rajoituksen sopusoinnusta kansainvälisten ihmisoikeusvelvoitteiden kanssa samoin kuin EU-oikeudesta seuraa vaatimuksia muun muassa toimivaltuuksien yksilöimiselle. Ehdotettu sääntely ei siten mahdollistaisi yleisestä, kohdentamattomasta ja kaikenkattavasta tietoliikenteen seurannasta säätämistä.”

Puolustusministeriö pitää tätä rajausta riittävänä eikä katso tarkoituksenmukaiseksi säätää nimenomaisesta tietoliikenteen yleisen, kohdentamattoman ja kaiken kattavan seurannan kiellosta tiedustelutoiminnassa laissa sotilastiedustelusta. Lisäksi nyt käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksessa esitetään säädettäväksi useita säännöksiä, joidenka perusteella tietoliikennetiedustelun olisi oltava kohdennettua niin fyysisesti kuin hakuehdoin sekä ajallisesti eikä tietoliikennetiedustelu voisi näin kohdistua kaikkeen Suomen rajan ylittävään tietoliikenteeseen

4. Tietoliikennetiedustelun tehokkuus

BaseN Oy kiinnittää lausunnossaan huomiota viestintäverkoissa liikkuvan tietoliikenteen määrään. Lisäksi lausunnossa kiinnitetään huomiota tietoliikenteen salaukseen.

Puolustushallinnossa tähän on kiinnitetty huomiota jo käsiteltävänä olevan hallituksen esityksen pohjana olevan esiselvityksen laatimisen vaiheessa (Suomalaisen tiedustelulainsäädännön suuntaviivoja. 2015). Kaapeleiden ja kuitujen osalta on huomioitava se, että niistä mainitaan käytännössä aina niiden kokonaiskapasiteetti, mikä ei käytännössä koskaan ole käytössä. Lisäksi kaikki Suomen rajan ylittävät kaapelit ja kuidut eivät ole käytössä kaiken aikaa. Tietoliikennetiedustelussa pystytään valitsemaan merkitykselliset viestintäverkkojen osat ja suodattamaan pois epäoleellista liikennettä.

Julkisista lähteistä saatujen tietojen mukaan noin puolet tietoliikenteestä on tällä hetkellä salattua. Tämän lisäksi myös salatusta tietoliikenteestä voidaan muodostaa olennaista tiedustelutietoa salausta purkamatta.

5. Tietoliikennetiedustelujärjestelmään liittyvät riskit

VTT ja CSC kiinnittävät lausunnoissaan huomiota siihen, että tietoliikennetiedustelujärjestelmän mahdolliset tekniset epävarmuudet ja viat avaavat mahdollisuuden järjestelmän väärinkäyttöksiin. Lisäksi VTT toteaa, ettei hallituksen esityksessä ole käsitelty väärinkäytöksistä aiheutuvia rangaistuksia ja vastuuta taikka niiden luomaa pelotevaikutusta.

Lausunnoissa esitetyt seikat on tunnistettu puolustushallinnossa. Tietoliikennetiedustelujärjestelmä rakennetaan niin, että erityistä huomiota kiinnitetään nimenomaan käyttöoikeuksien hallintaan ja käyttäjien toiminnan seuraamiseen ja varmentamiseen, toimintatapoihin ja hyväksymisprosesseihin. Kaikessa edellä tarkoitettussa keskeisessä asemassa on tarkat ja luotettavat lokitiedot, joiden perusteella esimiehet sekä sisäinen ja ulkoinen lailisuusvalvonta voivat todeta toiminnan asianmukaisuuden tai mahdolliset rikkeet.

Mahdollisten rikkeiden osalta sotilastiedusteluviranomaisen virkamies on virkamieslain-säädännön ja rikoslain alainen. Lisäksi Puolustusvoimien sotilasvirassa palveleviin sovelletaan myös sotilaskurinpitolainsäädäntöä, jossa puuttumiskynnys on vielä edellä mainittua lainsäädäntöä alhaisempi. Jos rikkeitä ja väärinkäytöksiä havaitaan, tulee niihin puuttua voimassa olevan lain mukaisesti. Sotilastiedusteluviranomaisen sisäisten toimien lisäksi toimintaa valvoo ulkopuolinen tiedusteluvaltuutettu, jolla on toimimisvelvollisuus havaitessaan sotilastiedusteluviranomaisen virkamiehen rikkeisiin ja toimintaan.

6. Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen

FiCom, CSC, Elisa Oyj ja DNA Oyj ovat lausunnoissaan kiinnittäneet huomiota käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 40 §:n tarkoittamaan sotilastiedusteluviranomaisen mahdollisuuteen asentaa ja poisottaa laite, menetelmä tai ohjelmisto yrityksen tietämättä. Lausunnonantajat katsovat, ettei sotilastiedusteluviranomaisella tulisi olla pääsyä teleyritysten tai tietoyhteiskunnan palvelujen tarjoajien laitetiloihin tulisi olla kiellettyä.

