HE 104/2026 vp

Hallituksen esitys eduskunnalle laiksi sotilastiedustelusta annetun lain muuttamisesta ja siihen liittyviksi laeiksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan muutettavaksi sotilastiedustelusta annettua lakia, puolustusvoimista annettua lakia, rajavartiolakia ja rikoslakia sekä viittä muuta lakia.

Sotilastiedustelusta annetun lain tietoliikennetiedustelua koskevaa sääntelyä ehdotetaan muutettavaksi siten, että tietoliikennetiedustelussa kyetään paremmin määrittämään hakuehtoja tietoliikennetiedustelun tarkemmaksi kohdentamiseksi. Sotilastiedusteluviranomaiselle mahdollistettaisiin teknisten tietojen käsittely viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi. Tietoliikennetiedustelusta poistettaisiin kielto käyttää viestin sisältöön meneviä hakuehtoja sekä kielto käyttää Suomessa olevaa tai oletettavasti olevaa telepäätelaitetta tai -osoitetta hakuehtona. Esityksessä ehdotetaan, että muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta ilmoittamisesta luovuttaisiin.

Esityksessä ehdotetaan säädettäväksi uudesta tietojärjestelmätiedustelun toimivaltuudesta, jonka avulla voitaisiin hankkia tietoa sotilaallisesta toiminnasta tai kansallista turvallisuutta vakavasti uhkaavaan toimintaan hyödynnettävän tietojärjestelmän toiminnasta Suomessa.

Rajavartiolaitokselle ehdotetaan säädettäväksi toimivalta avustaa sotilastiedusteluviranomaista ja suorittaa tiettyjä yksittäisiä tiettyjen tiedustelumenetelmien käyttöön liittyviä toimenpiteitä sotilastiedusteluviranomaisen pyynnöstä. Lisäksi sotilastiedusteluviranomaisen ulkopuoliselle henkilölle mahdollistettaisiin rajatuissa tilanteissa sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa toimiminen.

Sotilastiedusteluviranomaisen ja eräiden muiden viranomaisten välistä tietojenvaihtoa esitetään laajennettavaksi velvoitteidenhoitoselvitysten laatimiseksi ja tilanteissa, joissa tietojen saaminen olisi välttämätöntä tiedustelutehtävän suorittamiseksi. Esityksessä ehdotetaan lisäksi tehtäväksi yksittäisiä säädöshuoltoon liittyviä muutoksia sekä käytännön tiedustelutoiminnassa havaituista tarkennustarpeista johtuvia muutoksia.

Puolustusvoimista annettuun lakiin ehdotetaan lisättäväksi säännökset tiedonhankinnasta yleisesti saatavilla olevista lähteistä ja peitteen käyttämisestä tällaisessa tiedonhankinnassa.

Esityksellä toteutettaisiin pääministeri Petteri Orpon hallituksen hallitusohjelman kirjauksia tiedustelulainsäädännön kehittämisestä.

Ehdotetut lait on tarkoitettu tulemaan voimaan mahdollisimman pian.

———

SISÄLLYS

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

Sotilastiedustelusta annettu laki (590/2019) tuli voimaan 1.6.2019. Laki sisältää keskeiset säännökset sotilastiedustelutoiminnasta, kuten toimivaltuudet tietoliikennetiedustelussa. Tiedustelulainsäädännön kokonaisuus on toiminut tarkoitetulla tavalla. Lainsäädännön myötä uhkiin liittyvän tilannekuvan voidaan katsoa parantuneen jopa merkittävästi. Viranomaisten laajentuneiden toimivaltuuksien lisäksi niiden valvontaa on toteutettu tehokkaasti ja tuloksellisesti. Toiminnan käynnistyminen, teknologian ja globaalin toimintaympäristön muutos ovat kuitenkin tuoneet esiin muutostarpeita, joita ei ole pystytty voimassa olevan lain valmistelun yhteydessä tunnistamaan.

Eduskunta on hyväksynyt tiedustelulainsäädännöstä annetun valtioneuvoston selonteon (EK 70/2022 vp. – VNS 11/2021 vp.) johdosta seuraavan hallintovaliokunnan mietinnön (HaVM 35/2022 vp.) mukaisen kannanoton. Kannanotossa eduskunta edellyttää, että hallitus muutoinkin tarkastelee tiedustelulainsäädännön toimivuutta, vaikutuksia ja mahdollisia muutostarpeita, huolehtii lainsäädännön ajantasaisuudesta muuttuvassa toimintaympäristössä sekä varmistaa tiedustelutoiminnan ja sen valvonnan riittävät resurssit.

Lisäksi lainsäädännön muutostarpeita on tunnistettu myös eduskunnalle toimitetussa selvityksessä sotilastiedustelulainsäädännön toimivuudesta.

Pääministeri Petteri Orpon hallituksen hallitusohjelmassa (jakso 10.1 Kansallista turvallisuutta ja yhteiskunnan kriisinkestävyyttä vahvistetaan) on useita tiedustelulainsäädännön kehittämistä koskevia kirjauksia. Tiedustelulainsäädäntö on osa maanpuolustusta ja kansallisen turvallisuuden suojaamista.

Hallitusohjelman mukaan hallitus kehittää tiedustelulainsäädäntöä viranomaisten toimintakyvyn turvaamiseksi tiedustelutoiminnasta saatujen kokemusten, teknologisen kehityksen ja Suomen Nato-jäsenyyden johdosta. Tiedustelulainsäädäntöä tarkistetaan tiedustelutoimivaltuuksien sekä tiedonsaanti- ja luovutusoikeuksien osalta vastaamaan muuttuneen turvallisuus- ja kybertoimintaympäristön vaatimuksia.

Hallitus varmistaa, että tiedustelutoimivaltuudet vastaavat teknologiseen kehitykseen. Mahdollistetaan muun muassa tiedustelu laite- ja järjestelmäketjuihin ja viestin sisältöön kohdistuvien hakuehtojen käyttö tiedustelutoiminnassa. Lisäksi hallitusohjelman mukaan arvioidaan tiedustelutoimivaltuuksien laajentaminen vakituiseen asumiseen käytettävään tilaan.

Hallitusohjelman mukaan arvioidaan viranomaisten avustamisvelvollisuuden laajentaminen Suomessa sijaitseville palveluntarjoajille, kuten konesaliyrityksille. Selvitetään mahdollisuus säätää toimivaltuus käsitellä ja hyödyntää avoimista lähteistä saatavia suuria tietovarantoja.

Hallitusohjelman mukaan hallituskauden aikana säädetään toimivaltuus vaikuttaa ulkomailla olevaan laitteeseen tai ohjelmistoon, jota käytetään Suomen kansallista turvallisuutta vaarantavaan kybervakoiluun tai -vaikuttamiseen.

Lisäksi hallitusohjelman mukaan säädetään Rajavartiolaitokselle oikeus käyttää suorituskykyä tiedusteluviranomaisen tukemiseen ja oikeus tietojen luovuttamiseen tiedusteluviranomaiselle.

1.2 Valmistelu

Puolustusministeriö on 28.8.2024 asettanut hankkeen valmistelemaan ehdotukset sotilastiedustelusta annetun lain ja siihen liittyvien lakien tarkistamiseksi. Hankkeen toimikaudeksi on asettamispäätöksessä asetettu 29.8.2024–01.06.2025. Hankkeen toimikautta on jatkettu 26.5.2025 annetulla päätöksellä 31.12.2025 saakka. Hanketta varten on asetettu työryhmä, johon kuuluivat puolustusministeriön, Pääesikunnan, sisäministeriön ja suojelupoliisin edustajat. Työryhmään kuuluivat pysyvinä asiantuntijoina edustajat tiedusteluvalvontavaltuutetun toimistosta sekä Rajavartiolaitoksen esikunnasta.

Hallituksen esityksen luonnoksesta järjestettiin lausuntokierros 27.11.2025-16.1.2026. Lausuntokierros toteutettiin Lausuntopalvelu.fi -palvelun kautta. Hallituksen esitysluonnokseen annetut lausunnot ovat julkisesti saatavilla lausuntopalvelussa osoitteessa lausuntopalvelu.fi. Lisäksi luonnosta koskevat lausunnot ja hankkeen asiakirjat ovat saatavilla valtioneuvoston verkkosivustolta tunnuksella PLM007:00/2024.

2 Nykytila ja sen arviointi

2.1 Turvallisuusympäristön muutos

2.1.1 Selonteot

Maailmanpolitiikan valtasuhteiden murros vaikuttaa Suomen puolustuksen toimintaympäristöön. Kiihtyvä strateginen kilpailu ja demokratioiden ja autoritääristen valtioiden välinen globaali vastakkainasettelu ovat johtamassa monenkeskisen yhteistyön sirpaloitumiseen ja alueellistumiseen. Yhdysvaltojen ja Kiinan välillä käydään kilpailua poliittisesta, sotilaallisesta, taloudellisesta ja teknologisesta johtoasemasta maailmassa. Venäjä on puolestaan asemoinut itsensä vastakkainasetteluun Yhdysvaltoja ja muita länsimaita vastaan, osittain yhteistyössä Kiinan kanssa.

Suomen turvallisuusympäristön muutosta on kuvattu kattavasti keväällä 2022 julkaistussa valtioneuvoston ajankohtaisselonteossa turvallisuusympäristön muutoksesta[1] ja vuoden 2024 puolustusselonteossa[2]. Selontekojen mukaan Suomen ja Euroopan turvallisuus- ja toimintaympäristössä on tapahtunut perustavanlaatuinen ja pitkäkestoinen muutos Venäjän Ukrainaa vastaan käynnistämän hyökkäyssodan myötä. Yhteiskunnan kriisinsietokyvyn, kansallisen puolustuskyvyn ja sisäisen turvallisuuden ylläpitämisen merkitys Suomen turvallisuudelle korostuu.

Venäjän hyökkäyssodalla Ukrainaan on perustavanlaatuisia ja pitkäkestoisia vaikutuksia turvallisuusympäristöön Euroopassa ja Suomen lähialueilla. Venäjä on osoittanut, ettei se kunnioita toisten valtioiden suvereniteettia ja alueellista koskemattomuutta ja on toimillaan loukannut YK:n peruskirjaa sekä rikkonut eurooppalaista sopimuspohjaista turvallisuusjärjestystä.

---

[1] Ajankohtaisselonteko turvallisuusympäristön muutoksesta. Valtioneuvoston julkaisuja 2022:18. http://urn.fi/URN:ISBN:978-952-383-772-0

[2] Valtioneuvoston puolustusselonteko. Puolustusministeriön julkaisuja 2024:5. http://urn.fi/URN:ISBN:978-951-663-423-7

Euroopan ja Suomen turvallisuustilanne on vakavampi ja vaikeammin ennakoitavissa kuin kertaakaan kylmän sodan päättymisen jälkeen ja tämän muutoksen arvioidaan olevan pitkäkestoinen. Valtioneuvoston ajankohtaisselonteon (2022) mukaan Venäjän vaatimukset ja sotilaalliset toimet Euroopan turvallisuusarkkitehtuurin muuttamiseksi vaikuttivat myös Suomen ulko-, turvallisuus- ja puolustuspoliittiseen liikkumatilaan. Suomi haki puolustusliitto Naton jäsenyyttä 17.5.2022. Suomesta tuli Naton jäsen 4.4.2023.

Venäjä on lisännyt Suomen ja kaikki muut EU-maat niin sanotulle epäystävällisten valtioiden listalle. Venäjän hyökkäyssota Ukrainaa vastaan on vaikuttanut perustavanlaatuisesti Suomen ja Venäjän kahdenvälisiin suhteisiin.

Turvallisuusympäristön muutoksen pitkäaikaisuudesta ja vakavuudesta huolimatta Suomeen ei kohdistu välitöntä sotilaallista uhkaa. Sotilaalliseen voimankäyttöön Suomea vastaan tai sillä uhkaamiseen tai poliittiseen painostukseen kuitenkin varaudutaan. Ukrainaan kohdistetut sotatoimet osoittavat, että nopea toimintavalmius, kyky vastata pitkäkestoiseen sotilaalliseen painostukseen ja kyky torjua laajamittaisia hyökkäysoperaatioita useassa suunnassa samanaikaisesti on tärkeää. Valtioneuvoston ajankohtaisselonteossa (2022) todetaan, että ”mikäli Suomi hakisi Naton jäsenyyttä, tulisi varautua laaja-alaiseen ja vaikeasti ennakoitavaan vaikuttamiseen ja riskeihin, kuten esimerkiksi jännitteiden kasvuun Suomen ja Venäjän välisellä rajalla. Suomi vahvistaa varautumistaan laaja-alaisten hybridivaikuttamisen keinojen kohteeksi joutumiseen sekä vaikuttamisen estämiseen ja siihen vastaamiseen.”

Venäjän hyökkäyksellä Ukrainaan on ollut laajamittaisia kielteisiä vaikutuksia globaalisti ja erityisesti Euroopan turvallisuuteen. Suomi on vastannut Venäjän hyökkäyssotaan osana Euroopan unionia. Venäjä on nostanut Ukrainan lisäksi vihollisekseen kollektiivisesti ne länsimaat, jotka ovat mukana asetetuissa vastatoimissa. Vallitsevissa oloissa Suomen kriittiseen infrastruktuuriin kohdistuva tiedustelun ja vaikuttamisen uhka on kohonnut sekä fyysisessä että kyberympäristössä Venäjän Ukrainassa aloittaman hyökkäyssodan sekä Suomen Nato-jäsenyyden myötä. Kiinteistöjen merkitys kansalliselle turvallisuudelle vaihtelee merkittävästi kiinteistön käyttötarkoituksen, sijainnin, kiinteistöllä sijaitsevien rakennusten ja rakennelmien sekä kiinteistöllä tai niiden lähistöllä mahdollisesti sijaitsevan kriittisen infrastruktuurin ja strategisten kohteiden perusteella.

Turvallisuustilanne Euroopassa ja Suomen lähialueilla on epävakaa ja turvallisuusympäristön muutos heijastuu myös Suomen rajaturvallisuustilanteeseen, mikä on näkynyt esimerkiksi maahantulon välineellistämisenä Venäjän toimesta. Tämä on ollut yksi keinoista pyrkiä vaikuttamaan Suomen kansalliseen turvallisuuteen ja yleiseen järjestykseen. Suomen on varauduttava siihen, että painostaminen jatkuu pitkäaikaisesti, ja että se saa aiempaa laajempia ja vakavampia muotoja. Kansallisen turvallisuuden uhkiin tulee varautua riittävästi niitä ennalta ehkäisten. Sotilaallisten voimakeinojen käyttäminen Suomea vastaan on Suomen Nato-jäsenyyden myötä entistä korkeamman kynnyksen takana. Suoran aseellisen vaikuttamisen kynnyksen ollessa aiempaakin korkeampi, korostuvat muut laaja-alaisen vaikuttamisen keinot. Siten myös kiinteistöjen omistuksen merkityksen Suomen kansalliselle turvallisuudelle voidaan katsoa korostuneen entisestään.

Venäjä käyttää laaja-alaisen vaikuttamisen keinoja – jotka käsittävät hybridivaikuttamisen sekä sen osana tarvittaessa sotilaallisen voimankäytön – edistääkseen strategisia tavoitteitaan. Venäjä käyttää näitä keinoja jatkuvasti myös avoimen konfliktin kynnyksen alapuolella, ja se kykenee säätelemään joustavasti vaikuttamisen intensiteettiä ja keinovalikoimaa tavoitteidensa saavuttamiseksi. Tavoitteena on muiden muassa vaikuttaa kohdemaan yhtenäisyyteen, päätöksentekoon ja kansalaismielipiteeseen sekä lisätä vastakkainasettelua, luoda pelkoa ja hämärtää tilannekuvaa. Poliittisten tavoitteidensa tukemiseksi Venäjä jatkaa aktiivista

tiedustelu- ja vaikuttamistoimintaa perinteisen tiedonhankinnan ja agenttitoiminnan ohella myös tietoverkoissa. Venäjä hyödyntää toiminnassaan valtiollisten viranomaisten lisäksi yhtä lailla yrityksiä ja koulutus- ja tutkimuslaitoksia kuin rikollisryhmittymiä ja aktivisteja.

Mahdollisuudet hyödyntää kybertoimintaympäristöä vihamielisissä tarkoituksissa lisääntyvät, kun infrastruktuuri ja teknologia kehittyvät ja käyttäjämäärät kasvavat. Vihamieliset toimijat kohdistavat jatkuvasti länsimaihin tietoverkkotiedustelua, kybervakoilua ja kybervaikuttamista ja pyrkivät vaikuttamaan fyysisesti niiden kriittiseen infrastruktuuriin. Valtiollisten toimijoiden lisäksi vihamielisestä toiminnasta vastaavat entistä enemmän myös poliittisesti motivoituneet tai valtiollisesti ohjatut ei-valtiolliset toimijat.

Suomen on aina ja kaikissa turvallisuustilanteissa varauduttava Suomeen kohdistuvaan sotilaalliseen voimankäyttöön sekä sillä uhkaamiseen ja poliittiseen painostukseen. Kansalliselle turvallisuudelle aiheutuva uhka voi konkretisoitua hyvinkin pitkällä, kymmenien vuosien aikajänteellä ja uhkaa kansalliselle turvallisuudelle voi olla vaikea todentaa tiettynä ajanhetkenä. Suomi huolehtii kyvystään vastata pitkään jatkuvaan sotilaalliseen painostukseen sekä pitkäkestoiseen ja laajamittaiseen sodankäyntiin kansallisin voimavaroin ja osana Natoa. Suomeen kohdistuvaa sotilaallista painostusta ja voimankäyttöä voidaan ehkäistä vain vahvalla pelotteella ja puolustuksella, mikä edellyttää riittävää resursointia.

Suomen sotilaallinen puolustusjärjestelmä on osajärjestelmistä muodostuva kokonaisuus, joka tuottaa sotilaallisessa maanpuolustuksessa vaadittavat suorituskyvyt. Puolustusjärjestelmän valmiutta säädellään uhkatasoa vastaavaksi. Kykyä kaikkien operatiivisten toimintaympäristöjen valvontaan on kehitetty viimeisten vuosien aikana. Erityisesti avaruus- ja kybertoimintaympäristöt, informaatioulottuvuus sekä tiedustelutoimiala vaativat tiivistä yhteistyötä hallinnonalojen ja muiden keskeisten toimijoiden välillä, mukaan lukien kansainväliset kumppanit.

Puolustusvoimien yhteisiä suorituskykyjä kehitetään tukemaan kansallista puolustuskykyä ja liittokunnan tarpeita. Sotilastiedustelujärjestelmää kehitetään mahdollistamaan ennakkovaroitus ja valtiojohdon tukeminen ja syvä ja suunnitelmallinen tulenkäyttö sekä hyödyntämään liittokunnan tuki. Kaukovaikuttamiskyvyn korkealla valmiudella ja ulottuvuudella ennaltaehkäistään ja rajoitetaan hyökkääjän mahdollisuuksia toimeenpanna, johtaa ja ylläpitää operaatioita.

Puolustusvoimien yhteisiä suorituskykyjä ovat sotilastiedustelu, johtamisjärjestelmä, kaukovaikutteiset asejärjestelmät, erikoisjoukot ja logistiikka. Toimintaympäristön muutos ja teknologioiden kehittyminen ovat asettaneet uusia vaatimuksia sotilastiedustelulle erityisesti tiedonhankinnan osalta. Tiedustelun tapahtuessa enenevässä määrin verkossa sotilastiedustelusta annetun lain toimivaltuudet sekä tiedustelukykyjen kehittäminen ovat edelleen parantaneet kykyä muodostaa tilannekuvaa ja antaa ennakkovaroitus valmiuden säätelemiseksi. Sotilastiedustelun lainsäädännön arviointi on jatkuvaa. Sotilastiedustelun suunnitelmallinen integrointi Naton tiedustelutoimintaan on täydentänyt tilannekuvaa ja ennakkovaroituksen antamista. Sotilastiedustelun ja suojelupoliisin tiivis yhteistyö on vankka perusta suomalaiselle tiedustelulle kaikissa yhteyksissä.

Puolustushallinto varautuu laaja-alaisen vaikuttamisen ennaltaehkäisyyn ja torjuntaan yhdessä muiden turvallisuustoimijoiden kanssa osana kokonaisturvallisuuden mallia ja kokonaismaanpuolustuksen kehittämistä. Vaikuttamisen tunnistaminen, siihen varautuminen ja vaste edellyttävät tiedustelun, erikoisjoukkojen, kyberpuolustuksen, informaatiopuolustuksen ja strategisen viestinnän kehittämistä kansallisessa ja kansainvälisessä yhteistyössä.

Sotilastiedustelujärjestelmää kehitetään niin, että se mahdollistaa ennakkovaroituksen ja valtiojohdon tukemisen sekä syvän ja suunnitelmallisen tulenkäytön ilman viivettä ja sallii liittokunnan tuen hyödyntämisen. Kansallisen järjestelmän yhteensopivuutta liittolaisten järjestelmien kanssa parannetaan. Yhteensopivuuden ohella keskiössä on tietojen yhdistely ja jakaminen operatiivisille käyttäjille. Kykyä käyttää tiedustelumenetelmiä monipuolisesti normaali- ja poikkeusoloissa kehitetään.

Suomi huolehtii kansallisen tiedustelun kehittämisestä vastaamaan lisääntyneisiin vaatimuksiin ja turvallisuusympäristön muutoksiin. Suomella on valmius tunnistaa, ennaltaehkäistä ja torjua vakoilua, hybridivaikuttamista, terrorismia ja sotilaallista uhkaa niin fyysisessä kuin kybermaailmassa. Jo vakiintuneen kansainvälisen tiedusteluyhteistyön lisäksi Suomi osallistuu aktiivisesti Naton tiedusteluyhteistyöhön.

2.1.2 Tiedusteluviranomaisten katsaukset

Sotilastiedustelun julkisessa katsauksessa[3] vuodelta 2025 todetaan, että Suomen Nato-jäsenyys, tiivistynyt kansainvälinen puolustusyhteistyö sekä Euroopan turvallisuusympäristön muutos ovat lisänneet Venäjän tietotarpeita Suomesta. Tiedustelupalveluiden mielenkiinnon kohteita ovat etenkin Suomen Nato-politiikan toimeenpano, puolustusyhteistyön kehittyminen, kansainvälisten joukkojen toiminta Suomessa sekä Naton esikuntien ja joukkorakenteiden kehittäminen. Lisäksi Ukrainan sodan aikana on korostunut tarve hankkia tietoa puolustusvälineteollisuuden tuotantokapasiteetista ja Puolustusvoimien materiaalisen suorituskyvyn kehittymisestä. Puolustusjärjestelmään kohdistuva tiedustelun uhka kohdistuu ensisijaisesti Puolustusvoimien suorituskykyihin ja käyttöperiaatteisiin sekä valmiuteen.

Suomen lähialueilla Venäjälle keskeisiä asioita ovat Kuolan niemimaalle sijoitetut strategiset suorituskyvyt, rajoittamaton pääsy Atlantille pohjoisten merireittien kautta sekä arktinen alue. Se pyrkii myös rajoittamaan Naton toimintaa Itämeren alueella ja heikentämään Suomen ja Ruotsin integroitumista Natoon sekä vaikuttamaan maiden Nato-jäsenyyksien sisältöön.

Venäjä on aloittanut sotilaspiirejä koskevan asevoimareformin. Suomen suunnalla toimivaa Leningradin sotilaspiiriä vahvennetaan suunnitelmien mukaan merkittävästi tulevaisuudessa. Kun edellä kerrotut muutokset saadaan päätökseen, ne kasvattavat Suomen lähialueella olevien joukkojen vahvuutta todennäköisesti noin 30 000:sta noin 80 000 sotilaaseen. On kuitenkin todennäköistä, että niin kauan kuin Ukrainan sota jatkuu nykyisenkaltaisena kulutussotana, Suomen lähialueella oleva sotilaallinen voima ei kasva merkittävästi. Ukrainan sodan päättymisen jälkeen Venäjä kuitenkin todennäköisesti priorisoi luoteista suuntaansa ja pyrkii nopeuttamaan uudistusten toimeenpanoa.

Venäjä pyrkii vaikuttamaan Suomen turvallisuuspoliittisiin ratkaisuihin ja antaa ymmärtää, että Naton infrastruktuurin sijoittaminen Suomeen johtaisi jännitteiden lisääntymiseen. Venäjä todennäköisesti lisää kaikkien laaja-alaisen vaikuttamisen keinojen käyttöä pyrkiessään aiheuttamaan hajaannusta Naton ja Euroopan unionin sisällä. Näihin keinoihin lukeutuvat kyber- ja informaatiovaikuttaminen, energiapolitiikka, vaikuttaminen energia- ja muuhun kriittiseen infrastruktuuriin, siirtolaisten ohjailu ja erilaiset tiedusteluoperaatiot.

---

[3] Sotilastiedustelun julkinen katsaus 2025. Pääesikunta.
https://puolustusvoimat.fi/documents/1948673/2014902/PV_sotilastiedustelu_raportti_2025_web.pdf/4de8d666-6bff-642d-2d07-df71154b33bd?t=1737029070219

Suojelupoliisin vuoden 2025 kansallisen turvallisuuden katsauksessa[4] on kuvattu toimintaympäristön muutosta tiedustelun osalta. Katsauksen mukaan Venäjä ja Kiina muodostavat merkittävimmän tiedustelullisen uhkan Suomelle. Venäjä yrittää hankkia Suomesta tietoa niin henkilö- kuin kybertiedustelun keinoin. Vaikuttaminen on aina kuulunut Venäjän tiedustelu- ja turvallisuuspalveluiden toimintaan, mutta sen kohteet ja aktiivisuus ovat vaihdelleet maailmanpoliittisen tilanteen mukaan. Natoon kuuluvat Venäjän rajanaapurit ovat sen tiedustelun erityisen mielenkiinnon kohteena. Venäjän ja länsimaiden välien viilennyttyä Venäjän vaikuttaminen on muuttunut astetta vakavampaan suuntaan, josta esimerkkinä voidaan pitää Venäjän sabotaasitoimintaa Euroopassa.

Venäjän tiedustelupalveluiden Suomeen kohdistama toiminta kyberympäristössä on ollut jo vuosien ajan erittäin aktiivista, mutta se on lisääntynyt ja tarkentunut viime aikoina entisestään. Vaikka Venäjän henkilötiedustelu on vaikeutunut, henkilötiedustelun uhka ei kuitenkaan ole pitkällä aikavälillä vähentynyt, sillä Venäjän tiedontarpeet eivät ole kadonneet minnekään. Sekä tiedustelun että laaja-alaisen vaikuttamisen tilannekuvassa entistä suurempaan rooliin ovat nousseet eri valtioiden käyttämät sijaistoimijat. Valtiollinen toimija pyrkii häivyttämään jälkensä välikäsien kautta, oli kyse sitten Venäjän, Kiinan tai Iranin toiminnasta. Sijaistoimijoiden avulla itsevaltaisten maiden voimaviranomaiset haluavat hämärtää todellisuutta, helpottaa tekojen kiistettävyyttä ja luoda uudenlaista epävarmuutta. Rekrytointi voidaan hoitaa sosiaalisessa mediassa ja maksu kryptovaluutoilla. Tehtävän suorittaja ei aina välttämättä itsekään tiedä, kenen lukuun toimii.

Venäjän turvallisuus- ja tiedustelupalveluilla on perinteisesti ollut pysyvää läsnäoloa niin Suomessa kuin muissa maissa. Tiedustelupalvelujen edustajat ovat toimineet pääosin diplomaattisen peitteen suojassa, mutta Venäjä pyrkii aikaisempaa enemmän hyödyntämään välikäsiä sekä muita peitteitä kuin diplomaattipeitettä.

Venäjän tiedustelun läsnäolo Suomessa ja muualla Euroopassa on kuitenkin merkittävästi vähentynyt hyökkäyssodan vastineena toteutettujen diplomaattipeitteellä toimineiden tiedustelu-upseerien karkotusten myötä. Tilanteeseen vaikuttavat myös matkustukseen kohdistuvat rajoitukset ja se, että yhä harvempi Suomessa haluaa sodan vuoksi olla tekemisissä venäläisten toimijoiden kanssa.

Venäjän henkilötiedustelun uhka ei kuitenkaan ole pitkällä aikavälillä vähentynyt.

Muuttunut toimintaympäristö on ajanut myös Venäjän tiedustelu- ja turvallisuuspalvelut muuttamaan toimintaansa. Venäjä pyrkii aikaisempaa enemmän hyödyntämään välikäsiä sekä muita peitteitä kuin diplomaattipeitettä. Ne eivät tule korvaamaan laajamittaisesti tai nopeasti diplomaattipeitteen hyödyllisyyttä. Venäjä yrittää myös edelleen sijoittaa tiedustelu-upseereitaan diplomaatin tehtäviin.

Venäjän tiedustelutoimijat joutuvat enenevässä määrin toimimaan Venäjältä käsin. Tiedustelua voi kohdistua Venäjällä oleviin tai matkustaviin, Suomessa asuviin henkilöihin. Myös epäasiallisten keinojen käyttö on mahdollista Venäjällä.

[4] Kansallisen turvallisuuden katsaus 2025. Supo. https://katsaus.supo.fi/etusivu

2.1.3 Valtioneuvoston selonteko tiedustelulainsäädännöstä

Valtioneuvosto on antanut selonteon tiedustelusta[5] vuonna 2021. Sen mukaan tiedustelulainsäädäntö on osa yhteensovitettua kansallisen turvallisuuden suojaamisen ja maanpuolustuksen tavoitteiden toteuttamista, ja se on ollut voimassa lyhyen aikaa.

Tiedustelutoimivaltuuksien käyttöä määrittävät tiedustelun tarkoitus ja kohde, yleiset ja erityiset edellytykset sekä toimintaa koskevat yleiset periaatteet.

Tiedustelua koskevan lainsäädännön keskeisin tavoite, kansallisen turvallisuuden parantaminen, on toteutunut, ja tiedonhankinta kansalliseen turvallisuuteen ja maanpuolustukseen kohdistuvista uhkista on uusien tiedustelutoimivaltuuksien myötä tehostunut. Ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteinen kokous on tärkeä toimija ulko- ja turvallisuuspoliittisesti merkittävien kehityslinjojen huomioon ottamisessa tiedustelussa ja tiedustelun toteutumisen seurannassa. Suomen turvallisuusympäristö on tiedustelulainsäädännön hyväksymisen jälkeen ollut jatkuvassa muutoksessa. Muutokset muodostavat yhteiskunnalle, sen toiminnoille ja jäsenille uusia uhkia ja uhkien yhdistelmiä. Siten lainsäädännön arviointi on jatkuva, käynnissä oleva prosessi tiedustelulainsäädännön soveltamisesta saatujen kokemusten tullessa jatkuvasti laajemmiksi. Uusiin ja monesta suunnasta ilmeneviin uhkiin varaudutaan jatkossakin ajantasaisen lainsäädännön keinoin perustuslaista johtuvat edellytykset ja reunaehdot huomioon ottaen.

Selonteossa todetaan myös, että sotilastiedustelusta annetun lain 66 §:ssä säädetään tietoliikenteen tiedonhankinnan teknisten tietojen käsittelystä, mikä edeltää varsinaista tietoliikennetiedustelua. Säännöksessä teknisten tietojen keräämisen hetkellisyyttä ei ole tarkemmin määritelty, ja määrittelyä linjataan tuomioistuimessa. Hankittavien tietojen ja toiminnan luonne huomioon ottaen hetkellisyys on osoittautunut ongelmalliseksi.

Lisäksi teknisten tietojen keräämiseksi tarvittava lupa voi olla voimassa lyhyemmän aikaa kuin varsinainen tietoliikennetiedustelu, mikä johtaa lupahakemuksen uusimiseen. Luvan voimassaoloaika tulisi yhteensovittaa varsinaisen tietoliikennetiedustelun kuuden kuukauden lupa-aikaan. Tällä hetkellä teknisten tietojen käsittelyllä saatuja tietoja voidaan käyttää vain tietoliikennetiedustelun kannalta merkityksellisen viestintäverkon osan löytämiseen.

Teknisten tietojen käsittelyssä on tunnistettu kuitenkin saatavan tietoja, joita voitaisiin käyttää myös varsinaisessa tietoliikennetiedustelussa hakuehtoina sekä käytettävien hakuehtojen tarkentamisessa ja kehittämisessä.

Teknisten tietojen käyttö hakuehtoina rajaisi entisestään saatavaa tietoa, kohdistuisi tarkemmin kohteeseen ja tehostaisi toimintaa. Tämä vähentäisi tarpeetonta puuttumista yksilön oikeuksiin.

Lainsäädännön mukaisten toimivaltuuksien kehittämisessä on otettava huomioon uusien teknologioiden kehittyminen, jotka usein turvaavat entistä paremmin yksityisyyden suojaa, mutta toisaalta mahdollistavat myös laittoman toiminnan tai kansallista turvallisuutta vaarantavan toiminnan salaamisen.

---

[5] Valtioneuvoston selonteko tiedustelulainsäädännöstä. Valtioneuvoston julkaisuja 2021:94. http://urn.fi/URN:ISBN:978-952-383-500-9

2.1.4 Viestintäverkko, tietoliikenne ja tietoliikenteen tiedustelu

Viestintäverkon fyysinen rakenne

Digitalisoituneessa maailmassa ja yhteiskunnassa yhteiskunnan ja ihmisten toiminta ovat vahvasti riippuvaisia tietoliikennejärjestelmästä. Tietoliikennejärjestelmä koostuu lukuisista tietoliikenteen välittämiseen tarvittavista laitteista sekä välittämiseen tarvittavista suuremmista ja pienemmistä tietoliikennekaapeleista ja johdoista. Suurimmat kaapelit, kuten merikaapelit, koostuvat valokuitupareista (yksi kuitu vie ja toinen tuo), kun taas pienemmät johdot voivat olla kuparikaapeleita. Tavanomainen merikaapeli sisältää 48 kuituparia.

Valokuidussa liikkuva tieto on muunnettu valoksi, kun taas kuparijohdoissa tieto liikkuu sähkönä. Valokuidun tietoliikenteen tiedon siirron tehokkuus perustuu siihen, että valokuidussa tietoa siirretään laserilla ja yhdessä valokuidussa voidaan siirtää tietoa kymmenillä eri aallonpituuksilla, jotka näkyvät kuidussa eri värisinä valoina, multipleksaustekniikan (Dense Wavelenght Division Multiplexing Access, DWMA) avulla. Yksittäisen aallonpituuden tiedonsiirtokapasiteetti on vuonna 2025 Suomessa yleensä noin 100–400 Gbps. Näin ollen yksittäinen valokuitupari voi teoriassa kuljettaa tietoa kymmeniä terabittejä sekunnissa. Valokuiduissakin valo heikkenee, joten noin 80–100 kilometrin välein kuitupari on liitettävä kuitureitin varrella laitteistolle, joka vahvistaa signaalia.

Optisen siirtojärjestelmän päässä olevalla vastaanottimella aallonpituudet muunnetaan asiakassignaaleiksi, jotka ohjataan kytkimille tai reitittimille. Kytkimillä ja reitittimillä tietoliikenteen bittivirta käsitellään digitaalisella tasolla ja ohjataan seuraaville laitteille reititysohjeistuksen (reititysprotokollan) mukaisesti. Asiakassignaalin siirto optiselta lähettimeltä tai vastaanottimelta kytkimelle tai reitittimelle voi tapahtua joko valokuitua tai kuparikaapelia pitkin.

Tietoliikenne

Jotta tietokone tai muu päätelaite toimisi halutulla tavalla ja laitteet toimisivat niille annettujen komentojen mukaisesti, edellyttää se ihmiselle visuaalisesti tulkittavissa olevan tiedon muuntamista binäärikoodiksi. Binääriluvut 1 ja 0 edustavat ”päällä” ja ”pois päältä” vaihtoehtoja. Binäärijärjestelmä on yksinkertaisin tapa käsitellä tietoa elektronisilla laitteilla. Tämä yksinkertaisuus tekee binäärijärjestelmästä luotettavan ja tehokkaan tavan toteuttaa digitaalista logiikkaa ja laskentaa.

Vastaavasti tietoliikenteessä on kyse ykkösistä ja nollista, ja tietoliikenne on käytännössä peräkkäisiä numeroita 1 ja 0. Numero 1 tai 0 muodostaa yhden bitin, ja kahdeksan bittiä muodostaa yhden tavun. Yksi tavu edustaa erilaisia arvoja tai merkkejä, kuten kirjainta, numeroa tai erikoismerkkiä.

Jotta tietoliikennejärjestelmässä olevat laitteet ja niissä käytettävät ohjelmat voisivat kommunikoida ja toimia yhdessä, vaatii tämä erilaisia teknisiä säännöstöjä ja standardeja, eli protokollia. Esimerkiksi tietoliikenneprotokollat (kuten web-sivustojen käyttämät HTTPS ja internetissä yleisesti käytettä TCP/IP) määrittävät, miten tietoa siirretään verkkojen välillä, kun taas salasanojen ja tietoturvan protokollat (kuten SSL/TLS) varmistavat, että tieto kulkee turvallisesti.

Tarkempana esimerkkinä voidaan tarkastella laajasti käytettyä IP-protokollaa (Internet Protocol). Se on tietoliikenneprotokolla, joka toimii internetin ja muiden tietoverkkojen

perustana. IP-protokollan tarkoituksena on mahdollistaa tietojen siirto laitteiden välillä verkossa, riippumatta niiden fyysisestä sijainnista. IP-protokollan keskeisiä omaisuuksia ovat:

- IP-osoitteet: Jokaisella verkkoon liitetyllä laitteella on yksilöllinen IP-osoite, joka mahdollistaa sen tunnistamisen ja paikantamisen verkossa

- Pakettilähetys: IP-protokolla pilkkoo datan pieniin paketteihin, jotka kulkevat verkon kautta määränpäähän tehokkainta reittiä pitkin

- Reititys: Protokolla auttaa löytämään parhaan reitin, jota pitkin datapaketti kulkee lähettäjältä vastaanottajalle.

Esimerkiksi tilanteessa, jossa henkilö haluaa lähettää 2–3 megatavun kokoisen valokuvan, joudutaan kuvatiedosto tyypillisesti jakamaan noin 2000 pakettiin. Tiedon lähettäjän käyttämä laitteisto muodostaa paketin, johon merkitään tarvittavat tiedot paketin ohjaamiseksi vastaanottajalle. Näitä tietoja ovat muun muassa IP-osoite, jolla vastaanottava laite yksilöidään ja käytetty sovellus, kuten web-palvelu, sähköpostipalvelin, videopuhelun vastaanottava mobiililaite tai sisällönjakoalusta. Jokainen yksittäinen paketti kulkee yksittäiselle paketille nopeinta ja tehokkainta reittiä pitkin määränpäähänsä.

Usein tietoliikenteessä ei kuitenkaan käytetä vain yhtä protokollaa, vaan niitä tarvitaan useita luotettavan tiedonsiirron mahdollistamiseksi. Tämän takia IP-protokolla yhdistetään TCP-protokollaan (yhdessä TCP/IP-protokolla). TCP-protokolla käytöllä saadaan IP-protokollan ominaisuuksien lisäksi ominaisuuksina:

- Tiedonsiirron hallinta: TCP vastaa tiedon pilkkomisesta pienempiin paketteihin ja niiden kokoamisesta vastaanottajalle oikeaan järjestykseen

- Virheiden tarkistus: TCP tarkistaa, että kaikki paketit on vastaanotettu ja korjaa mahdolliset tiedonsiirrossa tapahtuneet virheet

- Luotettavuus: Jos jokin paketti katoaa matkalla, TCP lähettää sen uudelleen varmistaen tiedonsiirron täydellisyyden.

Näin ollen esimerkiksi tilanteessa, jossa käyttäjä haluaa avata verkkosivun, päätelaite lähettää pyynnön käyttäen TCP-protokollaa, joka pilkkoo pyynnön paketteihin. IP-protokolla huolehtii pakettien reitittämisestä oikealle verkkopalvelimelle. Verkkopalvelimen TCP-protokolla vastaanottaa paketit, kokoaa ne yhteen ja lähettää vastauksen samalla tavalla takaisin. Lukuisien protokollien käytön jälkeen ja laitteiden välisen tiedonvaihdon jälkeen käyttäjä näkee päätelaitteensa näytöllä halutun sivuston.

Kuten kuvatussa esimerkissä TCP/IP-protokollaparista, usein käytössä on lukuisia eri protokollia; tiedonsiirron sujuvoittamiseksi paketit muodostuvatkin useista protokollakerroksista. Eri kerroksilla on eri käyttötarkoituksia – yhdellä kerroksella saatetaan kuvata sitä, mille laitteelle viesti on tarkoitettu, toisella sitä, miten liikenne on salattu. Etenkin monimutkaisemmissa tiedonsiirtojärjestelmissä tai yhteyksien jälleenmyyntijärjestelyissä protokollakerroksia voi olla toistakymmentä kappaletta. Liikenteen ohjaaminen asiamukaisesti vastaanottajalle edellyttää kaikkien kerrosten käsittelyä. Eri järjestelmien välisen yhteensopivuuden varmistamiseksi protokollat noudattavat useimmiten kansainvälisiä standardeja.

Jokainen tietojärjestelmä tuottaa oman yksilöllisen digitaalisen jalanjälkensä tietoliikenteeseen sen mukaan, miten järjestelmä viestii, kuinka usein, minkä kanssa ja missä muodossa tietoliikenne on. Näin ollen myös ilman viestinnän sisältöä, tietojärjestelmän tietoliikenteen teknisiä tietoja analysoimalla voidaan tietojärjestelmästä ja sen toiminnasta saada paljon tietoa. Tietojärjestelmän tunnistaminen tietoliikennevirrasta ei välttämättä edellytä viestinnän sisällön tai muun perustuslain 10 §:n suojaaman yksityisyyden piirissä olevan tiedon läpikäyntiä, vaan tietoa voidaan saada jo teknisestä ohjausliikenteestä sekä muista järjestelmien ja laitteiden välisestä liikenteestä.

Keskeisiä analyysissä käytettäviä tekniikoita on esimerkiksi tietoliikenteen ulosvirtausanalyysi. Tietojärjestelmän tietoliikenteessä on tiettyjä säännönmukaisuuksia, kuten tietoliikenteen pakettikokojakauma, tietoliikenteen saapumisajat, tietoliikennesession kesto ja tietoliikenteen määrällistä vaihtelua. Esimerkiksi tietokanta- ja internetpalvelimen tuottamat tietoliikennevirrat näyttävät erilaisilta.

Tietojärjestelmät kommunikoivat myös tietyn säännönmukaisuuden mukaisesti. Tietojärjestelmissä on usein ajastettuja prosesseja, pulssivälejä sekä synkronointikuvioita. Tietoliikennevirrasta on selvitettävissä suoraan se, ettei se ole ihmiskäyttäjän tuottamaa.

Myös aiemmin kuvatut protokollat vaikuttavat tietoliikenteen rakenteeseen. Käytettävät protokollat vaikuttava siihen, miten esimerkiksi IP-paketit muodostuvat, mikä vaikuttaa osaltaan siihen, miltä tietoliikennevirta näyttää ja minkälainen on sen säännönmukaisuus.

Tietoliikenneverkon kuvauksessa todetusti nykyaikainen viestintäverkko koostuu useista tietoa kuljettavista kuiduista ja niitä yhdistävistä laitteistoista. Keskeisiä laitteistoja ovat reitittimet.

Useimmiten tietoliikennepaketin lähettäjä ja vastaanottaja eivät ole suorassa yhteydessä toisiinsa. Tällöin laitteiden välillä on yksi tai useampi reititin eli tietoliikenteen ohjaamiseen suunniteltu laite. Reitittimet tarkastelevat niille saapuvia tietoliikennepaketteja, ja joko siirtävät paketit niiden vastaanottajille, mikäli reititin on suoraan kytköksissä vastaanottajaan, tai ohjaavat paketit seuraavalle reitittimelle, joka on vastaanottajaa lähempänä. Reitittimet keskustelevat keskenään reititysprotokollien, kuten BGP (Border Gateway Protocol) tai IS-IS (Intermediate System to Intermediate System) avulla. Reititysprotokollilla vaihdetaan tietoa siitä, mitä kautta eri IP-osoitteet ovat parhaiten saavutettavissa. Tämä tarkoittaa sitä, että sähköisen viestinnän yksittäiseen viestiin, kuten lähetettyyn valokuvaan, liittyvät tietoliikennepaketit eivät kulkeudu samaa reittiä pitkin vastaanottajalle, vaan ne menevät jokaiselle yksittäiselle paketille tehokkainta ja nopeinta reittiä pitkin vastaanottajalle. Näin ollen kokonainen viesti ei liiku viestintäverkon osassa aina edes peräkkäisinä tietoliikennepaketteina.

Tietoliikenteen salauksesta

Yksityiset henkilöt ja eri toimijat pyrkivät salaamaan tietoliikenteensä mahdollisimman pitkälle. Salauksissa on kyse tekniikoista, joilla verkossa tapahtuva viestintä muutetaan sellaiseen muotoon, etteivät ulkopuoliset voi lukea tai muokata sitä esimerkiksi ilman oikeaa salausavainta. Salauksella varmistetaan ennen kaikkea sitä, että vain oikeat vastaanottajat näkevät sisällön, tietoa ei voida muuttaa huomaamatta, lähettäjä ja vastaanottaja ovat oikeita ja viestin lähettämistä ei voida kieltää myöhemmin.

Yksi keskeinen tietoliikenteen salauksen keino on VPN-palvelut (Virtual Private Network). VPN-palveluiden yhtenä ominaisuutena on viestinnän niin kutsuttu kapselointi, jossa esimerkiksi aiemmin kuvattuja IP-paketteja paketoidaan uusiin IP-paketteihin. Niin kutsutussa

kapseloinnissa varsinaisen viestin vastaanottajan ja lähettäjän tiedot ovat näin ollen toisen viestin, eli IP-paketin tai useiden IP-pakettien sisällä.

VPN-palveluiden kautta luodaan myös virtuaalisia sisäverkkoja eri organisaatioiden käyttöön. Virtuaalisen sisäverkon avulla organisaation edustajat voivat toimia eri puolilla maailmaa käyttäen kuitenkin organisaation omia järjestelmiä vastaavalla tavalla kuin toimistolla ollessaan.

Tietoliikennetiedustelu

Tiedustelua kuvataan usein palapelin kokoamisena. Tiedustelumenetelmät täydentävät toisiaan ja niillä saadaan hankittua erilaista tietoa vertauskuvallisen palapelin kokoamiseksi. Jotta kokonaisuutta pystyttäisiin selvittämään, edellyttää tämä usein aluksi kokonaisuuden reunojen selvittämistä esimerkiksi tietoliikennetiedustelulla.

Tietoliikennetiedustelulla on erityspiirteistään johtuen tärkeä muita tiedustelumenetelmiä täydentävä ja niiden käytön mahdollistava funktio. Sen menetelmällinen erityisluonne mahdollistaa maanpuolustukseen ja kansalliseen turvallisuuteen kohdistuvien uhkien lähteiden paikantamisen sekä uhkien taustatahojen tunnistamisen. Tietoliikennetiedustelun avulla tehdyt havainnot ovat monessa tapauksessa välttämätön edellytys sille, että toisenlaiseen kohdentamislogiikkaan perustuvia tiedustelumenetelmiä ylipäätään voidaan käyttää.

Tietoliikennetiedustelussa tiedonhankinta kohdistuu Suomen rajan ylittävään tietoliikennekaapeliin ja siinä kulkeviin valokuitupareihin. Fyysisesti tietoliikennejärjestelmään ohjataan toisin sanoen valokuitujen valoa, mikä vastaa ykkösiä ja nollia. Binäärikoodia tulkitsemalla laitteistot muodostavat tavuja ja tavuista paketteja. Paketit muodostavat loppujen lopuksi kokonaisen viestin, kuten kuvan, tai osan siitä. Ilman viestin sisältöäkin paketeista voidaan saada olennaista tietoa, kuten tietoja viestin lähettäjästä ja vastaanottajasta.

Varsinainen tietoliikennetiedustelu perustuu hakuehtojen käyttöön. Pohjimmiltaan hakuehto palautuu ykkösten ja nollien sarjaan, jota järjestelmässä verrataan järjestelmään tulleeseen tietoliikenteeseen. Jos numerosarjat ovat yhtenevät, voidaan kyseistä tietoliikennettä, tarkemmin sanottuna paketteja, tarkastella tarkemmin. Tarkastelun kohteena on esimerkiksi se, sisältääkö tietoliikennepaketti viestin, ketkä ovat olleet viestin osapuolina ja mistä viesti on peräisin. Sähköisen viestinnän ja salauksen lisääntyminen ovat johtaneet siihen, että tietoliikenteen pakettivirrasta enenevä määrä liittyy muuhun kuin viestin merkityssisältöön.

Tarkemman analyysin lopputulosta voidaan käyttää esimerkiksi tiedusteluraporteissa ja tiedustelun tarkemmassa kohdentamisessa sekä uusien hakuehtojen määrittämisessä.

2.1.5 Tietojärjestelmät

Tietojärjestelmä voidaan määritellä järjestelmäksi, jossa käsitellään ja käytetään tietoa tietyssä tarkoituksessa. Teknisesti tarkasteltuna se yhdistää laitteet, ohjelmistot ja säännöt niin, että tieto saadaan talteen, sitä voidaan käyttää ja sitä voidaan lähettää ja vastaanottaa.

Etenkin viimeisen 20 vuoden aikana teknologisen kehityksen kiihtyvä tahti on johtanut siihen, että ihmisten ja organisaatioiden käyttämä tieto ei ole käytännössä säilössä yksittäisellä laitteella. Nykyinen tietoyhteiskunta perustuu tietoverkkojen, tiedon säilömiseen ja käsittelyyn tarkoitettujen palvelimien, ihmisten käyttämien erilaisten päätelaitteiden sekä automaatioon

tarkoitettujen sensoreiden ja pientietokoneiden muodostamasta kokonaisuudesta. Myös sotilastiedusteluviranomaisen torjumat uhat toimivat keskeisesti näitä järjestelmiä hyödyntäen.

Tietojärjestelmässä ei siis ole kyse vain yksittäisestä laitteesta tai ohjelmistosta, vaan nykymaailmassa kokonaisuudet koostuvat lukuisista yhteen toimivista laitteista ja ohjelmistoista. Viime kädessä yksittäisellä laitteella käytettävän palvelun takaa löytyy usein lukuisin laitteiden ja ohjelmistojen ketjuja.

2.1.6 Muutokset turvallisuustilanteessa

Kuten valtioneuvoston ulko- ja turvallisuuspoliittisen selonteossa on tuotu esiin maailmanpolitiikan valtasuhteiden murros vaikuttaa Suomen puolustuksen toimintaympäristöön. Kiihtyvä strateginen kilpailu ja demokratioiden ja autoritääristen valtioiden välinen globaali vastakkainasettelu ovat johtamassa monenkeskisen yhteistyön sirpaloitumiseen ja alueellistumiseen. Yhdysvaltojen ja Kiinan välillä käydään kilpailua poliittisesta, sotilaallisesta, taloudellisesta ja teknologisesta johtoasemasta maailmassa. Venäjä on puolestaan asemoinut itsensä vastakkainasetteluun Yhdysvaltoja ja muita länsimaita vastaan, osittain yhteistyössä Kiinan kanssa.

Laajalti digitalisoitunut ja verkottunut yhteiskunta on kiinteä osa kybertoimintaympäristöä. Tämä ympäristö on luonut uuden mahdollisuuden valtioille toteuttaa tavoitteitaan uusin keinoin. Näitä tavoitteita voivat olla mm. oman politiikan ja näkemyksen vahvistaminen, toisten valtioiden demokratian heikentäminen vaikuttamalla yhteiskunnan kriittisiin toimintoihin kuten vaaleihin, kriittiseen infrastruktuuriin tai tiedonvälitykseen. Tätä toimintaa kuvataan usein termeillä hybridivaikuttaminen tai laaja-alainen vaikuttaminen.

Laajasti verkottunut ja digitalisoitunut maailma avaa mahdollisuuden myös uuden tyyppiselle pysyvälle uhkatoiminnalle, kuten matalan intensiteetin kyberoperaatioille sekä edistyneille jatkuville kyberuhkatoimijoille. Ensimmäinen näistä tarkoittaa toimintaa, jota ei kansainvälisen oikeuden kontekstissa voida nähdä aseelliseksi hyökkäykseksi tai sotilaalliseksi voimankäytöksi; kyse voidaan katsoa olevan yleiskielisesti haitan teosta. Jälkimäisessä on kyse korkeatasoisesta, huomaamattomasta, pysyvästä kyberuhkasta, joka kohdistuu esimerkiksi kriittiseen infrastruktuuriin sekä valtioon ja jonka tavoitteena on esimerkiksi vakoilu, tiedonkeruu tai järjestelmän haltuunotto esimerkiksi poliittisten päämäärien saavuttamiseksi. Keskeistä on myös se, että vaikka toimijan yksittäiset toimenpiteet pystyttäisiin torjumaan, uhkatoimija jatkaa toimintaansa ja todennäköisesti kohdistaa toimintaansa Suomea vastaan uudelleen.

Teknologinen kehitys mahdollistaa kyberuhkatoimijoille suorastaan teollistuneet ja automatisoidut hyökkäysketjut. Tämä tarkoittaa sitä, että hyökkäysten nopeus ja määrä kasavavat, ja toimijat automatisoivat tietoturva-aukkojen skannausta, lateraaliliikennettä sekä datan analysointi- ja kiristystyökaluja. Geopoliittiset jännitteet ohjaavat niin matalan intensiteetin kyberoperaatioita kuin edistyneitä jatkuvia kyberuhkatoimijoita.

Tämän takia Suomen on huolehdittava kansallisen tiedustelun kehittämisestä vastaamaan lisääntyneisiin vaatimuksiin ja turvallisuusympäristön muutoksiin. Suomella on oltava valmius tunnistaa, ennaltaehkäistä ja torjua vakoilua, hybridivaikuttamista, terrorismia ja sotilaallista uhkaa niin fyysisessä kuin kybermaailmassa. Jo vakiintuneen kansainvälisen tiedusteluyhteistyön lisäksi Suomi osallistuu aktiivisesti Naton tiedusteluyhteistyöhön.

2.2 Lainsäädäntö ja käytäntö

2.2.1 Sotilastiedustelun kohteista ja kohdentamisesta

2.2.1.1 Sotilastiedustelun kohteet

Sotilastiedustelusta annetun lain 4 §:ssä määritellään sotilastiedustelun kohteet. Kohteista osa voidaan katsoa ainoastaan sotilastiedustelun yksinomaisiksi kohteiksi ja osa kohteista on luonteeltaan kohteita, jotka ovat osittain päällekkäisiä siviilitiedustelun kanssa.

Sotilastiedustelun yksinomaisissa kohteissa on kyse ennen kaikkea sotilaallisesta toiminnasta. Sotilaallisen toiminnan käsitettä ei ole kuitenkaan määritelty laissa, eikä käsitettä ole tiettävästi käsitelty myöskään oikeustieteellisessä kirjallisuudessa (HE 203/2017 vp s. 183). Ainoa oikeudellinen kuvaus sotilaallisesta toiminnasta löytyy kumotun puolustusvoimista annetun lain (402/1974) muuttamista koskeneesta hallituksen esityksestä (HE 172/1999 vp). Kyseisen lain esitöissä otettu sisäinen näkökulma sotilaalliseen toimintaan on ohjannut ymmärtämään käsitteen muun muassa valtakunnan alueellisen koskemattomuuden turvaamisen strategisena, operatiivisena ja taktisena suunnitteluna, puolustusvalmiuden ylläpidon ja kehittämisen suunnitteluna, sodanajan johtamisjärjestelmän ylläpitämisenä, sotilaallisena tiedusteluna, sodanajan organisaatioista ja määrävahvuuksista päättämisenä, henkilöstön sijoittamisesta ja sodanajan tehtävään määräämisenä sekä sodanajan joukkojen varustamisena ja huollon suunnitteluna sekä niiden valmistelutoimenpiteinä.

Edellä mainittu kuvaus sotilaallisesta toiminnasta ei sellaisenaan päde sotilastiedustelun asiayhteydessä, koska siinä kiinnostus kohdistuu vieraaseen sotilaalliseen toimintaan. Tällaisessa ulkoisessa tarkastelussa sotilaalliseksi toiminnaksi katsotaan 1) valtiollinen ja ei-valtiollinen sotilaallisesti järjestäytyneiden joukkojen toiminta, 2) sotilaallisiin voimakeinoihin, kuten aseistukseen ja sotatarvikkeisiin liittyvä toiminta tai 3) muihin näihin rinnastuva, sotavoimaa käyttävien joukkojen toiminta (HE 198/2017 vp s. 34 ja HaVL 7/2018 vp s. 4).

Valtiollinen toiminta palautuu jonkin vieraan valtion asevoimien toimintaan tai siihen rinnastuvaan kansainvälisen, sotilaallisen liittouman tai järjestön toimintaan, kun taas ei-valtiollisella toiminnalla tarkoitetaan sellaista sotilaallisesti järjestettyä, aseistettua tai varustettua toimintaa, jolla ei ole edellä tarkoitettua valtiollista alkuperää tai jonka tällaista alkuperää ei voida tunnistaa. Sotilaalliselle toiminnalle tyypillistä ovat suuret joukkokokonaisuudet, sotilaallisten toimenpiteiden valmistelu ja johtaminen, sotilaallinen järjestäytyminen, sotilaallinen kouluttautuminen ja varustautuminen vahvemmin kuin tavanomaisilla voimankäyttövälineillä. Lisäksi sotilaallinen toiminta vaatii usein vahvaa taloudellista resursointia, johon pääsääntöisesti vain valtioilla on varaa (HE 203/2017 vp s. 183).

Sotilastiedustelusta annetun lain 4 §:n 1 momentin 1 kohdan mukaan sotilastiedustelun kohteena on vieraan valtion asevoimien ja niihin rinnastuvien joukkojen järjestäytyneiden joukkojen toiminta ja toiminnan valmistelu. Toiminnan on oltava luonteeltaan sotilaallista. Vieraan valtion asevoimiin rinnastuvaa joukkoa on arvioitava sen perusteella, miten järjestäytynyttä toiminta on, mitkä ovat joukon käytössä olevat resurssit ja minkälaista toiminta on kokonaisuutena arvioiden (PuVM 9/2018 vp. s. 10).

Tarkoitettua toimintaa ei ole rajattu koskemaan vain Suomeen kohdistuvaa toimintaa, vaan sotilastiedusteluviranomaisen on voitava hankkia laajasti tietoa vieraan valtion asevoimien tai siihen rinnastuvien järjestäytyneiden joukkojen toiminnasta silloinkin, kun tästä ei aiheudu välitöntä sotilaallista uhkaa Suomelle. Hankitun tiedon perusteella pyritään jäsentämään,

vähentämään ja myös hyödyntämään turvallisuuspoliittisen ympäristön epävarmuustekijöitä maanpuolustuksessa ja kriisiin varautumisessa (HE 203/2017 vp. s. 183–184).

Keskeisenä päämääränä on myös antaa ennakkovaroitus tiedustelun asiakkaille. Vihamielinen valtio pyrkii usein toteuttamaan vaikuttamisensa niin, ettei kohdevaltiolla ole välttämättä täyttä varmuutta, onko kyse tavoitteellisesta ja ohjatusta operaatiosta vai ei. Oikea-aikaisen objektiivisen tiedon pohjalta valtiojohdolle syntyy enemmän liikkumatilaa erilaisten painostuskeinojen kohdistuessa Suomeen. Tästä johtuen erilaisia tapahtumia ja kehityskaaria seurataan kokonaisvaltaisesti.

Selvää on se, että sotilastiedustelutoimintaa on kohdistettava Puolustusvoimien tehtävien mukaisesti Suomen ulkoiseen uhkaan. Sotilastiedustelun tehtäväkenttään eivät kuulu Suomen sisäiset asiat, kuten valtion sisäinen konflikti tai demokraattisessa yhteiskuntaelämässä tapahtuva vaikuttaminen, kuten yleislakko. Tästä on kuitenkin erotettava vieraan valtion asevoimien tai niihin rinnastuvien järjestäytyneiden joukkojen organisoimat tai muutoin tukemat tilanteet, jotka saadaan näyttämään valtion sisäiseltä kuohunnalta.

Kohdan mukaista toimintaa on varsinaisen sotilaallisen toiminnan ja siihen rinnastuvien joukkojen toiminnan lisäksi myös toiminnan valmistelu sekä sotilaalliset suunnitelmat ja aikeet. Suomen maanpuolustuksen kannalta keskeistä tietoa voidaan myös saada muiden valtioiden välisestä konfliktista tai vieraan valtion sotilaallisista harjoituksista.

Valmistelu ja suunnitelmat kattavat myös esimerkiksi sotilaspoliittisen päätöksenteon ja sotilaallisen suunnittelu- ja kehitystoiminnan sekä asejärjestelmien kehittämisen ja hankinnan. Valmistelu ja suunnitelmat voivat kohdistua myös kohdevaltion sisäisen kuohunnan lietsomiseen. Vihamielisen valtion tavoitteena voi olla myös muualla kuin Suomessa käynnistettävä vallankaappaus tai -kumous.

Sotilastiedustelusta annetun lain 4 §:n 1 momentin 2 kohdassa säädetään sotilastiedustelun kohteeksi luonteeltaan sotilaallinen tiedustelutoiminta, joka kohdistuu Suomen maanpuolustukseen. Kansainvälisen oikeuden mukaan jokainen suvereeni valtio nauttii alueellista koskemattomuutta ja poliittista riippumattomuutta suhteessa muihin valtioihin. Useimmat valtiot sietävät tiettyyn pisteeseen asti vieraiden valtioiden tiedusteluviranomaisten toimintaa.

Ulkomaisella tiedustelutoiminnalla tarkoitetaan sellaista vieraan valtion toimintaa, jonka päämääränä on oman valtion etujen edistämiseksi tai Suomen tai toisen vieraan valtion vahingoksi hankkia tietoa, jonka salassapitoon tiedustelun kohteena olevalla valtiolla on erityinen intressi. Vieraan valtion tiedonhankinnan kohteena voi olla esimerkiksi Suomen turvallisuus- puolustuspolitiikka, Suomen sotilaallinen valmius ja maanpuolustuksen kehitys, sotilaallinen suorituskyky, yhteiskunnan kriisinsietokyky, huoltovarmuus sekä maanpuolustukseen liittyvä tutkimus ja tuotekehitys.

Sotilastiedustelulla pyritään havaitsemaan ja tunnistamaan henkilöitä, jotka paljastavat maanpuolustuksen kannalta salassa pidettävää tietoa ulkomaiselle tiedustelupalvelulle, ja henkilöt, joita tällainen palvelu pyrkii värväämään. Tiedonhankinta voi kohdistua myös tiedustelupalvelun avoimeen ja salaiseen tiedonhankintaan. Myös ulkomaisen tiedustelupalvelun Suomea koskevat tiedonhankintatavoitteet ja -prioriteetit sekä tiedustelukohteet voivat olla sotilastiedustelun tiedustelutehtävän tavoitteena.

Sotilastiedustelusta annetun lain 4 §:n 1 momentin 4 kohdan mukaan sotilastiedustelun kohteena voi olla vieraan valtion sotatarvikkeiden kehittäminen ja levittäminen. Yleisesti

sotatarvikkeissa on kyse materiaalista ja teknologista, jota kehitetään hyvin resursoidulle taholle, kuten valtioille. Kohdan mukaisen toiminnan ei tarvitse muodostaa välitöntä uhkaa Suomelle, vaan tiedolla on merkitystä Suomen turvallisuusympäristössä tapahtuvien muutosten havaitsemiseksi ja sotilasstrategisen tilannekuvan muodostamiseksi. Kohdan mukainen tieto voidaan katsoa suorastaan välttämättömäksi Suomen sotilaallista puolustamista ja varautumista varten, ja tiedolla on merkitystä esimerkiksi varautumisen kannalta ja siviiliväestön suojelemiseksi.

Sotilastiedustelusta annetun lain 4 §:n 2 momentin mukaan sotilastiedustelun kohteena on toiminta, joka vakavasti uhkaa Suomen maanpuolustusta. Suomen maanpuolustuksella tarkoitetaan maanpuolustuksen kokonaisuutta, jolla turvataan alueellinen koskemattomuus, kansain elinmahdollisuudet ja perusoikeudet, valtiojohdon toimintavapaus sekä laillinen yhteiskuntajärjestys. Kohteena olevan toiminnan ei tarvitse olla luonteeltaan sotilaallista. Riittää, että toiminta uhkaa vakavasti Suomen kansallista turvallisuutta, eli toimintaa, jonka tavoitteena on aiheuttaa häiriöitä ja lamauttaa maanpuolustukselle tärkeitä toimintoja, kuten johtamista, logistiikkaa ja tietoliikennettä.

Tiedonintressin voidaan katsoa liittyvän ensi sijassa siihen, mikä taho tällaista uhkaa aiheuttaa ja mikä uhkaa selittää eli mitkä ovat uhkaan tarkoitusperät. Toiminnassa voi olla kyse vihamielisen valtion sijaistoimijoita käyttämällä toteutettu sabotaasi tai alueen haltuunotto. Kohdan mukaista tiedonhankintaa voidaan kohdistaa toimijaneutraalisti.

Suomen maanpuolustukseen kohdistuva uhka voi merkittävästi vaikeuttaa Suomen ulkopoliittista asemaa ja kaventaa sen poliittista liikkumatilaa. Uhkan vakavuuskriteerin voidaan katsoa täyttyvän myös tilanteissa, jotka voivat kehittyä alueellisen koskemattomuuden loukkauksiksi tai jotka vaarantavat yhteiskuntarauhan peruselementtejä, kuten väestön henkistä kriisinkestävyyttä ja toimintakykyä.

Kohdan tarkoittama tiedonhankinta kattaa yhteiskunnan elintärkeät toiminnot (johtaminen, kansainvälinen ja EU-toiminta, puolustuskyky, sisäinen turvallisuus, talous, infrastruktuuri ja huoltovarmuus, väestön toimintakyky ja palvelut sekä henkinen kriisinkestävyys). Toimintojen voidaan katsoa nivoutuvan valtiosääntöisiin ”superintresseihin”. Kyse on myös niistä intresseistä, joiden turvaamisesta on säädetty Puolustusvoimien tehtävissä.

Yhteiskunnan elintärkeisiin toimintoihin voidaan pyrkiä vaikuttamaan lukuisin erilaisin keinoin, kuten enenevissä määrin kybervaikuttamisella.

Edellä todettuja sotilastiedustelun kohteita voidaan pitää yksinomaan sotilastiedustelulle osoitettuina. Tämän lisäksi on myös sotilastiedustelun ja suojelupoliisin yhteisiä kohteita. Kohteisiin kohdistuvaa tiedustelua koordinoidaan tiedusteluviranomaisten kesken ja valtioneuvostotasolla osoittamalla esimerkiksi tiedustelun painopisteitä.

Sotilastiedustelusta annetun lain 4 §:n 1 momentin 3 kohdan mukaan sotilastiedustelun kohteena on joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö. Kyse on osaltaan proliferaatiovalvonnasta, jolla tarkoitetaan joukkotuhoaseiden ja niiden kantolaitteiden leviämisen estämistä sekä joukkotuhoasioiden valmistamiseen käytettävien laitteiden, välineiden, materiaalin ja tietotaidon leviämisen estämistä tahoille, jotka pyrkivät kehittämään joukkotuhoasetta.

Sotilastiedustelun tiedonhankinta kohdistuu ennen kaikkea valtiollisen sotilaallisen ja siihen rinnastuvan toimijan joukkotuhoaseisiin. Esimerkiksi Sergei Skripal -tapauksessa käytetty novitsok-hermomyrkky on selkeästi sotilaalliseen toimintaan kehitetty kemiallinen ase, jota

myös käytti vihamielisen valtion sotilastiedustelu. Siviilitiedustelussa korostuvat esimerkiksi terroristiset toimijat.

Sotilastiedustelusta annetun lain 4 §:n 1 momentin 5 kohdan perusteella sotilastiedustelun kohteena on kansainvälistä rauhaa ja turvallisuutta vakavasti uhkaava kriisi. Kohdassa tarkoitettu kriisi on aina yksittäisen valtion sisäistä hätätilaa laajempi kriisi, eli kriisillä on vaikutuksia myös valtion naapurimaihin. Tietoa voidaan hankkia esimerkiksi keskiössä olevan valtion tai siihen liittyvien valtioiden poliittisen tilanteen kehittymisestä sekä siitä, mitä ulko- ja turvallisuuspoliittisia seurauksia siitä voi Suomelle mahdollisesti aiheutua. Uhka kansainväliselle rauhalle ja turvallisuudelle voi syntyä myös epidemioiden ja pandemioiden kautta.

Se, onko kyse kansainvälistä rauhaa tai turvallisuutta vakavasti uhkaavasti kriisistä, voi määrittyä esimerkiksi sitä kautta, kutsutaan tasavallan presidentin ja ulko- ja turvallisuuspoliittisen ministerivaliokunnan kokous kokoon asian tiimoilta.

Sotilastiedustelusta annetun lain 4 §:n 1 momentin 6 kohdan mukaan sotilastiedustelu voi kohdistua kansainvälistä kriisinhallintaoperaatioiden turvallisuutta vakavasti uhkaavaan toimintaan. Suomi osallistuu kansainväliseen sotilaalliseen kriisinhallintaan, jonka tarkoituksena on kansainvälisen rauhan ja turvallisuuden ylläpitäminen tai palauttaminen taikka humanitaarisen avustustoiminnan tukeminen tai siviiliväestön suojaaminen.

Tiedonhankinnan tarkoituksena on varmista operaatioturvallisuus ja siihen osallistuvan henkilöstön henkilökohtainen koskemattomuus. Tietoa voidaan hankkia esimerkiksi kriisinhallintaoperaatioalueen olosuhteista ja kohdistuuko henkilöstöön väkivaltaisen iskun uhkaa. Tiedonhankinta voi olla myös ennakollista, jolla on merkitystä operaatioon osallistumispäätöksenteon kannalta.

Sotilastiedustelusta annetun lain 4 §:n 1 momentin 7 kohdan mukaan sotilastiedustelun kohteena voi olla Suomen kansainvälistä avun antamista vakavasti uhkaava toiminta. Kohta kattaa myös EU:n yhteisvastuulausekkeen mukaisen toiminnan.

Esimerkiksi yhteisvastuulausekkeen mukaisissa täytäntöönpanotilanteissa eli tilanteissa, joissa voi olla kyse luonnon tai ihmisen aiheuttamasta suuronnettomuudesta, on usein välttämätöntä saada tietoa isku- tai onnettomuusalueen olosuhteista. Sama koskee myös keskinäisen avunannon tilanteita, jollaisia voivat olla päätös lähettää EU:n taisteluosasto tai Naton nopean toiminnan joukko sotilasoperaatioon taikka suomalaisten asiantuntijoiden ryhmä ulkomailla toteutettaviin erityistehtäviin. Määritelty kohde soveltuu tiedonhankintaan paitsi käsityksen muodostamiseksi operaatiossa tarvittavista kyvyistä ja toteuttamispaikan olosuhteista, myös kulloinkin valitus mekanismin kautta lähetetyn henkilöstön turvallisuuteen vaikuttavista seikoista.

Sotilastiedustelusta annetun lain 4 §:n 2 momentti kattaa myös tilanteita, jotka ovat yhteisiä sotilas- ja siviilitiedustelulle. Sotilastiedustelun osalta kohdetta on käsitelty aiemmin.

2.2.1.2 Tiedustelutoiminnan rajoitusmekanismeista

Yleistä

Uhkaperusteisen tiedustelutoiminnan voidaan katsoa voivan kohdistua rajoittamattomaan joukkoon ihmisiä. Tämän takia laissa on säädetty erilaisista ohjaus-, rajaus- ja

rajoitusmekanismeista. Selkeimpiä rajaukset ovat esimerkiksi tiedustelumenetelmiä koskevissa yleisissä ja erityisissä edellytyksissä, jotka joko soveltuvat tai eivät sovellu.

Laissa säädetään myös koko sotilastiedustelutoimintaa koskevista periaatteista, jotka ovat tiedustelumenetelmän käyttöä koskevia edellytyksiä joustavampia ja ne kattavat erilaisia tilanteita. Periaate ennemminkin ohjaa ja rajoittaa tiedustelutoimintaa ja siitä päättämistä. Periaatteet voi nähdä optimointikäskyinä, joiden kautta toteutetaan jotain arvoa tai tavoitetta niin hyvin kuin oikeudelliset ja tosiasialliset reunaehdot sen mahdollistavat. Sotilastiedustelulainsäädännön osalta periaatteiden voidaan katsoa tuovan esiin tiedustelutoiminnan arvoperustan. Periaatteiden kautta sotilastiedustelutoiminnan päätöksentekoon tulee esimerkiksi perustuslain ja Suomea sitovien ihmisoikeussopimusten tutkintakäytännössä kehittyviä ratkaisuperusteita. Periaatteet näyttäytyvät ennen kaikkea harkintavaltaa jättävien säännösten yhteydessä, mikä korostuu sotilastiedustelutoiminnassa.

Perustuslakivaliokunta on korostanut, että velvollisuus osoittaa tiedustelutoimenpiteen yhteensopivuus tiedusteluun sovellettavien yleisten periaatteiden kanssa on kussakin yksittäistapauksessa aina tiedusteluviranomaisella, jolla on muutoinkin velvollisuus esittää riittävät perustelut tiedustelutoimenpiteen lakisääteisten edellytysten täyttymisestä (PeVL 35/2018 vp s. 16 ja PeVL 36/2018 vp s. 18).

Toimintaa yleisesti ohjaavien periaatteiden lisäksi laissa on säädetty minimointimekanismeista, joiden tavoitteena on suodattaa sotilastiedusteluviranomaisen hankkimaa tietoa siihen, mihin sotilastiedusteluviranomaisella on toimivalta. Sotilastiedustelussa tulee väistämättä hankittua tietoa, joka liittyy sivulliseen tai on muuten luonteelta sellaista, jota sotilastiedustelu ei saa hankkia. Minimointimekanismit toteutuvat esimerkiksi hetihävittämissääntelyn kautta.

Yleiset periaatteet

Perus- ja ihmisoikeuksien kunnioittamisen periaatteen (sotilastiedustelusta annetun lain 5 §) mukaan sotilastiedusteluviranomaisen on kunnioitettava perusoikeuksia ja ihmisoikeuksia sekä toimivaltuuksia käyttäessään valittava perusteltavissa olevista vaihtoehdoista se, joka parhaiten edistää näiden oikeuksien toteutumista. Perusoikeudet velvoittavat jo itsessään lainkäyttäjää perustuslain tasolla. Vaikka perusoikeuksia tuleekin toteuttaa jo suoraan sovellettavana oikeutena, useimmiten niiden merkitys ilmenee tulkintavaikutuksena lakeja sovellettaessa. Tulkinnan lopputuloksen on oltava sopusoinnussa perus- ja ihmisoikeusnormien kanssa. Perustuslakivaliokunta on lausuntokäytännössään todennut sotilastiedustelulainsäädännön osalta (PeVL 36/2018 vp. s. 15), että sen erityisluonne edellyttää säännöksiä perusoikeuksien ja ihmisoikeuksien kunnioittamisesta tiedustelun toimivaltuussääntelyn tulkintaan.

Suhteellisuusperiaatteen (sotilastiedustelusta annetun lain 6 §) mukaan sotilastiedustelun toimenpiteiden on oltava puolustettavia suhteessa tiedon hankinnalla saatavien tietojen tärkeyteen, tiedustelutehtävän kiireellisyyteen, tavoiteltavaan sotilastiedustelun päämäärään, sotilastiedustelun kohteeseen, muille tiedustelutoimenpiteen käytöstä aiheutuvaan oikeuksien rajoittamiseen sekä muihin asiaan vaikuttaviin seikkoihin. Lisäksi toimenpiteellä tulee olla riittävät tosiasialliset mahdollisuudet saavuttaa sotilastiedustelun hyväksyttävät päämäärät. Periaate näkyy ennen kaikkea toimenpiteiden oikeasuhtaisuuden arvioinnissa. Käytettyjen menetelmien ja niillä aiheutettujen haittojen, kuten yksityiselämän suojaan puuttumisen, on oltava järkevässä suhteessa tavoiteltuun päämäärään verrattuna. Tällä ei kuitenkaan tarkoiteta ainoastaan toimenpiteen ylimitoittamisen ehkäisemistä, vaan myös sitä, että päämäärän saavuttamisen kannalta toimenpide on riittävän tehokas. Suhteellisuusperiaate ohjaa myös käytettävissä olevien tiedustelumenetelmien valintaa senkin osalta, jos toisen tiedustelumenetelmän käytöllä tarvittava tieto voidaan saada lyhyemmässä ajassa; kohteen

yksityisyyden suoja kannalta voi olla perustellumpaa käyttää syvemmälle yksityisyyden suojaan puuttuvaa tiedustelumenetelmää, jos sitä voidaan käyttää lyhyemmän aikaa (HE 203/2017 vp. s. 193).

Suhteellisuusperiaatteen soveltamisessa voidaan ottaa huomioon myös tehtävän tärkeys: mitä vajavammasta uhasta on kyse ja mitä suuremmalla todennäköisyydellä uhan arvioidaan toteutuvan, sitä puolustettavampana perusoikeuksiin syvemmin kajoavien tiedustelumenetelmien käyttöä voidaan pitää. Vastaavasti suhteellisuusperiaate voi ohjata myös toiseen suuntaa esimerkiksi sen perusteella, ettei saatavilla tiedoilla voida olettaa olevan suurta merkitystä ja toisaalta se, että muilla tiedustelumenetelmillä puututtaisiin vähemmän kohteen oikeuksiin.

Suhteellisuusperiaatteen painoarvoa ovat korostaneet myös EIT ja EUT ratkaisukäytännössään. Etenkin tämä on noussut tietoliikennetiedustelua koskevissa tapauksissa (esim. Zakharov v. Venäjä, Weber ja Saravia v. Saksa ja Digital Rights C-293/12). Suhteellisuus korostuu ennen kaikkea siinä, että tietoliikennetiedustelulta edellytetään sen sivullisvaikutusten takia viimesijaisuutta.

Sotilastiedustelusta annetun lain 6 §:n viimeinen virke vaatimuksesta toimenpiteiden tosiasiallisesta soveltuvuudesta tarkoitukseensa ilmentää perustuslakivaliokunnan linjausta siitä, että perusoikeusrajoitus ei voi olla tarkoitukseensa soveltuva ja siten välttämätön, jos sillä ei edes periaatteessa voida saavuttaa sen perusteena olevaa hyväksyttävää tavoitetta (PeVL 36/2018 vp. s. 17 ja esim. PeVL 40/2017 vp. s. 4, PeVL 55/2016 vp. s. 4-5 ja PeVL 5/2009 vp. s. 3). Käytännössä tämä näkyy siinä, että sotilastiedusteluviranomaisen on esitettävä riittävät perustelu haetun tiedustelumenetelmän soveltuvuudesta tarkoitukseensa lupa-asian ratkaisevalle tuomioistuimelle tai muulle päätöksentekijälle (PuVM 9/2018 vp. s. 31)

Vähimmän haitanperiaate (sotilastiedustelusta annetun lain 7 §) ohjaa sotilastiedusteluviranomaisen toimivaltuuden käyttöä niin, ettei niillä saa puuttua kenenkään oikeuksiin enempää eikä kenellekään saa aiheuttaa suurempaa vahinkoa tai haittaa kuin välttämätöntä tehtävän suorittamiseksi. Lisäksi vähimmän haitan periaate sisältää vaatimuksen, jonka mukaan tiedon hankkimisessa ei saa puuttua luottamuksellisen viestin salaisuuteen muuten kuin mahdollisimman kohdennetusti ja rajoitetusti (LaVL 31/2018 vp. s. 3-4 ja PeVL 36/2018 vp. s. 17). Periaatteen soveltamisessa on huomioitava tiedustelun varsinaisen kohteen lisäksi myös sivulliset, koska säännöksessä mainitaan nimenomaisesti ”kenenkään”. Oikeuksien voidaan tarkoittaa ennen kaikkea perustuslaissa säädettyjä perusoikeuksia (HE 202/2017 vp. s. 170).

Vieraan valtion viranomaisorganisaatiot eivät nauti perusoikeussuojaa, joten niihin voidaan kohdistaa merkittävämpiä tiedustelutoimenpiteitä kuin ei-valtiolliseen kohteeseen (yksityishenkilöön). Haitta on siis vähäisintä silloin, kun tiedustelu kohdistuu vieraan valtion viranomaisten viestintään, vaikkakin tällaisen viestinnän havaitseminen voi vaatia luottamuksellisen viestin salaisuuden suojaan puuttumista

Käytännössä periaate ohjaa käyttämään tiedustelumenetelmää, joka aiheuttaa pienimmän vahingon tai haitan kohteelle. Toisin sanoen tiedustelumenetelmistä on valittava se, joka kaikista vähiten kajoaa kohdehenkilön perus- ja ihmisoikeuksiin. Periaatteen soveltamisen kannalta on huomioitava kohteiden osalta se, onko kyse valtiollisesta toimijasta vai ei-valtiollisesta toimijasta näiden erilaisen perusoikeussuojan takia. Toisaalta periaate ohjaa valitsemaan sen tiedustelumenetelmän, joka on parhaiten kohdennettavissa. Tarkka kohdentaminen rajaa siitä koituvaa vahinkoa tai haittaa sivullisille.

Sotilastiedusteluviranomaisen onkin arvioitava haitan astetta kohteessa, mutta myös haitan piiriin mahdollisesti tulevien sivullisten määrää.

Sivullisiin kohdistuvan haitan minimoimiseksi vähimmän haitan periaate edellyttää, että käyttöön valitaan tarkimmin kohdennettava tiedustelumenetelmä. Vähimmän haitan arviointi tapahtuu kokonaisuutena ja tapauskohtaisesti punnintana, jossa vastakkain on tavoiteltu hyöty ja yksilön oikeuksiin kajoamisen välttämättömyys tavoitteen kannalta.

Perustuslakivaliokunta on mietinnössään (PeVM 4/2018 vp. s. 7–8) katsonut, että välttämättömyysvaatimuksen täyttymiseksi ei riitä se, että luottamuksellisiin viesteihin kohdistuva tiedonhankinta katsotaan yleisesti edistävän maanpuolustusta tai kansallista turvallisuutta, vaan on osoitettava, että tiedustelumenetelmän käytöllä voidaan perustellusti olettaa saatavan tietoja toiminnasta, joka aiheuttaa uhkaa maanpuolustukselle tai kansalliselle turvallisuudelle. Periaatteen soveltamisessa onkin arvioitava puuttumisen välttämättömyyttä tehtävän kannalta.

Tarkoitussidonnaisuuden periaatteen mukaan sotilastiedusteluviranomainen saa käyttää toimivaltuutta vain laissa säädettyyn tarkoitukseen (sotilastiedustelusta annetun lain 8 §). Säännös voidaan nähdä sinänsä informatiivisena, että jo perustuslain nojalla viranomaisen on toimittava lain mukaisesti. Periaate muistuttaa, että toimivaltuuden käytön on perustuttava nimenomaiseen säännökseen ja siinä asetettuun tarkoitukseen, mutta toisaalta periaatteen voidaan katsoa sisältävän väärinkäytönkiellon, eli toimivaltuuksia saa käyttää ainoastaan säädetyn tarkoituksen ja kohteiden asettamissa rajoissa.

Syrjintä kielto (sotilastiedustelusta annetun lain 9 §) ilmaisee jo perustuslain 6 §:n 2 momentissa säädettyä kielto, jonka mukaan kaikenlainen syrjintä on kiellettyä. Säännöstä voidaan kuitenkin pitää merkityksellisenä sotilastiedustelutoiminnassa profiloinnin kiellon ilmaisuna. Ennen kaikkea profilointia voidaan pitää ongelmallisena yksityiselämää ja henkilötietojen suojaa sekä yhdenvertaisuutta koskevien perus- ja ihmisoikeuksien kannalta. Käytännössä profiloinnin voidaan katsoa olevan myös tehotonta, koska se usein kohdistuu tarpeettoman suureen määrään ihmisiä ja toisaalta se saattaa jättää myös potentiaaliset kohdehenkilöt seulonnan ulkopuolelle. Syrjintä kiellon tavoitteiden osalta sen voidaan katsoa olevan osittain päällekkäinen muiden periaatteiden kanssa.

Etenkin kansainvälisessä yhteistyössä voidaan puhua myös sääntelemättömästä tiedonvaihdon luottamusperiaatteesta. Oikeuskirjallisuudessa on katsottu, että sen perustuvan kansainvälisessä tiedonvaihdossa käytännössä edellytettävälle osapuolien keskinäisen luottamuksen vaatimukselle. Toiminnassa saatuja tietoja saa käyttää vain siihen tarkoitukseen, johon se on annettu, eikä tietoja saa luovuttaa edelleen ilman luovuttajan nimenomaista suostumusta. Tiedonvaihdon osapuolet luottavat näiden ehtojen kunnioittamiseen siitä riippumatta, onko luovutetussa asiakirjassa erillistä salassapitomerkintää tai luovutuksenkieltolauseketta (ks. myös KHO:2010:31).

Periaatteessa voidaan katsoa olevan kyse kansainvälisessä tapaoikeudessa vakiintuneesta normista, jolle on esittää painavat käytännön syyt. Periaatteen noudattamisella turvataan käynnissä olevia operaatioita ja siihen tietolähteenä tai muulla tavalla osallistuvien henkilökohtaista koskemattomuutta sekä kansainvälisiä suhteita. Osapuoli, joka menettää tämän luottamuksen kansainvälisessä turvallisuus- ja tiedustelupalveluyhteisössä, jää tiedonvaihdon ulkopuolelle, kunnes luottamus on jälleen rakennettu. Tiedusteluviranomaisen kannalta tiedonvaihdon luottamusperiaatteen kunnioittaminen on sen toimintaedellytysten kulmakivi.

Sotilastiedustelutoiminnassa voidaan myös tunnistaa edellä todettujen periaatteiden lisäksi merkittävä ohjaava tekijä, operaatioturvallisuus. Sotilastiedustelun keskeisenä edellytyksenä on toimiminen kohteelta salassa. Kaikessa sotilastiedustelun toiminnassa keskeisenä elementtinä on se, pystytäänkö toimenpide ja laajemminkin toiminta pitämään salassa. Tämä vaikuttaa operatiivisen toiminnan suunnittelun kaikilla tasoilla, myös lain soveltamiseen. Jos toimenpide aiheuttaa sotilastiedustelun edes osittaisen paljastumisen tai riski paljastumiseen nähdään liian suureksi, toimenpidettä ei toteuteta.

Minimointimekanismit

Se, missä yleiset periaatteet luovat ja tuovat ilmi sotilastiedustelun arvopohjaa ja ohjaavat käyttämään oikeaa tiedustelumenetelmää, minimointimekanismien kautta sinänsä oikean ja oikein käytetyllä tiedustelumenetelmällä saatuja tietoja pyritään rajaamaan tarkoitettuun. Rajauksella pyritään rajaamaan yksityiselämän suojaan puuttumista sen jälkeen, kun tiedustelumenetelmän edellytykset ovat täyttyneet ja niitä varsinaisesti käytetään. Tällä on myös tärkeä merkitys yksilön oikeusturvan kannalta. Minimointimekanismeihin voidaan lukea tiedustelukieltoja, tallenteiden ja asiakirjojen tarkastamista, tallenteiden tutkimista, ylimääräisen tiedon käyttöä, tietojen hävittämistä ja tiedonhankintakeinojen käytön keskeyttämistä koskevat säännökset sekä hyödyntämiskieltoa koskevat säännökset.

Minimointimekanismeilla on myös merkitystä sääntelyn ennakoitavuuden kannalta, sillä ne rajaavat sotilastiedustelua niin, että tiedustelumenetelmiä kohdistavaan vain sotilastiedustelun kohteen kannalta merkityksellisiin tietoihin välttäen sivullisiin kohdistuvaa tiedustelumenetelmän käyttöä. Näin ollen yksilö voi ennakoida tilanteita, joissa hän saattaa joutua tiedustelumenetelmän käytön kohteeksi.

Etenkin sotilastiedustelutoiminnassa minimointimekanismeilla on erityistä merkitystä sotilastiedustelun kohteiden ollessa ilmiötasolla ja tiedustelumenetelmien käytön näin ollen ollessa verraten laajasti sovellettavissa. Näin ollen myös viranomaisen harkintavalta ja erehtymisen mahdollisuus ovat mahdollisia. Minimointimekanismeilla rajoitetaan aiheetonta puuttumista yksityiselämän suojaan, joka voi tulla selkeimmin esiin tilanteessa, jos sinänsä tiedustelumenetelmän käytön edellytykset täyttyvät, mutta tiedustelumenetelmään käytettäessä huomataan asian tilan olevan täysin toinen.

Tiedustelukieltoa koskevilla sotilastiedustelusta annetun lain 82 ja 83 §:n säännöksillä on vastineensa oikeudenkäymiskaaren (4/1734) 17 luvun (571/1948) todistamiskieltoa koskevissa säännöksissä sekä pakkokeinolain 7 luvun 3 §:n takavarikko- ja jäljentämiskielloissa. Erona rikoksiin liittyvistä kuuntelu- ja katselukielloista on toki se, että sotilastiedustelun tarkoituksena ei ole toteuttaa rikosvastuuta. Kuuntelu- ja katselukieltojen tarkoituksena on siten kieltää oikeusvaltiollisten perusteiden vastaisten tietojen käyttö ja suojata luottamuksellisen viestin salaisuutta ja ihmisten yksityiselämää.

Merkittävimpänä tiedustelukieltona voidaan kuitenkin pitää tietoliikennetiedustelua koskevaa kieltoa: tietoliikennetiedustelussa ei voida pystytä varmistumaan täysin siitä, että järjestelmään tuleva tietoliikenne olisi aidosti ja tarkoitetusti luonteelta Suomen rajan ylittävää. Näin ollen järjestelmän piiriin tulee väistämättä myös Suomen sisäiseksi tarkoitettua tietoliikennettä. Tiedustelukiellon perustella tietoliikenne, jonka lähettäjä ja vastaanottaja ovat Suomessa, on hävitettävä. Tietoliikennetiedustelua koskevaa myös vastaavat kiellot, mitä lain 82 ja 83 §:ssä säädetään.

Tiedustelutietojen hävittämisen mukaan tiedustelumenetelmällä saatu tieto on hävitettävä viipymättä sen jälkeen, kun on käynyt ilmi, ettei tietoa tarvita sotilastiedustelun tehtävien

hoitamiseksi tai maanpuolustuksen kannalta taikka kansallisen turvallisuuden suojaamiseksi. Kyse on tiedustelutietojen yleisestä hävittämisvelvollisuudesta, joka koskee kaikkia tiedustelumenetelmiä ja kaikkea niillä saatua tietoa. Hävittämisvelvollisuus realisoituu heti, kun tiedon merkityksettömyys käy ilmi.

Vastaavasti tietojen hävittäminen koskee myös kiiretilanteessa päätetyssä tiedustelumenetelmän käytöstä saatuja tietoja tilanteessa, jossa kiireisestä tiedustelumenetelmän käytöstä päätöksen tehneen päätös ei pidä varsinaisessa päätöksenteossa. Näissä tilanteissa tiedustelumenetelmän käytöllä saatu tieto on hävitettävä välittömästi.

Tallenteiden ja asiakirjojen tarkastamista ja tallenteiden tutkimista koskevat säännökset takaavat omalta osaltaan yksilön oikeusturvaa rajoittamalla yksityiselämän suojaan puuttumista. Tarkastamisella ja tietojen hävittämisellä voidaan varmistua siitä, että vain asianmukaisia tietoja käytetään ja että esimerkiksi sivullisia koskevat tiedot hävitetään. Tarkastamisella ja tietojen hävittämisellä voidaan varmistua siitä, että vain asianmukaisia tietoja käytetään ja että esimerkiksi sivullisia koskevat tiedot hävitetään. Säännökset takaavat omalta osaltaan yksilön oikeusturvaa rajoittamalla yksityiselämän suojaan puuttumista.

Tiedustelumenetelmän käytön keskeyttämisestä säädetään sotilastiedustelusta annetun lain 85 §:ssä. Pykälän 1 momentin mukaan, jos käy ilmi, että telekuuntelu kohdistuu muuhun kuin luvan kohteena olevalta henkilöltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin taikka että teknisen kuuntelun kohteena oleva henkilö ei oleskele kuunneltavassa tilassa tai muussa paikassa, tiedustelumenetelmän käyttö on siltä osin keskeytettävä niin pian kuin mahdollista sekä kuuntelulla saadut tallenteet ja sillä saatuja tietoja koskevat muistiinpanot heti hävitettävä.

Vastaavasti pykälän 2 ja 3 momentissa säädetään radiosignaalitiedustelun keskeyttämisestä ja teknisen laitetarkkailun keskeyttämisestä.

Tietoliikennetiedustelun osalta keskeyttäminen on säädetty 86 §:n 1 momentin viittauksella lain 82 §:n 2 momenttiin. Näin ollen, jos tietoliikennetiedustelun aikana tai muulloin ilmenee, että kyseessä on viesti, jonka kuuntelu ja katselu on kielletty, toimenpide on keskeytettävä ja sillä saadut tallenteet ja sillä saatuja tietoja koskevat muistiinpanot on hävitettävä välittömästi. Toisin sanoen, jos tietoliikennetiedustelussa käytetty hakuehto kohdistuu väärään kohteeseen tai tietoliikenteeseen, johon se ei saisi kohdistua, hakuehdon käyttö on lopetettava ja sillä saadut tiedot poistettava.

Tiivistäen minimointimekanismit takaavat osaltaan yksilön oikeusturvaa ja ehkäisevät viranomaisen mielivaltaa. Kokonaisuutena arvioiden voidaan katsoa, että Suomessa säädetty kattavasti minimointimekanismeista. Lainsäädännössä on säännelty esimerkiksi tallenteiden ja asiakirjojen tarkastamisesta, tallenteiden tutkimisesta sekä tietojen hävittämisestä. Lisäksi on säädetty tiedustelukielloista. Minimointimekanismeja koskeva sääntely vaikuttaisi yleisesti ottaen myös vastaavan hyvin Euroopan ihmisoikeussopimuksen vaatimuksia.

Oikeasuhtaisuuden ja ennakoitavuuden toteutumista takaa se, että sotilastiedusteluviranomaisella on velvollisuus hävittää tiedustelukieltojen ja hävittämisvelvollisuuden alainen tieto. Menettelyä voidaan pitää omalta osaltaan riittävänä takaamaan yksilön oikeusturvaa ja oikeusvaltion periaatteiden toteutumista. Tiedustelukieltojen ja hävittämisvelvollisuuksien toteutumista valvovaa viranomaisen ulkopuolinen taho, tiedusteluvalvontavaltuutettu.

2.2.2 Haittaohjelmaa koskevan tiedon luovuttaminen

Yhteistyöstä muiden viranomaisten sekä yritysten ja muiden yhteisöjen kanssa säädetään sotilastiedustelusta annetun lain 18 §:ssä. Sen 2 momentin mukaan sotilastiedusteluviranomainen voi salassapitosäännösten estämättä tehtävänsä toteuttamiseksi luovuttaa yrityksille ja muille yhteisöille tiedustelun menetelmien ja järjestelmien kehittämiseksi haittaohjelmaan liittyvän tunnistamistiedon tai luovuttaa muun kuin henkilötiedon, jos tietojen luovuttaminen on välttämätöntä Puolustusvoimien toiminnan tai kansallisen turvallisuuden suojaamiseksi.

Lisäksi haittaohjelmaa koskevia tietoja voidaan luovuttaa lain 74 §:n nojalla, jos tieto on saatu käyttämällä tietoliikennetiedustelua.

2.2.3 Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen

Sotilastiedustelusta annetun lain 42 §:n mukaan sotilastiedusteluviranomaisen palveluksessa olevalla virkamiehellä on oikeus sijoittaa telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tekniseen kuunteluun, tekniseen katseluun, tekniseen seurantaan tai tekniseen laitetarkkailuun käytettävä laite, menetelmä tai ohjelmisto toimenpiteen kohteena olevaan esineeseen, aineeseen, omaisuuteen, tilaan tai muuhun paikkaan taikka tietojärjestelmään, jos mainitun tiedustelumenetelmän käyttö sitä edellyttää. Sotilastiedusteluviranomaisen 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. Laitteen, menetelmän tai ohjelmiston asentaminen tai sen poisottaminen ei saa tapahtua pysyväisluonteiseen asumiseen käytettävässä tilassa.

Lain esitöiden (HE 203/2017 vp, s. 253) mukaan säännöksessä on kyse ennen kaikkea tarkkailutyyppisiä keinoja tukevasta toimenpiteestä, jolla käytännössä mahdollistetaan kyseessä olevan toimivaltuuden tehokas käyttö. Käytännössä lupa asentamiseen ja poisottamiseen saadaan toimivaltuuden käyttöä koskevassa päätöksessä tai luvan myöntämisen yhteydessä.

Lain esitöissä (HE 203/2017 vp, s. 253–254) todetusti soveltajan harkintaan on jätetty, missä vaiheessa toimenpiteeseen ryhdytään ja milloin toimenpiteen käyttö lopetetaan. Tiedustelumenetelmän käytön paljastumisen estämisen kannalta tätä on pidetty välttämättömänä. Toimenpiteeseen ryhdyttäessä tulee lisäksi pohdittavaksi mahdollinen kiinnijäämisriski sekä toimenpiteen suorittamisesta kohteelle aiheutuvan vahingon riski. Sotilastiedusteluviranomaisen toimenpiteillä ei siten saa aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä laitteen, menetelmän tai ohjelmiston asentamisen ja poisottamisen yhteydessä. Asentaminen ja poisottaminen on pidettävä erillään varsinaisen tiedustelumenetelmän käytöstä, jonka aloittamisesta ja lopettamisesta päätetään erikseen.

2.2.4 Tietojärjestelmään kohdistuva tiedustelu kotimaassa

Sotilastiedustelusta annettu laki antaa mahdollisuuden sotilastiedusteluviranomaiselle sähköisiin viestintä- ja tiedonkäsittelyvälineisiin ja näiden väliseen viestintään kohdistuvan tiedonhankinnan käyttäen telekuuntelua (34 §), televalvontaa (37 §), teknistä kuuntelua (26 §) ja teknistä laitetarkkailua (32 §) sekä näitä tukevia toimivaltuuksia, kuten edellä mainittuihin tiedustelumenetelmiin käytettävän laitteen, menetelmän tai ohjelmiston sijoittamista muun muassa tietojärjestelmään (42 §). Luottamuksellisen viestin salaisuuden suojaan puuttuvien menetelmien kasuistisesta sääntelystä johtuen edellä mainittuja menetelmiä joudutaan lähes

poikkeuksetta käyttämään rinnan toistensa kanssa hankittaessa tietoa samasta uhkasta, esimerkiksi vieraan valtion kyberuhkatoiminnasta. Vaikka useita menetelmiä on välttämätöntä käyttää samanaikaisesti riittävän tiedon hankkimiseksi uhkasta, voi niiden rinnakkaiskäytölle muodostaa esteen se, että eri menetelmien kohdistaminen on määritelty toisistaan poikkeavalla tavalla.

Sotilastiedustelusta annetun lain 34 §:n 1 momentin mukaan telekuuntelulla tarkoitetaan teleosoitteeseen tai telepäätelaitteeseen vastaanotettavan taikka siitä lähetetyn sähköisen viestinnän palveluista annetun lain (917/2014) 3 §:n 43 kohdassa tarkoitetussa yleisessä viestintäverkossa tai siihen liitetyssä viestintäverkossa välitettävänä olevan viestin kuuntelua, tallentamista ja muuta käsittelyä viestin sisällön ja siihen liittyvien välitystietojen selvittämiseksi.

Sotilastiedustelusta annetun lain 36 §:n 3 momentin mukaan telekuuntelua koskevassa vaatimuksessa ja päätöksessä on mainittava toimenpiteen kohteena oleva henkilö, teleosoite tai telepäätelaite.

Sotilastiedustelusta annetun lain 37 §:n 1 momentin mukaan televalvonnalla tarkoitetaan tunnistamistietojen hankkimista viestistä, joka on lähetetty viestintäverkkoon kytketystä teleosoitteesta tai telepäätelaitteesta taikka vastaanotettu tällaiseen osoitteeseen tai laitteeseen, sekä teleosoitteen tai telepäätelaitteen sijaintitiedon hankkimista.

Sotilastiedustelusta annetun lain 38 §:n 3 momentin mukaan televalvontaa koskevassa vaatimuksessa ja päätöksessä on mainittava, vastaavasti kuin telekuuntelua koskevassa vaatimuksessa ja päätöksessä, toimenpiteen kohteena oleva henkilö, teleosoite tai telepäätelaite.

Sotilastiedustelusta annetun lain 32 §:n 1 momentin mukaan teknisellä laitetarkkailulla tarkoitetaan tietokoneen tai muun vastaavan teknisen laitteen taikka sen ohjelmiston toiminnan, sisältämien tietojen tai yksilöintitietojen muuta kuin yksinomaan aistinvaraista tarkkailua, tallentamista tai muuta käsittelyä rikoksen estämiselle merkityksellisen seikan tutkimiseksi.

Sotilastiedustelusta annetun lain 33 §:n 3 momentin mukaan teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava toimenpiteen kohteena oleva tekninen laite tai ohjelmisto.

Sotilastiedustelusta annetun lain 26 §:n 1 momentin mukaan teknisellä kuuntelulla tarkoitetaan rikoslain 24 luvun 5 §:n estämättä tapahtuvaa tietyn henkilön sellaisen keskustelun tai viestin, joka ei ole ulkopuolisten tietoon tarkoitettu ja johon keskusteluun kuuntelija ei osallistu, kuuntelua, tallentamista ja muuta käsittelyä teknisellä laitteella, menetelmällä tai ohjelmistolla keskustelun tai viestin sisällön tai sen osapuolten taikka 4 momentissa tarkoitetun henkilön toiminnan selvittämiseksi.

Sotilastiedustelusta annetun lain 27 §:n 4 momentin mukaan teknistä kuuntelua koskevassa vaatimuksessa ja päätöksessä on mainittava toimenpiteen kohteena oleva henkilö tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmä riittävästi yksilöitynä taikka tila tai muu paikka.

Teknisen kuuntelun toimivaltuutta voitaneen luonnehtia luottamuksellisen viestin suojaa nauttivaan viestintään kohdistuvan tiedon hankkimisen mahdollistavaksi yleistoimivaltuudeksi. Teknisen kuuntelun soveltamisalaa ei ole suoraan rajoitettu kyseisen toimivaltuuden määritelmäsäännöksessä. Sen sijaan sen soveltamisalaa on kavennettu säätämällä erikseen telekuuntelusta, televalvonnasta ja teknisestä laitetarkkailusta sekä niiden määritelmistä. Telekuuntelun ja televalvonnan määritelmäsäännöksistä ilmenee, että kyseisiä toimivaltuuksia

sovelletaan silloin, kun tiedonhankinta kohdistuu yleisessä viestintäverkossa tai siihen liitetyssä viestintäverkossa välitettävänä olevaan viestiin. Telekuuntelu ja televalvonta lienee ollut välttämätöntä erottaa teknisen kuuntelun alasta pääasiassa siksi, että ne muusta viestintään kohdistuvasta tiedonhankinnasta poiketen on pääsääntöisesti välttämätöntä toteuttaa viestinnän välittäjän (teleyrityksen) avustuksella, ja viestinnän välittäjän velvollisuudesta avustaa viranomaista telekuuntelun ja -valvonnan toteuttamisessa on siksi ollut tarve säätää erikseen. Teknisen laitetarkkailun määritelmäsäännöksen mukaan, jos viestintää koskeva tieto tai muu tieto sijaitsee teknisessä laitteessa, sovelletaan teknisen kuuntelun toimivaltuuden sijasta teknisen laitetarkkailun toimivaltuutta.

Sotilastiedustelusta annetun lain 32 §:n 2 momentissa on erikseen säädetty, että teknistä laitetarkkailua ei saa kohdistaa sellaiseen luottamukselliseen viestiin, jota koskevasta telekuuntelusta, televalvonnasta ja muusta teknisestä tarkkailusta säädetään erikseen.

Teknisen laitetarkkailun käyttöä koskeva tuomioistuimelle esitettävä vaatimus ja tuomioistuimen päätös sen sijaan eivät voi koskea henkilöä, vaan ne koskevat nykysääntelyn nojalla aina yksittäistä laitetta tai laitteen sisältämää ohjelmistoa.

Sotilastiedustelusta annetun lain 62 §:ssä säädetään ulkomaan tietojärjestelmätiedustelusta. Pykälän 1 momentin mukaan ulkomaan tietojärjestelmätiedustelulla tarkoitetaan tietoteknisin menetelmin suoritettavaa tietojen hankkimista Suomen ulkopuolelta olevasta tietojärjestelmästä. Puolustusvoimien tiedustelulaitos saa kohdistaa tietojärjestelmään ulkomaan tietojärjestelmätiedustelua, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

2.2.5 Tekninen laitetarkkailu

Sotilastiedustelusta annetun lain 32 §:n 1 momentin mukaan teknisellä laitetarkkailulla tarkoitetaan tietokoneen tai muun vastaavan teknisen laitteen taikka sen ohjelmiston toiminnan, sisältämien tietojen tai yksilöintitietojen muuta kuin yksinomaan aistinvaraista tarkkailua, tallentamista tai muuta käsittelyä tiedustelutehtävän kannalta tarpeellisen seikan selvittämiseksi.

Pykälän 2 momentin mukaan teknisellä laitetarkkailulla ei saa hankkia tietoa välitettävänä olevasta 34 §:ssä tarkoitetusta viestistä tai sen tunnistamistiedoista.

Pykälän 3 momentin mukaan sotilastiedusteluviranomaiselle voidaan antaa lupa valtiollisen toimijan tekniseen laitetarkkailuun tiedustelutehtävän suorittamiseksi.

Pykälän 4 momentin mukaan sotilastiedusteluviranomaiselle voidaan antaa lupa muun kuin valtiollisen toimijan tekniseen laitetarkkailuun, jos sillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Sotilastiedusteluviranomainen voi kohdistaa teknistä laitetarkkailua tiedustelutehtävään liittyvän henkilön todennäköisesti käyttämään tietokoneeseen tai muuhun vastaavaan tekniseen laitteeseen taikka sen ohjelmiston toimintaan.

Sotilastiedustelusta annetun lain 33 §:ssä säädetään teknisestä laitetarkkailusta päättämisestä. Sen 1 momentin mukaan tuomioistuin päättää teknisestä laitetarkkailusta tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta. Jos asia ei siedä viivytystä, tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää teknisestä laitetarkkailusta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia

on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua tiedustelumenetelmän käytön aloittamisesta.

Pykälän 2 momentin mukaan lupa voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Pykälän 3 momentin mukaan teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava: 1) toimenpiteen perusteena oleva tiedustelutehtävä, 2) toimenpiteen kohteena oleva tekninen laite tai ohjelmisto, 3) tosiseikat, joihin teknisen laitetarkkailun edellytykset ja kohdistaminen perustuvat, 4) luvan voimassaoloaika kellonajan tarkkuudella, 5) teknistä laitetarkkailua johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies ja 6) mahdolliset teknisen laitetarkkailun rajoitukset ja ehdot.

2.2.6 Tietoliikennetiedustelu

2.2.6.1 Tietoliikenteen teknisten tietojen käsittely

Teknisten tietojen käsittelystä säädetään sotilastiedustelusta annetun lain 66 §:ssä. Sen 1 momentin mukaan tietoliikennetiedustelun kohdentamiseksi Puolustusvoimien tiedustelulaitos voi viestintäverkon tietoliikenteestä hetkellisesti kerätä ja tallentaa tietoliikenteen teknisiä tietoja ja automaattisen tietojenkäsittelyn avulla käsitellä niitä tilastollista analyysiä varten.

Pykälän 2 momentin mukaan tilastollisen analyysin tulokseen ei saa sisältyä tietoa, josta voidaan tunnistaa yksittäinen luonnollinen henkilö.

Pykälän 3 momentin mukaan Puolustusvoimien tiedustelulaitoksen on hävitettävä kerätyt ja tallennetut tietoliikenteen tekniset tiedot välittömästi sen jälkeen, kun tilastollisen analyysin tulos on valmistunut.

2.2.6.2 Tietoliikennetiedustelun hakuehdot

Sotilastiedustelusta annetun lain 10 §:n 1 momentin 1 kohdan mukaan hakuehdolla tarkoitetaan tietoa, jonka perusteella tietoliikennetiedustelulla viestintäverkon osasta mahdollisimman rajatusti ja täsmällisesti valitaan tietoliikennetiedustelun kohteena oleva tietoliikenne ja puuttuminen luottamuksellisen viestin salaisuuden suojaan rajautuu tiedustelun tarkoituksen kannalta välttämättömään. Määritelmä on tehty eduskunnan myötävaikutuksella (PuVM 9/2018 vp. ja PeVL 36/2018 vp, ja PeVL 76/2018 vp.).

Sotilastiedustelusta annetun lain 68 §:n 3 momentin ja 70 §:n 2 momentin mukaan tietoliikennetiedustelussa ei saa hakuehtona käyttää Suomessa olevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.

Lain esitöissä (HE 203/2017 vp, s. 287) säännöstä perustellaan sillä, että jos telepäätelaitteen tai telepäätelaitteen haltija olisi Suomessa ja kyseisen telepäätelaitteen tai -osoitteen yksilöintitiedot olisivat sotilastiedustelun tiedossa, olisi tiedonhankinta suoritettava sotilastiedustelusta annetun lain 4 luvussa säädettyjen muiden tiedustelumenetelmien – telekuuntelun, tietojen hankkimisen telekuuntelun sijasta tai televalvonnan – avulla, sikäli kuin niille säädetyt edellytykset täyttyvät. Hallituksen esityksen mukaan tällä tavalla pystyttäisiin minimoimaan vaikutus sivullisten tietoliikenteeseen.

Lain 70 §:n 3 momentin mukaan pykälän tarkoittamassa tietoliikennetiedustelussa tietoliikenteen tiedustelun kohdentaminen ei saa tapahtua viestin sisällön perusteella, jollei

kohdentamisessa käytetä haittaohjelman sisältöä kuvaavaa tietoa. Muissa tapauksissa viestin sisältöä koskevan hakuehdon käyttö tietoliikenteen automaattisessa erottelussa on siis kielletty.

Edellä mainitun ns. sisällöllisen hakuehdon käytön kiellon todetaan lain esitöissä (HE 203/2017 vp, s. 144, 283, 287) tarkoittavan sitä, että luottamuksellisen viestin sisältöä kuvaavan hakuehdon käyttö on tietoliikennetiedustelussa täysin kielletty, eikä hakuehtoina siten saada käyttää luottamuksellisen viestin semanttiseen sisältöön kuuluvia ilmaisuja tai henkilöiden nimi- tai yksilöintietoja. Lain esitöiden mukaan kyse on tiedustelutoiminnalle asetetusta merkittävästä rajoituksesta, jonka tarkoituksena olisi mahdollisimman pitkälle turvata sivullisen asemassa olevien henkilöiden viestintäsalaisuuden ydinalue.

2.2.6.3 Tietoliikennetiedustelulla hankittujen tietojen hävittäminen

Sotilastiedustelusta annetun lain 86 §:ssä säädetään tietoliikennetiedustelulla hankittujen tietojen hävittämisestä. Pykälän 1 momentin mukaan sen lisäksi, mitä 82 §:n 2 momentissa säädetään, tietoliikennetiedustelulla saatu tieto on hävitettävä viipymättä sen jälkeen, jos on käynyt ilmi, että 1) viestinnän molemmat osapuolet olivat Suomessa silloin, kun viestintä tapahtui tai 2) lähettäjällä tai vastaanottajalla taikka tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta kyseisestä tiedosta 82 §:n 1 momentissa mainittujen säännösten nojalla.

Pykälän 2 momentin mukaan hävittämisestä vastaa sotilastiedusteluviranomainen. Jos Puolustusvoimien tiedustelulaitos on toimittanut tiedot suojelupoliisille tietoliikennetiedustelun teknisessä toteuttamisessa suojelupoliisin puolesta, hävittämisestä vastaa suojelupoliisi.

2.2.7 Maanpuolustusta ja kansallista turvallisuutta vaarantavaan tietojärjestelmän toimintaan puuttuminen

2.2.7.1 Kansainvälinen oikeus

Kansainvälinen oikeus kyberympäristössä

Suomi on julkistanut näkemyksensä kansainvälisestä oikeudesta kyberympäristössä 15.10.2020. Suomi katsoo, että kansainvälinen oikeus luo olennaiset puitteet vastuulliselle valtiokäyttäytymiselle kyberympäristössä. Myös YK:n hallitustenvälinen asiantuntijaryhmä (GGE) on samansuuntaisesti vahvistanut, että ”kansainvälinen oikeus ja varsinkin Yhdistyneiden Kansakuntien peruskirja ovat sovellettavissa [kyberympäristössä] ja olennaisia tekijöitä rauhan ja turvallisuuden ylläpitämisen samoin kuin avoimen, turvallisen, vakaan, saavutettavan ja rauhanomaisen informaatio- ja kommunikaatioteknologisen ympäristön edistämisen kannalta”. Kansainvälinen oikeus soveltuu siis myös kybertoimintaympäristöön.

Suomi katsoo, että *valtion täysivaltaisuuden eli suvereenisuuden periaate* koskee kiistatta kyberympäristöä. Suvereenisuus on kansainvälisen oikeuden primäärinormi, jonka loukkaus merkitsee kansanvälisesti oikeudenvastaista tekoa ja synnyttää valtion vastuun. Tämä sääntö koskee täysin myös kyberympäristöä. Luvattoman kybertunkeutumisen luonteesta ja seurauksista riippuu, katsotaanko sen loukkaavan kohdevaltion suvereenisuutta. Kyse on tapauskohtaisesta arvioinnista.

Useat valtiot pitävät mitä tahansa luvatonta tunkeutumista toisen valtion tietojärjestelmiin suvereniteetin loukkauksena, vaikka siinä ei aiheutettaisi fyysistä vahinkoa. Lisäksi laajasti on

jaettu näkemys, että suvereniteettia loukataan tilanteissa, joissa kyberoperaatio aiheuttaa pysyvän toimintakyvyn menetyksen taikka fyysistä vahinkoa tai henkilövahinkoja.