Puolustusministeriön näkemyksen mukaan lausunnonantajien huomiot ovat perusteltuja, vaikka tilanteet olisivatkin erittäin harvinaisia Suomessa.

Edellä tarkoitettun säännöksen yksityiskohtaisissa perusteluissa todetaan, mahdolliset toimet edellä tarkoitetuissa tiloissa tulisi toteuttaa mahdollisimman vähän haittaa aiheuttaen. Tämän voidaan katsoa jo sisältävän sen, ettei sotilastiedusteluviranomainen itsenäisesti suorittaisi laitteen, menetelmän tai ohjelmiston asentamista tai poisottamista. Muu ei olisi tarkoituksenmukaista.

Ehdotettu säännös laajentaisi laitteen, menetelmän tai ohjelmiston asentamisen ja poisottamisen käyttämisen myös telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta sekä televalvontaan, toisin kuin on voimassa olevassa lainsäädännössä. Tässä yhteydessä on syytä huomioda, että telekuuntelun, tietojen hankkimisen telekuuntelun sijasta sekä televalvonnan kohdalla asentamistoimivaltuuden käyttäminen tulisi lähtökohtaisesti sovellettavaksi ulkomaan tiedustelussa, koska on hyvin epätodennäköistä, että ulkomainen

teleyritys avustaisi sotilastiedusteluviranomaista kytkentöjen tekemisessä. Tämä myös aiheuttaisi merkittävän paljastumisriskin.

Suomen rajan sisällä käytettävien toimivaltuuksien käytössä toimittaisiin vastaavasti, kuten nykyisten poliisilain 5 luvussa tarkoitettujen telekuuntelun, tietojen hankkimisen telekuuntelun sijasta sekä televalvonnan kohdalla eli sotilastiedusteluviranomainen hakisi luvan tuomioistuimelta mainittujen toimivaltuuksien käyttämiseksi. Jos tiedustelumenetelmän käytöstä päättäisi tuomioistuin, niin myös tiedustelumenetelmän käyttöä koskevassa luvassa tulisi erikseen sallia laitteen, menetelmän tai ohjelmiston asentaminen. Näin ollen asentamistoimivaltuutta sovellettaessa tuomioistuinmenettelyssä tulisi yksittäistapauksellisesti myös arvioitavaksi toimivaltuuden toteuttamisen tapa. Asiassa on syytä korostaa sitä, ettei esimerkiksi telekuuntelua, televalvontaa tai tietoliikennetiedustelua saisi kiertää käyttämällä teknisen tarkkailun toimivaltuuksia, vaan sotilastiedusteluviranomainen saisi käyttää toimivaltuuttaan vain säädettyyn tarkoitukseen (tarkoitussidonnaisuuden periaate).

Laitteen, menetelmän tai ohjelmiston asentamisen ja poisottamisen yhteydessä tulisi aina pohtia sen mahdollisesti aiheuttamaa kiinnijäämisriskiä sekä myös asentamisen kohteelle aiheutuvaa mahdollista vahingon riskiä. Esimerkiksi salaa tietojärjestelmään asennettu teknisen laitetarkkailun ohjelmisto sisältää aina mahdollisen riskin tietojärjestelmän toiminnalle ja on omiaan heikentämään sen turvallisuutta. Sotilastiedustelun toimenpiteillä ei saisi aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä laitteen, menetelmän tai ohjelmiston asentamisen ja poisottamisen yhteydessä (vähimmän haitan periaate).

Käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 93 §:ssä ehdotetaan säädetäväksi teleyrityksen velvollisuus avustaa sotilastiedustelussa ja 17 §:ssä yhteistyöstä yhteisöjen kanssa. Jälkimmäisen pykälän 1 momentin mukaan sotilastiedusteluviranomaisen on tarpeen mukaan toimittava yhteistyössä muiden viranomaisten kanssa sotilastiedustelun tarkoituksenmukaiseksi hoitamiseksi. Tämä voi tarkoittaa esimerkiksi sotilastiedusteluviranomaisen ja teleyrityksille yhteisesti hyväksyttävien toimintatapojen ja -käytänteiden laatimista.

7. Tiedon luovuttaminen Viestintävirastolle

Viestintävirasto katsoo lausunnossaan, että, että viraston tehtävien hoitamisen kannalta on välttämätöntä, että sotilastiedusteluviranomaisella on salassapitosäännösten estämättä mahdollisuus luovuttaa tietoliikennetiedustelun avulla hankittu tieto haitallisesta tietokoneohjelmasta tai käskystä toimivaltaiselle viranomaiselle, kun tiedon luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi tai tiedon saajan etujen turvaamiseksi.