Yhdistyneiden kansakuntien yleiskokous on useilla päätöslauselmillaan vahvistanut YK:n alaisen asiantuntijaryhmän (UNGGE) vuonna 2015 hyväksymät vapaaehtoiset normit, jotka koskevat vastuullista valtiokäyttäytymistä kyberympäristössä. Normin 13 (b) mukaan valtioiden ei tulisi harjoittaa tai tietoisesti tukea ICT-toimintaa, joka tahallaan vahingoittaa kriittistä infrastruktuuria.

Tahallinen toisen valtion tietojärjestelmän vahingoittaminen tai sen käytön estäminen voidaan tulkita suvereniteetin loukkaukseksi. Epäselvempiä ovat tilanteet, joissa kohteena olevan järjestelmän tietoja ainoastaan manipuloidaan. On katsottu, että valtion datan, tietojärjestelmien ja infrastruktuurin häiritseminen olisi katsottava suvereniteetin loukkaukseksi, jos vaikutukset eivät ole vähäisiä.

Vihamielinen kyberhäirintä voi rikkoa myös tapaoikeudellista *toisen valtion sisäisiin asioihin puuttumisen kieltoa* edellyttäen, että sen tarkoituksena on painostaa tai pakottaa kyseistä valtiota asioissa, joiden suhteen sillä on vapaa määräysvalta (nk. domaine réservé).

Kyberympäristössä tällaisina toimina on pidetty muun muassa vaalijärjestelmän manipulointia, hallinnon tietojärjestelmien lamauttamista sekä julkisten palveluiden tarkoituksellista häirintää. Toiminnan luonteesta riippuen kyse voi olla sekä suvereniteetin että sisäisiin asioihin puuttumisen kiellon soveltamisesta.

Oma kysymyksensä on etenkin viime aikoina taajaan havaitut *laaja-alaiset ns. low-intensity -kybertoimet*. Monet nykyiset kyberoperaatiot ovat matalan intensiteetin toimia, jotka eivät aiheuta fyysistä vahinkoa. Niissä voidaan tunkeutua järjestelmiin, kerätä tietoa ja asentaa haitallisia ohjelmistoja myöhempää käyttöä varten. Lisäksi saatetaan aiheuttaa laajasti pienempää haittaa organisaation toiminnalle esimerkiksi hidastamalla tietojärjestelmien toimintaa. Joka tapauksessa toiminta pyritään pitämään kansainvälisen oikeuden loukkauksen alapuolella tai ainakin sellaisena, ettei sitä suoranaisesti voida loukkaukseksi tulkita.

Valtiot ovat erimielisiä siitä, loukkaavatko matalan intensiteetin kyberoperaatiot suvereniteettia. Osa valtioista katsoo, että vain vaikutuksiltaan merkittävät teot – esimerkiksi fyysistä vahinkoa tai vakavaa toiminnallista häiriötä aiheuttavat operaatiot – voivat loukata suvereniteettia. Toisten valtioiden mukaan kaikki ei-luvattomat tunkeutumiset toisen valtion tietojärjestelmiin ovat jo itsessään suvereniteetin loukkaus riippumatta siitä, syntyykö konkreettista vahinkoa. Jokaisella valtiolla on velvoite olla sallimatta sitä, että sen aluetta käytetään tavalla, joka aiheuttaa merkittävää haittaa muiden valtioiden oikeuksille. Tämä koskee myös kyberympäristöä. Tämä *huolenpitovelvoite (due diligence)* koskee kaikkia toimintoja, joihin sisältyy riski merkittävän rajat ylittävän haitan tuottamisesta.

Vaikka huolenpitovelvoitteen velvoittavuudesta kyberympäristössä on valtioiden välillä erimielisyyttä, velvoitteen sisällöstä on kuitenkin yhteneväisempi näkemys. Huolenpitovelvoite on lähtökohtaisesti toimimisvelvoite, ei lopputulosvelvoite, joten se ei edellytä haitallisten toimenpiteiden täydellistä estämistä. Se kuitenkin edellyttää kohtuullisia toimia, kun valtio tietää tai sen pitäisi tietää haitallisesta kybertoiminnasta alueellaan.

Yleisesti kyberympäristössä kohtuulliset estotoimet edellyttävät valtiota ryhtymään käytännöllisiin, teknisesti ja poliittisesti realistisiin toimiin estääkseen haitallisia kybertoimia, jos se on tietoinen niistä. Velvollisuus puuttua haitallisiin kyberoperaatioihin edellyttää valtioilta pyrkimyksiä pysäyttää tai rajoittaa sen alueelta lähteviä hyökkäyksiä, myös tekijän

ollessa kolmas osapuoli. Edellä todettujen lisäksi valtioilla on velvollisuus olla sallimatta verkkojen käyttöä toisen valtion oikeuksien vastaisesti.

Kun valtion kyberoperaatio loukkaa sen kansainvälisen oikeuden mukaisia velvoitteita, kyseessä on kansainvälisesti oikeudenvastainen teko. *Syyksilukemista* koskevat säännöt YK:n kansainvälisen oikeuden toimikunnan valtiovastuuartikloissa pätevät myös kyberympäristössä. Jos valtion elimiä tai yksityisiä ryhmiä tai yksityishenkilöitä, jotka toimivat valtion puolesta, voidaan tunnistaa valtion kansainvälisiä velvoitteita loukkaavan kyberoperaation tekijöiksi, valtiolla on niistä vastuu.

Vakiintunutta määritelmää siitä, milloin kyberhyökkäys vastaisi YK:n peruskirjan 2 artiklan 4 kappaleen tarkoittamaa *voimankäyttöä* tai 51 artiklan tarkoittamaa *aseellista hyökkäystä* ei toistaiseksi ole olemassa. On kuitenkin laajasti hyväksytty, että vastaavuus riippuu kyberhyökkäyksen seurauksista. Vastaavasti useimmat asiaa kommentoineet ovat samaa mieltä siitä, että mittakaavaltaan ja vaikutuksiltaan aseelliseen hyökkäykseen verrattava kyberhyökkäys vastaa aseellista hyökkäystä ja siihen voidaan vastata itsepuolustuksellisesti. Itsepuolustuksellinen voimankäyttö ei kuitenkaan saa olla suhteetonta tai ylimitoitettua. Kyberympäristössäkin tulee noudattaa sekä YK:n peruskirjan voimankäyttöä koskevia määräyksiä että peruskirjan tarkoitusta ja päämäärää, joka on aseellisen toiminnan eskaloitumisen estäminen.

Kansainvälinen humanitaarinen oikeus soveltuu kyberoperaatioihin vain, jos ne ovat osa aseellista konfliktia tai käynnistävät aseellisen konfliktin. Ei ole mitään syytä kiistää sitä, että kansainvälisen humanitaarisen oikeuden tarjoamaa suojaa tarvitaan silloin, kun kyberkeinoihin turvaudutaan käynnissä olevissa aseellisissa konflikteissa.

Aseellisessa selkkauksissa kaikkia aseita ja sodankäyntimenetelmiä on käytettävä siten, että kyetään noudattamaan kansainvälisen humanitaarisen oikeuden keskeisiä periaatteita, muun muassa erottelu periaatetta (*distinction*), suhteellisuusperiaatetta (*proportionality*) ja varotoimien periaatetta (*precautions*) samoin kuin näihin periaatteisiin perustuvia erityisiä sääntöjä.

Kansainvälisen humanitaarisen oikeuden mukaan sotatoimia saa kohdistaa vain sotilaskohteisiin ja taistelijoihin, ei siviileihin tai siviilikohteisiin. Erotteluperiaate tarkoittaa käytännössä sitä, ettei aseellisessa selkkauksessa saa toimenpiteitä kohdistaa suoraan esimerkiksi siviilien tietokoneisiin, sähköverkkoihin tai sairaalajärjestelmiin. Oman haasteen tuo se, että usein etenkin tieto- ja sähköverkkoja käytetään myös sotilaalliseen toimintaan. Kansainvälisen humanitaarisen oikeuden mukaan sotilaallisia kohteita ovat vain sellaiset kohteet, jotka luonteensa, sijaintinsa, tarkoituksensa tai käyttönsä vuoksi muodostavat tärkeän osan sotilastoiminnasta ja joiden täydellinen tai osittainen tuhoaminen, haltuunotto tai vaarattomaksi saattaminen merkitsee kulloinkin vallitsevissa olosuhteissa selvää sotilaallista hyötyä. Jos on epätietoisuutta siitä, onko jokin kohde siviili- vai sotilaskohde, kohdetta on pidettävä siviilikohteena.

Suhteellisuusperiaatteen mukaan hyökkäys on kielletty, jos sen odotettavissa olevat siviilivahingot ovat liian suuria suhteessa saavutettavaan välittömään sotilaalliseen hyötyyn. Tämän arvion tekeminen vaatii kunkin toimen osalta tapauskohtaista arviointi. Esimerkiksi, jos kybertoimenpide leviää armeijan viestintäjärjestelmästä ja lamauttaa samalla kaupungin sairaaloiden tietojärjestelmät, isku on todennäköisesti suhteellisuusperiaatteen vastainen ja laiton.

Sotatoimien yhteydessä on jatkuvasti huolehdittava siviiliväestön ja siviilikohteiden säästämisestä ja selkkausten osapuolten tulee ryhtyä kaikkiin käytettävissä oleviin varotoimiin niin hyökkäyksen yhteydessä kuin hyökkäysten vaikutusten varalta minimoidakseen sotatoimista siviiliväestölle ja -kohteille aiheutuvaa vahinkoa. Tämä korostaa sitä, että toimenpiteiden suorittajan on muun muassa käytettävä sellaisia keinoja, jotka on mahdollista rajata vain haluttuun kohteeseen. Käytännössä tämä tarkoittaa sitä, että kyse ei voi olla itsestään levittyvästä haittaohjelmasta tai koodista.

Arvioitaessa sitä, voivatko tietyt kyberkeinot tai menetelmät tuottaa kiellettyä vahinkoa, myös niiden nähtävissä olevat suorat ja epäsuorat vaikutukset tulee ottaa huomioon. Jatkuvasti on huolehdittava siitä, että siviiliväestön ja siviilikohteiden mukaan lukien olennaisen siviili-infrastruktuurin, siviileille tarkoitettujen palvelujen ja siviilitietojen (*civilian data*) suojelu voidaan varmistaa.

Lisäksi tietyt henkilöt ja kohteet nauttivat kansainvälisen humanitaarisen oikeuden alaista erityistä suojelua. Tallaisia ovat esimerkiksi lääkintähenkilöstö ja lääkintäyksiköt, kuten sairaalat ja niiden digitaalinen infrastruktuuri, humanitaarinen avustushenkilöstö ja humanitaarisiin avustusoperaatioihin käytettävät kohteet sekä sellaiset vaarallisia voimia sisältävät laitokset ja rakennelmat (padot, tulvapenkereet, ydinkäyttöiset sähkövoimalaitokset), joihin kohdistuva aseellinen toiminta voi aiheuttaa vaarallisten voimien vapautumisen ja sen seurauksena vakavia vahinkoja siviiliväestölle.

Yksilöt nauttivat samoista *ihmisoikeuksista* ja valtioilla on samat ihmisoikeusvelvoitteet niin verkossa kuin sen ulkopuolella. Lisäksi kullakin valtiolla on alueellaan ja lainkäyttövaltansa piirissä velvoite suojella yksilöitä näiden oikeuksien loukkauksilta muiden tahojen toimesta.

Toimenpiteet vihamielistä kybertoimintaa vastaan

Valtioilla on käytössään useita kansainvälisoikeudellisia laillisia keinoja, joilla valtio voi vastata sitä kohtaan tehtyyn suvereniteettirikkomukseen.

Retorsio tarkoittaa valtion epäystävällistä, mutta täysin laillista vastausta toisen valtion edeltävään toimintaan. Tyypillisiä retorsiotoimia ovat esimerkiksi diplomaattiset protestit sekä taloudelliset ja kaupalliset rajoitukset. Retorsiota voidaan käyttää myös silloin, kun alkuperäinen kybertoimi ei yksiselitteisesti olisi kansainvälisen oikeuden vastainen. Retorsiot eivät itsessään loukkaa kansainvälistä oikeutta, koska ne pysyvät valtion suvereenin harkintavallan piirissä.

Vastatoimet ovat sallittuja vain, jos edeltävä kansainvälisen oikeuden loukkaus voidaan lukea jonkin valtion syyksi. Vastatoimien poikkeuksellisesta luonteesta johtuen niiden käyttöä on rajoitettu monella tapaa. Keskeisin rajoitus on, että vastatoimien on oltava luonteeltaan väliaikaisia. Vastatoimella on myös oltava ajallinen yhteys kärsittyyn oikeudenloukkaukseen, eikä vastatoimiin voida ryhtyä jälkikäteen oikeudenloukkauksen päätyttyä. Nämä rajoitukset liittyvät siihen, että vastatoimia ei voi käyttää rangaistuksenluonteisesti vaan niiden ainoa laillinen tavoite on saada oikeudenloukkauksesta vastuussa oleva valtio lopettamaan oikeudenvastainen toimintansa ja tarvittaessa korvaamaan aiheuttamansa vahinko. Vastatoimia koskee myös suhteellisuusvaatimus: vastatoimien on oltava yhteismitallisia oikeudenloukkauksen vakavuuden, kyseessä olevan oikeuden ja kärsityn vahingon kanssa. Vastatoimia koskien on myös menettelysääntöjä, joiden mukaan vastatoimesta on ilmoitettava

etukäteen sen kohteena olevalle valtiolle. Vaatimuksesta voidaan poiketa, jos tilanne on niin kiireellinen, että se ei salli etukäteistä ilmoittamista. Edellytykset tulevat kansainvälisen oikeuden yleisestä valtiovastuusäännöistä.

Itsepuolustusoikeuden perusteella suoritettavat toimenpiteet ovat sallittuja ainoastaan, jos kyberhyökkäys ylittää aseellisen hyökkäyksen kynnyksen ja se voidaan lukea tietyn valtion syyksi. YK:n peruskirjan 51 artiklan mukaan valtio voi käyttää itsepuolustusta aseellista hyökkäystä vastaan. Kyberympäristössä kynnyksen voidaan katsoa ylittyvän, jos kybertoimien vaikutukset ovat fyysisesti tuhoisia, aiheuttava kuolemia tai vammoja taikka vastaavat mittakaavaltaan ja vaikutuksiltaan perinteistä aseellista hyökkäystä (esimerkiksi infrastruktuurin tuhoutuminen). Perustellusti katsotaan, että tällaisen hyökkäyksen uhriksi joutunut valtio voi vastata siihen joko verkkohyökkäyksellä tai aseellisesti. Toistaiseksi yksikään valtio ei ole vedonnut itsepuolustusoikeuden käyttöön kyberympäristössä toteutetun toimenpiteen osalta.

Erityistapauksena voidaan pitää tilannetta, jossa valtio ei itse tehnyt hyökkäystä, mutta ei myöskään estänyt sen alueelta tulevaa haitallista toimintaa kohtuulliseksi katsottavin toimenpitein. Valtio voi silloin loukata huolenpitovelvoitettaan, mikä voi johtaa kansainväliseen vastuuseen. Valtiolla, jonka alueelta kyberhyökkäys tulee, on velvollisuus ryhtyä kohtuullisiin toimiin estääkseen haitallisen kybertoiminnan omalta alueeltaan ja estää ei-valtiollisten toimijoiden hyökkäykset, jos se tietää niistä. Laiminlyönti voi myös johtaa siihen, että loukattu valtio ryhtyy vastatoimiin.

Välttämättömyysperiaate (plea of necessity) on poikkeuksellinen valtiovastuusääntöjen mukainen peruste, jonka nojalla valtio voi tilapäisesti jättää täyttämättä kansainvälisen velvoitteensa, jos tämä on ainoa keino suojella olennaista valtiollista etua vakavalta ja välittömältä vaaralta. Periaatteen soveltamiskynnys on erittäin korkea: valtion toimien on oltava välttämättömiä vaaran torjumiseksi, eivätkä ne saa vakavasti vaarantaa muiden valtioiden olennaisia etuja. Lisäksi välttämättömyys ei voi oikeuttaa toimia, jotka rikkoisivat ius cogens -tasoisia normeja tai jos valtio olisi itse myötävaikuttanut uhkan syntyyn.

Välttämättömyyteen vetoamisen edellytyksenä on siis ensinnäkin se, että vaaran on kohdistuttava valtion perustavanlaatuisiin etuihin, kuten kansalliseen turvallisuuteen, väestön hyvinvointiin tai kriittiseen infrastruktuuriin, jonka romahtaminen vaarantaisi valtion elintärkeitä toimintoja. Toiseksi vaaran tulee olla konkreettinen ja nopeasti realisoituva, esimerkiksi kriittisen infrastruktuurin lamauttamiseen tähtäävä hyökkäys. Kolmanneksi välttämättömyys soveltuu vain, jos mitään muuta laillista keinoa ei ole käytettävissä (esimerkiksi diplomatia, retorsio tai kohdennetut vastatoimet). Neljänneksi toimenpide ei saa loukata toisen valtion olennaisia etuja.

Kyberkontekstissa välttämättömyysperiaatteeseen vetoamista on pidetty teoreettisesti mahdollisena, mutta on arvioitu, että käytännössä sen soveltaminen olisi haastavaa, koska edellytykset sen soveltamiseen täyttyisivät harvoin. Kyberympäristön erityispiirteinä on muun muassa toiminnan nopeus, toiminnan alkuperän helppo häivytettävyys ja vahinkojen nopea eskaloituminen. Välttämättömyyden voidaankin katso olevan viimekätinen peruste oman velvoitteen tilapäiseen noudattamatta jättämiseen erittäin poikkeuksellisessa tilanteessa, jolloin mitään muuta keinoa elintärkeän kansallisen edun turvaamiseksi ei ole käytettävissä.

2.2.7.2 Kansallinen sääntely

Aluevalvontalain (755/2000) 1 §:ssä säädetään lain soveltamisalasta. Sen mukaan kyseisessä laissa säädetään Suomen alueellisen koskemattomuuden valvonnasta ja turvaamisesta. Lain 23

§:ssä säädetään aluevalvontaviranomaisista, joita ovat pykälän 1 momentin mukaan Puolustusvoimat, Rajavartiolaitos, poliisi, Tulli sekä niiden aluevalvontaan määrätyt virkamiehet.

Lain 31 §:ssä säädetään voimakeinojen käytöstä. Sen 1 momentin mukaan aluevalvontaviranomaisella on aluevalvontalaissa säädettyä tehtävää suorittaessaan oikeus vastarinnan murtamiseksi, henkilön kiinniottamiseksi, ajoneuvon, ilma-aluksen tai aluksen siirtämiseksi tai 25 §:ssä tarkoitetun määräyksen panemiseksi täytäntöön käyttää sellaisia tarpeellisia voimakeinoja, joita tehtävän tärkeys ja kiireellisyys, vastarinnan vaarallisuus, käytettävissä olevat voimavarat sekä muut tilanteen kokonaisarvosteluun vaikuttavat seikat huomioon ottaen voidaan pitää puolustettavina.

Pykälän 2 momentin mukaan voimakeinojen käyttämisestä päättä aluevalvontaa suorittava aluevalvontaviranomainen, jollei lain 33 tai 34 §:stä muuta johdu.

Lain 33 §:ssä säädetään sotilaallisten voimakeinojen käytöstä. Sen 1 momentin mukaan Puolustusvoimat ja rajavartiolaitos voivat käyttää Suomen alueellisen koskemattomuuden turvaamiseksi tarpeellista sotilaan henkilökohtaisen aseen käyttöä voimakkaampaa, sotavarustein tapahtuvaa asevoimaa.

Pykälän 2 momentin mukaan sotilaallisten voimakeinojen käytöstä päättää puolustusministeriö, jollei puolustusvoimien ylipäällikön toimivallasta muuta johdu taikka 34 §:ssä toisin säädetä.

Lain 34 §:ssä säädetään vihamielisen toiminnan torjumisesta. Sen 1 momentin mukaan Puolustusvoimien ja rajavartiolaitoksen tehtävänä on ryhtyä viivytyksettä kaikkiin tarvittaviin toimenpiteisiin valtakunnan turvallisuutta välittömästi ja vakavasti vaarantavan vihamielisen toiminnan torjumiseksi. Tällöin on tarvittaessa käytettävä sellaisia 33 §:ssä tarkoitettuja voimakeinoja, joita toiminnan vaarallisuus ja muut tilanteen kokonaisarvosteluun vaikuttavat seikat huomioon ottaen voidaan pitää puolustettavina. Toimenpiteeseen ryhtymisestä on viipymättä ilmoitettava puolustusministeriölle.

Pykälän 2 momentin mukaan vihamielisellä toiminnalla tarkoitetaan 1) vieraan valtion tai tunnuksettoman sotilaallisen ryhmän oikeudettomasti Suomen alueeseen kohdistamaa tai Suomen alueella toimeenpanemaa aseellista sotilaallista toimintaa, 2) vieraan valtion tai tunnuksettoman sotilaallisen ryhmän sota-aluksen tai sotilasilma-aluksen taikka vieraan valtion tai tunnuksettoman sotilaallisen ryhmän sotilasajoneuvon tuloa Suomen alueelle aluevalvontaviranomaisen antamasta varoituksesta huolimatta, 3) vieraan valtion sukellusveneen tai muun vedenalaisen kulkuvälineen tuloa luvatta Suomen aluevesille muussa kuin pinta-asemassa, 4) vieraan valtion tai tunnuksettoman sotilaallisen ryhmän Suomen alueella oleviin, valtakunnan turvallisuuden kannalta tärkeisiin kohteisiin oikeudettomasti kohdistamaa tiedustelua ja elektronista häirintää, 5) vieraan valtion tai tunnuksettoman sotilaallisen ryhmän aluevalvontatehtävässä olevaan suomalaiseen valtionilma-alukseen tai valtionalukseen oikeudettomasti kohdistamaa elektronista häirintää, 6) sitä, että vieras valtio tai tunnukseton sotilaallinen ryhmä oikeudettomasti käyttää Suomen aluetta 1–5 kohdassa tarkoitetussa toiminnassa kolmatta valtiota vastaan

Poliisilain 5 luvun 8 §:n 4 momentin mukaan poliisilla on oikeus lyhytaikaisesti estää teleosoitteiden tai telepäätelaitteiden käyttö tietyllä alueella. Toimenpiteen käytön on oltava välttämätön henkeä tai terveyttä uhkaavan vakavan vaaran torjumiseksi, eikä sillä saa aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi.

Sotilastiedustelusta annetun lain 37 §:ssä säädetään sotilastiedustelussa käytettävästä televalvonnasta. Säännöksen mukaan sotilastiedustelun televalvonnassa ei kuitenkaan voida estää telepäätelaitteen tai teleosoitteen käyttöä.

Poliisilain säännöksen yksityiskohtaisten perustelujen mukaan (HE 224/2010 vp, s. 98/II) kysymyksessä ei ole voimassa olevaan televalvontaan kuuluva tietyn teleosoitteen tai telepäätelaitteen käytön tilapäinen estäminen, vaan ennalta määrittämättömän teleosoitteiden ja telepäätelaitteiden joukon käytön lyhytaikainen estäminen vaaran torjumiseksi.

Poliisilain esitöissä (HE 224/2010 vp, s. 98/II–99/I) mainitaan esimerkkeinä toimivaltuuden käytöstä tilanteet, jossa on esimerkiksi uhattu räjäyttää pommi tietyssä paikassa tai kansainväliseen huippukokoukseen osallistuvaan henkilöön tiedetään kohdistuvan vakava uhka. Tällaisissa tilanteissa poliisi voisi estää teleosoitteiden ja telepäätelaitteiden käytön hetkellisesti, jotta räjähdettä ei kyettäisi laukaisemaan. Toimenpiteelle asetettaisiin kuitenkin telekuuntelun kaltainen vaaraedellytys. Toimenpiteen tulisi olla välttämätön ja vaaran tulisi olla vakava. Suojattavina intresseinä olisivat vain henki ja terveys. Toimenpiteellä ei saisi myöskään aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi. Tällä korostettaisiin vähimmän haitan periaatteen merkitystä toimivaltuuden käytössä.

Yksityiskohtaisten perustelujen mukaan toimivaltuuden käytölle on asetettu siten varsin tiukat edellytykset, joten sen käyttö olisi vain poikkeuksellisesti mahdollista. Lisäksi toimenpiteestä päättäisi keskusrikospoliisin, suojelupoliisin tai liikkuvan poliisin päällikkö taikka poliisilaitoksen päällikkö tai kiiretapauksessa pidättämiseen oikeutettu poliisimies.

Yksittäisten teleosoitteiden tai telepäätelaitteiden käytön tilapäinen estäminen määräytyisi pykälän 1 ja 2 momenttien mukaisesti.

Sotilastiedustelusta annetun lain 62 §:ssä säädetään ulkomaan tietojärjestelmätiedustelusta. Sen 1 momentin mukaan sillä tarkoitetaan tietoteknisin menetelmin suoritettavaa tietojen hankkimista Suomen ulkopuolella olevasta tietojärjestelmästä. Pykälän 2 momentin mukaan Puolustusvoimien tiedustelulaitos saa kohdistaa tietojärjestelmään ulkomaan tietojärjestelmätiedustelua, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

Säännös ei sisällä televalvontaa vastaavaa toimivaltuutta puuttua kohteena olevan tietojärjestelmän toimintaan, vaikka se aiheuttaisi vakavaa vaaraa Suomen maanpuolustukselle tai kansalliselle turvallisuudelle.

2.2.8 Ilmoitusvelvollisuus

Sotilastiedustelusta annetun lain 89 §:ssä säädetään tiedustelumenetelmän käytöstä ilmoittamisesta. Pykälän 1 momentin mukaan telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta ja teknisen tarkkailun käytöstä sekä viestiin kohdistuvasta jäljentämisestä ja viestiin kohdistuvasta lähetyksen jäljentämisestä on viipymättä ilmoitettava tiedonhankinnan kohteena olleelle henkilölle kirjallisesti sen jälkeen, kun tiedustelumenetelmän käytön tarkoitus on saavutettu.

Hallituksen esityksen (HE 203/2017 vp, s. 317) mukaan momentissa lueteltaisiin ne tiedustelumenetelmät, joista ilmoitus tiedonhankinnan kohteelle olisi tehtävä. Kyse olisi sellaisista tiedustelumenetelmistä, joilla puututtaisiin tiedustelumenetelmän käytön kohteena olevan henkilön luottamuksellisen viestin suojaan. Pykälässä kytkettäisiin velvollisuus ilmoittaa tiedustelun kohteelle momentissa tarkoitetun tiedustelumenetelmän käytöstä

lähtökohtaisesti siihen ajankohtaan, kun tällainen tiedonhankinta on lopetettu. Vasta tämän hetken jälkeen tehtävä ilmoitus ei vaaranna käynnissä olevaa tiedonhankintaa. Tiedonhankinta on voitu lopettaa joko siksi, että sen tarkoitus on saavutettu tai siksi, koska tiedonhankinta on osoittautunut tuloksettomaksi.

Ilmoituksen tulisi olla sillä tavoin yksilöity, että kohde voisi tarvittaessa pyrkiä selvittämään häneen kohdistetun tiedustelumenetelmän käytön perusteita. Ilmoituksessa olisi mainittava esimerkiksi se, mistä tiedustelumenetelmästä on kysymys, sekä se, missä ja milloin sitä on käytetty. Taktisia ja teknisiä toteutustapaa koskevia yksityiskohtia ei viranomaisen tarvitsisi paljastaa. Ilmoitus voitaisiin tehdä kohteelle esimerkiksi kirjeitse viimeiseen tiedossa olevaan osoitteeseen.

Silloin, kun tiedustelumenetelmän käyttö on tosiasiallisesti lopetettu ennen luvan tai päätöksen voimassaolon päättymistä, eikä uutta lupaa ole haettu tai jatkopäätöstä tehty, tulisi ilmoitus kohteelle tehdä tosiasiallisesta lopettamishetkestä. Jos tiedonhankintaa jatkettaisiin jatkoluvan tai -päätöksen nojalla, tulisi ilmoitus tehdä joko tiedustelumenetelmän käytön tosiasiallisesta lopettamisesta taikka luvan tai päätöksen voimassaoloajan päättymisestä. Päätösten voimassaolon välillä voidaan hyväksyä muutaman päivän katkoksia, jotta tiedonhankintaa voidaan pitää yhdenjaksoisena. Tiedustelumenetelmän käytöstä tulisi näin ollen ilmoittaa kohteelle viipymättä sen jälkeen, kun käynnissä olevan tai tulevan tiedusteluoperaation turvaaminen ei ole enää tarpeen.

Se, kenelle ilmoitus on tehtävä, rajautuu käytännössä tiedustelumenetelmän käytön varsinaisiin kohteisiin. Ilmoitusvelvollisuutta ei ole sivulliselle esimerkiksi tilanteessa, jossa teknisellä laitetarkkailulla seurataan tietojärjestelmässä olevaa haittaohjelmaa ja tämän yhteydessä joudutaan käymään läpi organisaation työntekijöiden sähköposteja sen selvittämiseksi, mihin kaikkialle haittaohjelma on levinnyt. Henkilöille, joiden sähköpostiliikennettä on jouduttu käymään läpi, ei ole ilmoitusvelvollisuutta, koska he eivät ole tiedustelumenetelmän käytön kohteena.

Toisaalta tiedusteluviranomainen ei myöskään saa käsitellä sähköposteja muilta osin kuin haittaohjelmaa koskien; tiedusteluviranomaisella ei ole myöskään lupaa hankkia tietoja muilta osin kuin haittaohjelmaa koskien. Tiedot, jotka ovat haittaohjelmaa koskevan tiedon ulkopuolella, on hävitettävä ilman aiheeton viivytystä hetihävittämissääntelyn mukaisesti.

Pykälän 2 momentin mukaan muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta on ilmoitettava tiedonhankinnan kohteena olleelle henkilölle kirjallisesti sen jälkeen, kun tiedustelumenetelmän käytön tarkoitus on saavutettu, ja jos käsittelyssä on manuaalisesti selvitetty tietoliikennetiedustelun suorittamisen hetkellä Suomessa olevan henkilön luottamuksellisen viestin tunnistamistiedot tai sisältö. Muualla kuin Suomessa olevan henkilön luottamuksellisen viestin sisällön manuaalisesta käsittelystä ei sitä vastoin olisi ilmoittamisvelvollisuutta jo yksin siitä syystä, että tämä olisi usein mahdotonta esimerkiksi kohteen oikeaa henkilöllisyyttä koskevan epätietoisuuden vuoksi tai koska henkilöllisyydeltään sinänsä tunnistetun kohteen olinpaikka ei ole tiedossa tai kohtuullisella työllä selvitettävissä. Velvollisuutta ilmoittaa ei kuitenkaan ole, jos tietoliikennetiedustelulla saatu tieto on hävitetty 86 §:n perusteella.

Hallituksen esityksen (HE 203/2017 vp, s. 318) mukaan momentin velvollisuus ilmoittaa tietoliikennetiedustelusta rajattaisiin sellaisiin tapauksiin, joissa tietoliikennetiedustelun voidaan katsoa puuttuneen luottamuksellisen viestin salaisuuteen verrattain syvällisesti. Pykälän mukaisen rajatun ilmoittamisvelvollisuuden vastapainoksi tiedustelutoiminnan valvontaa koskevassa laissa (121/2019) säädetään yleisestä oikeudesta kannella

tiedusteluvalvontavaltuutetulle tai tehdä tutkintapyyntö, jotka ovat mahdollisia siitä huolimatta, onko tuomioistuin tehnyt esimerkiksi päätöksen ilmoituksen tekemättä jättämisestä. EIT:n ratkaisukäytännössä suppeampaa ilmoittamisvelvollisuutta on pidetty hyväksyttävä, jos taho, joka kokee tulleensa ilman perustetta tiedustelutoimenpiteen kohteeksi, voi laajasti kannella tai muuten saattaa asiansa tutkittavaksi tiedustelusta ulkopuoliselle viranomaiselle.

Tiedustelutoiminnan valvonnasta annetun lain 7 §:ssä säädetään tiedusteluvalvontavaltuutetun tehtävistä. Pykälän mukaan tiedusteluvalvontavaltuutetun tehtävänä on 1) valvoa tiedustelumenetelmien ja tiedustelutiedon käytön sekä muun tiedustelutoiminnan lainmukaisuutta, 2) valvoa perus- ja ihmisoikeuksien toteutumista tiedustelutoiminnassa, 3) edistää oikeusturvan toteutumista ja siihen liittyviä hyviä käytäntöjä tiedustelutoiminnassa ja 4) seurata ja arvioida toimialallaan lainsäädännön toimivuutta ja tehdä tarpeelliseksi katsomiaan kehittämisehdotuksia. Säännöksessä mainittu ”tiedustelutoiminnassa” viittaa siihen, että tiedusteluvaltuutettu voisi valvoa tiedustelua ylipäätään eikä vain siviili- ja sotilastiedustelulainsäädännössä mainittuja tiedustelumenetelmiä.

Laissa on säädetty valtuutetulle tehtäviensä toteuttamiseksi laajat ja vahvat toimivaltuudet. Valtuutetulla on muun ohella laajat tiedonsaanti- ja tarkastusoikeudet sekä oikeus määrätä tiedustelumenetelmän käytön keskeyttämisestä ja lopettamisesta sekä lainvastaisesti hankittujen tietojen hävittämisestä. Valtuutettu voisi myös antaa suosituksia, ohjeita, neuvoja ja lausuntoja sekä tehdä aloitteita. Valtuutettu voisi esimerkiksi avustaa sisäisen laillisuusvalvonnan tarkastussuunnitelmien laatimisessa ja antaa lausuntoja tiedusteluviranomaisille lainmukaisuuskysymyksistä. Kanteluihin ja tutkimispyyntöihin vastaaminen olisi keskeinen osa tiedusteluvaltuutetun toimintaa.

Lain 89 §:n 2 momentin mukaan muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tietoliikennetiedustelusta ei ole velvollisuutta ilmoittaa, jos tietoliikennetiedustelulla saatu tieto olisi hävitetty lain 86 §:n perusteella. Näin ollen, jos viestinnän käsittelyssä on selvitetty tietyn Suomessa olevan henkilön viestin sisältö, mutta samassa yhteydessä on havaittu tieto hävittämisvelvollisuuden piiriin kuuluvaksi, ei velvollisuutta ilmoittamiseen olisi.

Sotilastiedustelusta annetun lain esitöissä (HE 203/2017 vp, s. 318) ehdotettiin, että tietoliikennetiedustelusta olisi ilmoitettu vain sellaiselle Suomessa tietoliikennetiedustelun käytön hetkellä olleelle henkilölle, jonka luottamuksellisen viestin tai tallentaman tiedon *sisältö* on selvitetty manuaalisesti. Perustuslakivaliokunta piti hallituksen esityksestä antamassaan lausunnossaan (PeVL 36/2018 vp, s. 27–28) tätä ratkaisua riittämättömänä todeten, että sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen voivat olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että hallituksen esityksessä viitattu erottelu suojan reuna- ja ydinalueeseen ei ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen. Valiokunta totesi, että esimerkiksi paikkatietojen tai vierailtuja sivustoja koskevien tunnistamistietojen perusteella yksilöstä voidaan selvittää hyvinkin tarkasti yksityiselämän suojan ydinalueelle kuuluvia tietoja esimerkiksi henkilön poliittisesta vakaumuksesta tai sosiaalisista suhteista. Valiokunta piti tämän vuoksi välttämättömänä, että ilmoittamisvelvollisuus ulotetaan myös viestin tunnistamistietoihin kohdistuvaan manuaaliseen käsittelyyn, ja asetti tällaisen muutoksen tekemisen edellytykseksi lain käsittelylle tavallisen lain säätämisjärjestyksessä. Perustuslakivaliokunnan edellyttämän muutoksen johdosta lähtökohtainen tietoliikennetiedustelun ilmoittamisvelvollisuus laajeni osittain hallitsemattomaksi. Tämä on myös lisännyt tarpeettomasti ilmoituksen lykkäämistä ja ilmoittamatta jättämistä koskevien vaatimusten esittämistä tuomioistuimelle.

Pykälän 3 momentin mukaan tiedustelumenetelmän käytöstä on kuitenkin ilmoitettava tiedonhankinnan kohteelle viimeistään vuoden kuluttua sen käytön lopettamisesta.

Pykälän 4 momentin mukaan, jos tiedonhankinnan kohteena olevan henkilöllisyys ei ole tiedossa 1–3 momentissa tarkoitetun määräajan tai lykkäyksen päättyessä, tiedustelumenetelmän käytöstä on ilmoitettava kirjallisesti hänelle ilman aiheetonta viivytystä henkilöllisyyden selvittyä.

Pykälän 5 momentin mukaan kohteelle ilmoittamisesta on samalla annettava kirjallisesti tieto luvan myöntäneelle tuomioistuimelle.

Pykälän 6 momentin mukaan tuomioistuin voi pääesikunnan tiedustelupäällikön tai tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta päättää, että 1 ja 2 momentissa tarkoitettua ilmoitusta tiedonhankinnan kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedustelumenetelmän käytön turvaamiseksi, maanpuolustuksen kannalta tai kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saadaan tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi taikka hengen tai terveyden suojaamiseksi.

Hallituksen esityksen (HE 203/2017 vp, s. 319–320) mukaan ilmoitus saataisiin tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä sotilaallisen maanpuolustuksen turvaamiseksi tai kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoituksen lykkäämisestä tai kokonaan tekemättä jättämisestä päättäisi tuomioistuin, vaikka kysymys olisi sellaisesta tiedustelumenetelmästä, josta on päättänyt tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies. Ehdotuksen mukaisesti ilmoitusta voitaisiin lykätä enintään kahdeksi vuodeksi kerrallaan. Toistuvan ilmoittamisen lykkäämisen sijaan tulisi hakea kokonaan ilmoittamatta jättämistä, jos edellytykset ovat olemassa, koska esimerkiksi kymmenen vuoden kuluttua tehtävällä ilmoituksella ei käytännössä ole merkitystä kohteelle. Lykkäämistä ja uudelleen lykkäämistä tulisi hakea ennen määräajan päättymistä.

Lykkäämisen mahdollistavana perusteena olisi ensinnäkin käynnissä olevan tiedustelumenetelmän käytön turvaaminen. Tiedonhankinta voisi liittyvä mihin tahansa vireillä olevaan tiedusteluoperaatioon, myös siviilitiedusteluoperaatioon.

Lykkääminen olisi mahdollista myös maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi. Tämä tarkoittaisi sitä, että käsillä olisi oltava maanpuolustukseen, valtioon tai yhteiskuntaan kohdistuva uhka. Kuitenkin esimerkiksi yksityishenkilöihin kohdistuvat väkivallanteot voisivat kuulua maanpuolustuksen tai kansallisen turvallisuuden piiriin, jos ne laajuudeltaan tai merkitykseltään olisivat maanpuolustuksen tai kansallisen turvallisuuden kannalta merkittäviä ja voisivat siten muodostaa vakavan uhan sille.

Lisäksi lykkääminen olisi mahdollista hengen tai terveyden suojaamiseksi. Lykkäämisen kynnyksenä olisi, että se on perusteltua. Kynnys lykkäämiselle ei siis olisi kovin korkea.

Ilmoitus saataisiin jättää tuomioistuimen päätöksellä kokonaan tekemättä vain silloin, jos se on välttämätöntä maanpuolustuksen turvaamiseksi tai kansallisen turvallisuuden varmistamiseksi taikka hangen tai terveyden suojaamiseksi. Kynnys olisi näin ollen korkea.

Momentin merkitys voidaan katsoa korostuneeksi sotilastiedustelussa. Edellä todetusti etenkin tietoliikennetiedustelussa suorastaan hallitsemattomaksi laajentunut lähtökohtainen ilmoitusvelvollisuus on johtanut säännöksen varsin laajaan soveltamiseen.

Pykälän 7 momentin mukaan suunnitelmallisesta tarkkailusta, peitellystä tiedonhankinnasta, peitetoiminnasta, valeostosta, tietolähteen ohjatusta käytöstä, paikkatiedustelusta, muuhun kuin viestiin kohdistuvasta jäljentämisestä ja muuhun kuin viestiin kohdistuvasta lähetyksen jäljentämisestä ei ole velvollisuutta ilmoittaa tiedonhankinnan kohteelle, jos asiassa ei ole aloitettu esitutkintaa 79 tai 80 §:ssä tarkoitetun ilmoituksen perusteella. Jos esitutkinta aloitetaan, noudatetaan, mitä pakkokeinolain (806/2011) 10 luvun 60 §:n 2–7 momentissa säädetään.

Hallituksen esityksen (HE 203/2017 vp, s. 320) mukaan paikkatiedustelun osalta ilmoitus tehtäisiin sille, joka on ollut kyseisen tiedustelumenetelmän käytön kohteena sekä tarvittaessa myös paikan omistajalle tai haltijalle. Säännöksessä tarkoitetusta jäljentämisestä ja lähetyksen jäljentämisestä ilmoitus tehtäisiin tiedonhankinnan kohteelle.

Sotilastiedustelussa ei hankittaisi tietoja rikostorjuntaan tai esitutkintaan. Mikäli tällaisia tietoja tulisi sotilastiedusteluviranomaiselle, tietoja voitaisiin antaa aiemmin 76 ja 77 §:ssä säädetyn menettelyn mukaisesti. Jos 76 tai 77 §:ssä säädetyn mukaisesti annetun tiedon perusteella aloitettaisiin esitutkinta, noudatettaisiin pakkokeinolain 10 luvun 60 §:n 2–7 momentissa säädettyä.

Momentissa mainittujen tiedustelumenetelmien käytöstä ei sitä vastoin tarvitsisi lainkaan ilmoittaa, jos niiden kohteena olevassa asiassa ei aloitettaisi esitutkintaa.

Pykälän 8 momentin mukaan tiedustelumenetelmän käytöstä ei ole velvollisuutta ilmoittaa tiedustelumenetelmän käytön kohteelle, jos kohteena on ollut valtiollinen toimija.

Pykälän 9 momentin mukaan ilmoitusta koskevan asian käsittelyssä tuomioistuimessa noudatetaan, mitä 116 §:ssä säädetään.

2.2.9 Sotilastiedusteluviranomaisesta ulkopuolisen osallistuminen sotilastiedustelutoimintaan

Muiden viranomaisten osallistuminen

Sotilastiedustelusta annetun lain 18 §:ssä säädetään yhteistyöstä muiden viranomaisten sekä yritysten ja muiden yhteisöjen kanssa. Pykälän 1 momentin mukaan sotilastiedusteluviranomaisen on tarpeen mukaan toimittava yhteistyössä muiden viranomaisten kanssa sotilastiedustelun tarkoituksenmukaiseksi hoitamiseksi. Sotilastiedusteluviranomainen voi tehtävänsä toteuttamiseksi luovuttaa muille viranomaisille salassapitosäännösten estämättä muita tietoja kuin henkilötietoja, jos tietojen luovuttaminen on tarpeen maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi. Henkilötietojen luovuttamisesta säädetään henkilötietojen käsittelystä Puolustusvoimissa annetussa laissa.

Pykälän 2 momentin mukaan sotilastiedusteluviranomainen voi salassapitosäännösten estämättä tehtävänsä toteuttamiseksi luovuttaa yrityksille ja muille yhteisöille tiedustelun menetelmien ja järjestelmien kehittämiseksi haittaohjelmaan liittyvän tunnistamistiedon tai luovuttaa muun kuin henkilötiedon, jos tietojen luovuttaminen on välttämätöntä Puolustusvoimien toiminnan tai kansallisen turvallisuuden suojaamiseksi.

Pykälän 3 momentin mukaan tietojen luovuttamisesta rikostorjuntaan säädetään lain 6 luvussa, ja pykälän 4 momentin mukaan sotilastiedusteluviranomaisen ja muiden viranomaisten välisen yhteistyön järjestämisestä sekä yhteistyöhön osallistuvista tahoista ja niiden tehtävistä voidaan antaa tarkempia säännöksiä valtioneuvoston asetuksella.

Viranomaisten ulkopuolisen osallistuminen tiedustelutoimintaan

Sotilastiedustelusta annetun lain 51 §:ssä säädetään tietolähdetoiminnasta. Pykälän 1 momentin mukaan tietolähdetoiminnalla tarkoitetaan muuta kuin satunnaista luottamuksellista, tiedustelutehtävien hoitamiseksi merkityksellisten tietojen vastaanottamista suomalaisen viranomaisen ulkopuoliselta henkilöltä (*tietolähde*).

Pykälän 2 momentin mukaan sotilastiedusteluviranomainen saa pyytää tähän tarkoitukseen hyväksyttyä, henkilökohtaisilta ominaisuuksiltaan sopivaa, rekisteröityä ja tiedonhankintaan suostunutta tietolähdettä hankkimaan 1 momentissa tarkoitettuja tietoja (*tietolähteen ohjattu käyttö*), jos tietolähteen ohjatulla käytöllä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

Pykälän 3 momentin mukaan tietolähteen ohjatussa käytössä tietoja ei saa pyytää hankittavaksi sellaisella tavalla, joka edellyttäisi viranomaiselle kuuluvien toimivaltuuksien käyttöä tai joka vaarantaisi tietolähteen tai muun henkilön hengen tai terveyden. Ennen tietolähteen ohjattua käyttöä tietolähteelle on tehtävä selkoa hänen oikeuksistaan ja velvollisuuksistaan sekä erityisesti hänelle lain mukaan sallitusta ja kielletystä toiminnasta. Tietolähteen turvallisuudesta on tarpeen mukaan huolehdittava tiedonhankinnan aikana ja sen jälkeen. Selvää on se, että tietolähteelle ei voida antaa tehtäviä, joilla kierrettäisiin viranomaisille annettujen toimivaltuuksien käyttöä. Esimerkiksi tiedonhankinta vakituiseen asumiseen käytettävästä tilasta ei ole mahdollista tietolähdettä käyttäen. Vastaavasti, lukuun ottamatta tietolähteen turvallisuudesta huolehtimista, tietolähdettä ei voida varustaa teknisen katselun ja kuuntelun mahdollistavalla laitteistolla.

Tietolähdettä ei voi käyttää muuhun kuin tietojen, jotka hän on saanut normaalissa toiminnassaan ja normaaleja sosiaalisia suhteitaan käyttäen. Esimerkiksi tilanteessa, jossa tietolähteelle olisi myönnetty pääsy tiettyyn tilaan ja tiettyihin laitteistoihin, tietolähde ei voi asentaa sotilastiedustelun tiedustelumenetelmien käyttämiseksi tarvittavaa ohjelmistoa, menetelmää tai laitteistoa.

Tietolähdetoiminnassa on otettava huomioon rikolliseen toimintaa osallistumisen riski, joka käytännössä voisi toteutua sitä kautta, että tietolähde ohjataan hankkimaan tieto paikasta, johon hänellä ei ole muutenkin kuin rikollisia keinoja käyttäen pääsy. Tarkimmin asiaa on käyty läpi pakkokeinoja koskien. Esimerkiksi pakkokeinolain 10 luvun 28 §:n 1 momentti, joka koskee peitetoimintaa, sisältää nimenomaisen kiellon tehdä rikoksia tai aloitetta rikoksen tekemiseksi. Pykälän 2 momentin mukaan sen estämättä, mitä 1 momentissa säädetään, peitetoimintaa suorittava poliisimies saa tehdä järjestysrikkomuksen tai muun siihen rinnastettavan rikoksen, josta on säädetty rangaistukseksi rikesakko, tai liikennerikkomuksen, jos teko on välttämätön peitetoiminnan tavoitteen saavuttamiseksi tai tiedonhankinnan paljastumisen estämiseksi.

Pakkokeinolain esitöiden mukaan 28 §:n 2 momentti ja 29 §:n 1 momentti viittaisivat etukäteiseen ja suunnitelmalliseen arvioon ja harkintaan. Lisäksi 29 §:n 1 momentin 1 kohta edellyttää, että toimenpiteen suorittamishetkellä on käsillä erittäin pätevät perusteet, joiden nojalla voidaan olettaa, että rikollinen toimenpide olisi tehty ilman peitepoliisin myötävaikutusta. Toimenpiteiden hyväksyttävyyttä arvioidaan lähtökohtaisesti ja

mahdollisuuksien mukaan ennen toiminnan aloittamista, kun päätöstä pakkokeinon käytöstä valmistellaan (HE 217/2022 vp, s. 55, ks. myös HE 222/2010 vp, s. 340–341). Sekä 28 §:n 2 momentissa ja 29 §:n 1 momentissa on kyse toimivaltuussääntelyn muotoon kirjoitetusta säännöksistä, jotka sääntelevät sitä, mitä peitetoimintaa suorittava poliisimies saa säännöksissä tarkemmin määritellyissä tilanteissa ja edellytyksillä tehdä (HE 217/2022 vp, s. 55).

Myös sotilastiedusteluntoiminnan osalta tietolähdetoiminnan osalta lähtökohtana voidaan pitää sitä, että jos tietolähde toimisi toisin kuin hänet on ohjeistettu tekemään tai oman harkintansa ja päätöksensä mukaan osallistuisi johonkin muuhun kuin ohjeistettuun toimintaa, olisi hän mahdollisesti toimiensa mukaisesti rikosoikeudellisessa vastuussa. Toki näissä tilanteissa asiaa arvioitaneen myöhemmässä rikosprosessissa erikseen esimerkiksi rikoslain 4 luvun vastuuvapausperusteita koskevan sääntelyn (kieltoerehdys, oikeuttamisperuste, anteeksiantoperuste) kautta. On huomattava, että tietolähteen oikeudenvastainen teko voi tulla tietoisuuteen vasta pitkänkin ajan kuluttua.

Oma kysymyksensä on myös rikosprovokaatio.

Laissa säädetystä tietolähdetoiminnasta pitää pitää erillään viranomaisen avustaminen. Yksityinen henkilö saattaa vapaaehtoisesta haluta antaa esimerkiksi kesämökkinsä sotilastiedusteluviranomaisen lyhytaikaiseen käyttöön esimerkiksi varastotilan tiedusteluoperaation tukipisteeksi. Itsestään selvää on, että sotilastiedusteluviranomaisen tiedonhankinta ei voi kohdistua näissäkään tilanteissa kotirauhan suojaamaan tilaan eikä tästä ole myöskään kyse avustamisessa.

Voimassa olevan tuloverolain mukaan tietolähteelle voidaan maksaa palkkio verottomasti. Sääntelyn taustalla on tietolähteen hengen ja terveyden suojaaminen.

Poliisilain 2 luvun 17 §:n 3 momentin mukaan sillä, joka poliisimiehen pyynnöstä tai tämän suostumuksella tilapäisesti avustaa poliisimiestä tilanteessa, jossa on välttämätöntä turvautua sivullisen apuun voimakeinojen käytössä erittäin tärkeän ja kiireellisen poliisin virkatehtävän suorittamisessa, on oikeus poliisimiehen ohjauksessa sellaisten voimakeinojen käyttämiseen, joihin poliisimies toimivaltansa nojalla hänet valtuuttaa.

Poliisilain 9 luvun 3 §:n 1 momentin mukaan jokainen on velvollinen päällystöön kuuluvan poliisimiehen määräyksestä avustamaan poliisia hengenvaarassa olevan kadonneen etsimisessä, ihmishengen pelastamisessa, loukkaantuneen auttamisessa sekä huomattavan omaisuus- tai ympäristövahingon torjumisessa, jollei tällaiseen toimenpiteeseen osallistuminen ole henkilön ikä, terveydentila tai henkilökohtaiset olosuhteet huomioon ottaen tai muusta erityisestä syystä kohtuutonta.

Pykälän 2 momentin mukaan edellä 1 momentissa tarkoitetuissa tapauksissa samoin kuin hukkuneen etsimiseksi yksityisten henkilöiden ja yhteisöjen on päällystöön kuuluvan poliisimiehen määräyksestä annettava poliisin käyttöön täyttä korvausta vastaan kohtuullisessa määrin elintarvikkeita, viestintävälineitä, kuljetus- ja työvälineitä sekä muita tarvittavia laitteita ja aineita.

Sotilastiedustelusta annetun lain 8 luvussa säädetään Puolustusvoimien virkamiehen ja asevelvollisen osallistumisesta sotilastiedusteluun. Luvussa säädetään Puolustusvoimien virkamiehen osallistumisesta sotilastiedustelun, asevelvollisuuslain mukaisessa palveluksessa olevan reserviläisen toimivaltuuksista, asevelvollisuuslain mukaisessa palveluksessa olevan virkavastuusta ja asevelvollisuuslain mukaisessa palveluksessa olevan vahingonkorvausvastuusta.

Sotilastiedustelusta annetun lain 91 §:n 1 momentin mukaan asevelvollisuuslain (1438/2007) mukaisessa kertausharjoituksessa oleva riittävän koulutuksen saanut reserviläinen saa avustaa sotilastiedusteluviranomaista radiosignaalitiedustelussa, ulkomaan tietojärjestelmätiedustelussa, teknisten tietojen käsittelyssä ja tietoliikennetiedustelun kohdentamisessa.

Pykälän 2 momentin mukaan asevelvollisuuslain 32 §:n 3 momentissa tarkoitettuun kertausharjoitukseen määrätty, mainitun lain 82 §:ssä tarkoitetussa ylimääräisessä palveluksessa oleva tai 86 §:n mukaisen liikekannallepanon aikaiseen palvelukseen määrätty riittävän koulutuksen saanut reserviläinen voi käyttää 1 momentissa säädetyn lisäksi suunnitelmallista tarkkailua, teknistä kuuntelua, teknistä katselua, teknistä seurantaa ja teknistä laitetarkkailua sekä ulkomaan tietojärjestelmätiedustelua tiedustelutehtävän suorittamiseksi. Tässä momentissa tarkoitetussa tiedustelussa ei saa hankkia tietoa viestin sisällöstä.

Pykälän 3 momentin mukaan puolustusvoimista annetun lain (551/2007) 47 §:n perusteella sotilastiedusteluviranomaisen palveluksesta eronnut asevelvollisuuslain mukaisessa kertausharjoituksessa oleva reserviläinen saa käyttää 4 luvussa tarkoitettuja tiedustelumenetelmiä.

Pykälän 4 momentin mukaan reserviläinen saa käyttää tässä pykälässä tarkoitettuja toimivaltuuksia ainoastaan tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa.

Sotilastiedustelusta annetun lain 95 §:ssä säädetään ilmaisukiellosta. Sen 1 momentin mukaan tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa kieltää sivullista ilmaisemasta tämän tietoon tulleita seikkoja tiedustelumenetelmän käytöstä, jos se on perusteltua tiedustelutoiminnan suojaamiseksi. Edellytyksenä on lisäksi, että sivullinen on tehtävänsä tai asemansa johdosta avustanut tai häntä on pyydetty avustamaan tiedustelumenetelmän käytössä.

Momentin toisen virkkeen perustelujen mukaan edellytyksenä olisi, että sivullinen olisi tehtävänsä tai asemansa johdosta avustanut tai häntä olisi pyydetty avustamaan tiedustelumenetelmän käytön toteuttamisessa. Ilmaisukieltoa ei siten voitaisi antaa kenelle tahansa henkilölle, esimerkiksi taloyhtiön asukkaalle tai muulle sivulliselle, joka sattumalta havaitsee teknisen tarkkailun laitteen asennuksen. Säännöksessä tiedustelumenetelmän käytöllä tarkoitettaisiin tiedustelumenetelmien käyttöä laajemmin, joka pitäisi esimerkiksi sisällään sotilastiedustelussa sekä siviilitiedustelussa käytettävien tiedustelumenetelmien käytön suojaamisen silloin, kun sotilastiedusteluviranomainen ja suojelupoliisi toimisivat yhteistyössä. Ilmaisukielto olisi perusteltua antaa ainakin silloin, jos tiedustelumenetelmän käyttö saattaisi paljastua ilman kiellon määräämistä sivulliselle.

Ulkomainen virkamies

Sotilastiedustelusta annetun lain 20 §:ssä säädetään kansainvälisestä yhteistyöstä. Pykälän 1 momentin mukaan sotilastiedusteluviranomainen voi Suomen kansallisten etujen mukaisesti tehtäviinsä liittyen tai kansallisen turvallisuuden suojaamiseksi 1) vaihtaa muita tiedustelutietoja kuin henkilötietoja ulkomaisten tiedustelu- ja turvallisuuspalveluiden taikka Pohjois-Atlantin liiton tai muun kansainvälisen järjestön taikka Euroopan unionin kanssa salassapitosäännösten estämättä, jos se on tarpeellista ja 2) osallistua tiedustelutietojen hankkimiseen ja arvioimiseen liittyvään kansainväliseen yhteistoimintaan.

Pykälän 2 momentin mukaan, jos yhteinen tiedonhankinta toteutetaan yhteistyössä sen valtion kanssa, jonka alueella tiedustelumenetelmiä on tarkoitus käyttää, sotilastiedusteluviranomaisen virkamiehen on noudatettava niitä rajoituksia ja ehtoja tiedustelumenetelmien käytölle, jotka kyseinen valtio asettaa.

Pykälän 3 momentin mukaan ulkomaisella toimivaltaisella virkamiehellä on pääesikunnan tiedustelupäällikön päätöksellä oikeus Suomen alueella sotilastiedusteluviranomaisen tehtävien hoitamiseksi toimia yhteistoiminnassa sotilastiedusteluviranomaisen virkamiehen kanssa ja tämän ohjauksessa ja valvonnassa käyttää 22, 24, 43, 47, 51, 60 ja 66 §:ssä tarkoitettuja tiedustelumenetelmiä. Ulkomainen virkamies on velvollinen noudattamaan sotilastiedusteluviranomaisen hänelle antamia määräyksiä, rajoituksia ja ohjeita.

Pykälän 4 momentin mukaan pääesikunnan tiedustelupäällikkö päättää kansainväliseen yhteistyöhön osallistumisesta ja tiedustelumenetelmien käytöstä.

Pykälän 5 momentin mukaan kansainvälinen yhteistyö on kielletty, jos on perusteltua aihetta epäillä, että jotakin henkilöä uhkaa yhteistyön tai tietojen luovuttamisen vuoksi kuolemanrangaistus, kidutus, muu ihmisarvoa loukkaava kohtelu, vaino, mielivaltainen vapaudenriisto tai epäoikeudenmukainen oikeudenkäynti.

Pykälän 6 momentin mukaan pykälässä tarkoitetussa tietojen luovuttamisessa ja vastaanottamisessa noudatetaan lisäksi, mitä siitä erikseen Suomea velvoittavissa kansainvälisissä sopimuksissa määrätään tai kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) säädetään. Henkilötietojen luovuttamisesta säädetään henkilötietojen käsittelystä Puolustusvoimissa annetussa laissa.

Pykälän 7 momentin mukaan pääesikunnan tiedustelupäällikkö päättää Pohjois-Atlantin liiton tai sen jäsenvaltion ajoneuvolla, aluksella tai ilma-aluksella taikka maa-asemalla tapahtuvan 60 §:ssä tarkoitetun radiosignaalitiedustelun käytöstä Suomen alueella. Tässä momentissa tarkoitetun yhteistyön on oltava Suomen etujen ja 13 §:ssä tarkoitettujen painopisteiden mukaista sekä tapahduttava sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa.

Pykälän mukaisesti kansainvälinen yhteistyön lähtökohtana on Suomen kansallinen etu ja pykälän nojalla toimittaessa Suomen on saatava siitä hyötyä maanpuolustuksen ja kansallisen turvallisuuden näkökulmasta.

Kun ulkomainen virkamies toimii pykälän 3 momentissa tarkoitetuissa avustavissa tehtävissä, varsinaisen tiedustelumenetelmää koskeva päätös tehdään tai lupa annetaan sen mukaan, mitä kyseisestä tiedustelumenetelmän käytöstä on säädetty.

2.2.10 Tietolähteen turvaaminen

Yhtenä keskeisenä tiedustelumenetelmänä voidaan pitää tietolähdetoimintaa. Parhaat tietolähteet pystyvät tuottamaan kaikkein syvällisintä tietoa ja tietoa kaikkein salaisimmista asioista. Tietolähteet myös saattavat oman henkensä ja terveytensä usein alttiiksi toimiessaan tietolähteenä. Tämän takia tiedusteluviranomaisen on pidettävä riittävissä määrin huolta tietolähteen turvallisuudesta.

Sotilastiedustelusta annetun lain 78 §:ssä säädetään tietolähteen turvaamisesta. Pykälän 4 momentin mukaan pääesikunnan tiedustelupäällikkö saa päättää, että tietolähteelle annetaan yksittäistapauksessa käytettäväksi vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka tietolähteen käytettäväksi valmistettavia vääriä asiakirjoja, jos se on

välttämätöntä tietolähteen hengen ja terveyden suojaamiseksi. Rekisterimerkintä on oikaistava sen jälkeen, kun tässä momentissa tarkoitettuja edellytyksiä ei enää ole.

Tietolähteen turvaaminen ulkomailla tilanteessa, jossa tietolähde on toimittanut ulkomailta käsin tietoja Suomen sotilastiedusteluviranomaiselle, voi olla haastavaa, jolloin tietolähteen saaminen pois kyseisestä maasta voisi olla tarkoituksenmukaisin keino tietolähteen turvaamiseksi. Tietyissä tilanteissa voi olla tarpeen myös järjestää tietolähde Suomen rajan yli myös muita kuin virallisia rajanylityspaikkoja hyödyntäen tai virallisen rajanylityspaikan kautta peitellysti. Tietolähde ei luonnollisestikaan hengen ja terveyden vaarannuttua voi saapua Suomeen virallisia reittejä pitkin, mistä syystä suomalaisen tiedusteluviranomaisen on avustettava esimerkiksi tietoja antamalla tai vääriä asiakirjoja toimittamalla tietolähteelle tämän rajanylityksessä sotilastiedustelusta annetun lain 78 §:n 4 momentin mukaisesti.

Rikoslain 17 luvun 7 §:ssä säädetään valtionrajarikoksesta. Sen 1 momentin mukaan, joka 1) ylittää tai yrittää ylittää Suomen rajan ilman siihen oikeuttavaa matkustusasiakirjaa, viisumia, oleskelulupaa tai matkustusasiakirjaan rinnastettavaa muuta asiakirjaa tai muualta kuin luvallisesta maahantulo- tai maastalähtöpaikasta tai vastoin lakiin perustuvaa muuta kieltoa kuin maahantulokieltoa, 2) muuten rikkoo rajan ylittämisestä annettuja säännöksiä tai 3) oleskelee tai liikkuu rajavyöhykkeellä tai ryhtyy siellä kiellettyyn toimeen rajavartiolain 51 §:n vastaisesti tai ilman mainitun lain 52 §:ssä edellytettyä lupaa, on tuomittava *valtionrajarikoksesta* sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Pykälän 2 momentin mukaan valtionrajarikoksesta ei tuomita ulkomaalaista, joka 1 momentissa tarkoitetun teon johdosta käännytetään tai karkotetaan maasta, eikä ulkomaalaista, joka pakolaisuuden perusteella hakee turvapaikkaa tai oleskelulupaa Suomessa. Valtionrajarikoksesta ei tuomita myöskään ulkomaalaista, joka on tehnyt 1 momentissa tarkoitetun teon sen vuoksi, että hän on ollut 25 luvun 3 tai 3 a §:ssä tarkoitetun ihmiskaupan kohteena.

Rikoslain 17 luvun 8 §:ssä säädetään laittoman maahantulon järjestämisestä. Muun muassa sen 1 momentin 2 kohdan mukaan, joka tuo tai yrittää tuoda Suomeen tai Suomen kautta muuhun maahan ulkomaalaisen, jonka 1 kohdassa tarkoitettu asiakirja on väärä, väärennetty, myönnetty toiselle henkilölle taikka saatu viranomaiselta asiakirjan myöntämisen kannalta merkityksellisen totuudenvastaisen tai harhaanjohtavan tiedon avulla, lahjomalla viranomainen tai virkamiehen väkivaltaisella vastustamisella.

2.2.11 Paikkatiedustelu ja jäljentäminen

Paikkatiedustelusta säädetään sotilastiedustelusta annetun lain 54 §:ssä. Pykälän mukaan paikkatiedustelulla tarkoitetaan muussa kuin pysyväisluonteiseen asumiseen käytettävässä paikassa tai sellaisessa paikassa, jossa tiedustelun kohteeksi on syytä olettaa joutuvan tietoa, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20 tai 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, toimitettavaa tiedustelua esineen, omaisuuden, asiakirjan, tiedon tai seikan löytämiseksi.

Sotilastiedustelusta annetun lain 55 §:ssä säädetään paikkatiedustelusta päättämisestä. Pykälän 1 momentin mukaan tuomioistuin päättää paikkatiedustelusta, kun se kohdistuu paikkaan, johon ei ole yleistä pääsyä tai johon yleinen pääsy on rajoitettu tai estetty paikkatiedustelun toimittamisajankohtana.

Kuitenkin säännöksen yksityiskohtaisten perusteluiden (HE 203/2017 vp, s. 266) mukaan pykälän 3 momentin mukaan pääesikunnan tiedustelupäällikkö tai tehtävään määrätty

tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättäisi muusta kuin 1 momentissa tarkoitetusta paikkatiedustelusta. Momentin alaan kuuluisivat sellaiset paikat, joihin on yleinen pääsy ja joihin yleistä pääsyä ei ole rajoitettu tai estetty paikkatiedustelun toimittamisajankohtana. Lisäksi momentin alaan kuuluisivat sellaiset kulkuneuvot, joita ei käytetä vakituiseen asumiseen.

Sotilastiedustelusta annetun lain 56 §:ssä säädetään jäljentämisestä. Pykälän mukaan sotilastiedusteluviranomaisella on oikeus sotilastiedustelussa jäljentää asiakirja tai esine. Jäljentäminen voidaan toimittaa ja usein toimitetaankin paikkatiedustelun yhteydessä. Jäljentäminen voi tulla kyseeseen myös esimerkiksi suunnitelmallisen tarkkailun toimivaltuuden käytön yhteydessä.

Jäljentämissäännöksen yksityiskohtaisissa perusteluissa (HE 203/2017 vp, s. 266) mainitaan esimerkkeinä asiakirjan jäljentämisestä siitä valokuvan ottaminen ja sen skannaaminen puhelimeen asennetulla skannausohjelmalla, sekä esimerkkinä esineen jäljentämisestä 3D-skannerin käyttäminen.

Jäljentämissäännös ei mahdollista ottaa näytteitä paikkatiedustelun tai muun tiedustelumenetelmän yhteydessä löytyvistä aineesta, omaisuudesta tai esineestä eikä myöskään sellaisten haltuunottoa näytteenottoa tai vaarattomaksi tekemistä varten.

Paikkatiedustelusäännöksen yksityiskohtaisten perustelujen (HE 203/2017 vp, s. 265) mukaan myöskään paikkatiedustelussa ei saada ottaa haltuun tilassa olevia esineitä, asiakirjoja tai muuta omaisuutta, vaan niitä koskevat tarvittavat tiedot tulee tallentaa esimerkiksi valokuvaamalla tai jäljentämällä. Jos tilassa oleva esine on tarpeen jäljentää, se tulee jäljentää sellaisella teknisellä laitteella tai menetelmällä, joka ei edellytä esineen haltuun ottamista.

2.2.12 Sotilastiedusteluviranomaisen tiedonsaantioikeudet

Puolustusvoimista annetun lain 17 §:ssä säädetään Puolustusvoimien, mukaan lukien sotilastiedusteluviranomainen, yleisestä tiedonsaantioikeudesta. Pykälän mukaan Puolustusvoimilla on oikeus saada viranomaiselta sekä julkista tehtävää hoitamaan asetetulta yhteisöltä laissa säädetyn tehtävän suorittamiseksi välttämättömät tiedot ja asiakirjat salassapitovelvollisuuden estämättä, jollei sellaisen tiedon tai asiakirjan antamista Puolustusvoimille tai tietojen käyttöä todisteena ole laissa kielletty tai rajoitettu.

Sotilastiedusteluviranomaisen yleistä tiedonsaantioikeutta täydentää henkilötietojen käsittelystä Puolustusvoimissa annetun lain 37 §. Sen 1 momentin 17 kohdan mukaan sen lisäksi, mitä muualla laissa säädetään, Puolustusvoimilla on oikeus saada sotilastiedustelutehtävien sekä sotilaskurinpidosta ja rikostorjunnasta annetun lain 86 §:n 1 momentissa tarkoitettujen rikosten ennalta- ja paljastamistehtävien suorittamiseksi salassapitosäännösten estämättä tarpeellisia tietoja Verohallinnolta verotuksen tietojärjestelmästä.

Velvoitteidenhoitoselvityksestä säädetään harmaan talouden selvitysyksiköstä annetun lain (1207/2010). Lain 5 §:ssä säädetään velvoitteidenhoitoselvityksestä ja 6 §:ssä velvoitteidenhoitoselvityksen käyttötarkoituksesta. Lain 6 §:n 1 momentin 39 kohdan mukaan velvoitteidenhoitoselvitys laaditaan tukemaan suojelupoliisin tehtäviä kansallisen turvallisuuden suojaamiseksi sitä vakavasti uhkaavalta toiminnalta.

HTSY-lain 7 §:n 1 momentin mukaan Harmaan talouden selvitysyksiköllä on oikeus saada salassapitovelvollisuuden estämättä viranomaiselta ne velvoitteidenhoitoselvityksen laatimiseksi välttämättömät tiedot, jotka velvoitteidenhoitoselvitystä pyytävä viranomainen on

oikeutettu saamaan selvityspyynnössä kuvattua käyttötarkoitusta varten. Säännös ei siten muuta selvitystä pyytäneen viranomaisen oikeutta salassa pidettäviin tietoihin.

Poliisin yleisestä tiedonsaantioikeudesta on säädetty poliisilain 2 §:n 1 momentissa. Poliisin yleistä tiedonsaantioikeutta voi kuitenkin rajoittaa suhteessa poliisilakiin sovellettavaksi tuleva erityissäännös, jossa oikeus luovuttaa tietoja on rajattu tarkkarajaisesti ainoastaan tiettyihin käyttötarkoituksiin. Aiemmin voimassa olevassa sääntelyssä kokoavasti todeten velvoitteidenhoitoselvityksessä keskeiset sosiaalivakuuttamista koskevat säännökset mahdollistivat tietojen luovuttamisen esitutkintaviranomaisille rikosten ennalta estämiseen ja selvittämiseen. Näin ollen ilman nimenomaista säädösmuutosta suojelupoliisi ei voinut saada tarvittavia tietoja kansallisen turvallisuuden suojaamisen perusteella, koska suojelupoliisi katsotaan poliisiksi.

2.2.13 Avointen lähteiden tiedonhankinta

Avointen lähteiden tiedustelu (Open source intelligence, OSINT) on tavanomaisoikeuden perusteella sallittu tiedustelulaji (ks. LaVM 44/2010 vp, s. 26). Avointen lähteiden sisältämä informaatio on kaikille tarkoitettua ja se on myös jokaisen saatavilla. Yksittäisen virkamiehen tekemällä avointen lähteiden tiedonhankinnalla ei lähtökohtaisesti puututa perus- ja ihmisoikeuksiin, ja siksi siitä ei ole toistaiseksi katsottu olevan tarpeen säätää laissa.

Avointen lähteiden tiedonhankintaa voidaan käyttää muiden tiedonhankintakeinojen tukena tai itsenäisenä keinona hankkia tietoa esimerkiksi tilanteissa, joissa muiden tiedonhankintakeinojen käyttö ei ole mahdollista tai tehokasta (ks. esim. HE 203/2017 vp, s. 218). Avointen lähteiden tiedonhankinta voidaan karkeasti jakaa rajattuun tiedustelukysymykseen perustuvaan tiedusteluun ja esimerkiksi mediaseurantaan.

Avointen lähteiden tiedonhankinnan vahvuuksiin kuuluvat sen nopeus, edullisuus, maantieteellinen rajoittamattomuus ja mahdollisuus kerätä tietoja myös tulevista tapahtumista (ks. HE 203/2017 vp, s. 218). Avointen lähteiden merkitys tiedustelulle ja viranomaistoiminnalle on merkittävä, ja avoimista lähteistä saaduilla tiedoilla voidaan myös täydentää muuta tiedustelutietoa tai toisin päin. Pelkästään avoimiin lähteisiin perustuva analysoidun tiedon on yleisesti myös katsottu olevan laajemmin jaettavissa.

Etsimällä ja yhdistämällä kerättyä tietoa saadaan muodostettua kokonaisuuksia, jotka kertovat tietoa toiminnasta enemmän kuin olisi muuten mahdollista. Avointen lähteiden tiedonhankinta edellyttää tiedon yhdenmukaista jaottelua, huolellista arviointia ja tiedon suodattamista. Tiedon suuren määrän haittapuolena on olennaisen tiedon hukkuminen massaan. Lisäksi on otettava huomioon avoimiin lähteisiin liittyvä disinformaation riski. Etenkin ulkomailla toimittaessa voi olla vaikeaa tunnistaa relevantteja ja luotettavia lähteitä laajasta informaatiotarjonnasta.

Tyypillisiä avoimia tiedonlähteitä ovat olleet muun muassa kirjallisuus, tilastot, kartat, lehdet, yksityisten ja viranomaisten julkaisut, viranomaisten julkiset rekisterit ja tietokannat, yleisölle suunnatut televisio- ja radiolähetykset sekä tietoverkon ja sosiaalisen median sisällöt (HE 203/2017 vp, s. 218). Viime vuosina erityisesti sosiaalisen median kautta saatavien havaintojen määrä on kasvanut suhteessa muihin lähteisiin. Esimerkiksi sosiaalisessa mediassa tilin käyttäjän itsestään ottama kuva voi olla kiinnostava sen takia, mitä kuvan taustalta näkyy sekä missä ja mihin aikaan kuva on otettu. Viimeaikaisesta kehityksestä todettakoon Ukrainan sodassa venäläisten sotabloggarien korostunut asema tiedon jakamisessa.

Avointen lähteiden informaatiota voidaan hankkia esimerkiksi ostamalla lähteiden seuranta- ja analyysipalveluita tai niitä koskevia selvityksiä yrityksiltä. Lisäksi voidaan käyttää erilaisia

ohjelmistoja, jotka seulovat julkisista lähteistä olennaisia tietoja sekä niissä tapahtuneita päivityksiä ja muita muutoksia. Tiedusteluviranomaisen keskeisenä tavoitteena on yhdistää avointen lähteiden tietoja muilla tiedonhankintakeinojen käytöllä ja kansainvälisellä tiedonvaihdolla saatuihin tietoihin seikkaperäisemmän käsityksen tai tilannekuvan muodostamiseksi. Avoimista lähteistä saatu tieto on myös hyvä keino varmistaa tiedonhankintakeinojen käytöllä tai tiedonvaihdolla saadun tiedon luotettavuus.

Avointen lähteiden tiedonhankintaan ei sisälly aktiivinen osallistuminen esimerkiksi verkkosivuilla tai sosiaalisessa mediassa käytävään keskusteluun tiedon hankkimiseksi. Tietoverkoissa suoritettavalla avointen lähteiden tiedonhankinnalle on tyypillistä erilaisiin palveluihin rekisteröityminen sellaisilla tiedoilla, jotka eivät paljasta tiedonhankinnan tarkoitusta tai toteuttajaa. Vastaavasti hakeutuminen sosiaalisen median käyttäjien suljettuun ryhmään, johon tarvitaan esimerkiksi ryhmän ylläpitäjän hyväksyntä, on avointen lähteiden tiedonhakuna sallittua, jos tiedonhankintaa toteuttava viranomainen harhauttaa ryhmän ylläpitäjää luulemaan häntä muuksi kuin hän todellisuudessa on. Poliisimies ei kuitenkaan saisi ryhmässä käydä aktiivista keskustelua muiden ryhmän jäsenten kanssa, jolloin kyse voisi olla esimerkiksi peitellyn tiedonhankinnan tai nettipeitetoiminnan käyttämisestä. Silloin, kun harhauttaminen ei kohdistu henkilöön, vaan tietojärjestelmään, niin tilanne on toinen. Myös hakeutuminen tietoverkon eri palveluihin, kuten keskustelufoorumille tai pimeän verkon myyntipalstalle, on avointen lähteiden tiedonhankintana katsottu olevan sallittua. Tällaisessa tilanteessa harhauttaminen voi kohdistua palveluntarjoajaan, kuten esimerkiksi pimeän verkon myyntipalstan ylläpitäjään. Asetelmaa voidaan verrata siihen, kun siviiliasuinen poliisimies ostaa lipun ja menee yleisötilaisuuteen, esimerkiksi musiikkifestivaaleille, poliisiasemansa peittäen.

Avointen lähteiden tiedonhankinta yleisessä tietoverkossa voi kohdistua sosiaalisen median palveluissa olevien henkilöiden profiileissa olevaan tietoon. Ihmiset julkaisevat tietoverkossa ja erityisesti sosiaalisessa mediassa itsestään ja elinympäristöstään merkittävästi yksityisyytensä suojan piiriin kuuluvaa tietoa. Esimerkiksi ihminen voi julkaista sosiaalisen median tilillään valokuvia kodistansa, kesämökiltänsä, perheestänsä ja kavereistansa. Avointen lähteiden tiedonhaun on katsottu olevan sallittua, jos se kohdistuu ihmisen yleisön saataville julkaisemaan tietoon. Avointen lähteiden tiedonhankintaa ei kuitenkaan saa käyttää toisen toimivaltuuden kiertämiseen.

Tietoverkossa toimittaessa on lähtökohtaisesti aina pyrittävä häivyttämään niin sanottua digitaalista jalanjälkeä, jottei avoimia lähteitä hyödyntävää virkamiestä päästä yhdistämään tiedonhankintaa suorittavaan viranomaiseen.

Puolustusvoimissa avointen lähteiden tiedustelua voidaan käyttää laajasti kaikissa Puolustusvoimien tehtävissä. Tarkemmin se, missä yhteydessä tiedonhankintaa suoritetaan, määräytyy Puolustusvoimien työjärjestysten ja määräysten mukaisesti. Selvää on se, että esimerkiksi henkilötietoja ei voida tallentaa kaikissa asiayhteyksissä, vaan sille on oltava selkeä syy.

Sotilastiedustelusta annetun lain 75 §:ssä säädetään sotilastiedustelun suojaamisesta. Sen 1 momentin mukaan sotilastiedusteluviranomainen saa käyttää vääriä, harhauttavia tai peiteltyjä tietoja, tehdä ja käyttää vääriä, harhauttavia tai peiteltyjä rekisterimerkintöjä sekä valmistaa ja käyttää vääriä asiakirjoja, kun se on välttämätöntä sotilastiedustelun paljastumisen estämiseksi.

Pykälän 2 momentin mukaan edellä 1 momentissa tarkoitettu rekisterimerkintä on oikaistava sen jälkeen, kun momentissa tarkoitettuja edellytyksiä ei enää ole.

Pykälän 3 momentin mukaan sotilastiedustelun suojaamisen järjestämisestä, sotilastiedustelun suojaamisesta vastaavasta virkamiehestä sekä yhteistyöstä rekisterinpitäjien kanssa voidaan antaa tarkempia säännöksiä valtioneuvoston asetuksella.

2.2.14 Rekrytointi Puolustusvoimissa

Puolustushallinnossa ennen kaikkea sotilastiedustelu salassa pidettävänä toimintana on keino saada havaintoja ja hankkia tietoa ennakollisesti kansallisen turvallisuuden uhista. Tietoa hankitaan myös uhasta, joka tapahtuu Suomen ulkopuolella ja kohdistuu Suomeen. Tiedonhankinta kohdistuu kohteisiin, joista säädetään sotilastiedustelusta annetun lain 4 §:ssä ja lain 4 luvussa säädettyjä toimivaltuuksia (tiedustelumenetelmiä) käyttäen. Puolustusvoimien tehtävät kattavat myös laaja-alaisesti muuta toimintaa, kuten rikostorjuntaa, kyberpuolustuksen ja Puolustusvoimien operaatio- ja muuhun turvallisuuteen liittyviä tehtäviä.

Vieraiden valtioiden Suomeen kohdistama toiminta on suunnitelmallista ja pitkäjänteistä. Niiden tavoitteena on heikentää Suomen maanpuolustuksen ja pahimmillaan tehdä toiminnot tehottomiksi, vaikeuttaa tehtävien suorittamista merkittävästi tai tehdä tehtävien suorittaminen ylipäätään mahdottomaksi. Useissa tehtävissä Puolustusvoimien henkilöstöä ja heidän työtehtäviään koskeva tieto on lähtökohtaisesti salassa pidettävää. Henkilöstötiedon julkisuus muodostaa tietyissä tilanteissa Puolustusvoimille organisaatiotason riskin vieraan valtion Puolustusvoimien henkilöstöön kohdistamien mahdollisten värväysyritysten tai muiden operaatioiden takia.

Puolustusvoimien viroissa toimivat pääsevät tehtävissään maanpuolustuksen ja kansallisen turvallisuuden kannalta salassa pidettäviin kriittisiin tietoihin. Näiden tietojen päätyminen ulkopuoliselle taholle syystä riippumatta voi aiheuttaa vahinkoa maanpuolustukselle ja kansalliselle turvallisuudelle. Ulkopuolisen, vihamielisen tahon kiinnostuksen kohteena voidaan erityisesti arvioida olevan operatiivisissa tiedustelutehtävissä ja sen tukitehtävissä, tietojen analyysitehtävissä ja teknologiaan liittyvissä tehtävissä toimivat virkamiehet. Henkilön tietojen julkisuus mahdollistaa Puolustusvoimien toimintaan liittyviä tehtäviä suorittavaan virkamieheen kohdistuvan uhan, vakavimmillaan konkreettisen hengen tai terveyden vaaran. Riskejä voi kohdistua myös edellä mainittujen virkamiesten lähipiiriin taikka sotilastiedustelun tai Puolustusvoimien rikostorjunnan kanssa yhteistyötä tekeviin henkilöihin kuten tietolähteisiin. Tiedusteluvalvontavaltuutettu on käsitellyt tarkemmin tiedusteluviranomaisen virkamiehiin ja heihin vakituisesti yhteydessä oleviin henkilöihin liittyviä uhkia kertomuksissaan vuodelta 2019[6] ja 2020[7].

Valtion virkamieslaissa (750/1994), joka on kaikkia valtion virkamiehiä koskeva yleislaki, säädetään virkojen ja määräaikaisten virkasuhteiden hakumenettelystä ja nimittämisestä. Lähtökohtaisesti Puolustusvoimien hakumenettelyihin sovelletaan valtion virkamieslakia, jolloin hakumenettely on pääsääntöisesti julkinen.

Valtion virkamieslain 6 a §:n mukaan virka on ennen sen täyttämistä julistettava haettavaksi. Virkamieslain 6 c §:n mukaan hakuilmoituksessa on mainittava viran tehtävät ja säädetyt kelpoisuusvaatimukset, hakuajan päättymisaika sekä se viranomainen, jolle hakemus on osoitettava. Edelleen ilmoituksessa on mainittava, onko virka perustettu tiettyyn yksikköön vai

[6] Tiedusteluvalvontavaltuutetun kertomus vuodelta 2019. K 14/2020 vp.
[7] Tiedusteluvalvontavaltuutetun kertomus vuodelta 2020. K 10/2021 vp.

onko se viraston yhteinen. Valtiovarainministeriö on antanut 28.10.2024 virantäytössä noudatettavista periaatteista ohjeen[8], jossa linjataan muut hakuilmoituksessa mainittavat seikat.

Nimitysmuistio muodostaa pohjan nimityspäätöksessä esitettäville perusteluille, ja muistiolla on merkitystä myös naisten ja miesten välisestä tasa-arvosta annetun lain (609/1986) noudattamista selvitettäessä ja yhdenvertaisuuslain (1325/2014) oikeussuojakeinojen kannalta. Viran tai virkasuhteen täyttöä koskevan nimityspäätöksen perusteiden tulee ilmetä riittävän selvästi ja avoimesti nimitysmuistiosta.

Virkamieslain 6 d §:n 2 momentin mukaan nimityspäätöksen tehneen viranomaisen on ilmoitettava viivytyksettä nimityksestä niille, jotka ovat virkaa tai virkasuhdetta hakeneet. Ilmoituksessa on mainittava täytettävänä ollut virka tai virkasuhde, päätöksen tehnyt viranomainen, nimityspäivä sekä virkaan tai virkasuhteeseen nimitetty. Virkamieslain 59 §:n 1 momentin mukaan viranhakija saa hakea virkaan tai virkasuhteeseen nimittämistä koskevaan päätökseen muutosta valittamalla, jollei virkamieslaissa toisin säädetä. Valitusaika alkaa nimityspäätöksen tiedoksisaannista. Nimityspäätöksen tulee täyttää hallintolain (434/2003) 44 §:ssä kirjalliselle hallintopäätökselle säädetyt vaatimukset. Päätöksessä on mainittava päätöksen tehnyt viranomainen ja päätöksen tekemisen ajankohta, päätöksen perustelut ja tieto nimitetystä sekä sen henkilön nimi ja yhteystiedot, jolta asianosainen voi pyytää tarvittaessa lisätietoja päätöksestä. Muiden hakijoiden nimet voivat ilmetä päätöksen jakelusta. Nimityspäätökseen on liitettävä valitusosoitus tai ilmoitus valituskiellosta. Nimityspäätöksessä asianosaisia ovat sekä nimitetty henkilö että muut hakijat.

Lainsäädäntö sisältää kuitenkin poikkeuksia. Valtion virkamieslain 59 §:n 2 momentin mukaan päätöksestä ei saa valittaa, jos nimittämistoimivalta kuuluu tasavallan presidentille tai valtioneuvoston yleisistunnolle nimitettäessä ministeriöiden ylimpiä virkamiehiä tai valtioneuvoston asetuksessa määritettyjen virastojen päällikköjä. Valitusoikeutta ei myöskään ole, jos henkilö nimitetään enintään kahden vuoden määräajaksi tai virka tai virkasuhde täytetään lain nojalla haettavaksi julistamatta tai päätös koskee Puolustusvoimien tai Rajavartiolaitoksen sotilasvirkaa, joka voidaan lain nojalla täyttää haettavaksi julistamatta. Sotilasvirkojen osalta valituskielto on voimassa, vaikka virka täytettäisiin avoimessa hakumenettelyssä.

Puolustusvoimissa on sotilasviroissa ja siviiliviroissa palvelevaa henkilöstöä. Lisäksi voi olla määräaikaisessa virkasuhteessa ja työsuhteessa olevaa henkilöstöä. Puolustusvoimista annetun lain (551/2007) 36 a §:n 1 momentin mukaan puolustusvoimien virat voidaan täyttää niitä haettavaksi julistamatta. Pykälän 2 momentissa säädetään viroista, jotka kuitenkin julistetaan haettavaksi.

Poliisin hallinnosta annetun lain 12 a §:n mukaan Keskusrikospoliisin ja paikallispoliisin virka tai virkasuhde, jossa tehtäviin kuuluu tietolähdetoiminta-, valeosto-, peitetoiminta- tai todistajansuojelutehtäviä tai niihin välittömästi liittyviä esimies- tai tukitehtäviä, voidaan täyttää niitä haettavaksi julistamatta, jos tehtävän luonne sitä välttämättä edellyttää. Välttämättömyyttä arvioitaessa otetaan huomioon: 1) poliisin henkilöstö- ja organisaatioturvallisuus, 2) täytettävä tehtävä ja siihen liittyvät uhkat, 3) tarve salaisen tiedonhankinnan suojaamiseen tai 4) muu erittäin tärkeä yleinen tai yksityinen etu.

[8] Ohje virantäytössä noudatettavista periaatteista VN/30496/2024. Valtiovarainministeriö.

Pykälän 2 momentin mukaan täytettäessä 1 momentissa tarkoitettu virka tai virkasuhde hakumenettelyssä keskusrikospoliisi ja paikallispoliisi voivat jättää ilmoittamatta virkaa tai virkasuhdetta hakeneiden nimet sekä nimitetyn nimen muille hakijoille, jos haettavan tehtävän luonne sitä 1 momentissa tarkoitetuin tavoin välttämättä edellyttää. Viran tai virkasuhteen täyttämisestä on kuitenkin ilmoitettava hakijoille ja nimityspäätöksessä on mainittava täytettävänä ollut virka tai virkasuhde, päätöksen tehnyt viranomainen sekä nimityspäivä.

Poliisin hallinnosta annetun lain 13 a §:n mukaan Suojelupoliisin virka tai virkasuhde voidaan täyttää niitä haettavaksi julistamatta, jos tehtävän luonne sitä välttämättä edellyttää. Välttämättömyyttä arvioitaessa otetaan huomioon 1) suojelupoliisin henkilöstö- ja organisaatioturvallisuus, 2) täytettävä tehtävä ja siihen liittyvät uhkat, 3) siviilitiedustelun suojaaminen tai 4) muu erittäin tärkeä yleinen tai yksityinen etu.

Pykälän 2 momentin mukaan seuraavat virat tai virkasuhteet julistetaan kuitenkin haettavaksi valtion virkamieslain mukaisesti: apulaispäällikkö, osastopäällikkö ja yksikön päällikkö sekä tehtävien suhteen niitä vastaavalla tasolla oleva virka tai virkasuhde.

Pykälän 3 momentin mukaan täytettäessä 1 momentissa tarkoitettu virka tai virkasuhde hakumenettelyssä suojelupoliisi voi jättää ilmoittamatta virkaa tai virkasuhdetta hakeneiden nimet sekä nimitetyn nimen muille hakijoille, jos haettavan tehtävän luonne sitä 1 momentissa tarkoitetuin tavoin välttämättä edellyttää. Viran tai virkasuhteen täyttämisestä on kuitenkin ilmoitettava hakijoille ja nimityspäätöksessä on mainittava täytettävänä ollut virka tai virkasuhde, päätöksen tehnyt viranomainen sekä nimityspäivä.

Poliisin hallinnosta annetun lain 15 j §:n nojalla vanhemman konstaapelin, vanhemman rikoskonstaapelin ja nuoremman konstaapelin virka voidaan täyttää sitä haettavaksi julistamatta. Täytettäessä virka haettavaksi julistamatta, viran täytöstä ei voi valittaa. Suojelupoliisin näkökulmasta virkalistat haettavaksi julistamatta täytettävien virkojen osalta eivät ole relevantteja, eikä kyseisiä vanhemman konstaapelin, vanhemman rikoskonstaapelin ja nuoremman konstaapelin virkanimikkeitä käytetä, koska tehtävät eroavat muusta poliisista ja kelpoisuusvaatimukset voivat olla rajoittavia. Poliisin hallinnosta annetun asetuksen 16 §:n mukaan kelpoisuusvaatimuksena vanhemmalla rikoskonstaapelilla, vanhemmalla konstaapelilla ja etsivällä on poliisin ammattikorkeakoulututkinto, poliisin perustutkinto tai poliisimiehistön virkatutkinto. Kyse on miehistötason viroista. Poliisin valeosto- ja peitetoiminta sekä tietolähdetoimintatehtäviä tai todistajansuojeluohjelmatehtäviä hoitaa yleensä vähintään alipäällystötasoinen virkamies, jonka vuoksi säännös ei sovellu näitä tehtäviä hoitavien virkamiesten rekrytointimenettelyyn.

Rajavartiolaitoksen hallinnosta annetun lain (577/2005) 12 §:n 2 momentin mukaan Rajavartiolaitoksen sotilasvirat voidaan täyttää niitä haettavaksi julistamatta. Rajavartiolaitoksen hallinnosta annetun lain 9 §:n 1 momentin mukaan sotilasvirkoja ovat upseerin, erikoisupseerin, opistoupseerin, merivartijan ja rajavartijan virat.

Ulkoasiainhallinnon niin sanotun ura- eli karriäärijärjestelmän puitteissa rekrytointivaiheen julkisen haun jälkeen uralla eteneminen tapahtuu ilman julkista hakumenettelyä. Ulkoasiainhallintolain (204/2000) 15 §:n 1 momentin mukaan ulkoasiainhallinnon virkoihin nimittää valtioneuvosto tai ulkoasiainministeriö sen mukaan kuin valtioneuvoston asetuksella säädetään.

Pykälän 2 momentin mukaan ulkoasiainhallinnon yleisvirat voidaan täyttää haettavaksi julistamatta. Osalla yleisvirkamiehiä on lain nojalla siirtymisvelvollisuus toiseen tehtävään tai virkapaikkaan.

Julkisuuslakia sovelletaan oikeuteen saada tietoa ja muuhun tietojen luovuttamiseen viranomaisen henkilörekisteristä. EU:n yleisen tietosuoja-asetuksen tietojen minimointi periaatteeseen perustuen valtiovarainministeriön ohjeistuksessa todetaan, että hakijoille tiedoksi annettavan nimityspäätöksen ei tulisi sisältää muiden kuin nimitetyn henkilötietoja ja vain valitun henkilön valinnan perustelut. Julkisuuslain salassapitoperusteet soveltuvat virantäyttöprosessiin kuten julkisuuslain 24 §:n 1 momentin 29 kohta, joka koskee soveltuvuus- tai muita arviointeja tai 24 §:n 1 momentin 31 kohta, joka koskee yksityisiä tietoja. Virantäytön yhteydessä voi myös tulla arvioitavaksi julkisuuslain asianosaisjulkisuutta koskeva 11 § tai julkisuuslain 24 §:ssä säädetyt salassapitoperusteet laajemminkin yleisöjulkisuuden (tietopyyntöjen) kohdalla.

2.3 Nykytilan arviointi

2.3.1 Haittaohjelmaa koskevan tiedon luovuttaminen

Haittaohjelmaa koskevan tiedon luovuttamista sääntelee sotilastiedustelusta annetun lain 18 §:n 2 momentti ja 74 §. Ensimmäinen näistä on sidottu tiedustelun menetelmien ja järjestelmien kehittämiseen, eli tietojen luovuttaminen on mahdollista tiedusteluviranomaisen toiminnan kehittämisen lähtökohdista. Lisäksi tiedon luovuttaminen on sidottu välttämättömyyteen.

Lain 74 §:ssä tiedonluovutus on sidottu tiedustelumenetelmään, jolla tieto on saatu. Näin ollen muilla tiedustelumenetelmillä saatua haittaohjelmatietoa ei voida luovuttaa tietoa tarvitsevalle taholle.

Sääntelyä voidaan pitää tarpeettoman tiukkana ottaen huomioon yhteiskunnan edelleen kehittyvän digitalisoitumisen ja teknologian kehittymisen. Haittaohjelmatoimijat, ennen kaikkea APT-toimijat[9], eivät ole tästä kehityksestä irrallisia, vaan pyrkivät kehittämään toimintaansa edelleen ja nopeammin kuin kohdevaltion viranomaiset ja tietoturvallisuuden kehittämiseen osallistuvat yksityiset toimijat pystyvät siihen vastaamaan. Näin ollen haittaohjelmaa koskevan tiedon luovuttaminen olisi voitava tapahtua maanpuolustuksen kannalta ja kansallisen turvallisuuden suojaamiseksi mahdollisimman matalalla kynnyksellä.

Sotilastiedustelulla on käytössään lukuisia tiedustelumenetelmiä. Haittaohjelmia koskevia tietoja voidaan saada myös muilla tiedustelumenetelmillä kuin tietoliikennetiedustelulla, ennen kaikkea tietoteknisiin menetelmiin perustuvien tiedustelumenetelmien (esimerkiksi tekninen laitetarkkailu ja ulkomaan tietojärjestelmäntiedustelu) avulla. Näin ollen haittaohjelmatietojen hankinta nimenomaan tietoliikennetiedustelulla ei ole perusteltua.

Haittaohjelmaa koskevan tiedon luovuttamista koskevassa sääntelyssä tulee huomioitavaksi myös perustuslakivaliokunnan kannanotto siitä, että haitallisen tietokoneohjelman tai käskyn sisältämä viesti ei nauti perustuslain 10 §:n 2 momentin mukaista suojaa (PeVL 62/2024 vp, s. 4).

2.3.2 Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen

Voimassa olevan sääntelyn perusteella pykälässä kuvatun toimenpiteen suorittaja on ainoastaan sotilastiedusteluviranomainen. Käytännön tiedustelutoiminnassa on kuitenkin havaittu tarve

[9] APT-lyhenne tulee englanninkielisistä sanoista Advanced Persistent Threat. Ks. Supo ”APT-operaatiot”, https://supo.fi/apt-operaatiot.

käyttää myös sotilastiedusteluviranomaisen ulkopuolista toimenpiteen suorittajana. Tämä liittyy ennen kaikkea toimivaltuuden tehokkaaseen käyttämiseen sekä tiedustelumenetelmän käytön paljastumisen estämiseen. Mikäli jatkossakin edellytettäisiin toimenpiteen suorittajaksi ainoastaan sotilastiedusteluviranomaista, tämä rajaisi toimenpiteen ja sitä seuraavan tiedustelumenetelmän käyttöä tavalla, joka voisi haitata sotilastiedusteluviranomaisen tehtävien toteuttamista.

Teknologian kehittymisen myötä tiedustelumenetelmien käytön paljastumisen estäminen vaatii myös sotilastiedusteluviranomaisen toiminnan kehittämistä. Käytännön tiedustelutoiminnassa on havaittu, että pykälässä tarkoitetun toimenpiteen tehokas suorittaminen ja tiedustelumenetelmän käyttäminen voi edellyttää myös ulkopuolisen laitteen tai tietojärjestelmän käyttämistä, jotta sotilasviranomainen saa pääsyn siihen kohteeseen, johon toimenpiteen ja tiedustelumenetelmän käyttäminen liittyy. Voimassa olevan sääntelyn perusteella tämä ei ole mahdollista, jolloin sotilasviranomaisen tehtävän kannalta tarpeellinen tieto voi jäädä katveeseen.

2.3.3 Tietojärjestelmätiedustelu kotimaassa

Kuten edellä on nykytilan kuvauksessa tuotu ilmi, nykyisissä tietojärjestelmissä ei ole kyse yksittäisistä laitteista ja ohjelmistoista. Tietojärjestelmän voidaan katsoa muodostuva 1) tietojenkäsittelylaitteista, tiedonsiirtolaitteista, tietoa käsittelevistä ohjelmista ja tietojen käsittelysäännöistä, 2) useiden eri laitteiden ja ohjelmistojen tai näiden osien muodostamasta maantieteellisesti ja loogisesti hajautetusta kokonaisuudesta ja 3) se voi kattaa myös osia, jotka kuuluvat samanaikaisesti johonkin toiseen tietojärjestelmään.

Tiedon hankkiminen edellä kuvatusta kokonaisuudesta on sinänsä mahdollista, mutta se edellyttää useiden eri toimivaltuuksien käyttöä. Näitä toimivaltuuksia ovat telekuuntelu, televalvonta, tekninen kuuntelu ja tekninen laitetarkkailu.

Esimerkiksi tekninen laitetarkkailu ei tunnista edellä tarkoitettua tietojärjestelmää kokonaisuutena. Jos tietoa hankittaisiin tietojärjestelmästä teknisellä laitetarkkailun kohdentamisvaatimuksen mukaisesti, tiedonhankinta on vaikeaa, se estyy tai vaatii pitkälle menevää laintulkintaa. Näin käy erityisesti sellaisissa tilanteissa, joissa tiedonhankinta ei kohdistu yksittäiseen laitteeseen tai sen ohjelmistoon, vaan useiden laitteiden, esimerkiksi useiden Internet-palvelimien, ja useiden ohjelmistojen muodostamaan kokonaisuuteen. Tällaisia kokonaisuuksia ovat useimmat nykyaikaiset viestinvaihtoon ja tietojen tallentamiseen tarkoitetut yleisölle saataville saatetut tai organisaatioiden käyttämät järjestelmät. Teknisen laitetarkkailun käyttäminen edellyttäisi jokaisen yksittäisen laitteen ja ohjelmiston tunnistamista ja osoittamista tiedustelumenetelmän lupavaatimuksessa.

Nykysääntelyn mukainen laitteen tunnistaminen teknisen laitetarkkailun edellytyksenä on ongelmallista monissa niistä tilanteista, joissa hankittava tieto sijaitsee jossakin tietoverkkoon kytketyssä palvelussa. Tällöin laite on yleensä yksilöitävissä vain jollakin sekundäärisellä tunnisteella, säännönmukaisesti tietoverkon teleosoitteella, esimerkiksi IP-osoitteella.

Laitteen tunnistaminen ja teknisen laitetarkkailun kohdistaminen laitetasolle asti tulee ongelmalliseksi myös, mikäli laitteen olemassaolosta ja käytöstä tai käyttäjästä tiedetään jollain muulla tiedustelumenetelmällä hankitun tiedon myötä, mutta tällä ei kyetä hankkimaan tarkempia yksilöiviä tietoja.

Telekuuntelun ja televalvonnan määritelmäsäännöksistä ilmenee, että kyseisiä toimivaltuuksia sovelletaan silloin, kun tiedonhankinta kohdistuu yleisessä viestintäverkossa tai siihen liitetyssä

viestintäverkossa välitettävänä olevaan viestiin. Telekuuntelun ja televalvonnan erottamisen voidaan katsoa olleen välttämätöntä erottaa teknisen kuuntelun alasta pääasiassa siksi, että ne muusta viestintään kohdistuvasta tiedonhankinnasta poiketen on pääsääntöisesti välttämätöntä toteuttaa viestinnän välittäjän (teleyrityksen) avustuksella, ja viestinnän välittäjän velvollisuudesta avustaa viranomaista telekuuntelun ja -valvonnan toteuttamisessa on siksi ollut tarve säätää erikseen.

Lisäksi yhdessä teleosoitteessa viestivä palvelu saattaa olla toteutettuna useamman eri laitteen kokonaisuutena tai niin sanottuna virtuaalipalvelimena, jossa yksi fyysinen palvelintietokone vastaa useamman loogisen virtualisoidun tietokoneen ohjelmien ajamisesta ja tietojen säilyttämisestä. Vielä lisäksi teknisen laitetarkkailun kohteena oleva laite saattaa olla tietoverkossa asemoitu niin, että kommunikointi ko. laitteen kanssa tapahtuu usean tiedonkäsittely- ja tiedonsiirtolaitteista muodostuvan ketjun kautta. Jotta tekninen laitetarkkailu varsinaisen tiedustelun kohteena olevaan laitteeseen onnistuisi, joudutaan ketjun muihin laitteisiin myös toteuttamaan teknistä laitetarkkailua tarvittavan tiedon saamiseksi.

Nykytilassa niin kutsuttu päästä-päähän salaus on lisääntynyt, mihin on osaltaan vaikuttanut se, että tekniikkaa käytetään muun muassa yleisimmissä viestintäpalveluissa. Salauksen yleistyminen on myös johtanut siihen, että telekuuntelulla ei aina saada riittävän laaja-alaisesti tietoa kohteen viestinnästä, vaan tieto lähetetyistä ja saapuneista viesteistä saadaan käytännössä kohteena olevasta laitteesta. Vaikka nykytilassa sinänsä tekninen laitetarkkailu osittain vastaa tähän ongelmaan, sillä ei kuitenkaan saada hankittua tietoa reaaliaikaisesti vastaavasti kuin telekuuntelulla. Toisaalta tiedon kulkiessa viestintäsovelluksessa, tietoa ei välttämättä saada hankittua edes telekuuntelulla.

Nykytilan kuvauksesta käy ilmi, että yhdessä ja samassa tietojärjestelmäkokonaisuudessa oleva sekä yhtä ja samaa tietoa koskeva tiedonhankinta pirstaloituu usean eri toimivaltuuden alle sen mukaan, sijaitseeko tieto tiedonhankinnan hetkellä jossain teknisessä laitteessa, yleisessä viestintäverkossa tai siihen liitetyssä viestintäverkossa taikka muussa viestintäverkossa kuin yleisessä viestintäverkossa tai siihen liitetyssä verkossa.

Tietojärjestelmän tiedustelun osalta keskeinen ongelma onkin se, että tietojärjestelmää ei pystytä etukäteen hahmottamaan täysin. Tiedustelumenetelmän käyttö voidaan aloittaa yksittäiseen laitteeseen, kuten päätelaitteeseen, kohdistuen. Päätelaitteeseen kohdistuvan tiedustelumenetelmän käytöllä voidaan saada tieto siitä, että päätelaite on yhteydessä mahdollisesti organisaation keskitettyyn palvelimeen. Jotta tiedustelumenetelmän käyttöä voitaisiin kohdistaa esimerkiksi organisaation käyttämään palvelimeen, olisi ensin haettava lupa telekuunteluun, jotta saataisiin tietoa siitä, mihin palvelimeen päätelaite on yhteydessä. Tämän jälkeen olisi haettava taas lupa tekniseen laitetarkkailuun, jotta palvelimesta saataisiin hankittua tietoa. Tietojärjestelmiin liittyvien laitteiden ja ohjelmistojen sekä tiedustelumenetelmien kohdentamisen monijakoisuus johtaa siihen, ettei maanpuolustuksen kannalta ja kansallista turvallisuutta vakavasti uhkaavasta toiminnasta saada kaikkea tarvittavaa tietoa. Oman lisänsä kokonaisuuteen tuo tiedon nopea liikkuvuus.

Edellä todettu johtaa siihen, että etenkin kybervakoilun ja –vaikuttamisen selvittämisessä nykytilaa voidaan pitää toimimattomana, koska tuomioistuimen sotilastiedustelun kohteeksi hyväksymä yksittäinen tekninen laite on käytännössä aina osa kokonaisuutta, johon kuuluu kymmeniä tai jopa satoja muita laitteita, joita vieras valtio hyödyntää Suomeen kohdistuvan vakoilunsa ketjutuksessa. Vihamielisessä valtiollisessa kybertoiminnassa hyväksi käytettävien laitteiden väliset yhteydet ja ketjut rakentuvat ja häviävät erittäin nopeasti, minkä takia niihin kohdistuvaan tiedonhankintaan ei ole mahdollista saada tuomioistuimelta lupaa käytettävissä olevan aikaikkunan puitteissa.

Ratkaisu on toimimaton myös sotilastiedusteluviranomaisen sotilaalliseen toimintaan ja muun kansallisen turvallisuudelle uhan muodostaviin organisaatioihin kohdistamassa tiedonhankinnassa, ja jopa yksittäisiin henkilöihin kohdistuvassa tiedonhankinnassa. Lähes poikkeuksetta nykyaikaiset digitaaliseen kommunikointiin ja tietojen käsittelyyn tai tiedon säilömiseen tarkoitetut tietojärjestelmät koostuvat useista yhdessä toimivista laitteista ja ohjelmistoista (esimerkiksi yksittäisen tietokoneen hyödyntämät pilvitallennustilat tai jonkin organisaation sähköpostiviestintään käyttämät palvelimet, tietoliikennelaitteet ja asiakasohjelmistot). Tämän takia nykyistä teknistä laitetarkkailua voidaan pitää toimimattomana.

Nykytilan laitekeskeinen lähestymistapa muodostaa ongelman esimerkiksi seuraavan kaltaisissa tilanteissa:

- erilaisiin pilvipalveluihin tallennetun tiedon hankkiminen;
- muut sellaiset verkon palvelut, joihin kommunikointi ja käyttäjäinteraktio tapahtuu yhden teleosoitteen kautta, mutta taustalla palvelua on toteuttamassa useampi palvelin;
- kyberuhkatoimijoiden moniosaisten, ketjutettujen ja maantieteellisesti hajautettujen Internetin päälle rakennettujen hyökkäysinfrastruktuureiden ja anonymisointiverkkojen tiedustelu;
- ulkomaantiedustelu, jossa toimintaympäristön rajoitteet vähentävät sotilastiedusteluviranomaisen mahdollisuutta yksilöidä laitetta, jossa hankittava tieto on tallennettuna.

Tässä käsiteltyjen tiedustelumenetelmien osalta on myös eroavaisuutta niiden kohdistamisen osalta. Telekuuntelu, televalvonta ja tekninen kuuntelu voidaan vaatia koskemaan tiettyä henkilöä ja kaikkia tämän henkilön käyttämiä telepäätelaitteita ja -osoitteita, jotka ovat luvan voimassaoloaikana kohdehenkilön hallussa tai käytössä. Päätöksen yksittäisen telepäätelaitteen tai -osoitteen kuulumisesta tuomioistuimen myöntämän luvan piiriin tekee erityisesti tiedustelumenetelmien käyttöön perehtynyt sotilaslakimies tai muu virkamies. Vastaava ei ole mahdollista teknisen laitetarkkailun kohdalla. Lisäksi teknistä laitetarkkailua ei voi kohdistaa teleosoitteen perusteella.

Tietojärjestelmien osalta voi tulla vastaan myös tilanteita, ettei ole selvää, mitä tiedustelumenetelmää olisi käytettävä. Esimerkiksi tilanteessa, jossa osana tietojärjestelmää kahden palvelimen yhdistävä reititin tai muu tietoliikenneyhteys voi olla osana yleistä viestintäverkkoa tai kyse on organisaation sisäverkosta. Näin ollen itse tiedonhankinnan hetkellä ei ole välttämättä selvää se, pitäisikö tietoliikenneyhteydestä tietoa hankittaessa käytettävä telekuuntelua vai teknistä kuuntelua. Toisaalta tekninen kuuntelua ei voitane katso alun perin tarkoitetun tähän tarkoitukseen, jolloin kyseeseen saattaisi tulla ainoastaan telekuuntelu, jonka käyttö on riippuvainen siitä, liikkuuko tieto yleisessä viestintäverkossa. Viime kädessä tilanteessa käsillä ei ole tiedustelumenetelmää, jota voitaisiin käyttää yksiselitteisesti.

2.3.4 Tekninen laitetarkkailu

Voimassa olevan lain mukaan tekninen laitetarkkailu voi kohdistua tiettyyn laitteeseen tai ohjelmistoon. Teknistä laitetarkkailua on rajoitettu nimenomaisesti myös siten, että se ei voi kohdistua viestintäverkossa välitettävänä olevaan viestiin, johon kohdistuvaan tiedonhankintaan sovelletaan sotilastiedustelusta annetun lain 34 §:ää. Näin ollen tekninen laitetarkkailu kohdistuu laitteen käyttämiseen, laitteeseen tallennettuun tietoon tai viestiin

taikka laiteessa käytettävään ohjelmistoon. Jotta tekninen laitetarkkailu olisi mahdollista, edellyttää tämä käytännössä laitteen, menetelmän tai ohjelmiston asentamista laitteeseen.

Erilaisten laitteiden ja ohjelmistojen määrä kasvaa jatkuvasti. Etenkin telepäätelaitteiden ja niissä käytettävien liittymien määrät ovat kasvaneet vuositasolla selvästi enemmän kuin tiedustelumenetelmien kohteena olevien henkilöiden lukumäärät. Lisäksi niin kutsuttu päästä päähän salaus on yleistynyt ja kaikkien saatavilla yleisesti käytössä olevien viestintäsovellusten kautta, mikä osaltaan heikentää telekuuntelun käyttömahdollisuuksia.

Useimmat ohjelmistot lisäksi voivat tallentaa tietoa pilvipalveluihin esimerkiksi varmuuskopioina, mutta käyttäjä voi itse vaikuttaa tähän.

Voimassa olevan lain perusteella tiedonhankintaa voidaan kohdistaa kohteeseen kattavasti henkilön hallussa oleviin telepäätelaitteisiin ja käyttämiin teleosoitteisiin viestintäverkossa esimerkiksi kohdistamalla telekuuntelua henkilöön, mutta vastaavalla laajuudella tiedonhankintaa ei voida kohdistaa itse laitteeseen tai henkilön käyttämiin laitteisiin ja ohjelmistoihin.

Televerkoissa toteutettava tiedustelu jättää ulkopuolelle esimerkiksi tallennuslaitteet, kuten kovalevyt ja ulkoiset muistivälineet, kuten USB-tikut. Lisäksi erilaisten ohjelmistojen kirjon voidaan arvioida kasvavan tekoälyn kehittymisen myötä. Näin ollen sotilastiedustelun kohteena olevalla voi olla käytössään lukuisien telepäätelaitteiden ja -osoitteiden lisäksi muita tallennusvälineitä sekä laitteissa käytettäviä ohjelmistoja. Tiedonhankinnan kohdistaminen tallennusvälineeseen voi olla aikakriittistä, sillä tieto tallennusvälineestä voi tulla yllättäen ja mahdollisuus asentaa siihen laite, menetelmä tai ohjelmisto, voi tulla vastaan yhtälailla yllättäen.

Jo nykyään sotilastiedustelutoiminnassa samaa kohdetta koskien saatetaan joutua tekemään samassa tiedustelutehtävässä useita peräkkäisiä teknisen laitetarkkailun vaatimuksia ja päätöksiä, joita joudutaan tekemään jopa viikoittain. Siten nykysääntelyn laite- ja ohjelmistokohtaisuus aiheuttaa samoissa asioissa useita peräkkäisiä lupien valmistelu- ja käsittelyprosesseja sekä sotilastiedusteluviranomaisessa että tuomioistuimessa. Teknistä laitetarkkailua koskevan harkinnan osalta olennainen on teknisen laitetarkkailun aiheuttama perusoikeusloukkaus, joka kohdistuu yksityisyyden ja luottamuksellisen viestinnän suojaan. Merkitystä tämän kannalta ei niinkään ole sotilastiedustelun kohteena olevan henkilön käyttämien laitteiden tai ohjelmistojen taikka näihin kohdistuvien teknisen laitetarkkailun lupien lukumäärällä. Olennaisempaa tämän sijaan on, voidaanko tietyn sotilastiedustelun kohteena olevan henkilön yksityisyyden tai luottamuksellisen viestinnän suojaa ylipäätään loukata hänen käyttämäänsä laitteeseen tai ohjelmistoon kohdistettavalla teknisellä laitetarkkailulla.

Lisäksi voidaan todeta, että tekninen laitetarkkailu on jo käytännössä hyvin samantyyppinen tai ainakin lähellä menetelmänä telekuuntelua ja televalvontaa, tosin tiedonhankinta tapahtuu laitteesta eikä siitä lähetetystä tai siihen saapuvasta sähköisestä viestistä.

Perustellulta siis vaikuttaisi, että teknistä laitetarkkailua koskeva sääntely muutettaisiin laite- tai ohjelmistokohtaisuuden lisäksi henkilösidonnaiseksi. Tällöin luvassa ei lueteltaisi erikseen kaikkia niitä laitteita tai ohjelmistoja, joita lupa koskee, vaan tuomioistuin myöntäisi luvan suorittaa teknistä laitetarkkailua laitteisiin ja ohjelmistoihin, jotka ovat sotilastiedustelun kohteena olevan henkilön käytössä. Muutoksen johdosta sotilastiedusteluviranomaisen ei tarvitsisi hakea erikseen yksittäisiä lupia kullekin kohteen käytössä olevalle laitteelle tai ohjelmistolle, jotka selviävät teknistä laitetarkkailua koskevan luvan myöntämisen jälkeen.