Puolustusministeriö yhtyy Viestintäviraston näkemykseen. Puolustusministeriö kiinnittää kuitenkin huomiota, että käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 17 §:n 2 momentissa on asetettu korkeampi kynnys tietojen luovuttamiselle kuin 1. lakiehdotuksen 71 §:ssä. Ensin mainitussa säännösehdoituksessa kynnys olisi ”välttämätön”, kun taas viimeksi mainitussa ”tarpeen”. Voidaan perustellusti kysyä, onko ”välttämättömyys” liian korkea kynnys tässä yhteydessä ja ovatko säännösehdoitusten kynnykset yhdenmukaiset. Ensin mainitussa yleisessä luovuttamisesta koskevassa säännöksessä oleva välttämättömyys-vaatimus voi olla omiaan vaikeuttamaan ja supistamaan tiedusteluviranomaisen raportointitoimintaa ja yleisemminkin tiedon jakamista. Esimerkiksi tietoturva-poikkeamat tietojärjestelmien haavoittuvuudet voivat tulla esiin myös muilla keinoin kuin

tietoliikennetiedustelulla, näistä tiedon luovuttaminen esimerkiksi Viestintävirastolle olisi korkeamman kynnyksen takana.

8. Yhdysliikennepisteisiin kohdistettavat tiedustelutoimenpiteet

FICIX ry toteaa lausunnossa, että yhdysliikennepisteisiin kohdistettavilla tiedustelutoimenpiteillä ei saavuteta sille asetettuja tavoitteita.

Puolustusministeriö näkee FICIX ry:n lausuntoa vastaavasti, ettei yhdysliikennepisteisiin kohdistettavilla tiedustelutoimenpiteillä saavutettaisi tiedustelutoiminnan tavoitteita eikä yhdysliikennepiteitä nähdä merkittävänä sotilastiedustelun kannalta. Tämä ei kuitenkaan tarkoita sitä, etteikö yhdysliikennepisteet voisi olla sotilastiedustelun kohteena, jos tiedustelutehtävä niin vaatisi.

9. Kytkennän suorittajan ja sotilastiedusteluviranomaisen välinen tietoliikenneyhteys

Suomen Erillisverkot Oy esittää lausunnossaan näkemyksen tietoliikennetiedustelun kohteena olevan viestintäverkon osan tietoliikenteen välittämisen teknisestä ratkaisusta.

Puolustusministeriö toteaa, että esitetty ratkaisu on tällä hetkellä hyvä, mutta mahdollisia muita ratkaisuja ei haluta sulkea pois mahdollisten muutosten osalta. Kytkennän suorittaminen ja tiedonsiirto ovat eri toimintoja, joista jälkimmäistä ei ole tarkoituksenmukaista säätää laissa.

10. Teknisten tietojen käsittely

VTT toteaa lausunnossaan, että käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 63 §:n perusteella sotilastiedusteluviranomainen voisi esitetyn säännöksen tarkoittamista tiedoista omassa jatkokäsittelyssään muodostamaan tietoja yhdistelemällä yksittäisiä henkilöitä koskevia tietoja.

Edellä tarkoitetun säännöksen mukaan teknisessä tietojen käsittelyssä ei saisi muodostua tietoa, josta pystyttäisiin tunnistamaan yksittäisiä henkilöitä. Säännöksessä todetaan lisäksi, että teknisen analyysin perusteena olevat tiedot on hävitettävä välittömästi sen jälkeen, kun tilastollisen analyysin tulos on valmistunut.

Teknisten tietojen käsittelyn tarkoituksena on tunnistaa niitä Suomen rajan ylittäviä viestintäverkon osia, joista tiedustelun kohteena olevan toiminnan kannalta merkittävää tietoliikennettä liikkuu. Tähän analyysiin sisältyviä tietoja ei ole teknisen analyysin valmistuttua mahdollista yhdistää keskenään niin, että niistä voitaisiin tunnistaa yksittäisiä henkilöitä; analyysissä on tietoa tietoliikennevirtojen liikkumisesta viestintäverkon osassa.

Teknisten tietojen käsittelyn käyttäminen muuhun kuin säännöksessä tarkoitettuun tarkoitukseen olisi myös käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 7 §:ssä esitetyn tarkoitussidonnaisuuden periaatteen vastaista. Tarkoitussidonnaisuuden periaatteen mukaisesti sotilastiedustelun toimivaltuutta saataisiin käyttää vain esitetyssä laissa säädettyyn tarkoitukseen, mikä tässä tapauksessa olisi teknisen analyysin tuottaminen, ei yksittäisten henkilöiden tunnistaminen. Jos sotilastiedusteluviranomainen toimisi muuten, sotilastiedusteluviranomainen ei toimisi lain mukaisesti.

11. Haavoittuvuuksien hyödyntäminen

VTT toteaa lausunnossaan, että tiedusteluviranomaisen tiedustelutarkoituksessa hyväksyttävä tietojärjestelmän haavoittuvuus voisi olla myös tieto, joka saattaisi olla merkityksellinen yritysten suojaamisen kannalta.