Käytössä olevia laitteita voidaan selvittää nykyisellään televerkossa suoritettavalla tiedonhankinnalla, telepäätelaitteen tai teleosoitteen yksilöintitietojen hankinnalla, henkilötiedustelun keinoin tai teknisellä laitetarkkailulla. Laitteet ja ohjelmistot ilmoitetaan tuomioistuimelle teknistä laitetarkkailua koskevassa hakemuksessa ja tuomioistuin myöntää tai hylkää luvan kyseisiin tietoihin perustuen.

Tiedustelumenetelmän käytön kohteena olevan käyttämien laitteiden ja ohjelmistojen yksilöintitietojen selvittäminen jäisi edelleen sotilastiedusteluviranomaisen virkamiehen virkavastuulla selvitettäväksi asiaksi. Samalla voitaisiin vahventaa perusteluvelvollisuutta koskien sitä, että tekninen laitetarkkailu kohdistuisi vain toimenpiteen kannalta välttämättömiin laitteisiin ja ohjelmistoihin. Tämä voitaisiin varmistaa edellyttämällä, että tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies tekisi asiasta erillisen päätöksen, jossa tulisi perustella, miksi toimenpiteen kohteeksi on valittu juuri toimenpiteen kohteena olevat laitteet tai ohjelmistot. Päätös olisi laillisuusvalvonnan, kuten tiedusteluvalvontavaltuutetun, piirissä.

Lisäksi olennaiseksi muodostuisi 1. lakiehdotuksen 85 §, jossa säädettäisiin muun muassa teknisen laitetarkkailun keskeyttämisestä, jos se kohdistuu muuhun kuin luvan kohteena olevan henkilön käyttämään laitteeseen tai ohjelmistoon.

2.3.5 Tietoliikenteen teknisten tietojen käsittely

Voimassa olevassa laissa teknisten tietojen käsittely on tarkoitettu erityisesti tietyltä maantieteelliseltä alueelta tai verkkoalueelta lähtöisin olevan tai sinne menevän tietoliikenteen tunnistamiseen. Toimivaltuus on ollut käyttökelpoinen ja tarkoituksenmukainen viestintäverkon osan tunnistamisessa. Toimivaltuuden käytöstä saatujen kokemusten perusteella on havaittu, että sitä pitäisi voida käyttää myös tietoliikennetiedustelun tekniseksi kehittämiseksi. Toimivaltuuden käyttöä ei olisi tarkoituksenmukaista laajentaa niin, että sitä kautta saataisiin varsinaista tiedustelutietoa, kuten tietoja yhdistelemällä tiedustelun kohteita koskevaa yksityiskohtaista tietoa.

Toimivaltuuteen liittyy lisäksi hetkellisyyden vaatimus, jota on tarkennettu oikeuskäytännössä. Ottaen huomioon, että käytännössä toimivaltuuden käytöllä ei saada muuta tietoa kuin tietoliikenteen teknistä tietoa, hetkellisyyden vaatimusta voidaan pitää perusteettomana. Hetkellisyyden toteuttaminen käytännössä, sen tavoitteet huomioon ottaen, vie suhteettoman paljon resursseja, eikä sitä pidetä tarkoituksenmukaisena.

Teknisten tietojen käsittelyssä ei saa syntyä tietoa, josta voidaan tunnistaa yksittäinen luonnollinen henkilö tarkoittaen sitä, että saatuja tietoja ei voida myöskään analysoida tavalla, joka tällaisen tiedon voisi tuottaa. Näin ollen myös puuttumista perusoikeuksiin voidaan pitää vähäisenä.

Voimassa olevan sääntelyn perusteella teknisten tietojen käsittelyssä saatua tietoa ei saa tallentaa sotilastiedustelun myöhempää käyttöä varten. Käytännön toiminnassa on havaittu, että teknisen analyysin taustalla olevista tiedoista olisi hyötyä myös myöhemmässä toimivaltuuksien käytössä, jossa voidaan selvittää saadun tietoliikenteen taustalla olevia tahoja ja muita seikkoja. Teknisten tietojen käsittelyssä saatua tietoa olisikin voitava käyttää myös varsinaisessa tietoliikennetiedustelussa tuotettavissa analyyseissa ja uusien hakuehtojen määrittämisessä.

2.3.6 Tietoliikennetiedustelun hakuehdot

Sotilastiedustelusta annetun lain 70 § koskee muun kuin valtiolliseen toimijan tietoliikenteeseen kohdistuvaa tiedustelua. Pykälän 1 momenttia täydennettiin lakiehdotuksen eduskuntakäsittelyssä niin, että muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvan tietoliikennetiedustelun käyttö edellyttää muun ohella myös sitä, että hankittavat tiedot eivät ole hankittavissa muulla tiedustelumenetelmällä. Koska kyseisen ns. viimesijaisuusedellytyksen soveltaminen jo sellaisenaan ratkaisee kysymyksen tietoliikennetiedustelun ja teletiedustelumenetelmien (ynnä kaikkien muidenkin tiedustelumenetelmien) välisestä suhteesta, voidaan lain 68 §:n 3 momentissa ja 70 §:n 2 momentissa säädetty erillinen ehdoton kielto käyttää hakuehtona Suomessa olevan telepäätelaitteen tai teleosoitteen yksilöivää tietoa katsoa tarpeettomaksi.

Lisäksi on tilanteita, joissa teletiedustelumenetelmien, kuten telekuuntelun, käyttäminen on mahdotonta, mutta telepäätelaitteen tai teleosoitteen yksilöivää tietoa olisi mahdollista käyttää tietoliikennetiedustelun hakuehtona sikäli kuin tämä olisi sallittua. Esimerkiksi sähköpostiosoite on oikeudelliselta luonteeltaan sotilastiedustelusta annetun lain 68 §:n 3 momentissa ja 70 §:n 2 momentissa mainittu teleosoite. Telekuuntelua ei ole mahdollista kohdentaa ja toteuttaa pelkästään sähköpostiosoitetta koskevan tiedon avulla, mutta tietoliikennetiedustelussa sähköpostiosoitetta koskevan tiedon käyttö hakuehtona olisi mahdollista. Tilanteessa, jossa sähköpostiosoitetta käyttävä taho siirtyy Suomen alueelle, on mahdotonta todentaa etukäteen tai siirtymisen aikana. Kielto voi muodostua kriittiseksi, jos kohteen siirtyminen Suomeen on tapahtunut esimerkiksi osana sotilaallisen suunnitelman täytäntöönpanoa. Lain 68 §:n 3 momentin ja 70 §:n 4 momentin nimenomaiset kiellot käyttää Suomessa olevan henkilön hallussa olevaa teleosoitetta hakuehtona estää tämän.

Toisaalta tiedonhankkiminen tällaisessa tilanteessa voi myös johtaa jopa kriittisen tiedon hävittämisvelvollisuuteen tilanteessa, jossa tieto on sinänsä saatu säännösten mukaisesti, mutta koska kohde on siirtynyt Suomen alueelle, tietoa ei olisi saanut alun perinkään hankkia. Kielto saattaa myös johtaa tilanteeseen, jossa kohteena olevat toimijat peittävät toimintansa käyttämällä VPN-palveluita ja näin näyttävät olevan Suomessa.

Lain esitöissä 68 §:n 3 momentissa ja 70 §:n 2 momentissa säädettyjä kieltoja perustellaan tarpeella minimoida vaikutus sivullisten tietoliikenteeseen. Käytännössä perustelu on osoittautunut paikkansa pitämättömäksi, koska käytettäessä telepäätelaitteen tai teleosoitteen yksilöivää tietoa tietoliikennetiedustelun hakuehtona, hakuehdon osuminen täysin sivulliseen liikenteeseen on epätodennäköistä; telepäätelaitteen tai teleosoitteen yksilöivää tietoa voitaneen pitää tarkimpana hakuehtona, jolloin sivullisten tietoliikennettä ei päädy automaattiseen käsittelyyn.

Kielto käyttää sisällöllistä hakuehtoa ei voida pitää tarkoituksen mukaisena hakuehdon määritelmän kannalta. Kuten nykytilan kuvauksessa on todettu, hakuehdon määritelmä säädettiin eduskunnan myötävaikutuksella. Määritelmän mukaisesti hakuehdolla tarkoitetaan tietoa, jonka perusteella tietoliikennetiedustelulla viestintäverkon osasta mahdollisimman rajatusti ja täsmällisesti valitaan tietoliikennetiedustelun kohteena oleva tietoliikenne ja puuttuminen luottamuksellisen viestin salaisuuden suojaan rajautuu tiedustelun tarkoituksen kannalta välttämättömään.

Käytännössä on havaittu, että kielto heikentää merkittävästi tietoliikennetiedustelun tehokasta kohdentamista ja sen voidaan katsoa johtavan lainsäätäjän nimenomaisen tarkoituksen vastaisesti tilanteisiin, joissa tiedusteluviranomaisten haltuun päätyy tarpeettomasti sellaista tiedustelun kohteena olevan uhkan kannalta epäolennaista sivullista viestintää, joka voi nauttia

luottamuksellisen viestin salaisuuden suojaa. Joka tapauksessa sotilastiedusteluviranomaisen velvollisuudesta hävittää viipymättä tietoliikennetiedustelulla hankittuja tietoja säädetään lain 84 ja 86 §:ssä. Hävittämisvelvollisuudella suojataan jatkossakin sivullisten viestintää.

Viestien semanttiseen sisältöön kohdistuvat hakuehdot ovat monessa tapauksessa mahdollista muotoilla sellaisiksi, että ne erottelevat kohdennetummin tietoliikennettä tietoliikennetiedustelun automaattisen ja manuaalisen käsittelyn piiriin kuin nykyisin nimenomaisesti sallitut, esimerkiksi IP-osoitealueita, autonomisten järjestelmien numeroita ja domain-nimiä koskevat hakuehdot. Salauksen yleistymisestä huolimatta viestin sisällön käyttäminen hakuehtona mahdollistaa keräyksen tarkentamisen. Tällöin tiedusteluviranomaisten analyysijärjestelmiin ei edes väliaikaisesti päätyisi niin useasti sellaisia viestejä, jotka eivät ole tiedustelutiedon hankinnan kannalta relevantteja.

Kokemukset ovat osoittaneet, että jo nykyisellään käytettävät hakuehdot ohjaavat tiedusteluviranomaisen analyysijärjestelmään vain hakuehdon mukaista tietoliikennettä. Nykytilassa tarkemmassa analyysissä voidaan käsitellä kuitenkin vain tietoa, jonka teknisissä tiedoissa on hakuehtoa vastaava tieto. Näin ollen, jos hakuehtoa vastaava tieto löytyy esimerkiksi sähköpostissa viestin edelleen lähettäjän tiedoista, tietoa ei voida analysoida tarkemmin; sisällöllisen hakuehdon käyttö mahdollistaisi myös tehokkaammin tiettyjen tahojen välisen viestiliikenteen seuraamisen.

Sotilastiedustelusta annetun lain esitöissä todetusti tietoliikennetiedustelusta säätäneiden eurooppalaisten vertailuvaltioiden lainsäädännöissä ei ole asetettu rajoituksia tai esteitä käyttää sisällöllisiä hakuehtoja, vaan sisällöllisten hakuehtojen käytölle asetetut rajoitukset voidaan katsoa omintakeiseksi suomalaiseksi ratkaisuksi.

2.3.7 Maanpuolustusta ja kansallista turvallisuutta vaarantavaan tietojärjestelmän toimintaan puuttuminen

Tietojärjestelmien ja -verkkojen globaali levinneisyys muodostavat uudenlaisen haasteen sotilaallisten ja kansallisen turvallisuuden uhkien torjumiselle. Kyberuhkatoimijat sekä muut kansallista turvallisuutta uhkaavat toimijat, jotka toiminnassaan hyödyntävät tietoverkkoja ja -järjestelmiä, toimivat pääsääntöisesti ulkomailla, mutta voivat tietoverkkoja pitkin vaikuttaa ja vakoilla Suomen alueella ja Suomen kansalaisten ja organisaatioiden käyttämissä tietojärjestelmissä.

Suomen kannan mukaisesti kansainvälinen oikeus pätee myös kybertoimintaympäristössä. Tämän takia Suomella on myös oikeus puolustaa suvereniteettiaan kyberympäristössä ja oikeus ryhtyä kansainvälisen oikeuden mukaisiin toimenpiteisiin, joilla Suomen suvereniteettiin kohdistuvat vihamieliset toimenpiteet ja muut haitalliset toimet voidaan estää.

Aluevalvontalaki antaa aluevalvontaviranomaisille mahdollisuuden ryhtyä tarvittaviin toimenpiteisiin vihamielisen toiminnan torjumiseksi, jos se välittömästi ja vakavasti vaarantaa valtakunnan turvallisuutta. Aluevalvontalain 34 §:n 2 momentin 1 kohdan mukaan vihamielistä toimintaa on muun muassa vieraan valtion tai tunnuksettoman sotilaallisen ryhmän oikeudettomasti Suomen alueeseen kohdistama tai Suomen alueella toimeenpanema aseellinen sotilaallinen toiminta.

Vaikka sinänsä aluevalvontalain soveltamisala ja toimivaltuudet voisivat soveltua myös kybertoimintaympäristössä, laki ei kuitenkaan toimi käytännössä siellä; voimassa oleva aluevalvontalain voidaan katso olevan säädetty fyysistä toimintaympäristöä, kuten maa- ja merialuetta sekä ilmatilaa koskien. Nämä toimintaympäristöt ovat luonteeltaan merkittävästi

erilaisia kuin kybertoimintaympäristö, joka on käytännössä kokonaan yksityisten tahojen omistuksessa. Näin ollen sääntelyn, jonka perusteella kybertoimintaympäristössä voidaan ryhtyä Suomea vakavasti vaarantavan toiminnan estämiseksi tai keskeyttämiseksi, on oltava erilaista.

Sinänsä aluevalvontalain mukainen vihamielinen toiminta voidaan estää myös Suomen alueen ulkopuolella, jos on selvää, että vaikutukset ilmenevät Suomessa. Esimerkiksi Suomeen suuntautuva ohjus voidaan torjua esimerkiksi kansainvälisellä vesialueella.

Lisäksi lain edellä viitattu 34 §:n 2 momentin 1 kohta viittaa aseelliseen sotilaalliseen toimintaan. Tällä hetkellä yksikään valtio ei ole todennut joutuneensa aseellisen sotilaallinen toiminnan kohteeksi kybertoimintaympäristössä. Lisäksi kansainvälisen oikeuden mukaisesti kybertoimenpiteiden, jotka ylittävät aseellisen voimankäytön kynnyksen, olisi aiheutettava vaikutuksia ihmisten hengelle tai terveydelle taikka fyysisiä vahinkoja. Näin ollen tilanteissa, joissa edellä mainitut edellytykset eivät täyty, ei voida myöskään ryhtyä aluevalvontalaissa tarkoitettuihin toimenpiteisiin.

Poliisilain televalvontaa koskeva säännös ei ota suoranaisesti kantaa siihen, voidaanko sillä estää telepäätelaitteen tai teleosoitetta käyttävän laitteen toiminta, vaan yksityiskohtaistenkin perustelujen perusteella vaikuttaisi siltä, että kyse on enemminkin telepäätelaitteen tai teleosoitteen käyttämiseksi tarvittavien sähkömagneettisten aaltojen estämisestä. Näin ollen vaikuttaisi siltä, että toimivaltuutta ei voisi käyttää esimerkiksi tietystä telepäätelaitteesta lähtöisin olevan valokuidussa liikkuvan tietoliikenteen estämiseen tai tämän telepäätelaitteen sulkemiseen viestintäverkkojen kautta viranomaisen toimesta etenkään tilanteessa, jossa toimija on Suomen rajan ulkopuolella.

Tosin säännöksen sanamuoto ei ota varsinaisesti kantaa siihen, miten telepäätelaitteen tai teleosoitteen käyttö estetään. Estäminen on kuitenkin sidottu tiettyyn alueeseen, mikä viitannee yksityiskohtaisten perustelujen mukaisesti nimenomaisesti sähkömagneettisten aaltojen estämiseen.

Joka tapauksessa poliisin ja rikostorjuntaviranomaisten toimivalta rajoittuu Suomen alueeseen.

Sotilastiedustelusta annetun lain 62 §:n nojalla Puolustusvoimien tiedustelulaitoksella on oikeus ulkomaan tietojärjestelmätiedusteluun. Toimivaltuuden nojalla sotilastiedusteluviranomainen voi hankkia tietoa Suomen rajan ulkopuolella olevasta tietojärjestelmästä tietoteknisin menetelmin. Kansankielisesti tiedustelumenetelmää voidaan kutsua hakkeroinniksi.

Säännös ei kuitenkaan anna mahdollisuutta tietojärjestelmän toiminnan estämiseen tilanteessa, jossa kohteena olevaa tietojärjestelmää käytettäisiin esimerkiksi Suomen elintärkeiden toimintojen toiminnan lamauttamiseen. Sotilastiedusteluviranomainen voisi näin ollen hankkia tietoa tietojärjestelmän toiminnasta, mutta ei voisi estää tietojärjestelmän Suomelle haitallista toimintaa.

Puolustusvoimilla on mahdollisuus puuttua Suomen rajan ulkopuolella olevan tietojärjestelmän toimintaan vasta tilanteessa, jossa sotilaallisen voimankäytön edellytykset täyttyvät. Kansainvälisessä oikeudessa kyberympäristössä tapahtuvan aseellisen voimankäytön on katsottu yleisesti tarkoittavan sitä, että jos kyberhyökkäyksen seuraukset vastaavat perinteisen aseellisen hyökkäyksen vaikutuksia – kuten kuolemia, vakavia loukkaantumisia tai merkittävää fyysistä tuhoa – se voidaan tulkita aseelliseksi voimankäytöksi YK:n peruskirjan 2(4) artiklan tarkoittamalla tavalla. Suvereniteetin kannalta on katsottu, että toimenpiteet, jotka johtavat esimerkiksi laitteiston tai ohjelmiston uudelleen asentamiseen, loukkaavat suvereniteettia.

Tietoverkkojen kautta tapahtuvassa vaikuttamisessa ja kohteena olevien tietojärjestelmien toiminnan estäminen tapahtuu käytännössä aina aseellisen voimankäytön kynnyksen alapuolella, jotta toiminta olisi helpommin kiistettävissä ja toisaalta tietäen se, ettei kohteena oleva valtio voi ryhtyä vahvempiin toimenpiteisiin vaikuttamistoimenpiteen ”vähäisyyden” takia. Käytännössä yksikään valtio ei ole todennut joutuneensa sellaisen kybervaikuttamisen kohteeksi, joka täyttäisi aseellisen voimankäytön kynnyksen.

Edellä todetusti suomalainen viranomainen ei voi puuttua akuuttiin tai perusteltuun potentiaaliseen vakavaan uhkaan Suomen rajan ulkopuolella, vaikka kohde olisi selkeästi tietty uhkan toteuttamisessa käytettävä tietojärjestelmä tai tietyn tietojärjestelmän olisi haivattu olevan tarpeellinen väline uhkan toteuttamisessa. Toimintaan puuttumisessa olisi kyse verkon yli tapahtuvasta, kohdennetusta laitteen tai tietojärjestelmän toimintaan puuttuvasta toimenpiteestä, jolla olisi vain vähän tai ei lainkaan vaikutuksia sivullisiin. Vaikka toiminta vaikuttaa sen kohteena olevan laitteen tai tietojärjestelmän toimintaan, ei siinä voitane katsoa olevan kyse sotilaalliseen tai aseelliseen voimankäyttöön rinnastuvasta vaikutuksiltaan vertautuvasta toiminnasta, vaan sitä vähäisemmästä, oman suojautumisen välttämättä edellyttämästä vastapuolen toimintaan kohdistuvasta vastatoimesta tai laillisen tilan palauttamisesta.

Oman kysymyksensä on niin kutsutut alhaisen intensiteetin kyberhyökkäykset sekä kehittyneet pysyvät kyberuhkatoimijat. Kummassakin tapauksessa toiminta ei ole pistemäistä, joka loppuisi yksittäisen toimen torjumisella. Edellä kuvatut kyberuhkat edellyttävät uudentyyppistä lähestymistä sen suhteen, miten uhkaa torjutaan. Tehokkainta torjunta on toiminnan estäminen ja haittaaminen tavalla, jonka johdosta uhkatoimija ei pysty toteuttamaan toimintaansa.

Kybertoimintaympäristön osalta on huomattava sen nopeatahtisuus. Ensimmäinen merkki tietomurrosta tai vahingonteosta saatetaan saada vasta siinä vaiheessa, kun hyökkäyksen päämäärä on saavutettu. Tässä vaiheessa ei enää voida ryhtyä tehokkaisiin estämistoimenpiteisiin. Jotta kyberhyökkäyksen estäminen tai keskeyttäminen olisi käytännössä mahdollista, toimenpiteet olisi pystyttävä suorittamaan esimerkiksi kyberhyökkäyksen komentopalvelimissa. Komentopalvelimet sijaitsevat käytännössä aina Suomen alueen ulkopuolella.

Kyberuhkiin vastaaminen tehokkaasti edellyttää sitä, että myös muihin kuin tietyllä hetkellä konkreettista uhkaa aiheuttavaan laitteeseen tai järjestelmään pystytään kohdentamaan toimenpiteitä. Haitallisessa toiminnassa käytettävä infrastruktuuri on laaja ja monitasoinen. Tämän takia pelkästään yhteen suoraan Suomeen kohdistuvaa uhkaa aiheuttavaan laitteeseen vaikuttamisella ei pystytä vaikuttamaan hyökkääjän muodostamaan uhkaan kokonaisuudessaan.

Ehkäisevien toimenpiteiden toteuttamisessa tarvitaan sotilastiedustelun arvio siitä, millä tavalla kyseiseen uhkaan on parasta vastata ja mihin kohtaan hyökkääjän toimintaa kohdistaa, jotta toimenpiteet ovat mahdollisimman tehokkaita ja oikeasuhtaisia. Vaikka sotilastiedusteluviranomaisella on ainoana viranomaisena mahdollisuus suorittaa ulkomaan tietojärjestelmätiedustelua, nykyisillä toimivaltuuksilla suomalainen viranomainen ei pysty tehokkaasti estämään Suomen alueen ulkopuolelta tulevaa Suomeen kohdistuvaa kyberuhkaa.

Useat valtiot myös hyödyntävät erilaisia julkisia kanavia omaa agendaa vahvistavien ja kohdevaltion demokratiaa heikentävien valeuutisten ja disinformaation levittämiseen esimerkiksi bottiverkkojen välityksellä tai tekoälyavusteisesti. Toimintaan ei pystytä vastaamaan perinteisin diplomaattisten tai rikostorjunnan keinoin. Mikäli disinformaation levittäminen uhkaa vakavasti kansallista turvallisuutta, siihen ei voida tällä hetkellä vaikuttaa

haittaamalla tai estämällä disinformaation levittämiseen liittyvää toimintaa kohdistamalla siinä käytettäviin järjestelmiin tai muuhun infrastruktuuriin toiminnan estäviä toimenpiteitä.

Nykytilassa ei voida ryhtyä vaikuttamistoimiin esimerkiksi tilanteessa, jossa selkeästi kyberuhkatoimijan kohteena on Suomi ja toiminta saataisiin lopetettua toimijan infrastruktuuria vastaan tehtävällä toimenpiteellä. Infrastruktuuria ja sitä hyödyntäen toteutettavaa kyberhyökkäystä tai sen valmistelua ei voida häiritä tai aktiivisesti estää tilanteessa, jossa esimerkiksi tiedusteluoperaation yhteydessä havaitaan sen muodostavan uhkan maanpuolustukselle tai kansalliselle turvallisuudelle. Etenkin kehittyneet jatkuvat kyberuhkatoimijat käyttävät monikerroksista tietoverkkoinfrastruktuuria, jossa infrastruktuuria ohjataan komentopalvelimien kautta. Uhkaa voidaan torjua tehokkaimmin estämällä komentopalvelimien komentojen pääsy alemmille kerroksille eikä kyberhyökkäys pääse koskaan maaliinsa.

Nykysääntely estää myös toimenpiteet sellaisten tietojärjestelmien toiminnan haittaamiseksi, jota käytetään tukemaan perinteisempiä fyysisen maailman uhkia tai niin kutsuttuja hybridiuhkia. Tällaisia tietojärjestelmiä voivat olla esimerkiksi uhkatoimijan käyttämät viestintäjärjestelmät, logistiikkajärjestelmät tai sosiaalisessa mediassa tapahtuvaan järjestelmälliseen valtiolliseen vaikuttamistoimintaan tarkoitetut tietotekniset ratkaisut. Lisäksi esimerkiksi toiminnanohjausjärjestelmän, jolla ohjataan droonien parvia Suomea kohti, toimintaan ei voida puuttua vaikka olisi tiedossa, että droonit matkaavat Suomea kohti.

Kyberympäristö on luonut uuden mahdollisuuden valtioille toteuttaa tavoitteitaan uusin keinoin. Näitä tavoitteita voivat olla muun muassa oman politiikan ja näkemyksen vahvistaminen sekä toisten valtioiden demokratian heikentäminen vaikuttamalla yhteiskunnan kriittisiin toimintoihin, kuten vaaleihin, kriittiseen infrastruktuuriin tai tiedonvälitykseen. Tätä toimintaa kuvataan usein termeillä hybridivaikuttaminen tai laaja-alainen vaikuttaminen.

Vaikka Suomi voi nykytilassa suojautua vaikuttamisyrityksiltä ja vastata niihin erilaisilla tavoilla, kuten hyödyntämällä diplomatiaa, osana Euroopan unionia asettamalla pakotteita tai suorittamalla rikostutkintaa, kaikissa tapauksissa nämä keinot eivät ole riittäviä eikä niillä saavuteta haluttua lopputulosta. Näissä tapauksissa valtiolla olisi oltava mahdollisuus, työkaluja, vaikuttaa suoraan kyseiseen sitä uhkaavaan toimintaan soveltuvilla keinoilla.

Selkeä toimivalta, päätöksentekojärjestelmä ja kyky vastata Suomeen kohdistuviin muihinkin kuin sotilaallisiin uhkiin normaalioloissa on oleellinen osa kansallista turvallisuutta ja yhteiskunnan elintärkeiden toimintojen turvaamista. Useilla länsimailla on vastaava toimivalta vastata niihin kohdistuviin uhkiin. Kansainvälisellä yhteistyöllä osana liittoumaa (NATO) on erittäin suuri merkitys uhkiin vastaamisessa. Tulevaisuudessa liittokunnan viitekehyksessä voi ilmetä jäsenmaiden kategorisointia sen suhteen, millä jäsenmailla on toimivalta ja kyky vaikuttaa kybertoimintaympäristössä ja millä ei. Tehokkaan kansainvälisen yhteistyön edellytyksenä on selkeä ja toimiva kansallinen lainsäädäntö.

2.3.8 Tietoliikennetiedustelulla hankittujen tietojen hävittäminen

Sotilastiedustelusta annetun lain 86 §:ää voidaan pitää säädösteknisesti epäselvänä sen suhteen tilanteessa, jossa tietoliikennetiedustelujärjestelmään tullut tieto on poistettu 82 §:n 2 momentin tai 84 §:n 1 momentin perusteella, eli tieto on osoittautunut tiedustelukiellon alaiseksi tai tietoa ei ole käytetty tai tarvittu sotilastiedustelutoiminnassa. Lähtökohtaisesti tietoja hävitetään tietoliikennetiedustelujärjestelmästä välittömästi sillä perusteella, että tieto on perusteetonta eikä sitä tarvita sotilastiedustelutoiminnassa.

Nykytilassa sääntelyä ei voida pitää täysin selkeänä, ottaen huomioon lain 82 §:n 2 momentin ja 84 §:n 1 momentin, joissa säädetään nimenomaisesti perusteettomuusperusteella hävitettävästä tiedosta. Lisäksi sanotun lain 86 §:ssä viitataan erikseen edellä tarkoitettuun 82 §:n 2 momenttiin.

Huomioiden säädösteknisen epäselvyyden olisi tarkoituksenmukaista muuttaa 86 §:n hävittämissääntelyä vastaamaan käytäntöä eli maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi tarpeeton tieto poistetaan välittömästi. Tämä vastaisi sitä, mitä tietoliikennetiedustelusta siviilitiedustelussa annetun lain 15 §:ssä säädetään Suojelupoliisin tietojen hävittämisestä.

Hävittämisvelvollisuudella on merkitystä ennen kaikkea ilmoitusvelvollisuuden kannalta. Jos tieto hävitetään välittömästi, tietoliikennetiedustelussa pääsääntöisesti automaattisesti, sotilastiedusteluviranomaisella ei edes ole tietoa, jonka perusteella ilmoitus voitaisiin tehdä tiedustelumenetelmän käytön kohteeksi joutuneelle.

2.3.9 Ilmoitusvelvollisuus

Viranomaisen salassa käyttämistä tiedonhankintamenetelmistä ilmoittaminen liittyy olennaisesti oikeusturvaan. Yksilön oikeusturvan kannalta on tärkeää, että salaisen tiedonhankintakeinon käytöstä on lähtökohtaisesti ilmoitettava menetelmän käytön kohteeksi joutuneelle. Mikäli yksilö ei saa tietoa siitä, että häneen on kohdistettu salaista tiedonhankintaa, ei hänellä ole myöskään mahdollisuuksia varmistua siitä, onko keinojen käyttö ollut lainmukaista. Yksilön mahdollisuus käyttää oikeussuojakeinoja ja saada esimerkiksi korvausta lainvastaisesta toimenpiteestä ei voida tällöin toteutua.

Toisaalta on nähty, että ilmoittamisella on myös väärinkäytöksiä ennaltaehkäisevä merkitys, ja tätä on pidetty jopa ilmoittamisen pääasiallisena merkityksenä. Ilmoittamisella on lisäksi merkitystä yleisesti tiedonhankintakeinojen käytön luotettavuuden kannalta. Yhteisöllä on yleisesti intressi valvoa, että tiedonhankintakeinoja käytetään hyväksyttävissä rajoissa.

Edellä kuvatut ilmoittamisvelvollisuudelle asetetut tavoitteet voidaan kuitenkin saavuttaa useammalla eri tavalla.

Euroopan ihmisoikeustuomioistuimen (EIT) ratkaisukäytännössä ilmoituksen tekeminen tiedonhankintakeinon käytöstä on yhdistetty siihen, että yksilöllä on mahdollisuus haastaa viranomaisten toimenpiteiden laillisuus. Ihmisoikeustuomioistuin ei kuitenkaan edellytä, että ilmoitus on tehtävä kaikissa tilanteissa. Sen mukaan ilmoittaminen jokaiselle toimenpiteen kohteelle saattaisi vaarantaa niitä pitkän tähtäimen tavoitteita, joiden vuoksi tiedonhankintaan alun perin ryhdyttiin. Ilmoittaminen saattaisi myös paljastaa tiedustelupalvelun työskentelymenetelmiä, toiminta-alueita tai agentteja.

Sotilastiedustelusta annetun lain 89 §:n esikuvana on ollut merkittävissä määrin poliisilain 5 luvussa ja pakkokeinolain 10 luvussa säädetystä salaisesta tiedonhankinnasta ilmoittaminen. Kummassakin tapauksessa tiedonhankinta liittyy nimenomaan rikoksien ennalta estämiseen, paljastamiseen ja esitutkintaan, joiden tarkoituksena on rikosvastuun toteuttaminen. Näin ollen kohteena olevalla henkilöllä voidaan katsoa olevan myös korostunut tarve saada tieto häneen kohdistuneista salaisista viranomaistoimenpiteistä jo oikeudenmukaista oikeudenkäyntiä silmällä pitäen. Tiedustelutoiminta ei kohdistu rikolliseen toimintaan eikä tiedustelutoiminnassa pyritä toteuttamaan rikosvastuuta. Tiedustelumenetelmien käyttö voi liittyä rikosvastuun toteuttamiseen poikkeuksellisesti sotilastiedustelusta annetun lain 79–80 §:n niin kutsutuissa

palomuurisäännöstilanteissa. Näissä tapauksissa tiedustelumenetelmien käytöstä ilmoittaminen voi käytännössä tapahtua esitutkintapöytäkirjan asianosaisjulkisuuden kautta.

EIT:n ratkaisukäytäntöä (ennen kaikkea Centrum för Rättvisa ja sitä ennen ratkaisu esimerkiksi Kennedy) ja kansainvälistä vertailua (viimeisimpänä Ruotsi) koskevista kappaleista käy ilmi, että EIS:n 13 artiklan suojaama oikeus tehokkaisiin oikeussuojakeinoihin voidaan toteuttaa monilla eri tavoilla. Ilmoittamista ei ole pidetty merkityksellisenä, jos henkilöillä ja yhteisöillä on oikeus saada asiansa selvitetyksi muilla riittävillä keinoilla eikä keino ole sidottu ilmoituksen tekemiseen. Tiedustelutoiminnan valvonnasta annetussa laissa (121/2019) säädetään jokaiselle, joka epäilee joutuneensa tiedustelumenetelmän käytön kohteeksi, oikeus saattaa asiansa tiedusteluvalvontavaltuutetun tutkittavaksi. Henkilö voi saattaa asiansa tiedusteluvalvontavaltuutetun käsiteltäväksi, vaikka tiedustelumenetelmän käytön osalta tuomioistuin olisi tehnyt päätöksen siitä, ettei tiedustelumenetelmän käytön kohteeksi joutuneelle tehdä ilmoitusta.

Valtuutetulla on laajat tiedonsaantioikeudet, minkä lisäksi valtuutettu valvoo toimintaa etukäteen, reaaliaikaisesti ja jälkikäteisesti. Valtuutetulla on myös laajat oikeudet keskeyttää tiedustelumenetelmän käyttö ja saattaa asioita esitutkintaan. Päätöksen merkittävimmin yksityisyyden suojaan puuttuvista tiedustelumenetelmistä tekee tuomioistuin, jonka käsittelyssä edustettuna on myös tiedusteluvalvontavaltuutettu.

Yksityiskohtaisemmin lain 89 §:n 2 momentti näyttäisi tarkoittavan myös sitä, että ilmoitusvelvollisuus kohdistuu tiedonhankinnan mahdollisen kohdehenkilön ohella hyvin laajasti myös sellaisiin henkilöihin, jotka eivät ole olleet tiedonhankinnan kohteena, vaan jotka syystä tai toisesta kommunikoivat tiedonhankinnan kohteen kanssa tai ovat tiedustelutehtävän näkökulmasta varsinaisia sivullisia.

Etenkin tietoliikennetiedustelun käyttöä koskeva ilmoitusvelvollisuus poikkeaa käytännössä merkittävästi muiden tiedustelumenetelmien käyttöä koskevasta ilmoitusvelvollisuudesta, joka kohdistuu vain siihen henkilöön, joka on tiedustelumenetelmää koskevassa vaatimuksessa ja päätöksessä mainittu kyseisen tiedustelumenetelmän kohdehenkilönä. Voimassa oleva ilmoitusvelvollisuus vertautuu siihen, että suunnitelmallisesta tarkkailusta olisi velvollisuus ilmoittaa myös kaikille niille henkilöille, joita koskien tarkkailua suorittava virkamies on tehnyt näköhavainnon puolen vuoden mittaisen tarkkailun aikana, ja siihen, että tilaan kohdistuvasta teknisestä katselusta olisi velvollisuus ilmoittaa kaikille niille henkilöille, jotka sattumalta ovat lyhytaikaisesti käyneet katselun kohteena olevassa tilassa. Tietoliikennetiedustelun osalta ongelma voi kuitenkin kertautua monikymmenkertaiseksi johtuen tietoliikennetiedustelujärjestelmään tulevan tietoliikenteen määrän takia.

Voimassa olevaa sääntelyä ei voida myöskään pitää soveltamisen kannalta selkeänä. Tietoliikennetiedustelua koskeva ilmoitusvelvollisuuden edellytyksenä on, että 1) henkilö on ollut Suomessa häneen kohdistuneen tietoliikennetiedustelun hetkellä, 2) hänen viestinsä tai tallentamansa tiedon sisältö taikka tunnistamistieto on selvitetty, 3) edellä mainittujen tietojen selvittäminen on tehty manuaalisesti, 4) selvitetyt tiedot ovat luottamuksellisen viestin alassa ja 5) tietoja ei ole hävitetty.

Monipolvinen sääntely johtaa vaikeisiin tulkintatilanteisiin siitä, keille kaikille ilmoitus olisi tehtävä ja ketkä kaikki ovat ilmoitusvelvollisuuden piirissä kulloisellakin hetkellä. Sääntely myös edellyttää tiedusteluviranomaisten seuraavan aktiivisesti tilannetta ja tilanteen kehittymistä muun muassa sellaisten tunnistamistietojen osalta, jotka eivät ole olleet tiedonhankinnan varsinaisina kohteina.

Voimassa olevan tietoliikennetiedustelua koskevan sääntelyn mukaisesti tiedustelumenetelmän kohteena on kohteen tietoliikenne, käytännössä tietyn organisaation tietoliikenne. Näin ollen tiedustelumenetelmän käytön tarkoituksena ei ole saada tietoja tietyn henkilön toiminnasta, vaan organisaation toiminnasta, kuten vieraan valtion asevoimien tai tähän liittyvän yksityisen organisaation toiminnasta. Yksittäisellä henkilöllä ei ole useinkaan käytännön merkitystä.

Tietoliikennetiedustelulla tietoon voi tulla hyvin laajasti eri tahojen tietoliikenneyhteyksiin liittyviä tunnistamistietoja, joita saattaa olla tarpeen säilyttää. Tiedustelutoiminnan tavoitteet eivät välttämättä kuitenkaan edellytä sen selvittämistä, onko kunkin tunnistamistiedon taustalla luonnollinen henkilö vai ei, kuka kyseinen luonnollinen henkilö on, tai nauttiiko viesti, johon tunnistamistieto liittyy, luottamuksellisen viestin salaisuuden suojaa. Voimassa oleva ilmoitusvelvollisuus vaikuttaisi ääritilanteessa johtavan siihen, että tiedusteluviranomainen joutuisi selvittämään käytännössä turhien tietojen osalta muilla keinoin tunnistamistietoa käyttäneen henkilöllisyyden, jolloin henkilön yksityiselämän suojaan puututaan tarpeettomasti henkilön itsensä lisäksi myös tiedustelutoiminnan kannalta. Lähtökohtaisesti tiedusteluviranomaisella ei ole tarvetta selvittää henkilöllisyyttä esimerkiksi tilanteessa, jossa täysin sattumalta henkilön käyttämää tunnistetieto on tullut tietoliikennetiedustelujärjestelmään.

Voimassa olevassa laissa säädettyä ilmoitusvelvollisuutta voidaan pitää myös laajahkona ottaen huomioon kansainvälisessä vertailussa esiin tuotujen verrokkivaltioiden, kuten Norjan ja Ruotsin, ratkaisut sekä se, mitä EIT on todennut ilmoitusvelvollisuudesta ratkaisukäytännössään ottaen huomioon tiedustelutoiminnan valvonnan kokonaisuuden.

Käytännössä ilmoittamisvelvollisuuden osalta keskeiseksi on noussut lain 89 §:n 6 momentti, jonka nojalla tuomioistuimen päätöksellä ilmoitus voidaan jättää tekemättä tai sen tekemistä voidaan lykätä. Ottaen huomioon sotilastiedustelun kohteet, ilmoittamatta jättämispäätöksiä haetaan taajaan, etenkin jos kohteena olevaan toimintaan voi edes vähäisissä määrin liittyä muitakin kuin valtiollisia toimijoita.

Eduskunnan oikeusasiamies on todennut vuotta 2024 koskevassa kertomuksessaan tarkastaneensa Helsingin käräjäoikeuden tiedustelumenetelmien käyttöön liittyviä lupa-asioita. Poliisilain 5 a luvun 35 §:n ja sotilastiedustelusta annetun lain 116 §:n mukaan tiedustelumenetelmää koskeva lupa-asia käsitellään Helsingin käräjäoikeudessa. Tarkastuksella kävi ilmi muun muassa, että lainsäätäjän tarkoitus tiedustelumenetelmän käytöstä ilmoittamisesta ei ehkä toteudu tarkoitetulla tavalla.

Valtiollisille toimijoille ei ole velvollisuutta ilmoittaa lain 89 §:n 8 momentin nojalla. Käytännössä ilmoitusvelvollisuus ei toteudu, eikä sillä ole myöskään näin ollen ollut merkitystä henkilöiden oikeusturvan kannalta. Voidaan katsoa, että ilmoitusvelvollisuus ja sitä kautta oikeusturva ovat toteutuneet tiedusteluvalvontavaltuutetun kautta. Valtuutetun laajan kaiken tiedustelutoiminnan kattavan valvonnan kautta voidaan katsoa oikeusturvan toteutuneen myös laajemmin kuin yksittäisen henkilön kohdalla, sillä valtuutettu voi puuttua ja puuttuu laajasti tiedusteluviranomaisen mahdollisesti lainvastaiseen menettelyyn laajoilla toimivaltuuksillaan. Näin ollen valtuutetun voidaan katsoa toteuttavan henkilön oikeusturvaa myös niiden osalta, jotka eivät tee tutkimispyyntöä.

Oman lisänsä ilmoittamisvelvollisuuden toteuttamiseen tuo se, kenelle ilmoitus olisi tehtävä, etenkin jos henkilöstä saadut tiedot ovat hataria ja henkilön olinpaikasta ei ole tietoa. Kohteena olleen henkilön katoaminen ja olinpaikan hämärtäminen saattavat osaltaan kertoa siitä, että henkilö on ollut asianmukaisesti tiedustelun kohteena. Ilmoitusvelvollisuuden toteuttaminen voi olla haastavaa tilanteissa, joissa henkilö on ilmoittanut yhteystietojaan asianmukaisten

viranomaisten rekistereihin ainoastaan häivyttääkseen todelliset tarkoitusperänsä. Tiedusteluviranomaisen resurssien käyttäminen pelkästään henkilön henkilöllisyyden ja olinpaikan selvittämiseen ei voida pitää tarkoituksen mukaisena resurssien käyttönä.

Kaiken kaikkiaan voidaan todeta, että ilmoituksen tekemistä koskevalla sääntelyllä ei voida katsoa olevan suurta merkitystä henkilön oikeusturvan toteutumisen kannalta ottaen huomioon tiedusteluviranomaisten korostunut tarve toiminnan salassapitoon ja toisaalta tiedusteluviranomaisiin kohdistuva moniportainen valvontajärjestelmä. Lisäksi sääntelyä voidaan pitää monipolvisena ja epäselvänä moninaiset tulkintatilanteet huomioon ottaen. Ilmoituksen tekemättä jättämisen hakeminen tuomioistuimelta aina tiedustelumenetelmää käytettäessä johtaa myös tarpeettomaan hallinnolliseen taakkaan tiedusteluviranomaisen puolelta lisäten myös tuomioistuimen taakkaa.

Tiedusteluvalvontavaltuutetun voidaan katsoa toteuttavan myös ilmoitusvelvollisuuden yhdeksi tavoitteeksi asetetun ennalta estävän vaikutuksen. Jos käytännössä kuka tahansa voi pyytää valtuutettua tutkimaan, onko tutkimispyynnön tekijä joutunut tiedusteluviranomaisen oikeudettoman tiedonhankinnan kohteeksi, laajentaa tämä mahdollisten oikeudellisten jatkotoimenpiteiden esittäjien joukkoa huomattavasti suuremmaksi siitä, mitä se olisi ainoastaan ilmoitusvelvollisuuden nojalla. Tämä ohjaa osaltaan tiedusteluviranomaista toimimaan lainmukaisesti ja kohdentamaan toimintaansa tarkasti.

2.3.10 Sotilastiedustelusta ulkopuolisen osallistuminen sotilastiedusteluun

Muun viranomaisen osallistuminen

Sotilastiedustelusta annetun lain 18 §:ssä säädetään lähinnä viranomaisten välisestä yhteistyöstä ja tietojen vaihdosta. Yhteistyön ei voida katsoa kattavan sitä, että toinen viranomainen voisi osallistua tiedustelun operatiiviseen toimintaan.

Etenkin Rajavartiolaitoksella on toimivaltansa osalta sotilastiedustelun kannalta keskeinen rooli Suomen raja-alueen valvojana. Esimerkiksi lähitulevaisuudesta Suomen ja Venäjän välisen rajan sulku saattaa päättyä jopa nopeasti. Rajan avautuminen saattaa aiheuttaa merkittävän nousun Suomen rajaylitysten määrään, mikä antaa mahdollisuuden myös Suomen turvallisuudelle haittaa haluaville ihmisille helpomman mahdollisuuden päästä rajan yli osana isompaa joukkoa.

Sotilastiedustelun kannalta etenkin yllättävät tilanteet voivat tulla ensin Rajavartiolaitoksen tietoon, mutta Rajavartiolaitoksella ei ole mahdollisuutta suorittaa toimenpiteitä sotilastiedustelun hyväksi. Tilanteissa saatetaan tunnistaa sotilastiedustelun näkökulmasta esimerkiksi, että henkilö mitä ilmeisemmin liittyy sotilastiedustelun kohteena olevaan toimintaan. Tiedon toimittaminen sotilastiedusteluviranomaiselle ei ole yksinään riittävää, koska tunnistettu henkilöä ei tilanteen kiireellisyyden vuoksi ehditä saattaa suunnitelmallisen tarkkailun piiriin sotilastiedusteluviranomaisen toimesta.

Toisaalla lainsäädännössä, kuten sotilaskurinpidosta ja rikostorjunnasta Puolustusvoimissa annetussa laissa (89/2025), on säädetty toisen viranomaisen antamasta avusta Puolustusvoimille. Lain 187 §:ssä säädetään poliisin, Rajavartiolaitoksen ja Tullin antamasta avusta ja yhteistoiminnasta. Pykälässä tarkoitetussa avussa ei ole kyse virka-avusta, vaan siitä, että jos Pääesikunnalla ei ole toimivaltuutta rikostorjunnassa tarkoitetun tehtävän hoitamiseksi tarpeellisen toimenpiteen suorittamiseen, poliisi, Tulli tai Rajavartiolaitos voi pyynnöstä suorittaa sellaisen toimivaltaansa kuuluvan yksittäisen toimenpiteen. Vastaavaa sääntelyä ei ole

sotilastiedustelusta annetussa laissa, minkä takia Rajavartiolaitos ei voi tehdä avustavia toimenpiteitä sotilastiedustelulle.

Sotilastiedustelun tehtävät palautuvat loppujen lopuksi valtiolliseen toimijaan. Rajavartiolaitoksen tehtävän on rajaturvallisuuden ylläpitäminen ja valtion sisäisen turvallisuuden ja yleisen järjestyksen ylläpitämisestä. Rajavartiolaitoksen tehtävien voidaan katsoa olevan yhteen kietoutuneita kansallisen turvallisuuden käsitteen kanssa, mihin liittyvää tiedonhankintaa toteuttavat tiedusteluviranomaiset. Voikin todeta, että tosiasiallisesti sotilastiedustelun tiedonhankinnan kohteet ovat osa myös Rajavartiolaitoksen tiedonhankinnan tehtäväpiiriä kansallisen turvallisuuden viranomaisena. Voidaankin katsoa, että rajaylitykseen liittyvien toimenpiteiden kohdistaminen sotilastiedustelun kohteisiin on usein rajaylitystilanteessa toisiaan vastaavat tai ainakin hyvin lähellä toisiaan. Rajavartiolaitoksen avustamisoikeus edellyttäisi Rajavartiolain muuttamista.

Jos Rajavartiolaitoksen mahdollisuudesta suorittaa yksittäisiä toimenpiteitä sotilastiedusteluviranomaiselle olisi säädetty, edellä kuvatussa esimerkissä henkilö olisi saatu suunnitelmallisen tarkkailun alaiseksi. Rajavartiolaitoksen olisi toki toimittava sotilastiedusteluviranomaisen alaisena toimenpiteitä suorittaessaan.

Viranomaisten ulkopuolisen osallistuminen tiedustelutoimintaan

Sotilastiedustelusta annetun lain 42 §:ssä säädetään laitteen, menetelmän tai ohjelmiston asentamisesta ja poisottamisesta. Pykälässä tarkoitetun toimivaltuuden käyttöön liitoksissa olevan toimenpiteen voi suorittaa sotilastiedusteluviranomaisen palveluksessa oleva virkamies. Näin ollen muu taho ei voi toimenpidettä suorittaa.

Sotilastiedustelusta annetun lain 51 §:ssä säädetään tietolähdetoiminnasta. Tietolähdetoiminnassa olennaista on se, että tietolähteellä on pääsy kohteena olevassa toiminnassa hyödynnettäviin tietoihin. Pykälän 3 momentti sisältää nimenomaisen kiellon siitä, ettei tietolähteen ohjatussa käytössä tietoja voida pyytää hankittavaksi tavalla, joka edellyttäisi viranomaiselle kuuluvien toimivaltuuksien käyttöä tai joka vaarantaisi tietolähteen tai muun henkilön hengen tai terveyden.

Poliisilain 2 luvun 17 §:ssä säädetään tilanteista, joissa poliisi voi pyytää ulkopuolista henkilöä käyttämään voimakeinoja poliisitehtävän suorittamiseksi tietyissä tilanteissa poliisin toimivallassa. Lisäksi lievemmästä ulkopuolisen antamasta avusta säädetään poliisilain 9 luvun 3 §:ssä.

Edellä kuvatusti sotilastiedustelusta annettu laki ei anna mahdollisuutta käyttää sotilastiedusteluviranomaisen ulkopuolista henkilöä esimerkiksi sotilastiedustelusta annetun lain 42 §:ssä säädetyn toimenpiteen suorittamiseen, vaikka tämä voisi olla tiedustelutoiminnan kannalta tehokkainta ja toisaalta vähentää tarvetta käyttää ohjattua tietolähdetoimintaa. Lisäksi tietyissä tilanteissa, jos ulkopuolinen taho voisi suorittaa laitteen, menetelmän tai ohjelmiston asentamisen tai poisottamisen yksittäisenä toimenpiteenä, olisi tästä mahdollisesti aiheutuva hengen ja terveyden vaara pienempi avustavalle henkilölle kuin mitä se olisi, jos henkilöä pitäisi käyttää ohjattuna tietolähteenä.

Sotilastiedusteluviranomaisella on toimivalta itse suorittaa kyseiset toimenpiteet, mutta sotilastiedusteluviranomaiselle voi käytännössä olla mahdotonta päästä suorittamaan toimenpide. Ottaen huomioon poliisilaissa säädetyt mahdollisuudet poliisin käyttää viime

kädessä myös ulkopuolisia henkilöitä voimankäytössä, voidaan sotilastiedustelusta annetun lain 42 §:n toimenpiteitä pitää lievempinä.

Sotilastiedusteluviranomaista voi avustaa vapaaehtoisesti myös viranomaisen ulkopuolinen henkilö. Henkilö voi antaa vaikkapa tilapäisesti autonsa sotilastiedusteluviranomaisen käytettäväksi. Sotilastiedusteluviranomaisen tavanomaisesta avustamisesta ei ole tarkoituksen mukaista säätää erikseen, sillä toiminta perustuu sopimusvapauteen. Toisaalta, koska toiminnasta ei ole tähän mennessä säädetty, avustajalle ei ole voitu maksaa palkkiota verovapaasti, ja tätä kautta avustajan henkeä ja terveyttä ei pystytä suojaamaan parhaalla mahdollisella tavalla.

Tässä esityksessä ehdotetaan erikseen säädettäväksi viranomaisen ulkopuolisen henkilön oikeudesta muun muassa asentaa ohjelmisto sotilastiedustelun kohteena olevaan laitteeseen sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa. Tilanteen voidaan luonteensa vuoksi sinänsä katsoa olevan lähellä tietolähdetoimintaa, joten ehdotetusta uudesta toiminnasta pitäisi pystyä myös maksamaan verottomana palkkio.

Yllä kuvatuille avustajille olisi voitava maksaa palkkio verottomasti vastaavin perustein kuin tietolähteelle. Palkkio olisi käytännössä katsottava vähäiseksi. Tästä myös seuraa se, että sotilastiedusteluviranomainen ei voi kiertää esimerkiksi kilpailutusta koskevia säännöksiä eikä muun yleissääntelyn perusteella voi pyrkiä minimoimaan esimerkiksi maksettuja veroja.

Sotilastiedustelu voi pyytää ulkopuolista suorittamaan tavanomaisia palveluita, kuten taloyhtiön huollosta vastaavaa tahoa avaamaan tietyn tilan oven. Toimenpiteissä avustaneelle voidaan määrätä ilmaisukielto lain 95 §:n mukaisesti. Sääntely ei kuitenkaan annan suoraa mahdollisuutta suorittaa perinteisesti viranomaiselle kuuluvia toimenpiteitä, kuten tietyn tiedustelumenetelmän käytön mahdollistavan laitteen, menetelmän tai ohjelmiston asentamista.

Ulkomainen virkamies

Nykytilassa ulkomainen virkamies voi toimia avustavissa tehtävissä sen mukaan, mitä sotilastiedustelusta annetun lain 20 §:n 3 momentissa on säädetty. Avustavat tehtävät on rajattu tiettyihin tiedustelumenetelmiin, joita ovat 1) tarkkailu ja suunnitelmallinen tarkkailu, 2) peitelty tiedonhankinta, 3) peitetoiminta, 4) valeosto, 5) tietolähdetoiminta, 6) radiosignaalitiedustelu ja 7) teknisten tietojen käsittely. Tiedustelumenetelmät on rajattu niihin, joiden voidaan katsoa puuttuvan vähäisesti perusoikeuksiin eikä yhdelläkään niistä puututa luottamuksellisen viestin salaisuuteen. Yhteistoiminta tapahtuu aina sotilastiedusteluviranomaisen määräysvallassa ja sen vastuulla.

Rajausta ainoastaan tiettyihin tiedustelumenetelmiin ei voida pitää tarkoituksen mukaisena, sillä jopa välttämätöntä tietoa tuottavat toimivaltuudet jäävät sääntelyn ulkopuolelle.

Lisäksi avustaminen aiheuttaa tulkinta epäselvyyttä sen suhteen, miten kiinteästi sotilastiedustelun virkamiehen on oltava itse tiedustelumenetelmän käytön suorittamisessa mukana. Tämä saattaa aiheuttaa toiminnan paljastumisriskin ja viime kädessä hengen ja terveyden vaarantumisen.

Nykytilassa ulkomainen virkamies ei voi osallistua esimerkiksi tietoliikennetiedustelun tiedonhankintaan. Selvää on, että ulkomainen virkamies tai viranomainen ei voi tehdä omia tietoliikennetiedustelun liityntöjä yleiseen viestintäverkkoon, mutta osallistuminen tietoliikenteen tekniseen ja sisällölliseen analysointiin – etenkin tietoliikenteen salauksen

yleistyessä – tuottaisi aiempaa kohdennetumpaa ja parempaa tietoa sotilastiedusteluviranomaiselle.

Vastaavasti eri viestintäsovellusten salaus on kehittynyt, mistä syystä telekuuntelulla ei välttämättä aina saada haluttua tietoa viestin sisällöstä. Näin ollen tiedustelumenetelmät, joissa tietoa hankitaan päätelaitteesta, korostuvat. Näissä tilanteissa ulkomaisella virkamiehellä voi olla osaamista ja välineistöä, joilla tietoa saadaan hankittua.

Muilta osin kansainvälistä yhteistyötä koskeva sääntely voidaan katsoa toimivaksi. Päätöksenteon, vastuun ja toimivallan on oltava edelleen sotilastiedusteluviranomaisella.

2.3.11 Tietolähteen turvaaminen

Ulkomailla toimittaessa tietolähteen turvallisuudesta huolehtiminen voi olla haastavaa. Etenkin tilanteessa, jossa tietolähde on toimittanut merkittäviä tietoja sotilastiedustelulle, tietolähdettä on voitava turvata. Joissain tapauksissa tietolähteen turvaaminen ei ole tämän asemamaassa mahdollista, joten järkevintä olisi saada tietolähde Suomen alueelle tai Suomen alueen kautta kolmanteen maahan.

Sotilastiedustelusta annetun lain 78 §:n 4 momentti antaa sotilastiedusteluviranomaiselle mahdollisuuden antaa muun muassa väärä asiakirja tietolähteelle, jos se on välttämätöntä tämän hengen tai terveyden suojaamiseksi. Kaikissa tilanteissa väärien asiakirjojen antaminen ei ole kuitenkaan käytännössä mahdollista tai esimerkiksi rajan ylittäminen virallisen rajanylityspaikan kautta on muuten erittäin vaarallista. Lisäksi raja saatetaan joutua ylittämään sinänsä virallisen rajanylityspaikan kautta, mutta niin, etteivät rajaviranomaiset tiedä rajan ylittämisestä.

Nykytilassa vaikuttaisi siltä, että sotilastiedusteluviranomaisen avustaessa tietolähteen epätavallisessa rajanylityksessä, syyllistyisi sotilastiedusteluviranomaisen virkamies rikoslain 17 luvun 8 §:ssä tarkoitettuun rikokseen. Esimerkiksi kylmän sodan aikana toteutetussa KGB:n kaksoisagentin Gordievskin pelastamisoperaatiossa keskeinen tietolähde kuljetettiin rajaviranomaisten tietämättä Suomen kautta Norjaan ja edelleen Yhdistyneeseen kuningaskuntaan. Voimassa olevan rikoslain kannalta järjestelyissä avustaneet joutuisivat rikosvastuuseen avustettuaan kaksoisagentin laittomassa maahantulossa.

Edellä kuvatussa esimerkissä, jossa Suomea käytettiin kauttakulkuun, tietolähde olisi myös syyllistynyt rikoslain 17 luvun 7 §:ssä tarkoitettuun valtionrajarikokseen, sillä henkilöllä ei ollut asianmukaista asiakirjaa Suomen rajan ylittäessään. Lisäksi, jos tietolähde ylittäisi Suomen rajan sotilastiedustelusta annetun lain 78 §:n 4 momentissa tarkoitettuja asiakirjoja käyttäen, saattaisi tietolähde syyllistyä asian ilmi tullessa myös valtionrajarikokseen, koska asiakirjat ovat olleet vääriä.

Jotta suomalainen tiedusteluviranomainen voisi luoda luottamukselliset suhteet kaikista merkittävimpiin tietolähteisiin, voidaan arvioida, että tietolähteen turvallisuudesta huolehtimista pitää merkittävänä edellytyksenä suhteen luomiselle ja syventymiselle. Tilannetta, jossa suomalainen viranomainen saisi tietolähteeltä merkittäviä tietoja ja jättäisi tietolähteen oman onnensa varaan tämän hengen ja terveyden vaarannuttua, voidaan pitää epätoivottavana.

2.3.12 Paikkatiedustelu ja jäljentäminen

Sotilastiedustelun kohteina ovat sotilastiedustelusta annetun lain 4 §:n mukaan muun muassa vieraan valtion sotilaallinen toiminta ja ulkomainen tiedustelutoiminta. On ilmeistä, että esimerkiksi Suomessa tapahtuvaan vieraan valtion sotilastiedustelun toimintaan kohdistettavan paikkatiedustelun yhteydessä voi löytyä sellaisia aineita, joita mahdollisesti voidaan käyttää räjähteiden valmistukseen tai esimerkiksi myrkyllisiä kemikaaleja. Löydettyjä aineita ei kuitenkaan yleensä ole mahdollista tunnistaa tai niiden vaarallisuutta arvioida pelkästään visuaalisesti paikkatiedustelun yhteydessä. Lisäksi esimerkiksi ulkomaiseen tiedustelutoimijaan kohdistettavan paikkatiedustelun yhteydessä voi löytyä sellaisia asiakirjoja, joiden osalta on oletettavissa, että niihin sisältyy kemiallisen käsittelyn avulla näkymättömäksi tehtyä kirjoitusta tai muita salaustoimenpiteitä.

Molemmissa edellä mainituissa tapauksissa omaisuus tai erä siitä tulisi voida ottaa haltuun laboratorio-olosuhteissa suoritettavan analysoinnin mahdollistamiseksi ja aineen tunnistamiseksi. Esimerkiksi räjähteen lähtöaineeksi tai toksiiniksi epäillystä aineesta voitaisiin monessa tapauksessa ottaa niin pieni näyte, ettei omaisuuden väheneminen ole silmin havaittavissa. Vaikka aine, esine tai omaisuus olisi tarpeen ottaa haltuun kokonaisuudessaan, olisi se ainakin osassa tapauksista ilmeisesti mahdollista vaihtaa ulkoisesti sitä muistuttavaan, mutta vaarattomaan aineeseen, esineeseen tai omaisuuteen, jolloin uhkan aiheuttava taho ei ainakaan välittömästi havaitsisi haltuunottoa ja paljastumisriski kyetään minimoimaan.

Haltuunotto- ja näytteenottotoimivaltuus on tarpeen esimerkiksi erittäin vakavien hybridivaikuttamisen tai laaja-alaisen vaikuttamisen pyrkimysten estämiseksi ja näihin liittyvien rikosten rangaistavaksi säädettyyn valmisteluun kohdistuvan esitutkinnan mahdollistamiseksi.

Sotilastiedustelusta annetun lain 79–80 §:ssä (ns. palomuuripykälä) säädetään niistä edellytyksistä, joilla sotilastiedusteluviranomaisella on oikeus tai velvollisuus ilmoittaa tiedustelumenetelmän käytön avulla tietoon tulleesta rikoksesta poliisille. Jo tapahtuneen rikoksen ilmoittamiskynnys on palomuurisääntelyssä sidottu ilmaisuun ”voidaan olettaa tehdyksi rikos”, kun taas vielä estettävissä olevan rikoksen ilmoittaminen edellyttää tietoa rikoksen hankkeilla olosta. Pelkästään siitä seikasta, että esimerkiksi paikkatiedustelun yhteydessä löydetään jokin sellainen aine, esine tai omaisuus, jota ei voida tunnistaa, ei voine synnyttää sellaista olettamaa rikoksen tapahtumisesta tai sellaista tietoa rikoksen hankkeilla olosta, että palomuuri-ilmoituksen tekeminen poliisille olisi mahdollista. Koska asiasta ei voida ilmoittaa poliisille, tulisi sotilastiedusteluviranomaisen voida ottaa haltuun aine, omaisuus tai esine sen analysoimiseksi. Sikäli kuin analyysi osoittaisi, että aine, omaisuus tai esine on esimerkiksi rikoksentekoon ilmeisesti käytettävä, tulisi palomuurisääntely sovellettavaksi. Poliisi voisi saamansa palomuuri-ilmoituksen perusteella ryhtyä rikoksen torjumiseksi välttämättömiin toimenpiteisiin ja valmisteluriskosta koskevaan esitutkintaan.

Paikkatiedustelusta päättämisestä säädetään lain 55 §:ssä, jonka sanamuoto ja perustelut ovat ristiriidassa. Koska ajoneuvo on paikka, johon ei ole yleistä pääsyä paikkatiedustelun ajankohtana, päättää siitä säännöksen mukaan tuomioistuin, kun taas säännöksen esityöt (HE 203/2017 vp, s. 266) sinänsä yksiselitteisesti näyttäisivät osoittavat päätösvallan pääesikunnan tiedustelupäällikölle tai tehtävään määrätylle tiedustelumenetelmien käyttöön erityisesti perehtyneelle sotilaslakimiehelle tai muulle virkamiehelle. On selvä, että sovellettavaksi tulee lain sanamuoto.

Ristiriidan taustalla on ilmeisesti se, että paikkatiedustelutoimivaltuuden esikuvana on toiminut pakkokeinolain 10 luvussa säännelty paikanetsinnän toimivaltuus. Paikkatiedustelun

määritelmäsäännöksestä poiketen pakkokeinolain 10 luvun 1 §:n 4 momenttiin sisältyvässä paikanetsinnän määritelmäsäännöksessä paikanetsinnän kohdistuminen kulkuneuvoon mainitaan erikseen. Sen mukaan paikanetsinnällä tarkoitetaan etsintää, joka toimitetaan muussa kuin pykälän 2 tai 3 momentissa tarkoitetussa paikassa, vaikka siihen ei ole yleistä pääsyä tai yleinen pääsy siihen on rajoitettu tai estetty etsinnäin toimittamisajankohtana, taikka jonka kohteena on kulkuneuvo. Pakkokeinolain 15 §:n 1 momentin mukaan paikanetsinnästä päättää pidättämiseen oikeutettu virkamies.

Edellä kuvattu luo epäselvyyden ajoneuvoon kohdistuvan paikkatiedustelun osalta ja siitä päättämisen osalta. Kulkuneuvoon kohdistuvasta paikkatiedustelusta olisi perusteltua säätää omana paikkatiedustelun alalajina ja siitä päättäväksi tahoksi olisi perusteltua vastaavasti kuin pakkokeinolaissa paikanetsintää koskien osoittaa se organisatorisesti vastaavalle tasolle, eli tiedustelumenetelmien käyttöön erityisesti perehtyneelle sotilaslakimiehelle tai muulle virkamiehelle.

2.3.13 Sotilastiedusteluviranomaisen tiedonsaantioikeudet

Sotilastiedusteluviranomainen voi saada Puolustusvoimista annetun lain 17 §:n nojalla viranomaiselta sekä julkista tehtävää hoitamaan asetetulta yhteisöltä laissa säädetyn tehtävän suorittamiseksi. Säännöstä täydentää se, mitä on säädetty henkilötietojen käsittelystä Puolustusvoimissa annetun lain 37 §:ssä.

Poliisin osalta, mukaan lukien suojelupoliisi, on katsottu, että velvoitteidenhoitoselvityksen kannalta keskeistä tietoa koskeviin säännökset ovat erityissääntelyä suhteessa poliisin yleiseen tiedonsaantioikeuteen. Tietojen luovutusta koskeva oikeus koskee nimenomaisesti tietoja, jotka ovat välttämättömiä rikosten selvittämistä ja syytteeseenpanoa varten. Koska erityissääntelyssä poliisia koskien tiedonluovutus on erikseen rajattu, tiedon luovuttaminen ei ole ollut mahdollista suojelupoliisille esimerkiksi kansallisen turvallisuuden suojaamiseksi. Tästä johtuen oikeudesta luovuttaa tietoja suojelupoliisille on jouduttu säätämään erikseen.

Koska Puolustusvoimien oikeudesta saada tietoja ei ole edellä kuvatulla tavalla rajoitettu erityislainsäädännössä, sotilastiedusteluvirnaomaisella on oikeus saada tietoja Puolustusvoimista annetun lain 17 §:n nojalla vastaavassa laajuudessa kuin suojelupoliisilla.

Edellä todettu ei kuitenkaan anna sotilastiedusteluviranomaiselle oikeutta saada harmaan talouden selvitysyksiköstä annetussa laissa tarkoitettua velvoitteidenhoitoselvitystä, josta olisi nimenomaisesti säädettävä lain 6 §:ssä.

2.3.14 Tiedonhankinta yleisesti saatavilla olevista lähteistä

Tarve avoimista lähteistä hankittavalle tiedolle on Puolustusvoimissa laajempi kuin rikostorjunta ja tiedustelutoiminta. Avoimet lähteet tarjoavat jopa merkittävää tietoa esimerkiksi Puolustusvoimien tutkimustoimintaan ja kyberpuolustukseen. Kuten muutenkin Puolustusvoimien toiminnassa, tiedonhankintaan saattaa liittyä tarve virkamiehen ja taustaorganisaation peittämiseen.

Usein avointen lähteiden tieto saattaa olla sinänsä julkista, mutta tiedon hankkiminen saattaa edellyttää sen tekemistä peitellysti. Esimerkiksi tietyissä tapauksissa viranomaiselle esitetty sähköinen tietopyyntö edellyttää jonkin vastausosoitteen ilmoittamista, mikä ei Puolustusvoimien toiminnan ja tiedonsaannin jatkuvuuden näkökulmasta voi aina olla yhdistettävissä Puolustusvoimiin. Näin ollen yleisesti saatavilla olevista lähteistä tehtävässä tiedonhankinnassa olisi voitava käyttää myös kevyitä peitteitä tiedonhankinnan suojaamiseksi.

Palveluiden kehittymisen myötä yhä useammin tietoa jaetaan erilaisten sovellusten ja viestintäsovellusten ryhmissä. Sinänsä ryhmät voivat olla avoimia, joihin hyväksyminen tapahtuu automaattisesti tai sen kummemmin halukasta liittyjää selvittämättä. Ryhmissä saattaa olla tuhansia, satojatuhansia ja jopa miljoonia jäseniä. Näin ollen ryhmää voidaan pitää käytännössä avoimena. Ryhmään liittyminen edellyttää usein käytettävään sovellukseen rekisteröitymistä, mikä myös voi paljastaa tietoja tietoa hankkivan asemasta ja tiedonhankinnan todelliset tarkoitusperät.

Yleisesti saatavilla olevien lähteiden suuri tietomäärä asettaa haasteita sen käsittelylle. Erityisesti yleisessä tietoverkossa on valtava määrä tietoa ja siellä olevalle tiedolle on ominaista sen suuren määrän lisäksi myös nopea tiedon päivittyminen tai poistuminen. Tiedon kerääminen käsin on työlästä, hidasta, ja tärkeää tietoa voi jäädä saamatta, koska tieto poistuu esimerkiksi pikaviestipalvelun ryhmästä ja kanavasta nopeasti.

Yleisesti saatavilla oleviin lähteisiin kohdistuvan tiedonhankinnan valvonta ja tiedon tallentaminen ovat myös jääneet jossain määrin avoimiksi toiminnan ollessa tavanomaisoikeudellista. Etenkin teknologian ja yleisesti saatavilla olevien lähteiden sisältämien tietojen määrän kasvu ovat johtaneet siihen, että suuren tietomäärän ja yleisesti saatavilla olevista lähteistä hankitun tiedon analysointi ristiin kehittyneellä tiedonkäsittelyllä tai tekoälyllä voi paljastaa merkittäviä tietoja henkilöistä ja kohteena olevasta toiminnasta. Lisäksi, koska tiedon hävittämisestä ei ole erityistä sääntelyä, käsittelemätöntä tietoa saattaa kertyä vuosien ja vuosikymmenien aikana merkittäviä määriä, mitä ei voida pitää myöskään viranomaistoiminnan näkökulmasta tarkoituksenmukaisena.

Teknologian kehittymisen myötä myös vihamielinen kybertoiminta ja tietomurrot ovat lisääntyneet merkittävästi. Joissain tapauksissa toiminnassa hankittu tietomassa jaetaan esimerkiksi pimeässä verkossa (kuten Tor-verkossa) yleisesti saataville. Nykytilassa, joka perustuu tavanomaiseen oikeuteen, ei ole täysin selvää, voiko muu kuin toimivaltainen rikostorjuntaviranomainen hankkia rikoksella hankitun tietomassa itselleen. Tietomassat voivat sisältää erittäin tärkeää tietoa esimerkiksi Puolustusvoimien varautumisen, tutkimustoiminnan ja kyberpuolustuksen näkökulmasta. Edellä kuvattujen tietoaineistojen osalta viranomaisen tiedonhankinta saattaa täyttää jonkin rikostunnusmerkistön.

Koska Puolustusvoimat on laaja organisaatio, nykyinen tavanomaiseen oikeuteen perustuvaa tiedonhankintaa voivat tehdä kaikki Puolustusvoimien hallintoyksiköt. Erilaisiin palveluihin kirjautumisen edellytyksenä olevan nimimerkin luomista ja sen käyttöä koskevaa laillisuusperustaa ja sen valvontaa voidaan pitää tällä hetkellä epäselvänä, mistä syystä sääntelylle on tarvetta.

Yleisesti saatavilla olevien lähteiden tiedonhankinta (tiedonhaku ja kerääminen) ei aina edellytä henkilötietojen käsittelyä. Jos kuitenkin käsitellään henkilötietoja, niin viranomaisen on yleisesti saatavilla olevien lähteiden tiedonhankinnassa otettava huomioon myös henkilötietojen käsittelyä koskeva lainsäädäntö. Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Henkilötietoja ovat esimerkiksi nimi, puhelinnumero, sijaintitiedot ja nimimerkki. Henkilötietojen käsittelyn osalta sääntelyä voidaan pitää selkeänä, sillä henkilötietojen käsittelystä Puolustusvoimissa säädetään henkilötietojen käsittelystä Puolustusvoimissa annetussa laissa.

2.3.15 Rekrytointi Puolustusvoimissa

Puolustusvoimien tarpeena on osaamisen hankkimisen näkökulmasta hyödyntää yhtäältä normaalia julkista hakumenettelyä, toisaalta menettely aiheuttaa toiminnallisen ja

työturvallisuusongelman tietyissä tilanteissa. Osaamistarpeiden kannalta henkilöstön rekrytointi on mahdollistettava avoimella menettelyllä, ja toisaalta olisi mahdollistettava ei-julkinen menettely. Puolustusvoimien tiettyjen tehtävien kannalta on ongelma, että virkaa hakeneiden ja nimitetyn nimet ovat julkisia. Puolustusvoimien työtä haittaavien vieraiden valtiollisten toimijoiden toiminta on pitkäjänteistä ja vuosia kestävää, jolloin riskin muodostaa mahdollisuus kerätä nimilistoja ja tarkempien tietojen kerääminen asiakirjoista. Toimintaan osallistuvien henkilöiden hengen ja terveyden suojaaminen ja sen myötä myös esimerkiksi tiedustelumenetelmien ja sen rakenteiden suojaaminen alkaa rekrytoinnin käynnistämisestä.

Puolustusvoimien toimintaa sekä henkilöstöä koskevia nimilistoja voidaan muodostaa, koska haettavaksi julistetun viran ja määräaikaisen virkasuhteen hakijoiden nimet ovat julkisia, virastoilla on velvollisuus ilmoittaa valitun nimi ja lisäksi tiedot annetaan nimityspäätöksestä ja sen perusteluista muutoksenhakua varten. Hakemuksen lähettämistä haettavana olevaan tehtävään ei voi rajoittaa vaan kaikki määräajassa, ja sen jälkeenkin tulleet hakemukset ovat virantäyttöprosessissa käsittelyssä. Tällöin hakijoilla on asianosaisasema ja sen myötä oikeus valittaa viran täyttöä koskevasta päätöksestä. Muutoksenhakuprosessia varten hakijalle on valtiovarainministeriön virantäyttöä koskevan ohjeistuksen mukaan annettava hänen sitä pyytäessään hakijalista, nimitysmuistio ja ansioyhteenvetoa koskeva asiakirja. Edellä mainitut asiakirjat sisältävät pelkkää nimeä laajemmin tietoa.

Tällä hetkellä Puolustusvoimia koskeva lainsäädäntö on epäsymmetriassa poliisiviranomaisia ja siviilitiedusteluviranomaisia koskevan lainsäädännön kanssa. Rekrytointimenettelyjä koskevaa sääntelyä tulisi harmonisoida samankaltaiseksi muita turvallisuusviranomaisia koskevan rekrytointisääntelyn kanssa, koska sääntelyn taustalla vaikuttavia julkisia intressejä voidaan pitää verrannollisina. Puolustusvoimia koskeva sääntely on toiminut tarkoituksenmukaisesti, mutta muuttuneessa turvallisuusympäristössä on havaittu tiedonhankintaa, jota toteutetaan rekrytointiprosessien kautta. Poliisin hallinnosta annetun lain sääntelyllä on pystytty tilkitsemään näitä haasteita, minkä lisäksi julkisen intressin osalta sääntelyä voidaan verrata myös muiden turvallisuusviranomaisten rekrytointisääntelyyn.

3 Tavoitteet

Esityksen tavoitteena on päivittää vuonna 2019 uutena voimaan tullutta lakia sotilastiedustelusta hallitusohjelmakirjausten ja käytännön soveltamistoiminnassa havaittujen tarpeiden mukaisesti. Esityksen tavoitteena on mahdollistaa ja turvata sotilastiedusteluviranomaisen tarkoituksenmukainen ja tehokas toiminta sekä kansallisesti että osana liittokuntaa.

Tavoitteena on ylläpitää ja parantaa kansallista turvallisuutta, kun sotilastiedustelun kohteista saataisiin entistä tarkemmin ja kohdennetummin tietoa, ja kun analysoitua tietoa pystyttäisiin aiempaa paremmin jakamaan sitä tarvitseville. Sotilastiedusteluviranomaisen kykyä kerätä tietoa sotilastiedustelun kohteista parannettaisiin mahdollistamalla eri toimijoille tiettyjen tietojen luovuttaminen sotilastiedusteluviranomaiselle salassapitosäännösten estämättä. Lisäksi esitys parantaa tietoliikennetiedustelun osalta yksityisen viestin salaisuuden suojaa parantamalla samalla kuitenkin sotilastiedustelun tiedonhankintaa.

Tavoitteena on lisäksi mahdollistaa Rajavartiolaitokselle sotilastiedusteluviranomaisen tukeminen tietyissä rajatuissa tilanteissa sekä selkeyttää Maa-, Meri- ja Ilmavoimien roolia sotilastiedustelutoiminnassa.

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen

Sotilastiedustelusta annetun lain 42 §:ään lisättäisiin uusi 2 momentti, jonka mukaan sotilastiedusteluviranomaisen ulkopuolinen henkilö voisi suorittaa pykälän 1 momentissa tarkoitetun toimenpiteen. Nykytilassa toimenpiteet ovat mahdollisia sotilastiedusteluviranomaiselle.

Toimenpiteen suorittajan olisi toimittava viranomaisen ohjeiden mukaisesti tarkasti. Vastaavasti viranomaisen antamat ohjeet eivät saisi jättää toimenpiteen suorittajalle harkintavaltaa toimenpiteen suorittamisen toteuttamisen suhteen. Koska toimenpiteen suorittajalla ei olisi itsenäistä harkintavaltaa toimenpiteen osalta, toimisi hän tältä osin viranomaisen toimivallassa. Näin ollen myös mahdollisesti aiheutuvista vahingoista vastaa sotilastiedusteluviranomainen vahingonkorvauslain (412/1974) 4 luvun säännösten mukaisesti. Mahdollisissa vahingonkorvauksessa olisi kyse vastaavasta tilanteesta kuin jos viranomainen olisi itse tehnyt asennuksen ja tästä aiheutuisi ennakoimattomia vahinkoja asennuksen kohteeseen.

Jos toimenpiteen suorittaja ei noudattaisi hänelle annettuja ohjeita ja toimisi ohjeiden ulkopuolella, vastaisi toimenpiteen suorittaja aiheutuneista vahingoista henkilökohtaisesti. Tältä osin vahingonkorvausvastuun voidaan katso rinnastuvan siihen, että ohjattu tietolähde tekisi omaehtoisesti muita toimenpiteitä viranomaisen hänelle antaman ohjeistuksen ulkopuolelta.

Pykälään ehdotetaan lisättäväksi uusi 3 momentti, jonka mukaan sotilastiedusteluviranomainen voisi suorittaa pykälän 1 momentissa tarkoitetun asennukset tai poisottamisen käyttämällä myös ulkopuolista laitetta tai tietojärjestelmää. Jo nykyisin 42 §:n voidaan katso mahdollistavan tämän, sillä säännös ei ota kantaa esimerkiksi siihen, miten tietojärjestelmän suojaus voidaan kiertää. Uudessa säännöksessä nimenomaisesti todettaisiin tämän olevan mahdollista.

Tässäkin tapauksessa toimenpiteen osalta korostuu riskiarviointi sen suhteen, että toimenpide ei aiheuta vahinko sivulliselle, ja toimenpiteiden tarkka suunnittelu.

Kotimaassa tapahtuva valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu

Sotilastiedustelusta annetun lain 4 luvussa säädettäisiin uudesta tietojärjestelmätiedustelun toimivaltuudesta, jonka avulla voitaisiin hankkia tietoteknisin menetelmin tietoa sotilaallisesta tai kansallista turvallisuutta vakavasti uhkaavaan toimintaan hyödynnettävän tietojärjestelmän toiminnasta, sen sisältämistä tiedoista, tietojärjestelmän osien välillä liikkuvista viesteistä sekä tietojärjestelmään saapuvista tai siitä lähtevistä viesteistä.

Tietojärjestelmällä tarkoitettaisiin tietojenkäsittelylaitteista, tiedonsiirtolaitteista, tietoa käsittelevistä ohjelmista ja tietojen käsittelysäännöistä muodostuvaa kokonaisuutta. Tietojärjestelmä voi muodostua useiden eri laitteiden ja ohjelmistojen tai näiden osien muodostamasta maantieteellisesti ja loogisesti hajautetusta kokonaisuudesta. Tietojärjestelmä voi kattaa osia, jotka kuuluvat samanaikaisesti johonkin toiseen tietojärjestelmään. Tietojärjestelmätiedustelu kohdistuisi toistensa kanssa tietyssä kansallista turvallisuutta uhkaavassa tai sotilaallisessa tarkoituksessa kommunikoivien laitteiden ja virtuaalisten

järjestelmien muodostamaan loogiseen kokonaisuuteen, jolloin lupaa ei edellytettäisi vaadittavan erikseen jokaiseen sellaiseen laitteeseen, joka kuuluu kokonaisuuteen.

Tietojärjestelmätiedustelulla tietoa voisi hankkia joko kokonaisesta tietojärjestelmästä tai jostain tietojärjestelmän sellaisesta loogisesta tai fyysisestä osasta, joka toteuttaa tietojärjestelmän jotakin toiminnallisuutta tai joka muutoin voidaan määrittää tietojärjestelmässä omaksi osakseen perustuen tietojärjestelmän käyttäjään tai tietojärjestelmän osan perustellusti oletettuun tietosisältöön.

Kotimaan tietojärjestelmätiedustelun voidaan kokonaisuutena katsoa kattavan voimassa olevista toimivaltuuksista muun muassa telekuuntelun ja teknisen laitetarkkailun. Tämän takia päätöksentekijänä olisi oltava tuomioistuin. Tuomioistuimen myöntämän luvan tulisi koskea tietojärjestelmää, jolloin yksittäisen teleosoitteen, tiedonkäsittelylaitteen, tiedonsiirtolaitteen tai tietoa käsittelevän ohjelman ja tietojen käsittelysäännön kuulumisesta kohteena olevaan tietojärjestelmään päättäisi erityisesti tiedustelumenetelmien käyttöön perehtynyt sotilaslakimies tai muu virkamies. Päätösten tulisi olla perusteltuja ja niihin tulisi kohdistaa laillisuusvalvontaa.

Kotimaan tietojärjestelmätiedustelua koskevassa vaatimuksessa ja päätöksessä olisi tehtävä muiden seikkojen ohella selkoa toimenpiteen kohteena olevan tietojärjestelmän rajauksesta perustuen kuvaukseen tietojärjestelmän toiminnasta, sen tietojenkäsittelysäännöistä, siihen kuuluvien laitteiden tai ohjelmien tunnisteista, sen käyttämistä teleosoitteista, sen käyttäjien teleosoitteista tai muista käyttäjätiedoista tai jostakin näiden yhdistelmistä siten, että tiedon hankinta voidaan kuvauksen perusteella teknisesti rajata.

Laissa säädetyt kuuntelukiellot ulotettaisiin koskemaan myös kotimaan tietojärjestelmätiedustelua vastaavalla tavalla kuin ne nykytilassa koskevat telekuuntelua ja sen sijasta tapahtuvaa tietojen hankkimista, teknistä kuuntelua ja teknistä laitetarkkailua.

Laissa säädetty 42 § (laitteen, menetelmän tai ohjelmiston asentaminen) ehdotetaan laajennettavaksi kattamaan myös uuden kotimaan tietojärjestelmätiedustelun.

Maanpuolustusta ja kansallista turvallisuutta vaarantavan tietojärjestelmän toimintaan puuttuminen

Sotilastiedustelusta annetun lain 62 §:ään lisättäisiin uusi momentti. Momentin mukaan sotilastiedusteluviranomainen voisi suorittaa Suomen rajan ulkopuolella olevassa tietojärjestelmässä toimenpiteitä, joilla voitaisiin estää tietoteknisin menetelmin Suomen ulkopuolella olevan tietojärjestelmän käyttö taikka haitata tai muokata sen toimintaa, jos tietojärjestelmällä tai sen kautta voidaan aiheuttaa vakavaa vaaraa Suomen maanpuolustukselle tai kansalliselle turvallisuudelle.

Nykyisessä kyberuhkaympäristössä selkeiden aseellisen voimankäytön ja sotilaallisen voimankäytön täyttäviä kyberhyökkäyksiä ei ole tapahtunut tai ainakaan niitä ei ole tunnustettu tapahtuneen. Sen sijaan merkittäviksi kyberuhkiksi ovat nousseet matalan intensiteetin kyberhyökkäykset ja edistyneet pysyvät kyberuhkat. Näiden merkittävyys on siinä, että yksittäisen toimenpiteen torjunta ei riitä uhkatoimijan toiminnan pysäyttämiseen. Toimintaan voidaan puuttua tehokkaimmin toimenpiteillä, joilla estetään tai haitataan uhkatoimijan infrastruktuurin toimintaa uhkan toteutumisen estämiseksi.

Vastaavasti, tällä hetkellä nopeatahtisesti kehittyvässä sotilaallisessa toimintaympäristössä sotilaallinen toiminta on enenevissä määrin riippuvainen tietoliikenneyhteyksistä ja erilaisten laitteiden ja laitteistojen ohjausjärjestelmistä. Tilanteessa, jossa Suomeen kohdistettaisiin esimerkiksi droonihyökkäys, uhkan torjunta on tehokkainta toteuttamalla ohjausjärjestelmässä toimenpiteitä, jotka estävät droonien ohjaamisen Suomen alueelle tai ylipäänsä droonien lähettämisen.

Estävien ja haittaavien toimenpiteiden suorittaminen olisi tarkoituksen mukaista osoittaa sotilastiedusteluviranomaiselle, jolla on jo nykyisin mahdollisuus käyttää ulkomaan tietojärjestelmätiedustelua sotilastiedustelun kohteeseen.

Toimenpiteiden olisi oltava kansainvälisen oikeuden mukaisia, suhteellisia ja tilapäisiä. Toimenpiteiden suorittaminen edellyttäisi ulko- ja turvallisuuspoliittisten näkökantojen huomioon ottamista, jotka huomioitaisiin sotilastiedustelusta annetun lain 15 §:n sekä ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteisen kokouksen kautta.

Sotilastiedusteluviranomainen on ainut viranomainen, jolla on toimivaltuus hankkia tietoa ulkomailla olevasta tietojärjestelmästä. Näin ollen sotilastiedusteluviranomaisella on käsitys siitä, minkä toimijan järjestelmästä on kyse ja milloin järjestelmästä tai sen kautta aiheutetaan vakavaa vaaraa Suomen maanpuolustukselle tai kansalliselle turvallisuudelle. Ulkomaan tietojärjestelmä on suunnitelmallista toimintaa, joka edellyttää pitkäkestoista ja hienovaraista valmistelua. Näin ollen resurssien jaon ja käytettävissä olevan ajan kannalta ei voida pitää järkevänä, että tarkoitetuissa tilanteissa jokin toinen viranomainen ryhtyisi toimenpiteiden suorittamiseksi toteuttamaan vastaavia tietoteknisiä toimenpiteitä.

Tietoliikennetiedustelu

Sotilastiedustelusta annetun lain 4 luvussa säädettäisiin uudesta toimivaltuudesta, hakuehtojen määrittämisestä. Hakuehtojen määrittämisestä tietoliikenteen virrasta kohteena olevan tahoon liittyvien tietoliikenteen säännönmukaisuuksien ja ominaispiirteiden avulla pyrittäisiin löytämään tietoja, joita voidaan käyttää edelleen varsinaisessa tietoliikennetiedustelussa hakuehtona. Laissa säädetty hakuehdon määritelmä ohjaa siihen, että hakuehtojen olisi rajattava tiedon määrä välttämättömään.

Varsinaisista tietoliikennetiedustelun toimivaltuuksista poistettaisiin kielto käyttää viestin sisältöön meneviä hakuehtoja. Käytäntö on osoittanut, että sähköisen viestinnän teknisiksi tiedoiksi katsottavat tiedot eivät pysty kaikissa tilanteissa rajaamaan tietomassaa tarkoitetulla tavalla, vaan järjestelmään tullutta tietoa olisi voitu rajata esimerkiksi tiettyä erityistä sisällössä olevaa sanaa käyttämällä. Toisaalta tietoliikenteen tekninen tieto, kuten puhelinnumero, voi olla myös viestin sisällössä.

Tietoliikennetiedustelusta poistettaisiin myös kielto käyttää Suomessa olevaa tai oletettavasti olevaa telepäätelaitetta tai -osoitetta hakuehtona. Tiedustelun kohteena oleva toimija saattaa saapua tietoliikennetiedustelun käytössä olon aikana Suomeen, ja tahoa olisi välttämätöntä pystyä seuraamaan, kunne kohdennetumpia tiedustelumenetelmiä päästää käyttämään.

Tietoliikennetiedustelun ilmoittamisesta luopuminen

Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta ilmoittamisesta luovuttaisiin. Kohteeksi itsensä epäilevä voi edelleen pyytää tiedusteluvalvontavaltuutettua

tarkastamaan, onko henkilö joutunut tiedustelumenetelmän kohteeksi ja onko asiassa menetelty lainmukaisesti.

Tiedonhankinta yleisesti saatavilla olevista lähteistä

Puolustusvoimista annettuun lakiin lisättäisiin säännökset tiedonhankinnasta yleisesti saatavilla olevista lähteistä. Tietoa voitaisiin hankkia automaattisesti ja manuaalisesti. Liityntä Puolustusvoimiin voitaisiin peittää käyttämällä vääriä, harhauttavia tai peiteltyjä tietoja. Päätös toiminnasta tehtäisiin tiedonhankintaa suorittavassa Puolustusvoimien hallintoyksikössä sisäisen määräyksen mukaisesti.

Pääesikunta tekisi päätöksen niistä hallintayksiköistä, jotka voisivat käyttää edellä tarkoitettua peitettä ja hallintoyksikön päällikkö päättäisi peitteen käyttämisestä.

Sotilastiedusteluviranomaiset ja tehtävien tukeminen

Rajavartiolaitokselle ehdotetaan säädettäväksi toimivalta avustaa sotilastiedusteluviranomaisia tiettyjen sotilastiedustelun tiedustelumenetelmien käytössä. Sotilastiedusteluviranomaisen määritelmää ehdotetaan laajennettavaksi siten, että sotilastiedusteluviranomaisia olisivat tietyiltä osin myös Maa-, Meri- ja Ilmavoimat, jotka voisivat käyttää tiedustelumenetelmistä radiosignaalitiedustelua ja tavanomaista tietolähdetoimintaa. Lisäksi sotilastiedusteluviranomaisen ulkopuoliselle mahdollistettaisiin rajatuissa tilanteissa sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa toimiminen.

Lisäksi ehdotetaan säädettäväksi sotilastiedusteluviranomaisen palveluksesta eronneen virkamiehen avustavasta roolista tiedustelumenetelmien käytössä ja riittävän koulutuksen saaneiden osallistumisesta tiettyjen rajattujen tiedustelumenetelmien käyttöön asevelvollisuuslain mukaisessa palveluksessa tai vapaaehtoisesta maanpuolustuksesta annetun lain mukaisissa harjoituksissa tai niiden erityistehtävissä.

Muuta

Henkilöön kohdistuvan teknisen laitetarkkailussa voidaan katsoa olevan kyse uudentyyppisestä sääntelyratkaisusta, eikä vastaavaa ole poliisilaissa tai pakkokeinolaissa. Toisaalta vastaava henkilöperusteinen kohdentaminen on mahdollista jo telekuuntelun ja televalvonnan osalta.

Sotilastiedustelusta annettuun lakiin ehdotetaan tehtäväksi yksittäisiä säädöshuoltoon liittyviä muutoksia sekä käytännön tiedustelutoiminnassa havaituista tarkennustarpeista, ja toisaalta muusta lainsäädännöstä johtuvia muutoksia.

Sotilastiedusteluviranomaisen ja eräiden muiden viranomaisten tietojenvaihtoa esitetään laajennettavaksi velvoitteidenhoitoselvitysten laatimiseksi ja tilanteissa, joissa tietojen saaminen olisi välttämätöntä tiedustelutehtävän suorittamiseksi. Tietojenvaihtosääntelyä päivitettäisiin vastaamaan voimassa olevaa sääntelyä suojelupoliisin osalta.

Esityksessä ehdotetaan myös tehtävän lakiin tekniseksi katsottavia muutoksia, jotka liittyvät sotilastiedustelun toimintaan.

Esityksessä ehdotetaan myös Puolustusvoimista annetun lain muutoksia Puolustusvoimien rekrytointien julkisuuteen.

4.2 Pääasialliset vaikutukset

4.2.1 Taloudelliset vaikutukset

Vaikutukset julkiseen talouteen

Esitetyillä muutoksilla ei arvioida olevan merkittäviä taloudellisia vaikutuksia. Esitettyjen muutosten voidaan arvioida tehostavan sotilasviranomaisten resurssien käyttöä, kun esimerkiksi tietoliikennetiedustelun hakuehtoja kyettäisiin määrittämään ja tietoliikenteen reitittymisen muutoksia seuraamaan entistä tarkemmin ja siten kohdistamaan tietoliikennetiedustelua tarkoituksenmukaisemmin.

Ehdotetut muutokset asevelvollisuuslain nojalla palvelevien sekä vapaaehtoisesta maanpuolustuksesta annetun lain mukaisessa harjoituksessa olevien toimivaltuuksiin voivat kasvattaa henkilöstökustannuksia ja toisaalta myös turvallisuusselvityksistä aiheutuvia kustannuksia, mutta kustannukset ovat viime kädessä riippuvaisia siitä, missä laajuudessa harjoituksia järjestetään ja missä laajuudessa sotilastiedusteluviranomaisen palveluksesta eronneita virkamiehiä palkataan.

Sotilastiedusteluviranomaiselle säädettäväksi esitetty uusi toimivaltuus tietojärjestelmän käytön estämiseksi tai sen toiminnan haittaamiseksi edellyttää 20 henkilötyövuoden, eli noin 2 miljoonan euron kohdentamista sotilastiedusteluviranomaiseen.

Esitetyt uudet toimivaltuudet sekä toimivaltuuksien kohdentamista ja niitä koskevia lupa-aikoja koskevat muutokset vähentäisivät sotilastiedusteluviranomaisen tuomioistuin käsittelyyn kuluvaa työmäärää. Tämä johtuisi siitä, että kotimaan tietojärjestelmätiedustelu vähentää tarvetta tehdä tuomioistuimelle vaatimus telekuuntelusta, teknisestä laitetarkkailusta ja televalvonnasta. Lisäksi henkilöön kohdistuva tekninen laitetarkkailu vähentää vaatimusten määrää, koska jokaisesta tietyn henkilön käyttämästä laitteesta tai luvasta ei tarvitsisi esittää vaatimusta tuomioistuimelle. Teknisten tietojen käsittelyä koskevien vaatimusten määrä laskisi lupa-ajan noustessa kuuteen kuukauteen.

Vastaavasti tuomioistuimen työmäärä, joka koskee edellä mainittuja tiedustelumenetelmiä, laskisi. Sotilastiedusteluviranomaisen mahdollisuus tehdä päätös telekuuntelun käytöstä kiiremenettelyssä laskisi lievästi tuomioistuimen työmäärää, koska päätöstä ei tarvitsisi tehdä tuomioistuimen päivystyksessä.

Henkilöstöä koskevat vaikutukset pystytään kattamaan Puolustusvoimien määrärahoista.

Ehdotetut muutokset antaisivat sotilastiedusteluviranomaiselle oikeuden käyttää uusia tietoliikenteeseen kohdistuvia tiedustelumenetelmiä sekä tallentaa tietoliikennettä. Tämä edellyttää järjestelmäinvestointeja. Investoinnit pystytään kattamaan Puolustusvoimien määrärahoista.

Esitys aiheuttaa tarvetta kouluttaa sotilastiedusteluviranomaisen ja Rajavartiolaitoksen virkamiehiä. Jo nykyisellään kouluttaminen on Puolustusvoimissa osa normaalia toimintaa, eikä esityksestä aiheudu tämän takia mainittavia taloudellisia vaikutuksia.

Rajavartiolaitoksen mahdollisuus avustaa sotilastiedusteluviranomaista osaltaan laskee sotilastiedusteluviranomaisen tiedustelutehtävän aiheuttamia kustannuksia, koska sotilastiedusteluviranomaisen ei tarvitsisi kiireellisesti järjestää rajanylityspaikalle virkamiehiään.

Puolustushaarojen mahdollisuus käyttää tiettyjä tiedustelumenetelmiä edellyttää koulutusta, mutta tällä ei arvioida olevan taloudellisia vaikutuksia.

Esityksen ei arvioida aiheuttavan Rajavartiolaitokselle merkittäviä kustannuksia. Rajavartiolaitoksen suorittama sotilastiedusteluviranomaisen avustaminen tapahtuu osana Rajavartiolaitoksen normaaleja virkatoimia. Näin ollen toimenpiteet voidaan suorittaa olemassa olevilla resursseilla.

Tietojen vaihdon osalta ehdotuksella ei arvioida olevan myöskään taloudellisia vaikutuksia viranomaisille. Tietojenvaihto tapahtuisi nykyisten rakenteiden puitteissa, eikä siten edellyttäisi lisäresursointia.

Esityksessä ehdotettujen lakiehdotusten myötä tiedusteluvalvontavaltuutetun tehtävät saattavat lisääntyä. Uudentyyppiset toimivaltuudet ja ilmoitusvelvollisuudesta luopuminen edellyttänevät ainakin toiminnan käynnistyessä intensiivisempää valvontaa. Tätä on kuitenkin vaikea arvioida pidemmällä tähtäimellä, kun toiminta on vakiintunut. Eduskunta on joka tapauksessa sitoutunut antamaan tiedusteluvalvontavaltuutetulle lisää resursseja, jos se nähdään tarpeelliseksi tiedustelutoiminnan riittävän valvonnan kannalta.

Vaikutukset yrityksille

Yrityksille aiheutuu hallinnollisia kustannuksia viranomaisen avustamisesta. Viestinnän välittäjille aiheutuvien kustannusten ei arvioida nousevan siitä, mitä ne ovat jo nykyisellään. Aiheutuviin kustannuksiin vaikuttaa tiettyjen tiedustelumenetelmien käyttöön tarvittavien lupien määrä.

Datakeskuspalvelun tarjoajille aiheutuisi uusia kustannuksia. Kustannukset liittyvät etenkin kotimaassa suoritettavan tietojärjestelmätiedustelun edellyttämien kytkentöjen tekemiseen. Kustannusten määrä on riippuvainen siitä, miten usein tiedustelumenetelmiä käytetään. Lisäksi tietojen saanti yksityiseltä yhteisöltä aiheuttaa datakeskuspalvelun tarjoajalle hallinnollisia kustannuksia pyyntöihin vastaamisesta.

Datakeskuspalvelun tarjoajalla olisi oikeus saada valtion varoista korvaus välittömistä investointi- ja ylläpitokuluista, jotka johtuvat viranomaisten vaatimista laitteistoista ja järjestelmistä.

4.2.2 Vaikutukset yrityksiin

Esityksestä aiheutuisi yrityksille vähäisiksi arvioitavia hallinnollisia kustannuksia. Yrityksille aiheutuvat viranomaispalvelukustannukset kasvaisivat vähäisesti elinkeinoelämän eri toimialoille kohdistuvien viranomaiskyselyiden, tiedustelujen tai muiden velvoitteiden kautta.

Kyberturvallisuuslaki asettaa yrityksille muun muassa ilmoitusvelvollisuuden merkittävästä poikkeamasta valvovalle viranomaiselle. Lakiehdotus antaa sotilastiedusteluviranomaiselle mahdollisuuden asentaa muun muassa ohjelmiston kohteena olevaan laitteeseen, käyttää

yksityisen laitetta ohjelmiston asentamiseen sekä tehdä tietoliikennetiedustelun edellyttämä liityntä Suomen rajan ylittävään viestintäverkon osaan sitä hallitsevan tietämättä.

Mikäli yritys pystyy selvittämään, että laitteessa on sotilastiedusteluviranomaisen asentama vieras ohjelmisto tai viestintäverkossa vieras laite, on kyse tietoturvapoikkeamasta. Jos poikkeama on merkittävä, on toimijalla velvollisuus ilmoittaa tästä valvovalle viranomaiselle.

Pääsääntöisesti voidaan arvioida, että merkittävän poikkeaman kynnyksen ylittymistä voidaan pitää erittäin poikkeuksellisena. Tämä perustuu siihen, että sotilastiedustelutoiminta on jo lähtökohtaisesti vaivihkaista toimintaa, jonka ei ole tarkoitus paljastua. Joka tapauksessa tästä voidaan arvioida syntyvän pienehköjä kustannuksia, jos yritys havaitsee poikkeaman. Kustannukset koostuvat ilmoituksen tai raportin tekemiseen kuluvasta työajasta yksittäisen merkittävän poikkeaman havaitsemisesta. Muilta osin käynnistyy yrityksessä normaali poikkeaman hallintaprosessi. Toimenpiteet voivat aiheuttaa kustannuksia yritykselle. Mahdolliset vahingot korvataan siten kuin vahingonkorvauslaissa säädetään.

Ehdotettuja toimenpiteitä ei ole käytännössä koskaan tarkoituksenmukaista toteuttaa esimerkiksi teleyrityksen kriittistä tuotantoinfrastruktuuria hyväksi käyttäen. Ehdotetuissa toimenpiteissä käytetään käytännössä tiettyä yksittäistä laitetta, kuten reititintä, tai tiettyä yksittäistä tietojärjestelmän osaa. Lisäksi toimenpiteiden suunnittelussa on tarkkaan harkittava, etteivät ne aiheuta vähäistä suurempaa haittaa. Haitan on siis käytännössä näyttävä yksittäiselle käyttäjälle esimerkiksi tietoliikenneyhteyden hetkellisenä hidastumisena, ei koko teleyrityksen asiakaskunnalle näkyvänä tietoliikenneyhteyden hidastumisena.

Sotilastiedusteluviranomaisen ulkopuolisen laitteen käyttäminen esimerkiksi ohjelmiston asentamisessa tai poisottamisessa voi aiheuttaa käytettävän laitteen valmistaneelle yritykselle vaikutuksia sen aineettoman omaisuuden, sopimusvaikutusten ja sen toimintaan kohdistuvan luottamuksen kannalta. Vaikutukset tältä osin voidaan arvioida vähäisiksi, sillä toimenpiteiden tarkoituksena ei ole laajamittaisesti esimerkiksi asentaa yleisesti tietyn yrityksen valmistamiin tietoliikennelaitteisiin jo niiden valmistuksen vaiheessa esimerkiksi takaportteja. Yksittäisen laitteen käyttäminen ehdotettuun tarkoitukseen ei käytännössä voine aiheuttaa edellä kuvattuja vahinkoja.

Sotilastiedusteluviranomaisen toiminnasta aiheutuvaa haittaa yritykselle voidaan katsoa jossain määrin pienentävän se, että järjestelmässä tai laitteessa jo valmiiksi olevasta havaitusta haavoittuvuudesta ilmoitetaan sotilastiedusteluviranomaisen toimesta toimivaltaisille viranomaisille.

Kyberturvallisuuslain 10 § asettaa myös vastuun toimijan johdolle. Johdolla tarkoitetaan toimijan hallitusta, hallintoneuvostoa ja toimitusjohtajaa sekä muussa niihin rinnastettavassa asemassa olevaa, joka tosiasiallisesti johtaa sen toimintaa. Johdon vastuun konkretisoituminen sotilastiedustelusta johtuvista syistä voidaan arvioida käytännössä teoreettiseksi, jos toimija toimii kyberturvallisuuslain mukaisesti. Sotilastiedustelun toimenpiteet voivat osaltaan tuoda esiin sen, ettei toimija ole huolehtinut lakisääteisistä velvollisuuksistaan.

Esityksessä ehdotetaan muutettavaksi lakia niin, että sotilastiedusteluviranomainen voi toteuttaa tietoliikennetiedustelun edellyttämän liityntäpisteen viestintäverkon osaan salassa viestintäverkon osan haltijalta. Käytännössä säännös koskee muita kuin Suomen kriittisestä viestintäverkosta vastaavia tahoja, kuten keskeisiä teleyrityksiä. Sotilastiedustelusta annetun lain keskeiset periaatteet ja sotilastiedusteluviranomaisen vahingonkorvausvastuu ohjaavat siihen, että toimenpiteitä suoritetaan mahdollisimman vaivihkaisesti; toiminta pyritään aina pitämään salassa. Tästä johtuen esimerkiksi yhteiskunnan kannalta kriittiseen infrastruktuuriin

tehtävät toimenpiteet sisältävät käytännössä aina liian suuren riskin paljastumisesta tai vahinkojen aiheutumisesta, joten niiltä osin liityntäpistettä ei tultaisi toteuttamaan ilman viestintäverkon osan haltijan myötävaikutusta.

Esityksessä ehdotetaan lakia muutettavaksi niin, että viestinnän välittäjän lisäksi myös datakeskuspalvelun tarjoajalle tulisi velvollisuuksia avustaa sotilastiedusteluviranomaista. Vastaavasti laissa säädetty korvausvelvollisuus esitetään laajennettavaksi kattamaan myös datakeskuspalvelun tarjoajat vastaavasti kuin viestinnän välittäjät. Korvaus ei ole yhtä kattava kuin mitä sotilastiedustelusta annetussa laissa säädetään tiedonsiirtäjälle maksettavasta korvauksesta. Koska televerkkoon kohdistuvia tiedustelumenetelmiä koskevaa järjestelmää käyttävät myös muut viranomaiset (kuten poliisi ja Rajavartiolaitos), korvauksen kattavuutta ei voida tässä esityksessä käsitellä tarkemmin. Verrattuna esimerkiksi rikostorjunnassa käytettävään tiedonhankintaan, tiedusteluviranomaisten televerkkoihin kohdistuva tiedonhankinta on vähäisempää. Joka tapauksessa asiakokonaisuutta olisi selvitettävä omassa hankkeessaan, kuten eduskunnan liikenne- ja viestintävaliokunta on todennut (LiVL 1/2022 vp.). Edellä tarkoitettu aiheuttaa välillisiä vähäisiä kustannuksia datakeskuspalvelun tarjoajille.

Ehdotetut lakiehdotukset laajentaisivat sotilastiedusteluviranomaisen tietojen saantioikeutta yksityisiltä yhteisöiltä. Muutoksen myötä säännöksessä ehdotetut velvollisuudet koskisivat viestinnän välittäjien lisäksi myös datakeskuspalvelujen tarjoajia. Laajennusta ei voida pitää merkittävänä. Muutoksella ei olisi vaikutuksia muun muassa palveluissa käytettyihin päästä-päähän salauksiin eikä yrityksille aseteta velvoitetta tällaisten tai muidenkaan salausten purkamiseen taikka takaporttien asentamiseen.

Esityksessä ehdotetaan sotilastiedusteluviranomaiselle oikeutta suorittaa tietoteknisiä toimenpiteitä ulkomaan tietojärjestelmässä, jos tietojärjestelmällä tai sen kautta voidaan aiheuttaa Suomen maanpuolustukselle tai kansalliselle turvallisuudelle vakavaa uhkaa. Tietoteknisillä toimenpiteillä voidaan suoraan ehkäistä etenkin kriittisestä infrastruktuurista huolehtiville tahoille aiheutuvia vahinkoja. Mahdollisuus suorittaa toimenpiteitä ja toisaalta onnistuneiden toimenpiteiden voidaan katsoa nostavan kynnystä kohdistaa Suomeen yhteiskunnan toiminnan kannalta vakavimpia kyberuhkia. Kyberuhkaan vaikuttamisen voidaan arvioida pitkällä tähtäimellä vähentävän kyberuhkaan varautumisen kustannuksia ja aiheutuneiden vahinkojen vähenemisen kautta.

Toisaalta ehdotus voi eskaloituessaan aiheuttaa etenkin teleyrityksille kohonneen mahdollisuuden joutua kyberhyökkäyksen kohteeksi. Toimenpiteiden aiheuttamaa riskiä olisi arvioitava tarkasti ennen toimenpiteisiin ryhtymistä, mutta myös toimenpiteiden suorittamisen aikana. Sotilastiedusteluviranomaisen olisi huolehdittava osaltaan käytössään olevin kohtuullisin keinoin siitä, että etenkin Suomen kriittisestä infrastruktuurista vastuussa olevilla tahoilla on riittävä tieto mahdollisiin seurauksiin varautumiseksi. Toimenpiteiden luonne huomioon ottaen riski arvioidaan vähäiseksi ja poikkeukselliseksi.

4.2.3 Vaikutukset kansantalouteen ja elinkeinoelämään

Tiedustelulainsäädännön vaikutuksia yrityksiin, kansantalouteen ja elinkeinoelämään on arvioitava kokonaisuutena. Arvioitaessa lainsäädännön seurauksia tulee ottaa huomioon erityisesti vaikutukset yhteiskunnan digitalisoitumiskehitykseen ja yritysten toimintaedellytyksiin, sillä talouskasvun kannalta Suomen on välttämätöntä hyödyntää tehokkaasti tieto- ja viestintäteknologian tarjoamat mahdollisuudet toimintatapojen muuttamiseen ja tuottavuuden parantamiseen.

Sotilastiedustelulainsäädännön tarkoituksena olisi suojata Suomea, sen kansallista turvallisuutta ja siihen kuuluvaa kansantaloutta. Sotilastiedustelulainsäädännön keskeisenä tavoitteena on hankkia tietoa Suomen kansallisen turvallisuuden kannalta keskeisiin etuihin ja myös kansantalouteen kohdistuvista uhista ja torjua niitä. Näin ollen tiedustelulainsäädännön kehittämisen voidaan arvioida nostavan ulkovaltojen kynnystä kohdistaa maahamme vakoilua taikka tietoverkkojen kautta tai muuten suoritettavaa muuta haitallista toimintaa. Tiedustelukyvyn kasvattaminen ei kuitenkaan vähennä yhteisöiden tai yksilöiden omien suojautumistoimenpiteiden tarvetta ja merkittävyyttä, vaan ne pysyvät edelleen keskeisimpinä keinoina erilaisilta uhilta suojautumisessa. Toimiva sääntely ja uudet suorituskyvyt kuitenkin täydentäisivät Suomen digitaalisen ympäristön turvallisuutta ja edistävät elinkeinoelämän suojautumismahdollisuuksia ulkovaltojen aiheuttamia uhkia vastaan. Tässä suhteessa merkityksellistä olisi esimerkiksi se, että tiedustelumenetelmien käyttämisellä saatua tietoa voidaan edelleen luovuttaa yrityksille vakavien uhkien torjumiseksi tai tärkeiden taloudellisten etujen puolustamiseksi.

Kansantalouden ja sen osana toimivien yritysten toimintaedellytysten kannalta on tärkeää, että sotilastiedustelutoimintaa koskeva säädösperusta on selkeä. Riittävän täsmällinen ja tasapainoinen lainsäädäntö luo yritysten toiminnan suunnittelun ja investointipäätösten kannalta ennakoitavuutta. Tiedustelua koskevan sääntelyn ja tietosuojan merkityksen korostuessa digitaalisilla markkinoilla täsmällisen, tasapuolisen ja oikeasuhtaisen sääntelyn voidaan arvioida parhaimmillaan olevan Suomelle kansainvälisillä markkinoilla myönteinen kilpailutekijä.

Yhteiskuntaan kohdistuvien uhkien tunnistaminen, kriittisen infrastruktuurin ja yhteiskunnan taloudellisen elinkelpoisuuden säilyttäminen edellyttävät yhteistyötä julkisen ja yksityisen sektorin välillä. Tämä tarkoittaa tiedusteluviranomaisten sujuvaa tiedonvaihtoa yksityisen sektorin kanssa. Lakiehdotuksella pyritään luomaan riittävä oikeusperusta sille, että sotilastiedusteluviranomaiset voisivat luovuttaa tietoa yrityksille näiden merkittävien etujen suojaamiseksi. Tiedustelun tuottamaa tietoa voitaisiin tarvittaessa luovuttaa yksityisille yhteisöille vakavien uhkien torjunnan mahdollistamiseksi tai merkittävien taloudellisten tappioiden estämiseksi. Asiaa koskevaa sääntelyä sisältyisi käsiteltävänä olevaan ehdotukseen.

Tehokkaasti ja luotettavasti toimiva tiedustelujärjestelmä edellyttää viranomaisilta investointeja tiedustelussa käytettävään teknologiaan ja osaamiseen. Esitetyt tiedonhankintatoimivaltuudet edellyttävät teknologiainvestointeja ja panostamista turvalliseen tuotekehitykseen. Toiminnan luonteen vuoksi investoinneissa on huomioitava erityisesti hankittavan teknologian turvallisuus sekä järjestelmien toiminnan kannalta olennaiset huoltovarmuuskysymykset. Samoin olisi huomioitava mahdollisuudet sopimusperusteisen palvelutuotannon hyödyntämiseen, sillä teknologista osaamista ja resursseja olisi väistämättä tarpeen hankkia myös yksityiseltä sektorilta. Tämä voisi tarkoittaa nopeasti kehittyvän digitaalisen teknologian oloissa uusien liiketoimintamallien, työpaikkojen ja osaamisen syntymistä Suomeen. Viranomaisten teknologiainvestoinnit saattavat luoda tietyille korkean teknologian yrityksille myönteisiä mahdollisuuksia turvallisuusviranomaisten tarvitsemien palvelujen ja teknologian kehittämiseen.

Elinkeinoelämä toimii globaalissa, kansainvälisen talouden ja arvoverkostojen toimintaympäristössä. Globaalissa kilpailussa pienetkin tekijät vaikuttavat valtioiden kilpailukykyyn. Yritykset sijoittavat toimintonsa maakohtaisesti optimoiden koko yritystoimintansa omien yrityskohtaisten kilpailuetujen perusteella. Sijoittautumispäätökset ovat kokonaisarviointeja yritysten liiketoiminnan kannalta, joissa huomioidaan tekijöitä kuten esimerkiksi markkinatekijät, verotus, energian saatavuus, teknologinen osaaminen, suomalaisten korkea koulutustaso sekä luotettavuus ja rehellisyys, työvoimaan liittyvät

velvoitteet, kehittynyt infrastruktuuri ja yhteiskunta, yhteiskunnallinen ja poliittinen vakaus, kulutuskäyttäytyminen ja ilmastotietoisuus, sääntely ja sen ennustettavuus, vakaus, tarkkarajaisuus, hallinnollinen taakka sekä mahdolliset oikeudelliset riskit.