Tietojärjestelmien sisältämät haavoittuvuuksia koskevan tiedon luovuttaminen on aina tapauskohtaista harkintaa. Harkinnassa otetaan huomioon se, että haavoittuvuustiedon luovuttaminen yritykselle johtaa mahdollisesti siihen, että tieto siirtyy myös vieraiden valtioiden alueille sijoittuneiden organisaatioiden ja tahojen sekä mahdollisesti tiedustelun kohteena olevien käyttöön. Tässä tarkoituksessa tämä voisi vaikeuttaa tiedustelutoimintaa ja kansallisen turvallisuuden suojaamista.

Tiedustelutoiminnan lähtökohtaisena tarkoituksena on tiedon tuottaminen kansallisen turvallisuuden suojaamiseksi. Edellä tarkoitettujen tietojen osalta korostuu tiedusteluviranomaisen ammattitaito arvioida sitä, missä tilanteessa tieto on tarkoituksenmukaisinta luovuttaa edelleen. Toiminnan alettua ja siitä saatujen kokemusten nojalla käytännössä muotoutuvat myös ne käytänteet, joiden perusteella tietoturva haavoittuvuuksista voidaan kulloisessakin tilanteessa tarkoituksenmukaisimmin toimia.

12. Kytkennän käynnistäminen ja sulkeminen

Erillisverkot Oy on lausunnossaan todennut, että kytkennän sulkemisen pitäisi perustua kytkennän suorittamisen tapaan tuomioistuimen lupaan.

Käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 11 §:n 4 momentin mukaan tiedustelumenetelmän käyttö olisi lopetettava ennen päätöksessä tai luvassa mainitun määräajan päättymistä heti, kun käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole.

Lopettamispäätöksen tekee aina sotilastiedusteluviranomainen ja se on ilmoitettava kytkennän suorittajalle, jotta tämä voi kytkeä pois sotilastiedusteluviranomaisen pääsyn tuomioistuimen luvan mukaiseen viestintäverkon osaan. Tämä ei edellytä tuomioistuimen päätöstä.

Jos kytkennän sulkeminen edellyttäisi tuomioistuimen lupaa, saattaisi tämä tarpeettomasti viivästyttää sotilastiedusteluviranomaisen pääsyn estämistä viestintäverkon osaan.

13. Kustannukset teleyrityksille

Elinkeinoelämän keskusliitto EK, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, Elisa Oyj, DNA Oyj ja Telia Finland Oyj esittävät lausunnoissaan, että käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen säännöksistä aiheutuisi teleyrityksille ja tiedonsiirtäjille kustannuksia, sillä tiedustelumenetelmien käytöstä korvattaisiin ainoastaan järjestelmien kehittämiskustannukset, ei henkilötyövoimaa.

Käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 96 §:ssä esitetään säädettäväksi teleyrityksille suoritettavista korvauksista. Korvauskäytäntö vastaisi sitä, mitä nykyisin on poliisi-, esitutkinta- ja pakkokeinolakien osalta säädetty. Korvauskäytäntö on

säädetty sähköisen viestinnän palveluista annetun lain 299 §:ssä. Tämän lain kohdan muuttaminen kattamaan kaikki kustannukset saattaisi aiheuttaa merkittäviä kustannusvaihteluksia kaikille, suurimpana poliisi, viranomaisille, joilla on käytössään yleiseen viestintäverkkoon ulottuvia toimivaltuuksia.

Puolustusministeriön arvion mukaan teleyritysten vastuulle jäävien kustannusten arvioidaan olevan marginaalisia. Tämä johtuu siitä, että sotilastiedustelulle esitetään uusia toimivaltuuksia ja voidaan arvioida, että osaan rikosperusteisesta toiminnasta saataisiin tietoa jo aikaisemmassa vaiheessa ja toiminta ei välttämättä koskaan etenisi tilanteeseen, jossa rikosperusteisia toimivaltuuksia tarvittaisiin.

Maanpuolustuksen alalla osa teleyritysten yhteistyötä edellyttävistä saman tyyppisistä toimivaltuuksista siirtyisi myös poliisilta Puolustusvoimien käyttöön.

Puolustusministeriön käsityksen mukaan toimivaltuuksien käytöstä suoritettavien korvausten suorittamiseen on asetettu myös budjetäärisiä rajoitteita, ja yleisen näkemyksen mukaan korvausten suorittamista lakisääteisten tehtävien suorittamisessa käytettävien toimivaltuuksien osalta tulisi välttää.

Lisäksi sotilastiedustelutoiminnan vaivihkainen luonne ohjaa sotilastiedusteluviranomaista kehittämään järjestelmiä, joihin pääsy on mahdollisimman harvalla, etenkin mahdollisimman harvalla sotilastiedusteluviranomaisen ulkopuolisella henkilöllä. Tämän tavoitteen voidaan katsoa olevan yhteneväinen sotilastiedusteluviranomaisen ja teleyritysten kanssa.

Käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 97 §:ssä säädettäisiin tiedonsiirtäjälle suoritettavista korvauksista. Tiedonsiirtäjän määritelmä olisi keskeinen tietoliikennetiedustelussa.

Esitetyn 97 §:n mukaan tiedonsiirtäjällä olisi oikeus saada korvaus valtion varoista kaikista 1. lakiehdotuksen 94 ja 95 §:ssä, eli tietoliikennetiedusteluun liittyvästä avustamisesta, aiheutuneista kuluista. Tämä kattaisi myös henkilöstön käytöstä aiheutuvat kulut. Korvauksen määrittäisi Puolustusvoimien tiedustelulaitos, jolla olisi viranomaisista paras näkemys, mitkä kustannukset ovat oikeutettuja.

Puolustusministeriö esittää, että uuden lainsäädännön teleyrityksille asettamia velvoitteita ja korvauskäytäntöä seurataan tarkasti lain tultua voimaan.

14. Yritysten oikeus avata asiakkaiden luottamuksellista tietoliikennettä

CSC esittää lausunnossaan, että yritysten henkilöstön oikeudellinen vastuu tulisi määritellä selkeästi silloin, kun yritys joutuisi avaamaan asiakkaiden luottamuksellista tietoliikennettä.

Nyt käsiteltävänä olevassa hallituksen esityksessä ei esitetä säännöksiä, joiden nojalla yritys voitaisiin velvoittaa avaamaan asiakkaansa luottamuksellista tietoliikennettä sotilastiedusteluviranomaisen pyynnöstä.

15. Henkilötietojen käsittely

Tietosuojavaltuutetun toimisto ja Effi ry toteavat lausunnoissaan, että nyt käsiteltävänä olevaan hallituksen esitykseen ei sisälly ehdotuksia valmisteilla oleviksi laeiksi henkilötietojen käsittelystä. Taustalla on puolestaan mm. Euroopan unionin tietosuojadirektiivistä (2016/680) aiheutuva implementointitarve. Näin ollen pelkästään nyt käsiteltävänä olevien hallitusten esitysten pohjalta ei ole mahdollista saada kokonaiskuvaa ko. viranomaisten henkilötietojen käsittelystä.

Puolustusministeriö toteaa, että eduskunnassa on käsiteltävänä hallituksen esitys laiksi henkilötietojen käsittelystä Puolustusvoimissa (HE 13/2018 vp.), jossa esitetään säädettäväksi henkilötietojen käsittelyä Puolustusvoimissa koskeva uusi laki. Esityksessä on myös huomioitu sotilastiedustelua koskevan lainsäädännön tarpeet ja vaatimukset sille.

16. Ilmoitusvelvollisuus

Effi ry on todennut lausunnossaan, että yleisesti tiedustelumenetelmän käytön kohteelle ilmoittamisvelvollisuudesta ehdotetaan säädettäväksi poikkeuksia, jotka ovat Euroopan ihmisoikeustuomioistuimen (EIT) oikeuskäytännön kanssa ristiriidassa. Effi ry kiinnittää huomiota siihen, että jos yksityisen henkilön yksityisyyttä loukataan vahingossa, tästä ei tarvitse ilmoittaa.

Puolustusministeriön näkemyksen mukaan Effi ry:n lausunnossaan esittämää tilannetta koskisi näin saatujen tietojen hetihävittämisvelvollisuus. Käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 81 §:n mukaan tiedustelumenetelmällä saatu tieto olisi hävitettävä viipymättä sen jälkeen, kun on käynyt ilmi, ettei tietoa tarvita tai tietoa ei saa käyttää sotilastiedustelun tehtävien hoitamiseksi taikka tietoa ei tarvita maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi.

Hetihävittämisvelvollisuuden voidaan katsoa sisältävän myös tiedon hyödyntämiskiellon, sillä tällaista tietoa ei olisi missään vaiheessa pitänyt tulla tiedustelumenetelmien käytön yhteydessä ilmi.

Hallituksen esityksessä tiedustelutoiminnan valvonnasta (HE 199/2017 vp.) esitetään säädettäväksi uudesta viranomaisesta, tiedusteluvaltuutetusta. Tiedusteluvaltuutetun tehtävänä olisi tiedustelutoiminnan oikeudellinen valvonta. Kyseisen hallituksen esityksen lakiehdotuksessa säädettäisiin myös subjektiivisesta oikeudesta pyytää tiedusteluvaltuutettua ryhtyä tarvittaviin toimiin, jos henkilö kokee joutuneensa tiedustelumenetelmien käytön kohteeksi.