Lainsäädäntö on siis yksi päätöksentekoon vaikuttavista lukuisista seikoista. Suomen elinkeinorakenne on muuttunut entistä palvelukeskeisemmäksi ja innovaatiolähtöisemmäksi. Suomi on siirtynyt osaamis- ja teknologiaintensiivisille aloille, joiden klusterit houkuttelevat ulkomaisia suoria sijoituksia. Tietointensiivisen teollisuuden taloudellinen merkitys onkin kasvussa. Esityksen vaikutukset yritystoiminnalle ovat erilaiset riippuen muun muassa yrityksen toimialasta, koosta ja sen harjoittamasta kansainvälisestä toiminnasta.

Täsmällinen, tasapuolinen ja oikeasuhteinen lainsäädäntö vahvistaa Suomen mainetta ennustettavana ja luotettavan toimintaympäristönä. Tämä koskee jo Suomessa olevia ja Suomeen mahdollisesti investoivia toimijoita. Olennaista ICT-alan yritysten kilpailukyvyn kannalta on, että sääntely ei velvoita yrityksiä heikentämään tuotteidensa tai palveluidensa luotettavuutta esimerkiksi salausavaimien luovuttamisen, takaporttien asentamisen, salaustuotteiden käyttöön liittyvien rajoitteiden tai muiden liiketoiminnalle haitallisten velvoitteiden seurauksena.

Suomen maineen kannalta on huomionarvoista, että tiedusteluviranomaiselle ei tule sääntelyn perusteella suoraa ja rajoittamatonta pääsyä kaikkeen tietoliikenteeseen tai Suomen alueella sijaitsevien yritysten tietovarantojen sisältöön. Yksityisyyden suojaan kohdistuvien toimivaltuuksien käyttöön liittyy tuomioistuinten lupamenettely ja niiden käytön tarve tulee kyetä perustelemaan pitävästi ja kohdentamaan riittävästi. Yrityssalaisuuden suojaa puolestaan tukevat lakiin kirjatut käsittelykiellot ja hävittämisvelvollisuudet sekä tiedusteluviranomaisten kansainväliseen tiedonvaihtoon liittyvät kirjaukset.

Voimassa oleva sotilastiedustelusta annettu laki tuli voimaan 1.6.2019. Lain ei ole havaittu vaikuttaneen suoraan Suomeen kohdistuviin investointeihin. Suomi on edelleen saanut esimerkiksi uusia suuriakin datakeskusinvestointeja lain voimassa olon aikana.

Nykyisin viranomaisten kyky kansallista turvallisuutta vakavasti vahingoittavien valtiollisten vakoiluohjelmien tai -operaatioiden havaitsemiseen on rajallinen. Tietoliikennetiedustelun kokonaisuuden kehittäminen täydentäisi merkittävällä tavalla Suomen suojautumista vakavimpia tietoverkkouhkia vastaan. Lisäksi mahdollisuus suorittaa toimenpiteitä Suomen ulkopuolella olevaan tietojärjestelmään voidaan arvioida parantavan myös elinkeinoelämän suojautumista kaikkein vakavimpia tietoverkkouhkia vastaan.

Aiempaa paremman tiedon hankinnan ja suojautumisen paranemisen sekä kyberuhkien toteuttamiselle asetettavan kynnyksen nostamisen voidaan arvioida pitkällä tähtäimellä parantavan kansantaloutta, jos kyberuhkalta suojautumiseen ja sen aiheuttamiin vahinkoihin ei tarvitse käyttää kansantalouden resursseja enää yhtä paljon. Parhaimmillaan ehdotus parantaa Suomen kilpailukykyä turvallisena maana myös kyberympäristön osalta sekä aiheuttaa säästöjä julkiselle taloudelle.

Esityksessä ehdotetaan, että tietolähteen lisäksi myös avustajalle voitaisiin maksaa palkkio verottomasti. Sen lisäksi, mitä viranomaisen ulkopuolisen tahon mahdollisuudesta esimerkiksi asentaa ohjelmisto kohteena olevaan laitteeseen ehdotetaan säädettäväksi, myös tavanomaisesta avustamisesta olisi voitava maksaa palkkio verottomasti. Kuten tietolähteelle maksettavasti verottomasta palkkiosta on säädetty ja sen soveltamiskäytännöstä käy ilmi, palkkiot voidaan katsoa vähäisiksi.

4.2.4 Vaikutukset tiedonhallintaan

Tiedonhallintalaissa säädetään muun muassa tiedonhallinnan järjestämisestä ja kuvaamisesta, tietovarantojen yhteentoimivuudesta, teknisten rajapintojen ja katseluyhteyksien toteuttamisesta sekä tietoturvallisuuden toteuttamisesta. Tiedonhallintalailla varmistetaan viranomaisten tietoaineistojen yhdenmukainen hallinta ja tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi.

Esityksessä ehdotetaan lisättäväksi sotilastiedustelusta annettuun lakiin tietoliikennetiedustelun hakuehtojen määrittämistä koskeva uusi toimivaltuus (1. lakiehdotuksen 67 a §). Tämän lisäksi tietoliikenteen teknisten tietojen käsittelyä koskevaa sääntelyä (1. lakiehdotuksen 66 §) ja varsinaista tietoliikennetiedustelua koskevaa sääntelyä (1. lakiehdotuksen 68 ja 70 §). ehdotetaan muutettaviksi. Myös sotilastiedusteluviranomaisen oikeuteen saada tietoja muilta viranomaisilta ehdotetaan muutoksia. Puolustusvoimista annettuun lakiin (2. lakiehdotuksen 8 b §) ehdotetaan lisättäväksi uutta tiedonhankintaa yleisesti saatavilla olevista lähteistä koskevaa sääntelyä. Sotilastiedusteluviranomainen voisi ehdotetun sääntelyn nojalla hankkia ja käsitellä sekä tallentaa tietoja tehtäviensä suorittamiseksi laajemmin kuin nykyisten toimivaltuuksiensa puitteissa.

Tietoliikennetiedustelun kokonaisuudessa hakuehtojen määrittämisen toimivaltuus edellyttää uuden tietojärjestelmän perustamista sekä oikeus tallentaa tietoja teknisten tietojen käsittelyssä ja hakuehtojen määrittämisessä edellyttävät suljettuja tietoympäristöjä, joissa olevien tietojen käsittely edellyttää tuomioistuimen lupaa.

Vastaavasti oikeus tallentaa tietoliikennettä määräajaksi ja käsitellä sitä, edellyttää uusien korkean tietoturvan tietojärjestelmien rakentamista. Tietojärjestelmissä, joihin tietoa on tallennettu, olisi oltava rajapinnat tiedon käsittelyä koskeville tuomioistuimen lupaa edellyttäville tiedustelumenetelmille. Tiedonkäsittelyn edellytyksenä olevasta tuomioistuimen luvasta olisi voitava varmistua.

Lisäksi tiedonhankinta yleisesti saatavilla olevista lähteistä edellyttää uuden tietojärjestelmän perustamista. Muilta osin tarvittavat toiminnallisuudet voidaan toteuttaa jo käytössä olevissa tietojärjestelmissä.

Sotilastiedusteluviranomaisen ja Rajavartiolaitoksen välistä yhteistoimintaa ehdotetaan tiivistettäväksi (1. lakiehdotuksen 18 a §, 11. lakiehdotus ja 12. lakiehdotus). Viranomaiset käsittelevät tietoturvavaatimusten näkökulmasta vastaavia arkaluentoisia ja salassa pidettäviä tietoja järjestelmissään jo nykyisen sääntelyn puitteissa. Esityksessä ei ehdoteta muutoksia tietojärjestelmien ylläpitoa ja rekisterinpitoa koskevaan vastuunjakoon.

Esityksessä ei ehdoteta muutoksia tietojärjestelmien ylläpitoa ja rekisterinpitoa koskevaan vastuunjakoon. Laissa säänneltäisiin täsmällisesti ja tarkkarajaisesti siitä, mihin tarkoituksiin tietoja voidaan käyttää ja kenen käyttöön ja mitä tarkoitusta varten tietoja voidaan luovuttaa. Lisäksi laissa säädettäisiin täsmällisesti ja tarkkarajaisesti tietojen hävittämisestä. Sääntelystä ei arvioida aiheutuvan merkittäviä muutoksia tietojen luovuttamisen toteutustapaan tai tiedonhallintalain ja muun yleislainsäädännön mukaisten vaatimusten toteutumiseen.

Puolustusvoimien, sotilastiedusteluviranomaisen sekä tietoja vastaanottavien viranomaisten on jatkossakin noudatettava tietojen käsittelyssä samoja vaatimuksia, joita lainsäädännössä jo nykyään edellytetään salassa pidettävien, erityisiin henkilötietoryhmiin kuuluvien ja arkaluonteisten tietojen käsittelyltä. Tietojen käsittelyssä ja luovuttamisessa noudatettaisiin

viranomaiskohtaisten henkilötietolakien lisäksi tietosuojan yleislainsäädännössä, julkisuuslaissa ja tiedonhallintalaissa asetettuja vaatimuksia.

Puolustusvoimien, sotilastiedusteluviranomaisen ja muiden tiedonhallintalaissa tarkoitettuina tiedonhallintayksiköinä toimivien viranomaisten on arvioitava tiedonhallinnan muutosvaikutukset tiedonhallintalain 5 §:n 3 momentin mukaisesti ja päivitettävä tarvittaessa tiedonhallintamallinsa, asiakirjajulkisuuskuvaus sekä muu tarvittava dokumentaatio vastaamaan uuden sääntelyn mukaisia toimintamalleja.

Sotilastiedusteluviranomaisen oikeus pyytää harmaan talouden selvitysyksiköltä velvoitteidenhoitoselvitystä ei edellytä uusien tietojärjestelmien rakentamista. Tietojenvaihto tapahtuisi nykyisten rakenteiden puitteissa, eikä siten edellyttäisi lisätoimenpiteitä.

Esityksessä ei ehdoteta muutoksia voimassa olevaan asiakirjojen julkisuutta ja salassapitoa koskevaan sääntelyyn. Asianosaisen tiedonsaantioikeutta on voimassa olevassa lainsäädännössä rajoitettu, kun kyse on tiedustelumenetelmillä saaduista tiedoista. Asianosaisjulkisuutta ehdotetaan rajattavaksi vastaavin perustein myös ehdotetuilla uusilla tiedustelumenetelmillä ja niiden muutoksilla saatujen tietojen osalta.

4.2.5 Muut ihmisiin kohdistuvat ja yhteiskunnalliset vaikutukset

4.2.5.1 Perus- ja ihmisoikeudet

Sotilastiedustelusta annetun lain säännösten vaikutuksia perus- ja ihmisoikeuksiin on arvioitu laajemmin sotilastiedustelusta annetun lain säätämiseen johtaneessa hallituksen esityksessä (HE 203/2017 vp). Ehdotetut muutokset ovat merkityksellisiä usean perusoikeuden kannalta. Näitä ovat yhdenvertaisuus (PL 6 §), oikeus elämään sekä henkilökohtaiseen vapauteen ja koskemattomuuteen (PL 7 §), yksityiselämän suoja (PL 10§), sananvapaus ja julkisuus (PL 12 §), omaisuuden suoja (PL 15 §) sekä oikeusturva (PL 21 §). Ehdotettujen muutosten suhdetta perustuslaissa turvattuihin perusoikeuksiin sekä ihmisoikeuksiin käsitellään säätämisjärjestystä koskevassa jaksossa 10.

Turvallisuuden nimenomainen mainitseminen perustuslain 7 §:ssä korostaa julkisen vallan positiivista toimintavelvoitetta yhteiskunnan jäsenten suojaamiseksi (HE 309/1993 vp. s. 47). Ehdotetuilla muutoksilla olisi lähtökohtaisesti myönteisiä vaikutuksia perustuslain 7 §:n mukaiseen oikeuteen elämään sekä henkilökohtaiseen vapauteen ja koskemattomuuteen. Sotilastiedusteluviranomaisen toiminnan turvaamisella muuttuvassa turvallisuus- ja teknologiaympäristössä pystyttäisiin suojaamaan paremmin Suomen maanpuolustusta, kansallista turvallisuutta ja yhteiskunnan turvallisuutta sekä niiden alaan kuuluvia suojattavia oikeushyviä. Sotilastiedustelun kohteena oleviin uhkiin, jotka voidaan katsoa yhteiskunnan kannalta kaikista vakavimmiksi, ei esitetä muutoksia.

Ehdotetuilla muutoksilla, erityisesti tietoliikennetiedustelun hakuehtojen määrittämisellä, sisällöllisten hakuehtojen kiellon osittaisella poistamisella ja ilmoitusvelvollisuudesta luopumisella on merkitystä yksityiselämän suojan kannalta.

Tietoliikennetiedustelun hakuehtojen määrittäminen kohdistuisi sähköiseen viestintään sen konekielisessä muodossa, eli viestiä ei olisi mahdollista käsitellä tai selvittää sen sisältöä viestin ymmärrettävässä muodossa. Tietoteknisin keinoin konekielisestä tietoliikenteestä pystyttäisiin muodostamaan uusia hakuehtoja, muita kuin puhutun kielen sanoja, joilla varsinaista tietoliikennetiedustelua pystyttäisiin kohdentamaan aiempaa paremmin. Näin ollen varsinaisen

tietoliikennetiedustelun voidaan katsoa puuttuvan perustuslain 10 §:ssä turvattuun viestinnän salaisuuteen aiempaa vähemmän.

Tietoliikenteen teknisten tietojen käsittelyn muutosta koskeva ehdotus ja hakuehtojen määrittäminen antavat sotilastiedusteluviranomaiselle oikeuden tallentaa tietoja. Tietojen tallentaminen puuttuu henkilön yksityisyyden suojaan, mutta tällä ei voida arvioida olevan merkittäviä vaikutuksia yksilön perusoikeuksiin. Puuttumisen laajuuden voidaan arvioida olevan rajattu, sillä ainoastaan tallennetuista tiedoista ei voida tehdä syvälle käyviä päätelmiä yksilön henkilökohtaisesta elämästä.

Toisaalta esityksessä ehdotettu mahdollisuus käyttää viestinnän sisältöön meneviä hakuehtoja voidaan katsoa parantavan yksityisyyden suojaa. Mahdollisuus käyttää kielellisiä hakuehtoja yhdessä muun hakuehdon kanssa rajaisi jo tietoliikennetiedustelun hakuehtojen käytön vaiheessa sotilastiedustelun jatkokäsittelyyn tulee tietoa aiempaa tehokkaammin. Näin ollen voimassa olevan lain mahdollisuus käsitellä hakuehtoja vastaavaa tietoliikennettä automaattisesti ja manuaalisesti siirtyisi osittain aiempaa varhaisempaan vaiheeseen. Tämä tarkoittaisi myös sitä, että ehdotuksella ei voida katsoa olevan merkittäviä vaikutuksia yksityisyyden suojan toteutumisen kannalta.

Muun kuin viestin kielellistä sisältöä kuvaavien hakuehtojen käytön yhdessä muiden hakuehtojen kanssa ei voida arvioida merkittävästi vaikuttavan yksityisyyden suojaan. Puheena olevassa tapauksessa hakuehdon on liityttävä sotilastiedustelusta annetun lain 4 §:ssä tarkoitettuun kohteeseen tuomioistuimen luvan mukaisesti. Tämän voidaan katsoa parantavan sotilastiedusteluviranomaisen tiedonhankinnan tehokkuutta maanpuolustuksen ja kansallisen turvallisuuden suojaamisen kannalta sekä näihin liittyvien uhkien torjunnan parantavan Suomessa olevien henkilöiden turvallisuutta. Tilanteissa, joissa sanottu hakuehto on esimerkiksi niin kutsutun koteloidun tietoliikenteen sisällä, tiedonhankinnalla ei voida katsoa olevan uusia vaikutuksia perus- ja ihmisoikeuksien kannalta.

Hakuehtojen määrittäminen ja sisällöllisten hakuehtojen kiellon poistamisen voidaan arvioida osaltaan parantavan yksityisyyden suojaa tietoliikennetiedustelun tarkemman kohdentumisen myötä. Samalla luonnollisesti tiedustelu myös tehostuisi ja sen tuloksellisuus paranisi.

Lakiehdotuksen mukaan sotilastiedustelu voisi käyttää myös sivullisten laitteita tai tietojärjestelmiä, jos se olisi välttämätöntä menetelmän tai ohjelmiston asentamiseksi tai poisottamiseksi. Yksittäisen toimenpiteen ei arvioida puuttuvan merkittävästi omaisuuden suojaan, sillä toimenpiteen keston voidaan katsoa olevan varsin vähäinen. Joka tapauksessa nimenomaisesti olisi säädetty toimenpiteen rajoittumisesta vähäiseen haittaan ja toisaalta viranomaisen olisi suoritettava suuremmasta vahingosta vahingonkorvausta vahingonkorvauslain mukaisesti.

Merkittävintä perus- ja ihmisoikeuksiin kajoamista tarkoittavien tiedustelumenetelmien osalta päätöksenteko esitetään tapahtuvaksi edelleen tuomioistuimessa. Tiedustelumenetelmien käytön seurauksena tapahtuvaa perus- ja ihmisoikeuksien rajoittamista valvottaisiin edelleen lukuisin eri keinoin. Tehokkaalla ja monikerroksisella ennakollisella, reaaliaikaisella ja jälkikäteisellä valvonnalla ehkäistään perus- ja ihmisoikeuksia uhkaavat väärinkäytökset ja huonojen käytäntöjen muodostuminen.

Esityksessä ehdotetaan muutettavaksi sotilastiedustelusta annetun lain muun kuin valtiollisen toimijan tietoliikennetiedustelusta ilmoittamista koskevaa sääntelyä siten, ettei tiedustelumenetelmän käytöstä ilmoiteta käytön kohteeksi joutuneelle. Tämän voidaan osaltaan katsoa laajassa kontekstissa parantavan perusoikeuksien toteutumista, koska

sotilastiedusteluviranomaisen ei tarvitse ryhtyä selvittämään kaikkia ilmoitusvelvollisuuden alaisia tiedustelumenetelmän käytön kohteeksi joutuneiden tietoja. Tämä voisi viime kädessä tarkoittaa tiedustelumenetelmien käyttöä ja tiedonhankintaa sen selvittämiseksi, kenelle ilmoitus on konkreettisesti tehtävä. Ilmoitusvelvollisuutta koskevaa sääntelyä on lain säätämisen yhteydessä perusteltu oikeusturvanäkökohdilla.

Ehdotetuilla muutoksilla on siten liittymäpintaa oikeusturvan toteutumiseen. Ehdotetun muutoksen ei arvioida heikentävän oikeutta oikeusturvaan. Esityksessä ei ehdoteta muutoksia oikeuteen saattaa asia selvitettäväksi tiedusteluvalvontavaltuutetulle tai tiedustelumenetelmän käytön edellyttämään tuomioistuinmenettelyyn. Tiedusteluvalvontavaltuutetun tehtävänä on valvoa tiedustelutoimintaa ja sen lainmukaisuutta kokonaisvaltaisesti ennakollisesti, reaaliaikaisesti ja jälkikäteisesti, jolloin valvonnassa pystytään kiinnittämään huomiota toimintaan myös yksityisten henkilöiden näkökulmasta. Tiedusteluvalvontavaltuutetun tehtävänä on myös valvoa nimenomaisesti oikeusturvan toteutumista. Edellä todettu tarkoittaisi sitä, että vastuu oikeusturvan toteutumisesta siirtyisi selkeämmin tiedusteluvalvontavaltuutetulle.

Ilmoituksen tekemättä jättämisen ei voida katsoa merkittävästi muuttavan henkilön asemaa oikeussuojakeinojen käytön osalta. Se, että tiedusteluviranomainen toimii lainmukaisesti ja tiedustelumenetelmien käyttö kohdistuu oikein, on ensisijaisesti viranomaisen itsensä vastuulla. Ulkopuolisen oikeusturvan takeen toimintaan tuo tiedusteluvalvontavaltuutettu, jonka tehtävänä on puuttua lainvastaiseen menettelyyn aktiivisesti. Esitetty muutos siirtää vastuun oikeusturvan toteutumisesta selkeämmin tiedusteluvalvontavaltuutetulle, joka jo nykyisin pääsääntöisesti siitä vastaa.

Näin ollen tiedusteluvalvontavaltuutetun voidaan katsoa pitävän huolen tiedustelumenetelmän käytön kohteeksi joutuneen oikeusturvasta, vaikka kohteeksi joutunut ei saisi siitä ilmoitusta tai saisi asiaa tietoonsa. Toki, jos tiedusteluvalvontavaltuutettu saattaa asian esitutkintaan, henkilö saa tiedon kohteeksi joutumisesta rikosprosessin kautta. Edellä todetun lisäksi tietoliikennetiedustelu edellyttää tuomioistuimen lupaa.

Ehdotettu uusi toimivaltuus, valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu Suomessa, voi puuttua muun kuin valtiollisen toimijan yksityisyyden suojaan, jos toimivaltuuden käytön kohteena olevassa tietojärjestelmässä käsitellään myös muun kuin valtiollisen toimijan tietoja. Näitä tilanteita koskee kuitenkin hetihävittämissääntely ja tiedustelumenetelmän käytön keskeyttämistä koskeva sääntely, joiden kautta käsiteltäväksi päätyvä tieto viimeistään rajautuu vain välttämättömään.

Ehdotetuilla muutoksilla on jonkin verran vaikutusta perustuslaissa turvattuun julkisuusperiaatteen toteutumiseen. Toisaalta sääntelyn taustalla vaikuttaa painava yhteiskunnallinen intressi, joka edellyttää julkisuusperiaatteesta rajattua poikkeamista.

Ehdotetuilla muutoksilla tietolähteen turvaamiseen voidaan katsoa olevan myönteisiä vaikutuksia tietolähteen perus- ja ihmisoikeuksien suojan kannalta.

Ehdotetuilla muutoksilla puolustusvoimista annetun lain 36 a §:n sääntelyyn viran haettavaksi julistamiseen on liittymäpinta perustuslain 21 §:ssä turvattuun oikeusturvaan. Ehdotetun muutoksen myötä muuta kuin pykälän 2 momentissa tarkoitettua virkaa hakevilla ei välttämättä ole oikeutta saada tietoonsa virkaan valitun tai virkaa hakeneiden henkilöllisyyksiä. Tällä voi olla joissain tilanteissa vaikutusta hakijoiden mahdollisuuksiin arvioida virantäytön asianmukaisuutta. Henkilöillä on kuitenkin edelleen mahdollisuus kannella viranomaisen menettelystä virantäytössä. Virkojen täyttäminen julkisesti olisi edelleen pääsääntö ja

poikkeuksen kohdistuvan kohtuullisen pieneen joukkoon osaajia, joten vaikutusten voitaisiin katsoa kohdistuvan rajattuun joukkoon ihmisiä.

Ehdotetuilla muutoksilla puolustusvoimista annetun lain 36 a §:n sääntelyyn viran haettavaksi julistamiseen on liittymäpinta lisäksi perustuslain 6 §:ssä turvattuun yhdenvertaisuuteen. Yleisesti ottaen henkilön nimestä voidaan tiettyyn pisteeseen saakka tehdä arvio henkilön sukupuolesta ja kun nimitiedot jäisivät virkaa hakeneilta saamatta, hakijoilla ei olisi mahdollisuutta täysimääräiesti arvioida yhdenvertaisuuden toteutumista rekrytoinnissa. Hakijoiden on kuitenkin voimassa olevan lain mukaisesti mahdollista tehdä asiasta kantelu valtioneuvoston oikeuskanslerille tai eduskunnan oikeusasiamiehelle sekä nostaa kanne naisten ja miesten tasa-arvoa koskevan lakiin (609/1986), yhdenvertaisuuslakiin (1325/2014) tai rikoslain (39/1998) 47 luvun 3 §:n mukaiseen työsyrjintään perustuen.

Perus- ja ihmisoikeuksiin puuttuminen on esityksessä rajattu sääntelyllä mahdollisimman tarkasti siihen, mikä on yhteiskunnan tärkeiden, erityisesti kansallisen turvallisuuteen ja maanpuolustukseen liittyvien, intressien suojaamiseksi välttämätöntä. Esityksessä ehdotettujen säännösten käyttöala kohdistuu niihin henkilöihin, yksilöityihin ryhmiin ja toimijoihin, joihin kohdistettuna tiedonhankinnan ja toimenpiteiden voidaan arvioida olevan tehokasta ja suhteellisuusperiaatteen mukaista ja siten parhaiten edistävän yhteiskunnan ja yksilöiden turvallisuutta.

Ehdotuksen arvioidaan vahvistavan mainittujen perusoikeuksien toteutumista yhteiskunnassa siinä määrin, että tiedonhankinta- ja tiedonkäsittelytoimivaltuuksiin tehtävistä muutoksista seuraavat perus- ja ihmisoikeusvaikutukset ovat perusteltuja ja oikeasuhtaisia. Lisäksi on huomattava, että aiempaa paremmat edellytykset kohdentaa tiedustelumenetelmiä vähentävät sotilastiedustelun kohteen kannalta sivullisten ja tarpeettoman tiedon käsittelyä.

4.2.5.2 Yhdenvertaisuus ja sukupuolten tasa-arvo

Sotilastiedustelusta annetun lain 9 §:ssä säädetään syrjivän tiedustelutoiminnan kiellosta, eikä esitetyillä muutoksilla tietoliikennetiedusteluun ja teknisten tietojen käsittelyyn arvioida olevan vaikutuksia yhdenvertaisuuden ja sukupuolten tasa-arvon kannalta.

Ehdotettu muutos sotilastiedustelusta annetun lain 91 §:ään mahdollistaisi vapaaehtoisesta maanpuolustuksesta annetun lain 18 ja 19 §:ssä tarkoitetussa harjoituksessa olevan osallistumisen tiettyjen tiedustelumenetelmien käyttöön virkamiehen ohjauksessa ja valvonnassa. Vapaaehtoisten harjoitusten erityistehtäviin voi osallistua edellytykset täyttävät naiset ja miehet, jotka eivät ole suorittaneet varusmiespalvelusta tai eivät enää kuulu reserviin. Muutosesityksen arvioidaan lisäävään yhdenvertaisuutta, kun sotilastiedustelutoimintaan kykenee osallistumaan myös edellä kuvattuihin harjoituksiin osallistuvat. Todennäköisesti sotilastiedustelutoimialalla tarvittavaa erityisosaamista on kuitenkin vain hyvin rajatulla henkilöpiirillä, joten vaikutus ei kohdistuisi kovin laajasti.

4.2.5.3 Viranomaisten toiminta

Puolustusvoimat

Sotilastiedustelun avulla tunnistettavat uhat ovat kansainvälisiä, vakavia ja kohdistuvat valtion keskeisiin turvallisuusintresseihin. Nyt käsiteltävän esityksen myötä sotilastiedusteluviranomainen pystyisi tuottamaan Suomen turvallisuuden kannalta merkityksellistä tietoa ulkomaisista toimijoista ja olosuhteista päätöksenteon tueksi aiempaa

paremmin ja tehokkaammin. Esityksen myötä ylimmän valtiojohdon ja Puolustusvoimien johdon kyky reagoida Suomea vaarantaviin uhkiin arvioidaan parantuvan. Tiedonlisä parantaisi sotilastiedusteluviranomaisen kykyä informoida ylintä valtiojohtoa Suomen turvallisuusympäristössä tapahtuvista muutoksista.

Ehdotettu sääntely tiivistäisi sotilastiedusteluviranomaisen ja Suojelupoliisin yhteistoimintaa sekä tiivistäisi yhteistoimintaa myös Rajavartiolaitoksen kanssa. Aiempaa laajempi yhteistoiminta Rajavartiolaitoksen kanssa edellyttää päivystysjärjestelyistä huolehtimista.

Suojelupoliisille suoritettava tietoliikenteen teknisten tietojen käsittely aiheuttaa jonkin verran lisäkustannuksia sotilastiedusteluviranomaiselle.

Esitys asettaa korkeat laadulliset, koulutukselliset ja oikeudelliset vaatimukset täytäntöönpanolle.

Ehdotettu sääntely parantaisi Puolustusvoimien kykyä hoitaa sen lakisääteisiä tehtäviä.

Eräiden ehdotusten arvioidaan säästävän toimivaltaisten viranomaisten resursseja. Koska ehdotuksen johdosta jatkossa ei enää olisi tarvetta hakea ja käsitellä uutta lupaa aina, kun ilmenee saman tahon käytössä oleva, tiedonhankinnan kannalta olennainen luvan mukainen ulkopuolinen teleosoite tai telepäätelaite taikka laite tai ohjelmisto, etenkin telekuuntelua, televalvontaa ja teknistä laitetarkkailua koskevien tuomioistuinkäsittelyiden määrän voidaan arvioida vähenevän ja siten näihin tarvittavien resurssien säästyvän.

Ilmoitusvelvollisuudesta luopumisella muuhun kuin valtiolliseen toimijaan kohdistuvassa tietoliikennetiedustelussa olisi hallinnollista taakka keventävä vaikutus. Voimassa olevan lain mukainen ilmoitusvelvollisuus vie resursseja sekä sotilastiedusteluviranomaisessa että tuomioistuimessa, joka käsittelee ilmoituksen lykkäämistä tai tekemättä jättämistä koskevan asian sotilastiedustelusta annetun lain 89 §:n 6 ja 7 momentin mukaisesti.

Ehdotettu tiedonhankinta yleisesti saatavilla olevista lähteistä, tällaisen tiedonhankinnan suojaaminen ja sitä koskeva päätöksenteko edellyttävät koulutusta ja päätöksentekoon liittyvien prosessien luomista. Puolustusvoimissa on jo vakiintuneet toimintatavat tiedustelutoiminnassa, joten tästä ei arvioida aiheutuvan merkittävää vaikutusta tarvittaviin resursseihin tai vaativan uusia tietojärjestelmiä.

Esityksen mukaisesti sotilastiedusteluviranomaisen ja erityisesti tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa toteutettavat tiedustelumenetelmien käyttötilanteet tulisivat mahdollisesti kasvamaan. Tämän arvioidaan lisäävään koulutustarpeita, mikä on kuitenkin mahdollista toteuttaa osana normaalia toimintaa.

Virkaa hakevien henkilöllisyyden suojaaminen hakuprosessista lukien parantaa mahdollisuutta henkilöstöresurssin tarkoituksenmukaiseen käyttämiseen ja parantaa sotilastiedusteluviranomaisen mahdollisuutta työnantajana entistä paremmin ottaa huomioon työturvallisuutta koskevat työnantajavelvoitteet. Tärkeä elementti henkilöstön tunnistetietojen ei-julkisuudessa liittyy yksilön kannalta työturvallisuuden parantumiseen sekä tämän lähipiirin suojaamiseen.

Rajavartiolaitos

Rajavartiolaitokselle ehdotetaan säädettäväksi uusi tehtävä, sotilastiedusteluun osallistuminen. Rajavartiolaitokselle säädettäisiin mahdollisuus tukea sotilastiedusteluviranomaisia suorittamalla tiettyihin tiedustelumenetelmiin liittyviä yksittäisiä toimenpiteitä sotilastiedusteluviranomaisen pyynnöstä.

Uudet tiedustelutoimivaltuudet edellyttävät Rajavartiolaitoksen henkilöstön täydennyskoulutusta. Suurin osa tiedustelutoimivaltuuksista eivät menetelminä olisi Rajavartiolaitokselle uusia, vaan niitä vain käytettäisiin uudenalaisessa tarkoituksessa. Rajavartiolaitoksen osallistumisesta tiedusteluun ei arvioida aiheutuvan muiltakaan osin merkittäviä taloudellisia vaikutuksia.

Rajavartiolaitokselle säädettävän uuden tehtävän arvioidaan vaikuttavan vähäisessä määrin henkilöstön työmääriin, koska toimenpiteitä suoritettaisiin Rajavartiolaitoksen muiden lakisääteisten tehtävien yhteydessä. Rajavartiolaitos voisi kuitenkin kieltäytyä sotilastiedusteluviranomaisen pyynnöstä, jos sillä ei olisi tosiasiallista mahdollisuutta tämän tukemiseen esimerkiksi resurssien tai suorituskyvyn puuttumisen taikka Rajavartiolaitoksen oman kiireellisen lakisääteisen tehtävän vuoksi.

Rajavartiolaitokselle säädettävä uusi tehtävä, sotilastiedusteluun osallistuminen, ja sotilastiedustelussa käytettävät toimivaltuudet parantavat Rajavartiolaitoksen ja Puolustusvoimien yhteistyötä sekä tukevat sotilastiedustelua.

Tiedusteluvalvontavaltuutettu

Tiedusteluvalvontavaltuutetun vuoden 2025 vuosikertomuksesta käy ilmi, että tiedusteluvalvontavaltuutetulle on vuosina 2023 ja 2024 tehty 11 tutkimispyyntöä ja molempina vuosina on otettu yhdet kantelut tutkittavaksi. Tiedustelulakien voimaantulosta lähtien vuosittaisten tutkimispyyntöjen määrä on vaihdellut 20 ja 7 välillä.

Esitetyllä ilmoitusvelvollisuudesta luopuminen saattaa nostaa tutkimispyyntöjen määrää, jos ihmiset kokevat ilmoitusvelvollisuudesta luopumisen heikentävän heidän oikeusturvaansa ja ihmiset ryhtyvät aiempaa aktiivisemmiksi käyttämään ensisijaista oikeusturvansa taetta.

Toisaalta voidaan arvioida, että ihmisten halukkuus tehdä tutkimispyyntöjä ja kanteluita pysyy ennallaan. Tämä ei kuitenkaan poista sitä mahdollisuutta, että esimerkiksi julkisuudessa olevien tapausten johdosta tutkimispyyntöjen ja kanteluiden määrä kasvaa hetkellisesti jopa merkittävästi. Joka tapauksessa mahdollisuudesta tehdä tiedusteluvalvontavaltuutetulle tutkimispyyntö tai kantelu lienee tiedotettava aiempaa aktiivisemmin.

Sotilastiedustelusta annetun lain 20 §:ään ehdotetun muutoksen myötä ulkomaisella toimivaltaisella virkamiehellä on rajatuissa tilanteissa oikeus osallistua Suomen alueella tiedustelumenetelmän käyttöön Pääesikunnan tiedustelupäällikön päätöksellä. Sotilastiedusteluviranomainen vastaisi aina menetelmän käytön lainmukaisuudesta. On mahdollista, että kansainvälisen yhteistyön lisääntyessä tiedusteluvalvontavaltuutetun valvoman toiminnan määrä kasvaa lievästi.

Tietoliikennetiedusteluun ehdotettujen muutosten sekä uusien tiedonhankintatoimivaltuuksien myötä on odotettavissa, että tiedusteluvalvontavaltuutetun valvontakäynnit lisääntyvät hieman. Vuonna 2023 valvontakäyntejä on ollut 171 ja vuonna 2024 153. Tiedusteluvalvontavaltuutetun riittävistä resursseista tuleekin huolehtia vastaisuudessakin.

Maa-, Meri- ja Ilmavoimien mahdollisuus käyttää radiosignaalitiedustelua ja perusmuotoista tietolähdetoimintaa lisännee lievästi tiedusteluvalvontavaltuutetun valvontatointa.

Vaikutukset muihin viranomaisiin

Esityksen 10. lakiehdotuksen 37 a §:llä annettaisiin sotilastiedusteluviranomaiselle oikeus päivittää oma tietojärjestelmänsä vertaamalla sen sisältämiä tietoja muiden viranomaisten henkilörekistereihin. Ehdotetulla säännöksellä olisi vaikutusta niihin viranomaisiin, joiden järjestelmistä sotilastiedusteluviranomainen päivittäisi oman tietojärjestelmänsä henkilötiedot. Sotilastiedusteluviranomaisella olisi oikeus saada tiedot maksutta. Tietojen poimiminen tietojärjestelmistä tarkastettavaksi ja siihen liittyvä mahdollinen yhdistelytyö voivat aiheuttaa kustannuksia ja lisätyötä rekisterinpitäjälle. Tämä pyrittäisiin kuitenkin ottamaan huomioon aineistoa koskevissa tietopyynnöissä ja niiden rajauksissa. Käytännössä tietopyynnöstä aiheutuisi jossain määrin hallinnollista taakkaa pyynnön vastaanottajalle.

Ulko- ja turvallisuuspoliittisten vaikutusten arviointi

Uusi toimivaltuus Suomen rajan ulkopuolella olevan tietojärjestelmän toiminnan haittaamiseen edellyttää uudentyyppisiä päätöksentekoprosesseja. Säännöksen nojalla suoritetuilla toimenpiteillä voi olla sen luonteen mukaan jopa merkittäviä ulko- ja turvallisuuspoliittisia vaikutuksia.

Jo nykyisellään lain 15 §:ssä säädetään tiedustelutoiminnan yhteensovittamisesta, missä käsitellään valmistelevasti myös tiedustelutoimintaa, jos sillä voidaan arvioida olevan ulko- ja turvallisuuspoliittisia vaikutuksia. Suomen rajan ulkopuolella olevan tietojärjestelmän toimintaan vaikuttaminen edellyttää 15 §:ssä tarkoitetun kokoonpanon tehtävien kehittämistä tavalla, joka vastaa uudentyyppisestä toiminnan vaatimuksia.

Ulko- ja turvallisuuspoliittisesti merkittäviä toimenpiteitä käsiteltäisiin valmistelevasti ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteisessä kokouksessa.

4.2.5.4 Kansallinen turvallisuus ja maanpuolustus

Teknologian ja tietoliikenteen muutosten aiempaa parempi seuraaminen turvaa sotilastiedusteluviranomaisen kyvyn tuottaa ajantasaista tietoa päätöksenteon tueksi. Lisäksi kansainvälisen yhteistoiminnan saumattomuuden varmistaminen vaikuttaa myönteisesti sekä kansalliseen turvallisuuteen että Suomen toimintaan osana liittokuntaa ja samanmielisten valtioiden yhteisössä.

Viestintäverkkojen ja tietojärjestelmien määrä ja niiden merkitys osana yhteiskunnan toiminnan edellyttämien palveluiden tuottamista ja yhteiskunnan kriittisen infrastruktuurin toimintaa kasvaa jatkuvasti. Kyberuhkien ja -hyökkäyksien määrä on kasvanut ja kyberhyökkäykset kehittyvät jatkuvasti teknologian kehittyessä. Yhteiskunnan kannalta kriittiset toiminnot ovat entistä riippuvaisempia tietojärjestelmistä ja viestintäverkoista, joissa esiintyvällä kyberhäiriöllä voi olla merkittäviä haitallisia vaikutuksia paitsi häiriön kohteena olevaan toimijaan, myös yhteiskuntaan laajemmin. Myös ulko- ja turvallisuuspolitiikan muutokset ovat heijastuneet kyberympäristöön. Palvelunestohyökkäysten, murtautumisten, haittaohjelmien ja valtiollisen toiminnan riski on kasvanut ja uhkataso noussut. Kyberhyökkäyksiä käytetään osana yhteiskuntaan kohdistuvaa hybridivaikuttamista. Mahdollisuus suorittaa Suomen rajan ulkopuolella olevassa tietojärjestelmässä haitallisen kybertoiminnan keskeyttäviä ja sitä haittaavia toimenpiteitä parantaa kansallista turvallisuutta ja maanpuolustuksen edellytyksiä.

Lisäksi parhaimmillaan toimenpiteet johtavat siihen, ettei kyberturvallisuudesta vastaavien tahojen tarvitse käyttää haitallisen kybertoiminnan estämiseen nykytilaa vastaavaa määrää resursseja.

Esityksellä vahvistettaisiin osaltaan yhteiskunnan yleistä kyberturvallisuustasoa. Esityksellä parannettaisiin yhteiskunnan toiminnan kannalta keskeisten viranomaisten toimintaedellytyksiä muuttuneessa toimintaympäristössä. Esityksen tavoitteena on osaltaan välttää kyberhäiriöiden aiheuttamia keskeytyksiä yhteiskunnan toiminnan kannalta keskeisten palveluiden tai toimintojen jatkuvuudessa, sillä häiriö kriittisen palvelun tarjonnassa voi aiheuttaa yhteiskunnalle merkittävää vahinkoa. Yhdessä yhteiskunnan kriittisessä toiminnossa (esimerkiksi energiantuotannossa tai viestintäverkkojen toiminnassa) tapahtunut häiriö voi merkittävästi vaikuttaa myös muiden kriittisten palvelujen tarjoamiseen sekä aiheuttaa laajamittaisia haitallisia vaikutuksia yhteiskunnassa. Lisäksi vaikutukset eräiden kriittisten palvelujen jatkuvuuteen voivat aiheuttaa paitsi taloudellisia menetyksiä, myös esimerkiksi kansalaisten henkeen ja terveyteen kohdistuvia uhkia.

Esitys sisältää myös ehdotuksia, joilla vahvistetaan yhteistyötä ja tietojenvaihtoa viranomaisten ja muiden toimijoiden välillä. Tämän voidaan arvioida parantavan osaltaan yhteiskunnan ja sen toiminnan kannalta yhteiskunnan keskeisten toimialojen ja -palveluiden kykyä sietää kyberhäiriöitä.

Viestintäverkot ja tietojärjestelmät ovat globaalisti sidoksissa toisiinsa ja myös toiseen jäsenvaltioon kohdistuvalla kyberhyökkäyksellä tai -häiriöllä voi olla heijastevaikutuksia Suomeen.

Esityksellä arvioidaan olevan myös välillisesti myönteisiä vaikutuksia kansalaisten turvallisuudelle yhteiskunnan häiriöttömän toiminnan edistämisen kautta. Esityksen tavoitteena on vähentää kyberuhkien määrää ja estää niiden aiheuttamat vaikutukset yhteiskunnan toiminnan kannalta kriittiseen infrastruktuuriin. Näkyvien kyberhäiriöiden yleistyminen ja niihin puuttumatta jättäminen voivat vaikuttaa kansalaisten kokemukseen turvallisuudesta yhteiskunnassa.

Yhteistoiminnan Rajavartiolaitoksen kanssa voidaan arvioida parantavan maanpuolustusta ja kansallisen turvallisuuden suojaamista, kun tiedonhankinta pystytään aloittamaan aiempaa tehokkaammin heti kohteen tunnistamisesta ja saapumisesta raja-alueelle.

Reserviläisten ja vapaaehtoiseen harjoitukseen osallistuvien käyttäminen tietyissä sotilastiedustelun tehtävissä lisää asevelvollisten ja vapaaehtoisten henkilöiden mahdollisuuksia osallistua Puolustusvoimien toimintaan. Puolustusvoimat voi hyödyntää asevelvollisten erityisosaamista entistä laajemmin ja tämän voidaan katsoa osaltaan parantavan maanpuolustustahtoa. Puolustusvoimat voi kehittää asevelvollisuutta suuntaan, jossa aiempaa laajemmalle joukolle asevelvollisia voitaisiin tarjota heidän erityisosaamistaan hyödyntävää ja kehittävää koulutusta aiempaa paremmin.

4.2.5.5 Tietoyhteiskunta ja tietosuoja

Viranomaisten tiedonvaihtoa koskevilla muutoksilla arvioidaan olevan positiivisia vaikutuksia tietoyhteiskunnan ja tietosuojan kannalta. Etenkin tiedonluovutus haitallisista tietokoneohjelmista ja haitallisista käskyistä antaa tiedonsaajalle paremmat edellytykset suojautua näiltä uhkilta. Tämän voidaan katsoa osaltaan helpottavan viranomaisten ja muiden toimijoiden yhteistoimintaa näiltä uhkilta suojautumisessa ja niiden vaikutusten vähentämisessä.

Mahdollisuus puuttua Suomen raja ulkopuolella olevan haitallisen tietojärjestelmän toimintaan parantaa suomalaisen tietoyhteiskunnan turvallisuutta. Mahdollisuus toimia voidaan arvioida nostavan kynnystä tehdä haitallisia toimenpiteitä, kun uhkatoimijat huomaavat, että heidän toimintaansa haitataan. Lisäksi uusi toimivaltuus antaisi mahdollisuuden keskeyttää tällainen haitallinen toiminta aiempaa varhaisemmassa vaiheessa. Sotilastiedusteluviranomaisen mahdollisuus puuttua ulkomaisen tietojärjestelmän toimintaan voidaan katsoa parantavan tietoyhteiskunnan resilienssiä. Tältä osin vaikutukset voivat olla jopa merkittäviä tietyissä tilanteissa.

Ehdotetut muutokset eivät vaikuta yritysten mahdollisuuksiin tarjota esimerkiksi päästä-päähän salausta (E2EE). Lakiehdotuksissa ei esitetä helpottavaksi tai mahdollistettavaksi sotilastiedusteluviranomaisten aiempaa helpompaa pääsyä yritysten järjestelmiin tai palveluihin yleisesti. Lakiehdotusten ei arvioida vaarantava kaupallisten toimijoiden välistä välttämätöntä luottamuspääomaa, oikeutta yksityiseen viestintään sekä yritysvarallisuuden arvon säilyttämistä ja elinkeinotoiminnan taloudellisten edellytyksistä huolehtimista. Päästä-päähän salauksen voidaan arvioida edelleen olevan välttämätön Suomen kokonaisturvallisuudelle.

Ehdotettu oikeus käyttää sotilastiedusteluviranomaisen ulkopuolisen tahon laitetta tai tietojärjestelmän osaa voi yksittäistapauksellisesti hidastaa tai haitata kyseisen tahon tietoliikenneyhteyttä tai järjestelmän toimintaa. Vaikutukset arvioidaan kuitenkin vähäisiksi. Mahdollista kuitenkin on, että toimenpiteitä suunniteltaessa sotilastiedusteluviranomainen ei voi varautua kaikkiin yllättäviin tilanteisiin ja toimenpiteestä syntyy vähäistä suurempaa haittaa. Mahdolliset vahingot olisi korvattava vahingonkorvauslain mukaisesti.

Ehdotuksen nojalla tehtävien viranomaistoimien tarkoituksena on kuitenkin maanpuolustuksen, varautumisen ja kansallisen turvallisuuden kehittäminen ja sitä kautta myös tietosuojaan liittyvien oikeushyvien edistäminen tietojärjestelmissä ja viestintäverkoissa. Ehdotetut säännökset on laadittu yksityiselämän suojaan liittyvät perustuslailliset näkökohdat huomioon ottaen ja pyritty rajoittamaan vain välttämättömään esityksen tarkoituksen toteuttamiseksi. Myönteisen vaikutuksen näille oikeushyville voidaan arvioida olevan jopa merkittäviä.

Esityksellä ei arvioida olevan vaikutuksia viranomaisten vastuulla olevaan tietosuojaan, vaan tietosuoja toteutuisi voimassa olevan lainsäädännön mukaisesti.

4.2.5.6 Rajat ylittävät vaikutukset

Ehdotetuilla muutoksilla Suomen rajan ulkopuolella olevan tietojärjestelmän toimintaan vaikuttamisesta voi olla vaikutuksia Suomen kansainvälisiin suhteisiin. Sotilastiedusteluviranomaisella olisi esityksen mukaan oikeus estää Suomen ulkopuolella olevan tietojärjestelmän käyttö sekä haitata tai muokata sen toimintaa. Kansainvälisesti kyseessä on varsin tavanomainen toimintatapa tiedustelutoiminnassa, eikä tällaisella toiminnalla lähtökohtaisesti ole ollut merkittäviä vaikutuksia valtioiden välisiin suhteisiin. Esityksessä ehdotetut toimenpiteiden intensiteettiä voidaan muuttaa tilanteen edellyttämällä tavalla ja näin ollen myös eskalaatioriskiä voidaan säädellä varsin tarkasti. Parhaimmillaan varsin pienellä toimenpiteellä saadaan Suomen kansallisen turvallisuuden kannalta merkittävä hyöty.

Toimenpiteiden suorittaminen edellyttää tiivistä yhteistyötä toimenpiteen kohteena olevan valtion kanssa tilanteessa, jossa valtio on ystävällismielinen. Ensisijaisesti edellä tarkoitetun valtion olisi pystyttävä suorittamaan tarvittavat toimenpiteet uhkan ehkäisemiseksi ja poistamiseksi. Kaikissa tilanteissa tämä ei kuitenkaan ole mahdollista

Suoritettavien toimenpiteiden olisi oltava kulloiseenkin tilanteeseen soveltuvia ja suhteellisia. Ei voida kuitenkaan poissulkea, etteikö valtiot voisi omia intressejä ajaakseen esittää tällaisen toiminnan valtioiden välisenä selkkauksena, mihin Suomen valtiojohdon olisi varauduttava ja mahdollisesti otettava kantaa. Toimenpiteet voivat kuitenkin tapauskohtaisesti johtaa eskalaatioon, jos toimenpiteiden kohteena oleva valtio näin katsoo. Tosin lähtökohtaisesti toimenpiteiden suorittaja pyrittäisiin pitämään aina salassa.

Ehdotuksella voidaan toisaalta olettaa olevan positiivinen vaikutus Suomen maineeseen samanmielisten valtioiden keskuudessa.

Mahdollisuus suorittaa Suomen rajan ulkopuolella olevaan tietojärjestelmään kohdistettavia toimenpiteitä voi parantaa Suomen asemaan kansainvälisesti ystävällismielisten valtioiden parissa ja näin ollen antaa mahdollisuuksia aiempaa syvemmälle yhteistyölle ja -toiminnalle. Lisäksi suoritettujen toimenpiteiden myötä niiden voidaan arvioida nostavan kynnystä suorittaa Suomeen kohdistuvia haitallisia kybertoimenpiteitä.

Uusien hakuehtojen määrittämisen voidaan osaltaan katsoa parantavan Suomen asemaa kansainvälisessä yhteistoiminnassa. Suomen maantieteellisen aseman ja osaamisen perusteella voidaan arvioida, että Suomella on hyvät edellytykset hakuehtojen määrittämiseen ja tätä kautta hankittujen tietojen avulla parempaan asemaan kansainvälisillä foorumeilla.

Tietolähteen rajanylityksessä avustamisella voi olla myös vaikutuksia Suomen kansainvälisiin suhteisiin etenkin, jos tietolähde on ollut lähtömaansa yhteiskunnassa korkeassa asemassa.

5 Muut toteuttamisvaihtoehdot

5.1 Vaihtoehdot ja niiden vaikutukset

Nykytilan säilyttämistä ei pidetä tarkoituksenmukaisena vaihtoehtona jo siitäkin syystä, että sotilastiedustelusta annetun lain säätämisen yhteydessä eduskunta (HaVM 35/2022 vp) on edellyttänyt, että hallitus huolehtii lainsäädännön ajantasaisuudesta muuttuvassa toimintaympäristössä sekä varmistaa tiedustelutoiminnan ja sen valvonnan riittävät resurssit. Vallitsevassa maailmanpoliittisessa tilanteessa teknologia ja tietoliikenneyhteydet kehittyvät yhä kiihtyvässä tahdissa, mikä edellyttää myös sotilastiedusteluviranomaisten toimintatapojen kehittämistä. Tiettyyn pisteeseen saakka sotilastiedusteluviranomainen kykenee suuntaamaan toimintaansa muuttuvassa toimintaympäristössä myös voimassa olevin toimivaltuuksin, mutta käytännön tiedustelutoiminnassa on havaittu myös sellaisia muutostarpeita, jotka edellyttävät tiedustelulainsäädännön päivittämistä.

Tietoliikennetiedustelun kokonaisuus edellyttää sitä, että sotilastiedusteluviranomaisella on tieto globaalissa viestintäverkossa käytettävistä laitteista ja viestintäteknologiasta. Esityksessä ehdotetaan, että teknisten tietojen käsittelyssä sotilastiedusteluviranomainen voisi käsitellä teknisiä tietoja viestintäverkon osan määrittämisen lisäksi tietoliikenteen reitittymisen ja muutosten seuraamiseksi. Jos tarkoitettua analyysiä ei voitaisi tehdä, käytännössä sotilastiedusteluviranomainen ei voisi saada tietoa esimerkiksi siitä, mitä tietoliikenneteknologiaa sotilaallisesti Suomen kannalta merkittävässä valtiossa käytetään. Tieto käytettävistä tietoliikennelaitteista on erittäin merkittävää, jotta tietoliikennetiedustelu kohdistuu tarkoituksenmukaisesti ja toisaalta, että tietoliikenne saadaan purettua tulkittavaan muotoon.

Tietojen saaminen vieraan valtion viestintäverkkoa hallinnoivalta taholta on käytännössä mahdotonta. Toki tiedonhankinta saattaisi olla mahdollista muillakin keinoin tietyissä

tilanteissa, mutta se vie tarpeettomasti resursseja ja aiheuttaa merkittävää hengen ja terveyden vaaraa tietoa hankkivalle virkamiehelle.

Toisaalta yksityisten yhteisöjen velvollisuuksia voitaisiin laajentaa koskemaan laajasti viestintäverkon teknisiä tietoja, mutta tämä aiheuttaisi yrityksille kustannuksia. Laajoja tiedonluovutusvelvollisuuksia ei voida pitää myöskään EU-oikeuden näkökulmasta tarkoituksen mukaisena. Sotilastiedustelutoiminnan luonteen vuoksi liiallinen tukeutuminen ulkopuolisiin tahoihin ei ole myöskään toivottavaa.

Tietoliikennetiedustelun kokonaisuudessa uutena toimivaltuutena ehdotetaan hakuehtojen määrittämistä. Hakuehtojen määrittäminen on teknologisen kehityksen kiihtyvä tahti huomioon ottaen merkittävää. Ilman asianmukaisia hakuehtoja, tietoliikennetiedustelu ei kohdistu tarkoituksenmukaisesti.

Teknologisessa kehityksessä, jonka ajuri vallitsevassa maailmanpoliittisessa tilanteessa on sotilaallinen, esimerkiksi viestintäteknologiat saattavat muuttua nopeastikin ja niitä otetaan käyttöön laaja-alaisesti aiempaa nopeammassa tahdissa. Jos tiedustelun kohde ei enää käytäkään aiempaa viestintätekniikkaa, vaan vaihtaa sen kerralla täysin uuteen, eivät käytössä olevat hakuehdot enää kohdistu kohteena olevan toimijan tietoliikenteeseen. Näin ollen suomalainen tiedusteluviranomainen olisi käytännössä täysin kansainvälisen yhteistoiminnan varassa. Ottaen huomioon Suomen maantieteellisen aseman ja osaamisen, uusien hakuehtojen määrittämisellä saattaisi olla suurikin merkitys.

Teknisten tietojen käsittelyssä ja hakuehtojen määrittämisessä keskeistä on myös verrata tietoja historiatietoon. Näin tietoja pystytään varmentamaan tiettyyn pisteeseen ennen kuin esimerkiksi uutta hakuehtoa käytetään varsinaisessa tietoliikennetiedustelussa. Jos tästä ei pystyttäisi tekemään, saattaisi tämä johtaa tietoliikennetiedustelun käyttöön epätarkoilla hakuehdoilla ja tarpeettoman tiedon hankintaan.

Yhtenä vaihtoehtona voidaan katsoa olevan myös massamaisen tietoliikennetiedustelun salliminen, jossa tietoliikennetiedustelun kokonaisuuden eri osatoimivaltuuksista luovuttaisiin. Tämä ei kuitenkaan ole Suomen perustuslain mukaisesti mahdollista.

Ehdotettujen muutosten jättäminen tekemättä heikentäisi sotilastiedusteluviranomaisten kykyä toimia vallitsevassa turvallisuusympäristössä, jossa muut toimijat jatkuvasti kehittävät omia kyvykkyyksiään. Tämä voisi osaltaan vaarantaa sotilastiedustelun tarkoituksen eli tiedon tuottamisen ylimmän valtiojohdon päätöksenteon tukemiseksi ja Puolustusvoimien tehtävien suorittamiseksi.

5.2 Ulkomaiden lainsäädäntö ja muut ulkomailla käytetyt keinot

5.2.1 Euroopan ihmisoikeussopimus

Sotilastiedustelun toimivaltuuksien säätämisen sallittavuutta arvioitaessa suurin käytännön merkitys on Euroopan neuvoston piirissä vuonna 1950 tehdyllä Euroopan ihmisoikeussopimuksella (EIS; SopS 63/1999), johon Suomi liittyi vuonna 1989. Ihmisoikeussopimuksen noudattamista valvoo Euroopan ihmisoikeustuomioistuin (EIT), joka tässä tarkoituksessa käsittelee ja ratkaisee sopimusrikkomuksia koskevia valituksia. EIT on lukuisissa ratkaisuissaan ottanut kantaa siihen, miten ihmisoikeussopimuksen mukaista oikeutta luottamuksellisen viestin suojaan tulisi tulkita. Monet näistä ratkaisuista koskevat sähköistä viestintää ja muutamat tietoliikennetiedustelua tai siihen läheisesti rinnastuvia viranomaistoiminnan muotoja.

EIT:n tiedustelutoimintaa koskevasta keskeistä ratkaisukäytäntöä on arvioitu hallituksen esityksessä eduskunnalle laiksi sotilastiedustelusta (HE 203/2017 vp.) ja hallituksen esityksessä eduskunnalle siviilitiedustelulainsäädännöksi (HE 202/2017 vp.). Seuraavassa EIT:n käytäntöä käsitellään keskittyen ennen kaikkea uudempaan EIT:n ratkaisukäytäntöön.