Ilmoitusvelvollisuus ei ole EIT:n vakiintuneen ratkaisukäytännön mukaisesti absoluuttinen, sillä se voisi vaarantaa niitä pitkän tähtäimen tavoitteita, joiden vuoksi tiedustelumenetelmän käyttö aloitettiin. Lisäksi asiaa on käsitelty tarkemmin valiokunnalle toimitetussa muistiossa 22.2.2018.

17. Yrityssalaisuudet

EK ja Google kiinnittävät lausunnoissaan huomiota yrityssalaisuuden suojaan. EK pitää esitystä hyvänä, mutta muistuttaa, että yrityssalaisuuksia koskevasta tiedonluovutusrajoituksesta olisi perusteltua säätää perustelujen sijaan pykälätasolla. Google esittää huolensa siitä, ettei lakiehdotus aseta rajoituksia sille, minkälaista tietoa tiedusteluviranomainen

saa ilmaista muille toimijoille. Ongelmallista on myös se, ettei ole olemassa ulkopuolista tahoa, joka valvoisi, minkälaista tietoa tiedusteluviranomainen ilmaisee muille yksittäisille toimijoille. Google katsoo, että kaikkien lainsäädäntöön tulisi sisällyttää yleinen pääsääntö, jossa tällainen tietojen ilmaiseminen kielletään.

Lausunnonantajien huomiot koskien yrityssalaisuuden suojaa ovat perusteltuja.

Sotilastiedusteluviranomaisen oikeudesta luovuttaa tietoja ehdotetaan säädettäväksi muun muassa käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 17 §:ssä ja 19 §:ssä (Kansainvälinen yhteistyö) sekä 71 §:ssä (Haitallista tietokoneohjelmaa tai -käskyä koskevien tietojen luovuttaminen viranomaiselle, yritykselle tai yhteisölle).

Kansainvälistä yhteistyötä koskevan 19 §:n mukaan sotilastiedusteluviranomainen voisi salassapitosäännösten estämättä luovuttaa tietoja kansainvälisessä yhteistyössä, jos tietojen luovuttaminen ei ole vastoin kansallista etua. Tietojen luovuttaminen kansainvälisessä yhteistyössä tulisi ensinnäkin perustua sotilastiedusteluviranomaisen tehtävään. Käytännössä kyse voisi olla tiedustelumenetelmien tekniikkaa ja taktiikkaa, haittaohjelmia koskevista tiedoista tai turvallisuusuhkia koskevista analyyseistä taikka muusta sellaisesta tiedosta, jonka luovuttaminen olisi Suomen intressien mukaista.

Tiedon luovuttamisen tulee toisaalta aina olla kansallisen edun mukaista. Tällaisen edun piiriin kuuluvat esimerkiksi tiedot Suomen poliittisista tai taloudellisista suhteista toisen valtion kanssa, sotilastiedustelua tai sotilaallista maanpuolustusta koskevat tiedot taikka tiedot kansainvälisen tiedusteluyhteistyön turvaamiseksi.

Lisäksi kansallisen edun arvioinnissa olisi huomioitava muutkin sellaiset seikat, jotka saattaisivat huonontaa Suomen kansallista etua. Suomen edun mukaista ei olisi esimerkiksi luovuttaa vieraan valtion tiedusteluviranomaiselle tietoja suomalaisten yritysten yrityssalaisuuksista tai muita tietoja, jotka esimerkiksi heikentäisivät Suomen alueella oleskelevien perus- ja ihmisoikeuksia

Tietojen luovuttamisen hyväksyttävyyttä tulisi näin ollen arvioida yhtäältä kansallisen turvallisuuden suojaamisintressin ja toisaalta kansallisten etujen turvaamisintressin kannalta. Tässä kokonaisarvioinnissa sotilastiedusteluviranomaisen olisi otettava huomioon myös luovutettavan tiedon ominaisuudet sekä tiedon vastaanottajana oleva taho.

Puolustusministeriö pitää edellä käsiteltyä esitettyä sääntelyä riittävänä.

18. Rajavartiolaitoksen asema sotilastiedustelutoiminnassa

18.1 Sotilastiedusteluviranomaisen määritelmä

Rajavartiolaitos toteaa, että käsiteltävänä olevan hallituksen esityksen 10 §:n perusteissa on mainittuna Rajavartiolaitos sotilastiedusteluviranomaista tukevana viranomaisena eikä Rajavartiolaitosta ole esitettyssä pykälässä nimenomaisesti mainittu.

Perustuslain 10 §:n muuttamista koskevassa hallituksen esityksessä (HE 198/2017 vp.) käsitellään kattavasti kansallisen turvallisuuden käsitettä. Pykälän yksityiskohtaisten perustelujen mukaan ilmaisu ”kansallinen turvallisuus” sisältäisi sen, ettei tietoa uhkaavasta toiminnasta voisi hankkia mikä tahansa turvallisuuteen liittyviä tehtävien hoitava viranomainen, vaan tiedonhankinta voitaisiin lailla osoittaa vain kansallisesta turvallisuudesta

huolehtivien viranomaisten tehtäväksi. Nykyisessä valtion organisaatiossa nämä tehtävät on osoitettu sotilastiedustelun osalta Puolustusvoimien pääesikunnalle ja tiedustelulaitokselle sekä siviilitiedustelun osalta suojelupoliisille. Edellä sanottu ei kuitenkaan tarkoita sitä, etteikö myös muilta tahoilta niiden omia tehtäviään hoitaessaan voisi tulla tietoa, jolla olisi merkitystä kansallisen turvallisuuden kannalta.

Käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 10 §:n tarkoituksena on kuvata perustuslain muutoksen perusteluista vastaavasti ne sotilasviranomaiset, jotka hoitavat sotilastiedustelua ja hankkivat tietoa käyttämällä muun muassa laissa säädettyjä tiedustelumenetelmiä.

Säännöksen perusteluissa on lisäksi kuvattuna sotilastiedustelulle tulevan tiedon kokonaisuuskenttää. Sotilastiedustelussa käytettävä tieto ei ole aina tiedustelumenetelmin saatua, vaan valtaosa tiedosta tulee julkisista lähteistä ja menetelmillä, joista ei ole tarpeen säätää. Tästä esimerkkinä säännöksen perusteluissa on mainittuna esimerkiksi Puolustusvoimien logistiikkalaitos, joka esimerkiksi normaaliin hankintaprosessiinsa liittyen saa kaupallisessa tarkoituksessa tietoja. Nämä tiedot saattavat olla myös sotilastiedustelun kannalta tarpeellisia. Kyseessä ei ole kuitenkaan erityisiä lailla säädettäviä toimivaltuuksia edellyttävä toiminta.

Perusteluissa esimerkillä on kuvattu sitä, mistä tietoa tulee sotilastiedusteluviranomaiselle ja että kaikki tieto ei vaadi nimenomaisesti sotilastiedusteluviranomaisen tiedustelumenetelmän käyttöä.

Käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 17 §:ssä esitetään, että sotilastiedusteluviranomainen voi toimia yhteistyössä muiden viranomaisten ja yhteisöjen kanssa. Nimenomaan tämän yhteistyön kautta muut viranomaiset, kuten Rajavartiolaitos, voisi antaa salassapitosäännösten estämättä sotilastiedustelun kannalta tarpeellista tietoa, mitä ne ovat saaneet omien tehtäviensä, kuten aluevalvontatehtävien, kautta. Vastaavasti sotilastiedusteluviranomainen voi luovuttaa muille viranomaisille ja yhteisöille näille tarpeellista tietoa esimerkiksi tilannekuvasta tai tietystä mahdollisesti toteutuvasta tapahtumasta. Säännös vastaa perusteluiltaankin, mitä hallituksen esityksessä siviilitiedustelua koskevaksi lainsäädännöksi (HE 202/107 vp.) 1. lakiehdotuksen 5 a luvun 55 §:ssä esitetään. Ristiriitaisesti Rajavartiolaitos ei ole HE 202/2017 osalta kiinnittänyt huomiota siihen, että kyseisen 55 §:n perusteluissa todetaan käsiteltävänä olevaa hallituksen esitystä vastaavasti, että Rajavartiolaitos voi avustaa suojelupoliisia siviilitiedustelussa.

Puolustusministeriö katsoo, ettei Rajavartiolaitosta tai mitään muutakaan tahoa ole tarkoituksenmukaista mainita erikseen 10 §:ssä, joka koskee nimenomaisesti sotilastiedusteluviranomaisen määritelmää, jolla on erityistä merkitystä tiedustelumenetelmiä käyttävän viranomaisen määrittelemisessä. Lisäksi sotilastiedusteluviranomaisen määritelmä liittyy olennaisesti tiedusteluviranomaiselle säädettyisiin vastuisiin ja viranomaiseen kohdistettavaan valvontaan sekä siihen, ettei viranomaiselle pääse muodostumaan valtaketjittymään esitutkinta-, rikostorjunta- ja tiedustelutoimivaltuuksien kautta, minkä voidaan katsoa vaarantavan myös perustuslain 21 §:ssä turvatun oikeudenmukaisen oikeudenkäynnin, esitutkinnan puolueettomuuden sekä viime kädessä oikeusvaltioperiaatteen toteutumisen.

Puolustusministeriön näkemyksen mukaan Rajavartiolaitos on yksi tärkeimmistä yhteistyötahoista maanpuolustuksen alalla. Puolustusministeriö pitää tärkeänä sitä, että tähänastinen hyvä ja tärkeä yhteistyö jatkuu edelleen sellaisena kuin se on ollut. Nyt käsiteltävänä olevalla hallituksen esityksellä ei pitäisi olla siihen vaikutusta.

18.2 Rajavartiolaitoksen virkamies tiedustelumenetelmien käyttäjänä

Rajavartiolaitos esittää, että tietyissä tilanteissa heidän esitutkinta- ja rikostorjuntatoimivaltuuksia käyttävät virkamiehet voisivat käyttää sotilastiedusteluviranomaisen ohjauksen ja valvonnan alaisina käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 4 luvussa tarkoitettuja tiedustelumenetelmiä, mutta samanaikaisesti rajavartiolaitoksen virkamiehet säilyisivät kuitenkin omien esimiestensä alaisina.

Puolustusministeriön näkemyksen mukaan Rajavartiolaitoksen virkamiesten käyttämiselle käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen tarkoituksessa ei ole tarvetta.

Esitutkinta- ja rikostorjuntaviranomaisen toimivaltuuksissa ei ole kyse tiedustelutoiminnasta, jossa pyritään tunnistamaan ja kartoittamaan Suomeen kohdistuvia ulkoisia uhkia mahdollisimman varhaisessa vaiheessa.

Esitutkinta- ja rikostorjuntaa hoitavat virkamiehet eivät ole suoraan käytettävissä sotilastiedustelutoimintaan, koska he ovat saaneet koulutuksen ja osaamisensa nimenomaan niihin tehtäviin. Tarkoituksenmukaisinta olisikin, että esitutkinta- ja rikostorjuntaan resursoidut virkamiehet hoitavaisivat heille kuuluvia tehtäviä.

Lisäksi toisen hallinnonalan esitutkinta- ja rikostorjuntaviranomaisen virkamiehen toimiminen sotilastiedustelutoiminnassa olisi vaikeasti valvottavissa ja muodostaisi suuren riskin siitä, että tiedustelutoiminnassa saatuja tietoja käytettäisiin esitutkinnassa tai rikostorjunnassa niin sanottuja palomuurisäännöksiä kiertäen (käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 76 ja 77 §).

Oman ongelmansa valvonnan osalta tuo myös se, että Rajavartiolaitoksen esikunta toimii samalla sisäministeriön rajavartio-osastona.

Puolustusministeriö näkee, että viranomainen, jolla olisi useita eri perusteella käytettäviä toimivaltuuksia samanaikaisesti tai joka voisi tällaisia käyttää, on kritiikille altis. Viranomaisen valtakeskittymää pitäisi välttää, sillä se voisi vaarantaa oikeusvaltion periaatteen, esitutkinnan esteettömyyden ja tasapuolisuusperiaatteen toteutumisen sekä oikeudenmukaisen oikeudenkäynnin.

Nyt käsiteltävänä olevassa hallituksen esityksessä on kiinnitetty erityistä huomiota siihen, että esitutkintaa ja rikostorjuntaa koskevat tehtävät ja tekijät on eriytetty sotilastiedustelun tehtävistä ja tekijöistä.

18.3 Rajavartiolaitoksen mahdollisuus kirjata henkilötietoja sotilastiedustelurekisteriin

Rajavartiolaitos toteaa lausunnossaan, ettei heillä ole mahdollisuutta kirjata henkilötietoja sotilastiedustelurekisteriin.

Henkilötietojen kirjaamisen osalta on huomattava, että eduskunnassa on käsiteltävänä hallituksen esitys laiksi henkilötietojen käsittelystä Puolustusvoimissa (HE 13/2018 vp.). Kyseisen hallituksen esityksen 1. lakiehdotuksessa esitetään säännöstä, jonka perusteella muun muassa poliisille, Tullille ja Rajavartiolaitokselle voidaan antaa oikeus kirjata henkilötietoja sotilastiedustelurekisteriin. Tietoja, joita eri viranomaiset ovat saaneet omia tehtäviään hoitaessaan, voitaisiin kirjata Puolustusvoimien sotilastiedustelutehtävän suorittamiseksi. Tietojen kirjaaminen ei edellytä erikseen säädettyä sotilastiedustelutehtävää. Tulli ja poliisi eivät ole nähneet tätä esteenä yhteistyölle.

Muilta kuin henkilötietojen osalta erityistä sääntelyä ei tarvita, vaan toiminta tapahtuisi käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 17 §:n nojalla.

18.4 Yhteenveto

Puolustusministeriö ei näe esteitä sille, etteikö tähän mennessä tärkeä ja hyvin toimiva yhteistyö Rajavartiolaitoksen kanssa voisi jatkua käsiteltävänä olevasta hallituksen esityksestä, siinä muodossa kuin se on, huolimatta.

Puolustusministeriö kuitenkin tunnistaa, että Rajavartiolaitoksen esiin nostamat huolet liittyvät rikostorjunnan alaan. Puolustusvoimien ja Rajavartiolaitoksen rikostorjuntaa koskevien lakien osalta ei ole säädetty yhteistoiminnasta, minkä puolustusministeriö näkee puutteena. Tämä edellyttää muutoksia sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annettuun lakiin (255/2014).