Yksityiselämän suoja (EIS 8 artikla)

EIS 8(1) artiklan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. EIS 8(2) artiklan mukaan oikeus ei kuitenkaan ole rajoittamaton, sillä viranomaiset saavat puuttua sen käyttämiseen silloin, kun laki sen sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.

Euroopan ihmisoikeustuomioistuimen (EIT) vakiintuneen ratkaisukäytännön mukaan EIS 8(1) artiklassa mainitut yksityiselämän ja kirjeenvaihdon käsitteet pitävät sisällään sekä puhelinviestinnän, sähköpostiviestinnän muun luottamukselliseksi tarkoitetun sähköisen viestinnän (mm. Klass ja muut v. Saksa, 6.9.1978, Kopp v. Sveitsi, 25.3.1998, Copland v. Yhdistynyt Kuningaskunta, 3.4.2007, Liberty ja muut v. Yhdistynyt Kuningaskunta, 1.7.2008)). Suojan piirissä ovat sekä viestinnän sisältö että viestinnän tunnistamistiedot (mm. Malone v. Yhdistynyt Kuningaskunta, Weber ja Saravia v. Saksa, P.G. ja J.H. v. Yhdistynyt Kuningaskunta). Tunnistamistietojen osalta EIT on erikseen todennut, että tiedot esimerkiksi niistä puhelinnumeroista, joihin henkilö on viestinyt, muodostavat viestinnän elimellisen osan. Tällaistenkin tietojen luovuttaminen viranomaiselle ilman viestijän suostumusta muodostaa puuttumisen tämän yksityiselämään (Malone v. Yhdistynyt Kuningaskunta).

Viranomaisen ei tarvitse tosiasiassa käsitellä tietoja, jotta kyse olisi yksityiselämään puuttumisesta, vaan puuttumiseksi on katsottava jo se, että viranomainen kerää ja tallentaa niitä myöhempää käyttöä varten (Marper v. Yhdistynyt Kuningaskunta). Pelkkä sellaisen lainsäädännön olemassaolokin, joka mahdollistaa viestintäyhteyksien salaisen tarkkailun, puuttuu viestinnän osapuolten ja myös potentiaalisten osapuolten EIS 8 artiklan takaamiin oikeuksiin (Klass v. Saksa, Liberty ja muut v. Yhdistynyt Kuningaskunta). Valvonnan potentiaalisilla kohteilla on tällöin oltava oikeus EIS 13 artiklan takaamaan tehokkaaseen oikeussuojakeinoon kansallisen viranomaisen edessä. EIS 13 artiklan mukaan jokaisella, jonka yleissopimuksessa tunnustettuja oikeuksia ja vapauksia on loukattu, on oltava käytettävissään tehokas oikeussuojakeino kansallisen viranomaisen edessä siinäkin tapauksessa, että oikeuksien ja vapauksien loukkauksen ovat tehneet virantoimituksessa olevat henkilöt.

Vaikka henkilöön kohdistuvan salaisen valvonnan todennäköisyys olisi vähäinen, on hänen voitava tutkituttaa väitteensä EIS 8 artiklan mukaisten oikeuksiensa loukkaamisesta EIT:ssä, jos tehokkaat kansalliset oikeussuojakeinot puuttuvat (Kennedy v. Yhdistynyt Kuningaskunta).

Siitä, että sekä viestinnän sisältö että viestinnän tunnistamistiedot nauttivat EIS 8 artiklan mukaista suojaa, ei seuraa, että viranomaiset eivät niihin voisi puuttua. Yksityiselämään puuttuminen voi olla verrattain laajamittaistakin, kun se tapahtuu EIS 8 artiklan edellyttämissä puitteissa. EIS 8 artikla asettaa kolme ehtoa sille, että artiklan takaamiin oikeuksiin voidaan viranomaistoiminnassa puuttua: 1) puuttumisen on oltava kansallisen lain sallimaa, 2) sen on tapahduttava tiettyjen artiklassa erikseen lueteltujen etujen turvaksi ja 3) puuttumisen on oltava demokraattisessa yhteiskunnassa välttämätön. Yksi yksityiselämän ja siten myös

luottamuksellisen viestinnän suojaan puuttumisen mahdollistavista eduista on kansallinen turvallisuus.

EIS 8 artiklan takaamiin oikeuksiin puuttumisen on perustuttava kansalliseen lakiin. Vaatimuksen merkitys korostuu varsinkin silloin, kun oikeuksiin puututaan kohteelta salassa. Viranomaisen harkintavallan rajat ja harkintavallan käyttämisen tavat on riittävän selkeästi määriteltävä laissa, jotta voidaan torjua toimeenpanovallan salaiseen käyttöön sisältyvän mielivallan mahdollisuus (Malone v. Yhdistynyt Kuningaskunta, Amann v. Sveitsi, Telegraaf Media Nederland Landelijke Media B.V. ja muut v. Alankomaat, Rotaru v. Romania).

EIT on ratkaisuissaan toistuvasti korostanut sitä, että yksityiselämän suojaan puuttuvan, salaiset viranomaistoimenpiteet mahdollistavan lain on oltava oikeusvaltioperiaatteiden mukainen, kansalaisten saatavilla sekä laadultaan sellainen, että kansalaiset kykenevät ennakoimaan sen soveltamisen seuraukset omalta osaltaan (mm. Kruslin v. Ranska, Huvig v. Ranska, Lambert v. Ranska).

Kansallinen turvallisuus on yksi niistä eduista, joka EIS 8(2) artiklan mukaan voi oikeuttaa puuttumisen yksityiselämän suojaan. EIT on oikeuskäytännössään vain harvoin kyseenalaistanut vastaajavaltioiden väitteet siitä, että puuttuminen on tapahtunut kansallisen turvallisuuden vuoksi. Valtioilla vaikuttaisi olevan varsin laaja harkintamarginaali sen suhteen, millaisen toiminnan ne katsovat vaarantavan kansallista turvallisuuttaan ja siten voivan oikeuttaa EIS 8 artiklan takaamiin oikeuksiin puuttumisen. Taustalla on se, että kansallinen turvallisuus kuuluu perinteisesti valtiosuvereenisuuden piiriin (Bucur ja Toma v. Romania). EIT:n ratkaisukäytännön perusteella on selvää, että ainakin sotilaallinen maanpuolustus, terrorismin torjunta ja laittoman tiedustelutoiminnan torjunta kuuluvat kansallisen turvallisuuden piiriin (mm. Klass v. Saksa, Weber ja Saravia v. Saksa). Kansalliseen turvallisuuteen saattaa kuitenkin kohdistua monenlaisia uhkia, joita on vaikea ennakoida tai määritellä etukäteen. Tästä seuraa, että käsitteen selventäminen on ensisijaisesti jätettävä kansallisen käytännön varaan (Kennedy v. Yhdistynyt Kuningaskunta). Valtioiden harkintavaltaa saattaa omalta osaltaan lisätä se, että kansallisen turvallisuuden raja muihin sallittuihin perusteisiin (mm. yleinen turvallisuus ja epäjärjestyksen tai rikollisuuden estäminen) puuttua EIS 8(1) artiklan takaamiin oikeuksiin, voidaan tapauskohtaisesti mieltää häilyväksi.

Edellä kuvattuja tapauksia voidaan pitää EIT:n ratkaisukäytännön perustavina tapauksina, joihin vedotaan ja joita kehitetään EIT:n uudemmassa käytännössä. EIT:n uudemmasta ratkaisukäytännöstä voidaan nostaa esiin ratkaisu asiassa Roman Zakharov v. Venäjä, jossa EIT totesi salaisen tiedustelutoiminnan loukanneen ihmisoikeuksia. Valittaja esitti kolmen puhelinoperaattorin loukanneen yksityiselämän suojaa. Ratkaisun taustalla oli muun muassa kaksi oikeuden päätöstä, jotka oikeuttivat operaattoreita jälkikäteiseen salakuunteluun sekä operaattoreiden standardisopimuksen lisäys, jonka mukaan liittymä saatettiin sulkea ja puhelutiedot luovuttaa lainvalvontaviranomaisille, mikäli puhelinta käytettiin terroristisen uhkauksen välineenä. EIT:n mukaan valtion kansallinen lainsäädäntö ei ollut riittävän yksityiskohtainen suojaamaan valittajan oikeutta yksityisyyteen. Oikeussuojakeinot eivät voi käytännössä toteutua, jos kohteille ei pääsääntöisesti ilmoiteta salaisesta tiedonhankinnasta tai jos henkilöt eivät ilmoittamisen jälkeen saa pyydettäessä tietoa seurannasta. EIT katsoi, että oikeussuojakeinojen toteuttamiseksi kohteille pitää ilmoittaa seurannasta, ja antaa siihen liittyviä tietoja, kun se ei enää vaaranna seurannan tarkoitusta. Merkittävää tapauksessa oli myös se, että EIT otti sen käsiteltäväksi, vaikka valittaja ei edes väittänyt olleensa itse loukkauksen uhri.

Tapauksessa Big Brother Watch ja muut v. Yhdistynyt kuningaskunta EIT tutki Yhdistyneen kuningaskunnan signaalitiedustelujärjestelmää. EIT katsoi edelleen, että valtioilla on laaja

harkintavalta päättää, millainen tiedustelujärjestelmä on tarpeen kansallisen turvallisuuden suojelemiseksi. Tiedustelujärjestelmä sinänsä ei rikkonut EIS:n artiklaa 8.

Tuomioistuin katsoi kuitenkin, että modernin viestintäteknologian muuttuvan luonteen vuoksi sen tavallinen lähestymistapa kohdennettuihin signaalitiedustelujärjestelmiin oli mukautettava kuvaamaan paremmin sen erityispiirteitä, joihin liittyivät sekä riski väärinkäytöksistä että oikeutettu tarve toiminnan salassapidolle.

Erityisesti tällainen järjestelmä oli alistettava päästä päähän -suojatoimille, eli kansallisella tasolla oli tehtävä arviointi kunkin signaalitiedustelun tiedon hankinnan prosessin vaiheen osalta toimenpiteiden tarpeellisuudesta ja suhteellisuudesta. Lisäksi signaalitiedustelujärjestelmän käyttäminen oli alistettava riippumattomalle lupaharkinnalle, jossa on käytävä ilmi operaation kohde ja laajuus. Järjestelmän käytön on myös oltava valvonnan ja riippumattoman jälkikäteisen valvonnan alaisena.

Tuomioistuin määritteli näin ollen useita keskeisiä kriteereitä, jotka oli selkeästi määriteltävä kansallisessa laissa ennen kuin tällaisen järjestelmän voitiin katsoa olevan sopusoinnussa EIS:n vaatimusten kanssa. Soveltaen näitä uusia kriteereitä Yhdistyneen kuningaskunnan signaalitiedustelujärjestelmään, tuomioistuin totesi, että Yhdistyneen kuningaskunnan järjestelmässä oli kolme puutetta. Puutteet koskivat: 1) riippumattoman valtuutuksen puuttumista signaalitiedustelun luville, 2) signaalitiedustelussa käytettävät hakuehdot ja niiden luokat eivät käyneet ilmi lupahakemuksesta ja 3) henkilöä koskevat hakuehtoja ja -luokkia ei tarvinnut ilmoittaa lupahakemuksessa.

EIT totesi, että vaikka Yhdistyneessä Kuningaskunnassa sinänsä oli toiminnalle riippumaton ulkopuolinen valvoja ja oikeudellinen elin, jonka tarkoituksena on tutkia kansalaisten sille osoittamia valituksia, nämä eivät kuitenkaan olleet riittäviä. EIT katsoi, että Yhdistyneen Kuningaskunnan lainsäädäntö ei kokonaisuutena arvioiden kyennyt pitämään kansalaisten yksityisyyteen puuttumista siinä, mikä oli välttämätöntä demokraattisessa yhteiskunnassa. Näin ollen Yhdistyneen kuningaskunnan katsottiin rikkovan EIS:n 8 artiklaa.

Tapauksessa Centrum för Rättvisa v. Ruotsi kantajana oli ruotsalainen säätiö, jonka tehtävänä on suojella yksilöiden perusoikeuksia ja vapauksia. Kantajana oleva säätiö vetosi siihen, että sen viestintää on voitu siepata ja tutkia signaalitiedustelun avulla tai että näin voisi tapahtua tulevaisuudessa. Kantaja vetosi, että sen viestintä tapahtui päivittäin sähköpostitse, puhelimitse ja faksilla henkilöiden ja yritysten kanssa Ruotsissa ja ulkomailla, usein arkaluonteisissa asioissa.

Suuri jaosto totesi viidentoista äänen enemmistöllä (kaksi vastaan), että oli tapahtunut ihmisoikeussopimuksen 8 artiklan loukkaus. Se totesi erityisesti, että vaikka Ruotsin laajamittaisen signaalitiedustelujärjestelmän keskeiset ominaisuudet täyttivät lain laadulle asetetut vaatimukset, järjestelmässä oli kuitenkin kolme puutetta: 1) ei ollut selvää sääntöä henkilötietoja sisältämättömän aineiston tuhoamisesta, 2) signaalitiedustelulaki tai muu asiaankuuluva lainsäädäntö ei edellyttänyt, että päätöstä tiedustelutiedon välittämisestä ulkomaisille kumppaneille tehdessä olisi otettu huomioon yksilöiden yksityisyydensuoja ja 3) eikä ollut olemassa tehokasta jälkikäteistä valvontaa. Näiden puutteiden vuoksi järjestelmä ei täyttänyt päästä päähän -valvonnan vaatimusta, se ylitti vastaajavaltiolle tässä suhteessa jätetyn harkintavallan eikä kokonaisuudessaan suojannut mielivaltaisuudelta ja väärinkäytösten riskeiltä.

EIT ei ratkaisussaan torju ehdottomasti ns. massavalvonnan (bulk interception regime) käyttöä. EIT katsoo, että sillä torjuttavien uhkien vakavuus, uhkien takana olevien henkilöiden kyky

toimia paljastumatta tietoverkoissa ja sähköisen viestinnän reitityksen ennakoimattomuus perustelevat kansallista turvallisuutta vaarantavien uhkien tunnistamiseen tähtäävän massavalvonnan käyttöönoton kuulumista kansallisen harkintamarginaalin alaan. EIT on pitänyt yleisemminkin harkintamarginaalia laajana kansallisen turvallisuuden turvaamisen keinovalikoiman valinnassa (mm. Big Brother Watch kohta 275 ja Centrum för Rättvisa kohta 365). EIT painottaa kuitenkin, että sekä kohdistettujen että massavalvontajärjestelmien sääntelyn tulee vallan väärinkäytön estämiseksi täyttää ainakin edellä mainitut vähimmäisvaatimukset.

EIT toteaa myös tapauksessa Centrum för Rättvisa (kohta 239–245), että puuttuminen EIT 8 artiklan suojaamaan yksityiselämän suojaan on eri tasoista tietoliikenteeseen kohdistuvan tiedustelun eri vaiheissa. EIT jakaa prosessin neljään vaiheeseen: 1) tietoliikenteen hankkimiseen, 2) hakuehtojen tai hakuehtojen luokkien käyttäminen tietoliikenteen valikoimiseen, 3) suodatetun tietoliikenteen analysointi ja 4) tiedon säilyttäminen ja lopputuotteen tekeminen ja sen käyttäminen. Prosessin alussa tietoliikenteen hankkiminen, vaikka kattaakin suuren joukon ihmisiä, ei puutu henkilön yksityisyyden suojaan yhtä mittavasti kuin esimerkiksi vaiheessa kolme, jossa analyytikko tutkii suodatettua viestintää ja siihen liittyviä tietoja yhdistelemällä niitä.

EIT kiinnittää erityistä huomiota myös siihen, että ruotsalaista sääntelyä ja järjestelmää on jatkuvasti arvioitu ja tarvittaessa uudistettu myös yksityisyyden suojan parantamiseksi (kohta 351).

EIT katsoi tapauksessa myös, että Ruotsin laissa säädetty mahdollisuus kerätä tietoliikennettä signaalitiedustelun kehittämiseksi on kansallisen harkintamarginaalin rajoissa (päätöksen kohdat 291–293).

Keskeistä tapauksissa Big Brother Watch ja Centrum för Rättvisa on, että EIT kehitti oikeuskäytäntöään signaalitiedustelulle asetettavista lainsäädännöllisistä edellytyksistä (Big Brother Watch kohdat 343–361 ja Centrum för Rättvisa kohdat 257–278); Weber ja Saravia tapauksesta vakiintuneen lainsäädännölle asetettavan kuuden vaatimuksen sijaan (Weber ja Saravia kohta 95) EIT edellytti kahdeksan vaatimuksen täyttymistä (Big Brother Watch kohta 361 ja Centrum för Rättvisa kohta 275). Signaalitiedustelua koskevassa lainsäädännössä on säädettävä 1) perusteista, joiden perusteella tiedon hankinta voidaan sallia, 2) olosuhteista, joissa tiedonhankinta voi kohdistua henkilön viestintään, 3) luvan myöntämismenettelystä, 4) tiedon valinnassa, tutkimisessa ja käytössä noudatettavista menettelyistä, 5) varotoimista, joita on noudatettava luovutettaessa materiaalia eri osapuolille, 6) toimenpiteen kestosta, tiedon säilyttämisen rajoituksista ja olosuhteista, joissa tieto on poistettava ja tuhottava, 7) menettelyistä ja yksityiskohtaisista säännöistä, joilla riippumaton viranomainen valvoo edellä mainittujen takeiden noudattamista, ja valvojan valtuudesta puuttua lainvastaiseen toimintaan sekä 8) riippumattomasta jälkikäteisestä valvonnasta ja seuraamuksista.

Tehokkaat oikeusturvakeinot (13 artikla)

EIS 13 artiklan mukaan jokaisella, jonka EIS:n yleissopimuksessa tunnustettuja oikeuksia ja vapauksia on loukattu, on oltava käytettävissään tehokas oikeussuojakeino (”effective remedy”) kansallisen viranomaisen edessä siinäkin tapauksessa, että oikeuksien ja vapauksien loukkauksen ovat tehneet virantoimituksessa olevat henkilöt. Artiklan toteutumiseen liittyy olennaisesti ilmoitusvelvollisuus tai viranomaisen toimenpiteiden kohteena olleen henkilön oikeus saada asiansa selvitettäväksi. EIS 13 artiklaan koskevaa EIT:n käytäntöä on käyty laajemmin läpi HE 203/2017:ssä (s. 52–56) ja HE 202/2017:ssä, joten tässä yhteydessä siinä

esitettyihin tapauksiin viitataan yleisellä tasolla tarpeen mukaan keskittyen EIT:n uudempaan ratkaisukäytäntöön.

Ihmisoikeussopimuksen 8 artiklan kohdalla EIT on todennut, että oikeussuojakeinojen tulee olla niin tehokkaita, kuin mahdollista ottaen huomioon salaisen viranomaistoiminnasta luonnostaan aiheutuvat rajoitukset (Klass ym. v. Saksan liittotasavalta). Rajoituksista huolimatta oikeusturvajärjestelyt katsottiin riittäviksi 13 artiklan valossa, koska henkilöllä oli oikeus saattaa asiansa lain täytäntöönpanoa valvovan komission käsiteltäväksi ja valtiosääntötuomioistuimeen.

Oikeussuojakeino ei ole tehokas silloin, kun valittajalta puuttuu valittamiseen vaadittava oikeus (locus standi). Tavallisesti edellytetään, että väitetyn loukkauksen kohteena olevalla henkilöllä on suora pääsy oikeussuojakeinoon ilman välikäsiä. Oikeussuojakeinon tulee olla käytännössä saatavilla, sekä sellainen, että tuomioistuin pystyy puuttumaan väitettyyn loukkaukseen. Esimerkiksi tapauksessa Smith ja Grady v. Yhdistynyt kuningaskunta (1999) kansalliset tuomioistuimet pystyivät puuttumaan vain joihinkin väitetyn yksityiselämän loukkauksen puoliin voimatta kuitenkaan tehdä artiklan 8 mukaista arviointia puuttumisen oikeutuksesta ja suhteellisuudesta.

Oikeussuojakeinon tehokkuus edellyttää annetun päätöksen täytäntöönpanoa. Muutoksenhaun menestyminen ei sellaisenaan riitä tekemään oikeussuojakeinoa 13 artiklan mukaiseksi, mikäli tuomioistuinratkaisulla tai muulla päätöksellä ei ole konkreettisia seurauksia. Oikeuskeino ei ole tehokas, jos viranomaisten toimet tai laiminlyönnit estävät sen käytön. Näin esimerkiksi silloin, kun valittaja on saanut tuomioistuimelta määräyksen, jota viranomaiset eivät kuitenkaan noudata. Kun eräiden maiden kohdalla on toistuvasti tullut ilmi merkittäviä viivästyksiä kansallisten tuomioistuinten antamien tuomioiden ja päätösten täytäntöönpanemisessa, on EIT oikeuskäytännössään korostanut, että kansallisessa oikeusjärjestelmässä tulee olla riittävät oikeussuojatakeet myös tämän tyyppisiä viivytyksiä vastaan.

EIT on useissa aiemmissa ratkaisuissaan ottanut kantaa kysymykseen siitä, tuleeko ja missä tilanteissa tiedonhankinnan kohdehenkilöllä olla oikeus saada viranomaiselta tieto häneen kohdistetusta tiedonhankintatoimenpiteestä. Tapauksissa Klass v. Saksa ja Weber ja Saravia v. Saksa EIT piti ihmisoikeussopimuksen kannalta hyväksyttävänä sääntelyä, jonka mukaan tiedonhankinnan kohteelle oli ilmoitettava heti, kun ilmoittaminen ei enää vaarantanut tiedonhankinnan tarkoitusta. EIT kiinnitti huomiota myös siihen, että Saksan järjestelmässä ilmoittamisen ja toiselta puolen ilmoittamatta jättämisen edellytysten käsillä olon arviointi kuului riippumattomalle elimelle (G10-komissio), ei turvallisuusviranomaiselle.

Tapauksissa Association for European Integration and Human Rights ja Ekimdzhiev v. Bulgaria ja Dumitru Popescu v. Romania EIT totesi, että kansallinen sääntely, jonka mukaan tiedonhankinnan kohteelle ei tarvitse lainkaan ilmoittaa, on yleensä ihmisoikeussopimuksen vastainen. Arvioidessaan Venäjän lainsäädäntöä (Zakharov v. Venäjä) EIT totesi, ettei se edellyttänyt tiedonhankinnan kohdehenkilölle ilmoittamista missään tilanteessa. Kohdehenkilöllä oli mahdollisuus tulla tietoiseksi häneen kohdistetusta tiedonhankinnasta ainoastaan siinä tapauksessa, että häntä vastaan nostettiin rikossyyte. Kun suuri valtaosa tiedonhankinnan kohdehenkilöistä ei näin ollen ikinä saanut tietoa heihin kohdistetusta tiedonhankinnasta, eivät he myöskään voineet hakea oikeussuojaa lainvastaista viranomaistoimintaa vastaan. Venäjän lain sinänsä tunnustama kantelumahdollisuuden käyttö edellytti, että kantelija kykeni tarkoin yksilöimään kantelun kohteena olevan päätöksen, eikä tämä luonnollisesti ollut mahdollista, jos henkilö ei ollut lainkaan tietoinen päätöksen olemassaolosta. Edellä sanotun perusteella EIT katsoi, ettei Venäjän laki säätänyt EIS 13 artiklan edellyttämistä tehokkaista oikeussuojakeinoista.

Välttämätön demokraattisessa yhteiskunnassa -edellytykseen liittyy osaltaan myös vaatimus oikeussuojan saatavuudesta kansallisesti. Sopimusvaltion tuomioistuimen tai muun vastaavan elimen on voitava vähintään jälkikäteen varmistaa, että EIS 8 artiklan mukaisiin oikeuksiin puuttuminen oli yksittäistapauksessa suhteellista ja välttämätöntä. Tämä merkitsee sitä, että tiedonhankinnan kohdehenkilön on voitava valittaa tai kannella häneen kohdistetusta tiedonhankintatoimenpiteestä.

Valitus- tai kantelumahdollisuuden käytön edellytyksenä yleensä on, että henkilö saa viranomaiselta tiedon häneen kohdistetusta tiedonhankinnasta sen jälkeen, kun tiedonhankintakeinon käyttö on päättynyt (ks. yllä Zakharov v. Venäjä). Tästä ei kuitenkaan seuraa, että ilmoitus on tehtävä välittömästi tiedonhankinnan päätyttyä. Uhka, josta tiedonhankintamenetelmän avulla on hankittu tietoja, voi jatkua vuosia tai jopa vuosikymmeniä, jolloin ilmoituksen tekemistä on turvallisuusviranomaisten toiminnan suojaamiseksi välttämätöntä lykätä vastaavasti. Oikeussuojakeinon käytön mahdollistamiseksi ilmoitus olisi kuitenkin tehtävä sen jälkeen, kun ilmoittamatta jättämiselle ei enää ole yksilöllistä perustetta (Klass v. Saksa, Zakharov v. Venäjä).

Kuitenkin myös järjestelmä, joka ei lainkaan edellytä kohdehenkilölle ilmoittamista, voi olla sopusoinnussa ihmisoikeussopimuksen kanssa. Tällöin kanteluoikeus on tullut kansallisessa lainsäädännössä säätää niin yleiseksi, että kuka hyvänsä saa kannella pelkästään sen perusteella, että epäilee viranomaisten puuttuneen luottamuksellisen viestintänsä nauttimaan suojaan (Kennedy v. Yhdistynyt Kuningaskunta).

Uudemmassa ratkaisukäytännössään EIT on todennut tapauksessa Centrum för Rättvisa, että tehokkaan oikeusturvakeinon olisi oltava kaikkien niiden käytettävissä, jotka epäilevät joutuneensa salaisten viranomaistoimenpiteiden kohteeksi. EIT on todennut kohdennettujen salaisten viranomaisen toimenpiteiden osalta, että jälkikäteinen ilmoittaminen toimenpiteestä kohteelle tarjoaa riittävän tehokkaan oikeussuojan toimenpiteiden väärinkäyttöä vastaan. Toisaalta EIT on myös todennut, että järjestelmä, jossa kuka tahansa kohteeksi joutumista epäilevä henkilö voi käyttää oikeusturvakeinoa riippumatta ilmoituksesta, voi olla riittävä (Rättvisa kohta 271 sekä siinä viitatut Roman Zakharov v. Venäjä ja Kennedy v. Yhdistynyt Kuningaskunta).

EIT katsoo tapauksessa Centrum för Rättvisa, että oikeussuojakeinot, jotka eivät ole riippuvaisi ilmoituksesta, voivat olla myös tehokkaita tietoliikenteeseen kohdistuvassa tiedustelussa ja olosuhteiden mukaan voivat tarjota parempaa suojaa henkilölle kuin ilmoitukseen sidotut oikeussuojakeinot (tapauksen kohta 272). Etenkin tilanteessa, jossa salaiset viranomaisen toimenpiteet kohdistuvat kyseisen valtion ulkopuolella oleviin kohteisiin ja valtion ulkopuolella oleviin henkilöihin ja vaikka kohteen henkilöllisyys olisi sinänsä tiedossa, toimenpiteestä ilmoittamisella voi olla vähän tai käytännössä ei lainkaan merkitystä. Etenkin, jos henkilön olinpaikasta ei ole tietoa (tapauksen kohta 272).

EIT painotti useiden itsenäisten tiedustelutoimintaa valvovien elimien olemassaolon merkitystä järjestelmän hyväksyttävyydelle. Oikeusturvamekanismien lukuisuus kompensoi myös sitä, että tiedustelutoimista ei aina ilmoiteta niiden kohteelle. Valvontajärjestelmän osalta tuomiossa Centrum för Rättvisa kiinnitetään huomiota riippumattomuuteen ja valvonnassa esitettyjen huomioiden tosiasialliseen vaikuttavuuteen.

Tilanteessa, jossa ilmoitusvelvollisuutta ei ole, oikeusturvakeinon tehokkuuden kannalta on välttämätöntä, että sitä toteuttaa viranomaisesta riippumaton taho, joka takaa oikeudenmukaisen käsittelyn ja tarjoaa mahdollisuuksien mukaan kontradiktorisen menettelyn. Tällaisen viranomaisen päätökset on perusteltava ja niiden on oltava oikeudellisesti sitovia muun muassa

laittoman viestinnän kuuntelun lopettamisen ja laittomasti hankitun ja/tai tallennetun kuunteluaineiston hävittämisen osalta (tapauksen kohta 273 sekä siinä viitatut tapaukset Segerstedt-Wiberg ja muut v. Ruotsi ja Leander v. Ruotsi).

Ruotsalaisessa järjestelmässä valvovalla valtuutetulla on lähtökohtainen läsnäolovelvollisuus tuomioistuinmenettelyssä, pääsy asian kannalta merkityksellisiin asiakirjoihin ja oikeus lausua tuomioistuimessa niiden johdosta. EIT:n mielestä tällainen järjestely kompensoi osittain tuomioistuinmenettelyyn ja tuomioistuimen päätöksiin kohdistuvia julkisuuden rajoituksia (tapauksen kohdat 137–138).

EIT toteaa Ruotsin lainsäädäntöä arvioidessaan, että Ruotsin valvovalla viranomaisella on tarvittavat toimivaltuudet valvoa Ruotsin signaalitiedustelua alusta loppuun. Valvova taho pystyy arvioimaan laajasti signaalitiedusteluviranomaisen toimintaa eri näkökohdista, mukaan lukien tietoliikenteen hankinnan, analysoinnin, käytön ja hävittämisen. Keskeistä oli myös se, että valvoja pystyy arvioimaan käytettyjä hakuehtoja. Vaikka valvoja pystyy tietyiltä osin antamaan vain suosituksia tai ohjeistuksia (ei oikeudellisesti velvoittavia), EIT katsoi, että valvojalla on kuitenkin tämän lisäksi mahdollisuus keskeyttää tai että tallenteet ja muistiinpanot on tuhottava. Näillä toimenpiteillä oli myös oikeudellinen sitovuus. Oikeudellisesti sitomattomien suositusten ja ohjeistusten osalta EIT totesi, että signaalitiedusteluviranomainen oli käytännössä aina noudattanut niitä ja yhdessä tapauksessa asia oli saatettu hallituksen jatkokäsiteltäväksi (kohdat 347–350).

EIT totesi Ruotsin valvovan viranomaisen tehneen kahdeksassa vuodessa 102 tarkastusta ja tekevän vuosittaisen julkisen katsauksen (tapauksen kohdat 351–352). Näin ollen EIT totesi, ettei ole epäilystä siitä, etteikö ruotsalainen lainsäädäntö ja käytäntö tarjonneet tehokasta signaalitiedustelun valvontaa. EIT:n mukaan valvovan viranomaisen rooli sen kanssa, että valvonta osallistui myös asioiden arvioimiseen ennen päätöksen tekoa, yhdessä takaavat signaalitiedustelussa toimivan oikeusturvatakeen viranomaisen mielivaltaa vastaan (tapauksen kohta 353).

EIT toteaa Centrum för Rättvisa tapausta arvioidessaan, että oikeussuojakeinojen, jotka eivät ole riippuvaisia ilmoituksesta, on oltava toimenpiteen kohteeksi joutuneeksi epäilevien käytettävissä (tapauksen kohta 355). EIT toteaa, että Ruotsin lainsäädäntö antoi henkilöille mahdollisuuden saattaa asiansa tutkittavaksi (tapauksen kohta 356). EIT kuitenkin totesi, että Ruotsin järjestelmässä toimivaltainen valvonnasta vastaava elin (SIUN) myöntää myös luvat tietoliikenteeseen kohdistuvaan tiedonhankintaan. Näin ollen jälkikäteistä valvontaa suorittavaa ja henkilön oikeussuojasta huolehtivaa viranomaista ei voitu pitää erityisen objektiivisena tai sen suorittamaa käsittelyä perusteellisena. Myös kysymys eturistiriidasta nousee esiin, mikä voi houkutella käsiteltävänä olevan asian kohdalla asian ylimalkaiseen käsittelyyn (kohta 359). Tosin SIUN on myös ulkopuolisen valvonnan kohteena, mutta tällaista valvontaa käytännössä ei oltu koskaan suoritettu eikä tällaista lakisääteistä tehtävää oltu varsinaisesti myöskään säädetty (tapauksen kohta 360).

EIT katsoi, että SIUN:n kaksoisrooli heikensi tietoliikenteeseen kohdistuvan tiedonhankinnan jälkikäteistä valvontaa siinä määrin, että se aiheuttaa riskejä asianomaisten henkilöiden perusoikeuksien toteutumiselle (tapauksen kohta 372). Osaltaan tämänkin takia EIT katsoi, että Ruotsin lainsäädäntö ei täyttänyt EIS:n 8 artiklan vaatimuksia (tapauksen kohta 373).

5.2.2 Kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus

Kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen (KP-sopimus, SopS 7–8/1976) 17 artiklassa määrätään muun muassa viestinnän suojasta. Artiklan 1

kohdan mukaan kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon ei saa mielivaltaisesti tai laittomasti puuttua eikä suorittaa hänen kunniaansa ja mainettaan loukkaavia hyökkäyksiä. Artiklan 2 kohdan mukaan jokaisella on oikeus lain suojaan tällaista puuttumista tai tällaisia hyökkäyksiä vastaan. KP-sopimuksen 2 artiklan 1 kohdassa sopimusvaltioille asetetaan velvollisuus ryhtyä toimenpiteisiin sopimuksessa, mukaan lukien 17 artiklassa, turvattujen oikeuksien suojaamiseksi.

Yksityiselämän suojaa koskevia määräyksiä on myös muissa YK:n ihmisoikeussopimuksissa, kuten lapsen oikeuksia koskevassa yleissopimuksessa (SopS 59 ja 60/1991), jonka 16 artiklassa määrätään lapsen oikeudesta yksityisyyden, perheen, kodin ja kirjeenvaihdon suo-jaan, sekä vammaisten henkilöiden oikeuksia koskevassa yleissopimuksessa (SopS 26 ja 27/2016), jonka 22 artiklassa määrätään vammaisen henkilön oikeudesta yksityisyyden, perheen, kodin ja kirjeenvaihdon suojaan.

KP-sopimuksen täytäntöönpanoa valvova YK:n ihmisoikeuskomitea on antanut tulkintakannanottoja yksityisyyden suojaa koskevasta yleissopimuksen 17 artiklasta. Artiklaa koskevassa ihmisoikeuskomitean yleiskannanotossa (General Comment no. 16, 8.4.1988) tämän sopimusmääräyksen on tulkittu pitävän sisällään valtion velvollisuuden itse pidättäytyä 17 artiklan vastaisista toimenpiteistä ja lisäksi puuttua yksityisten tekemiin loukkauksiin lainsäädännöllisin keinoin. Artiklan ilmaisu ”kirjeenvaihto” tarkoittaa myös muita viestinnän muotoja, kuten puhelinkeskustelua ja sähköpostia. Kaikenlainen yksityisen viestinnän pidättäminen, sensurointi, tarkastus tai julkaiseminen muodostaa puuttumisen kirjeenvaihtoon.

Sopimuksen 17 artiklassa ei luetella perusteita, joilla artiklassa turvattuja oikeuksia voitaisiin rajoittaa. Artiklassa ainoastaan nimenomaisesti kielletään mielivaltaiset ja laittomat puuttumiset oikeuksiin. Mielivaltaisen puuttumisen kiellolla tavoitellaan sitä, että myös lakiin perustuvien puuttumisten tulee olla KP-sopimuksen määräysten ja tarkoituksen mukaisia ja kohtuullisia kussakin tapauksessa. Oikeuskirjallisuuden mukaan tulkinta-apua hyväksyttäville rajoitusperusteille on löydettävissä KP-sopimuksen muiden artiklojen rajoittamiskriteereistä ja Euroopan ihmisoikeussopimuksen 8 artiklassa tarkoitetuista rajoitusperusteista.

KP-sopimuksen 4 artiklan mukaan sopimusvelvoitteesta voidaan poiketa ainoastaan yleisen kansallista olemassaoloa uhkaavan hätätilan aikana. Tällaisen hätätilan tulee olla virallisesti sellaiseksi julistettu. Tällöin sopimusvaltiot voivat ryhtyä toimenpiteisiin, jotka merkitsevät poikkeamista niille KP-sopimuksen mukaan kuuluvista velvoituksista siinä laajuudessa kuin tilanne välttämättä vaatii. Lisäedellytyksenä on se, että tällaiset toimenpiteet eivät ole ristiriidassa valtion muiden kansainvälisen oikeuden mukaisten velvoitusten kanssa eivätkä merkitse pelkästään rotuun, ihonväriin, sukupuoleen, kieleen, uskontoon tai yhteiskunnalliseen syntyperään perustuvaa syrjintää.

KP-sopimuksen täytäntöönpanoa valvova YK:n ihmisoikeuskomitea on viimeisimmissä vuonna 2021 antamissaan Suomea koskevissa loppupäätelmissä (CCPR/C/FIN/CO/7) kehottanut sopimusvaltiota varmistamaan, että (a) kaiken tyyppistä, sekä siviili- että sotilastoimijoiden harjoittamaa, valvontaa ja puuttumista yksityiselämään, kuten verkkovalvontaa, telekuuntelua, viestintätietojen hankkimista ja tiedonhakua, säännellään asianmukaisella lainsäädännöllä, joka on sopusoinnussa yleissopimuksen, etenkin sen 17 artiklan, kanssa, laillisuus-, suhteellisuus- ja välttämättömyysperiaate mukaan lukien; ja (b) valvonta ja telekuuntelu edellyttävät tuomioistuimen antamaa lupaa, niitä valvotaan tehokkaiden ja riippumattomien järjestelmien avulla, ja niiden kohteena olevilla henkilöillä on asianmukaisesti käytettävissään tehokkaat oikeuskeinot oikeudenloukkaustapauksissa.

YK:n ihmisoikeusneuvostossa on hyväksytty useita raportteja yksityiselämän suojasta digitalisaation aikakaudella (A/HRC/27/37 (2014), A/HRC/39/29 (2018), A/HRC/48/31 (2021) ja A/HRC/51/17(2022)). YK:n ihmisoikeusneuvosto on myös kiinnittänyt huomiota lähdesuojan varmistamiseen toimittajien turvallisuutta koskevassa päätöslauselmassaan (A/HRC/RES/51/9 (2022)).

5.2.3 Euroopan unionin oikeus

EU:n perusoikeuskirjan (EUVL C 326, 26.10.2012) määräykset koskevat sen 51 artiklan 1 kohdan mukaan unionin toimielimiä, elimiä ja laitoksia toissijaisuusperiaatteen mukaisesti sekä jäsenvaltioita ainoastaan silloin, kun viimeksi mainitut soveltavat unionin oikeutta. EU:n perusoikeuskirjaa ei siten sovelleta tilanteissa, joissa on kysymys ainoastaan kansallisen lain soveltamisesta ja joita EU-oikeudessa ei säännellä. Kuitenkin EU-oikeuden soveltamisalan ulkopuolellakin perusoikeuskirjasta voidaan johtaa tulkinta-apua esimerkiksi tilanteissa, joissa Euroopan ihmisoikeustuomioistuin ei ole käsitellyt jotakin oikeutta tai siihen liittyvää kysymystä, josta on olemassa EU-tuomioistuimen oikeuskäytäntöä.

Perusoikeuskirjan 7 artiklan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa sekä viesteihinsä kohdistuvaa kunnioitusta. Perusoikeuskirjan 8 artiklan mukaan puolestaan jokaisella on oikeus henkilötietojensa suojaan. Henkilötietojen suojaan kuuluvien tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava laissa määritettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty ja saada ne oikaistuiksi. Riippumattoman viranomaisen on valvottava näiden sääntöjen noudattamista.

Perusoikeuskirjan 52 artikla määrää perusoikeuskirjalla turvattujen oikeuksien kattavuudesta. Artiklan 1 kappaleen mukaan perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla, ja kyseisten oikeuksien ja vapauksien olennaista sisältöä noudattaen. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan tehdä ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia. Saman artiklan 3 kappaleen mukaan, siltä osin kuin perusoikeuskirjan oikeudet vastaavat ihmisoikeuksien ja perusvapauksien suojaamista koskevassa eurooppalaisessa yleissopimuksessa taattuja oikeuksia, niiden merkitys ja kattavuus ovat samat kuin mainitussa yleissopimuksessa. Tämä ei kuitenkaan estä unionia määräämästä tätä laajemmasta suojasta.

Perusoikeuskirjan 52 artiklan 3 kohdasta seuraa, että perusoikeuskirjan 7 artiklan sisältö vastaa EIS 8 artiklan sisältöä. Perusoikeuskirjan johdannossa todetaan erikseen, että vahvistettavat oikeudet perustuvat paitsi Euroopan ihmisoikeussopimukseen, myös Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöön. EIT:n laajalla ihmisoikeussopimuksen 8 artiklaa koskevalla ratkaisukäytännöllä on näin ollen katsottava olevan relevanssia myös perusoikeuskirjan 7 artiklan tulkinnalle(lausunto EU:n liittymisestä Euroopan ihmisoikeussopimukseen, 2/13, EU:C:2014:2454, 170 kohta; tuomio Kadi ja Al Barakaat, C-402/05 ja C-415/04 P, 281–285 kohta; tuomio Internationale Handelsgesellschaft, C-11/70, 4 kohta.

Tiedustelulainsäädännön yhteydessä merkityksellisiä ovat EU-lainsäädäntöön sisältyvät poikkeukset, joiden perusteella EU-oikeuden soveltuminen on useissa säädöksissä rajattu kansallista turvallisuutta koskevien asioiden ulkopuolelle. Poikkeukset perustuvat Euroopan unionista tehdyn sopimuksen 4 artiklan 2 kohdan määräykseen, jonka mukaan kansallinen turvallisuus säilyy yksinomaan kunkin jäsenvaltion vastuulla. Unionilla ei siten ole kansallista turvallisuutta koskevaa toimivaltaa. EU-oikeuden soveltamisalan rajautuminen pois kansallista

turvallisuutta koskevan poikkeuksen perusteella ei kuitenkaan ole aina käytännössä yksiselitteistä. EU:n oikeusjärjestyksellä ja eräillä Euroopan unionin tuomioistuimen ennakkoratkaisuilla ja EU-lainsäädännön kumoamiskanteilla on siten merkitystä myös tiedustelutoiminnalle ja sitä koskevan kansallisen lainsäädännön kehittämiselle. Jäsenvaltion, joka vetoaa edukseen kansallista turvallisuutta koskevaan perusteeseen, on näytettävä toteen tarve turvautua kyseiseen perusteeseen (tuomio ZZ, C-300/11; tuomio Insinööritoimisto InsTiimi Oy, C-615/10, 35 kohta; tuomio komissio v. Suomi, C-284/05, 45 ja 47 kohta).

Poikkeuksen ei kuitenkaan voida katsoa olevan ehdoton, vaan tiedusteluviranomaisten toiminta saattaa tietyissä tilanteissa kuulua EU-oikeuden soveltamisalaan ja näin ollen kuulua EU:n perusoikeussääntelyn piiriin kansallisten perustuslaillisten säännösten ja kansainvälisten ihmisoikeussopimusten takaamien oikeuksien lisäksi. Kansallista turvallisuutta koskeva poikkeus ei näin ollen ole kaiken kattava poikkeus ja ei itsestään selvästi sulje pois kokonaan unionin oikeuden sovellettavuutta.

Unionin tuomioistuin on sittemmin vahvistanut tämän johtopäätöksen todeten, että kansalliseen turvallisuuteen vetoaminen ei voi oikeuttaa unionin oikeuden kiertämistä, perusoikeuskirjaan perustuva valvonta mukaan lukien. Tuomioistuin on selventänyt periaatetta liittyen jäsenvaltioiden järjestelyihin, joissa yleisesti ja erotuksetta on velvoitettu teleoperaattoreita säilyttämään viestintään liittyviä tietoja ja järjestämään niiden reaaliaikainen saatavuus tiedusteluviranomaisille kansallisen turvallisuuden suojaamiseksi. Tuomioistuin on myös määritellyt kansallisen turvallisuuden suojaamisen valtion elintärkeiden toimintojen ja yhteiskunnan perusetujen suojaamiseksi sekä valtion perusrakenteiden horjuttamiselta ja väestön uhkaamiselta suojaamiseksi (EUT yhdistetyt tapaukset C-511/18, C-512/18 ja C-520/10 kohdat 99 ja 135).

Tiedustelutoiminnan kannalta lähin yhteys on katsottava olevan niin kutsutulla data retention -sääntelyllä. Sähköisen viestinnän tietosuojadirektiivin tulkintaa koskeva Euroopan unionin tuomioistuimen oikeuskäytäntö kehittyy jatkuvasti. Tele2 Sverige -tuomion jälkeen paikka- ja liikennetietojen säilyttämistä ja käyttöä on arvioitu ainakin seuraavissa ratkaisuissa: tuomio Ministerio Fiscal, C-207/16; tuomio Privacy International, C-623/17; tuomio La Quadrature du Net ym., C-511/18, C-512/18 ja C-520/18; tuomio Prokuratuur, C-746/18; tuomio SpaceNet, C-793/19 ja C-794/19; tuomio Commissioner of An Garda Síochána, C-140/20; tuomio VD ja SR, C-339/20 ja C-397/20; tuomio Spetsializirana prokuratura, C-350/21; tuomio A. G. ja Lietuvos Respublikos generalinė prokuratūra, C-162/22; tuomio La Quadrature du Net ym., C-470/21; tuomio Procura della Repubblica presso il Tribunale di Bolzano, C-178/22. Euroopan unionin tuomioistuimen tulkintakäytännöllä on ollut vaikutusta rikosten torjuntaan liittyvään henkilötietojen käsittelyyn. Näissä yhteyksissä Euroopan unionin tuomioistuin on tulkinnut myös perusoikeuskirjan luottamuksellisen viestin salaisuuden suojaa koskevaa 7 artiklaa ja henkilötietojen suojaa koskevaa 8 artiklaa. Unionin tuomioistuin on katsonut, että kansallinen säännöstö, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on säilytettävä liikenne- ja paikkatiedot kansallisen turvallisuuden suojaamiseksi ja rikollisuuden torjumiseksi, kuuluu direktiivin 2002/58 soveltamisalaan (tuomio La Quadrature du Net ym., C-511/18, C-512/18 ja C-520/18, kohdat 100–104 ja tuomio Lietuvos Respublikos generalinė prokuratūra, C-162/22, kohta 28).

Unionin tuomioistuimen oikeuskäytännön mukaan "kun jäsenvaltiot panevat -- suoraan täytäntöön sähköisen viestinnän luottamuksellisuudesta poikkeavia toimenpiteitä asettamatta tällaisen viestinnän palveluntarjoajille käsittelyä koskevia velvollisuuksia, asianomaisten henkilöiden tietosuojaan ei sovelleta sähköisen viestinnän tietosuojadirektiiviä vaan ainoastaan kansallista oikeutta. Kyse ei kuitenkaan ole tällaisesta tilanteesta sillä "kaikki sähköisten viestintäpalvelujen tarjoajien suorittama henkilötietojen käsittely kuuluu [sähköisen viestinnän

tietosuojadirektiivin] soveltamisalaan, mukaan lukien käsittely, joka seuraa viranomaisten niille asettamista velvollisuuksista" (tuomio 6.10.2020, La Quadrature du Net ym., C-511/18, C-512/18 ja C-520/18, EU:C:2020:791, 101 kohta).

Sitä vastoin silloin, kun puuttuminen perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin, jota viranomaisten pääsy sähköisten viestintäpalvelujen tarjoajien säilyttämiin henkilöllisyyttä koskeviin tietoihin merkitsee, ilman, että mainittuja tietoja voidaan yhdistää suoritettua viestintää koskeviin tietoihin, ei ole vakavaa, koska näiden tietojen perusteella ei voida kokonaisuutena tarkasteltuna tehdä täsmällisiä päätelmiä niiden henkilöiden yksityiselämästä, joiden tiedoista on kyse, mainittu pääsy tietoihin voidaan oikeuttaa yleisesti rikosten ehkäisemisen, tutkinnan, selvittämisen ja syyteharkinnan alalla (ks. vastaavasti tuomio 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, 54, 57 ja 60 kohta).

Euroopan unionin tuomioistuin on myös katsonut, että tuomioistuimen vakiintuneessa oikeuskäytännössä on vahvistettu periaate, että kansallinen turvallisuus (sisältäen maanpuolustuksen) on yleisen edun mukainen tavoite ja kansallinen turvallisuus on merkittävämpi rajoitusperuste kuin rikostorjunta (tuomio 30.4.2024, La Quadrature du net ym., C470/21, kohta 97 ja vastaavasti tuomio 6.10.2020, La Quadrature du Net ym., C 511/18, C 512/18 ja C 520/18, EU:C:2020:791, 166 kohta).

Kaiken kaikkiaan jotkin seikat tiedusteluviranomaisten toiminnassa, kuten tietoliikenteeseen kohdistuva tiedonhankinta, ovat unionin oikeuden soveltamisalan ulkopuolella. EUT on myös korostanut, että salassa pidettävän tiedonhankinnan, joka on unionin oikeuden soveltamisalan ulkopuolella, olisi kuitenkin täytettävä EIS:n asettamat vaatimukset.

Tietosuojaa koskevassa oikeuskäytännössään EU-tuomioistuin on kiinnittänyt kaikkiaan huomiota muun muassa arvioinnin kohteena olevan järjestelyn valvontaan, käytettävissä oleviin riittäviin oikeussuojakeinoihin, tiedon antamiseen ja tietoturvaan sekä henkilöpiiriä, ennakkolupaa, tietoihin pääsyä, tietojen säilytysaikaa ja niiden hävittämistä koskeviin edellytyksiin (ks. tuomio Tele2 Sverige, C-203/15 ja C-698/15, 106–111, 117–119, 120–122 kohta; tuomio WebMind, C-419/14, 77–78 kohta; tuomio Schrems, C-362/14, 40 ja 95 kohta; tuomio Digital Rights Ireland, C-293/12 ja C-594/12, 56–67 kohta; tuomio UGT-Rioja ym., C-428/06 – C-434/06, 80 kohta). Erityisesti rikosten torjunnan osalta Euroopan unionin tuomioistuin on kiinnittänyt huomiota siihen, että pääsy matkapuhelimen tietoihin voi kattaa viestinnän sisällön ja välitystietojen lisäksi esimerkiksi valokuvia ja internetin selaushistorian. Pääsy tällaisten tietojen kokonaisuuteen voi mahdollistaa hyvin tarkkojen päätelmien tekemisen rekisteröidyn yksityiselämästä, kuten hänen päivittäisistä tottumuksistaan, vakituisista tai tilapäisistä oleskelupaikoistaan, päivittäisistä tai muista liikkumisistaan, suorittamistaan toimista ja sosiaalisista suhteistaan sekä sosiaalisista piireistä, joissa tämä henkilö liikkuu. Siten unionin tuomioistuin on katsonut, että matkapuhelimen tietoihin tutustuminen viranomaisen toimesta tarkoittaa perusoikeuskirjan 7 ja 8 artiklassa taattuihin perusoikeuksiin kohdistuvaa puuttumista, jota on pidettävä vakavana tai jopa erityisen vakavana (tuomio Bezirkshauptmannschaft Landeck, C-548/21, kohdat 92–93, 95).

Kootusti edellä viitatuista tuomioista voidaan tehdä johtopäätös, että oikeushyvien hierarkiassa kansallinen turvallisuus, sisältäen maanpuolustuksen, on korkeampi asema kuin rikosten torjunnalla. Näin ollen se on myös kauempana perusoikeuskirjan soveltamisesta. Lisäksi voidaan todeta, että tallennettavia tietoja ja niiden käsittelyä on arvioitava sen perusteella, miten syvällisiä päätelmiä niiden perusteella voidaan tehdä yksityishenkilön elämästä ja näin ollen tosiasiallisesti puuttuvat henkilön yksityiselämän suojaan.

5.2.4 Ulkomaiden lainsäädäntö

5.2.4.1 Ruotsi

Yleistä

Sotilastiedustelutoimintaa harjoittavat puolustusvoimien tiedustelu- ja turvallisuuspalvelu (Militära underrättelse- och säkerhetstjänsten, MUST), puolustusvoimien radiolaitos (Försvarets radioanstalt, FRA), puolustusvoimien materiaalilaitos (Försvaretsmaterielverk, FMV) sekä Kokonaismaanpuolustuksen tutkimuslaitos (Totalförsvarets forskningsinstitut, FOI).

Ruotsissa signaalitiedustelua puolustustiedustelussa ohjaa signaalitiedustelua koskeva laki (Lag om signalspaning i försvarsunderrättelseverksamhet, 2008:717) ja sitä täydentävä asetus (Förordning om signalspaning i försvarsunderrättelseverksamhet 2008:923). Puolustusvoimien radiolaitos (Försvarets radioanstalt, FRA) toimii kansallisena signaalitiedusteluviranomaisena.

Signaalitiedustelulain mukaan signaalitiedustelulla tarkoitetaan elektronisessa muodossa olevien signaalien hakemista (inhämta signaler i elektronisk form). Määritelmä on tekniikkaneutraali ja kattaa kaikki signaalitiedustelun menetelmät, kuten esimerkiksi kaapeli- ja radiosignaalitiedustelun sekä manuaalisen ja automaattisen tiedonkeräämisen. Signaalia ei saa kerätä, jos vastaanottaja ja lähettäjä ovat Ruotsissa. Kaapelitietoliikennettä saadaan tiedustella vain silloin, kun se ylittää Ruotsin rajan. Kielto ei kuitenkaan koske signaaleja, jotka kulkevat itsenäisesti teknisten järjestelmien välillä silloin, kun signaalit eivät sisällä henkilötietoja tai kun signaalit lähetetään ulkomaiselle sotilashenkilöstölle, ulkomaisille valtionaluksille, valtion ilma-aluksille tai sotilasajoneuvoille tai ne tulevat vastaavilta tahoilta ulkomailta.

Ruotsissa on syksyllä 2024 valmistunut loppumietintö (Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning (SOU 2024:59)) puolustustiedustelussa harjoitettavaa signaalitiedustelua koskevan lain tarkistamista koskien. Mietinnössä on muun muassa ehdotettu erityistä poikkeusta kieltoon kerätä kotimaista liikennettä, jos tällainen tiedustelu on merkityksellistä Ruotsin turvallisuuteen kohdistuvien ulkoisten uhkien torjumiseksi. Ehdotuksen tavoitteena olisi varmistaa, että sodan oloissa on mahdollista harjoittaa signaalitiedustelua Ruotsissa tapahtuvaa vihamielistä toimintaa vastaan, joka uhkaa Ruotsin suvereniteettia ja alueellista koskemattomuutta, myös ei-sotilaallisista lähteistä käsin. Mietinnössä on lisäksi ehdotettu muutettavaksi signaalitiedustelulain 1 §:ää siten, että signaalien kerääminen olisi mahdollista riippumatta siitä, ovatko signaalit välitettävinä vai tallennettuina. Signaalit voisivat olla tallennettuina esimerkiksi verkkoon liitetyissä laitteistoissa tai ohjelmistoissa.[10]

Ruotsissa on heinäkuussa 2025 lähetetty lausuntokierrokselle esitysluonnos (Fö2024/01478)[11], jossa huomioidaan sekä loppumietinnössä (SOU 2024:59) esitetty että esitetään uusia muutoksia tiedustelulakien päivittämiseksi. Ehdotettu uusi laki ja lakimuutokset on ehdotettu

[10] SOU 2024:59; s. 241.
[11] Fö2024:01478 Utkast till lagrådsremiss Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning (https://www.regeringen.se/contentassets/20faf90d0b7c40ba82a37dd85db22bf0/utkast-lagradsremiss-signalspaning-i-forsvarsunderrattelseverksamhet---en-modern-och-andamalsenlig-lagstiftning.pdf).

tulemaan voimaan kesäkuussa 2026. Selvitys sisältää luonnoksen hallituksen esitykseksi uudeksi laiksi signaalitiedustelusta puolustustiedustelutoiminnassa sodan tai sodan uhan aikana. Lisäksi ehdotetaan muutoksia lakiin signaalitiedustelusta puolustustiedustelutoiminnassa ja siihen liittyviin lakeihin. Signaalitiedustelulakia ehdotetaan muutettavaksi muun muassa siten, että signaalitiedustelu olisi mahdollista myös harjoitustoiminnassa.

Tietoliikennetiedustelun hakuehdot

Ruotsin signaalitiedustelulain 1 §:n 3 momentin säännöksen mukaan, mikäli toiminnan kannalta on välttämätöntä, voidaan signaaleja hankkia myös signaaliympäristössä, teknisessä kehityksessä ja signaalisuojassa tapahtuvien muutosten seuraamiseksi sekä tiedonhankinnassa käytettävän puolustustiedustelulain mukaisen toimialan tekniikan ja menetelmien kehittämiseksi.

Lain esitöiden (Prop. 2006/07:63) mukaan tällaista tietoa käytetään ainoastaan tiedusteluviranomaisen teknisten kyvykkyyksien kehittämiseksi, jotta tiedustelutehtäviin kyetään vastaamaan entistä paremmin. Teknisten tietojen keräyksestä ja teknisten tietojen käsittelystä ei siten muodostu sellaista tietoa, jota hyödynnettäisiin tiedustelutehtävään vastaamisessa. Lain esitöissä todetaan lisäksi, että tällaista saavutettua teknistä kyvykkyyttä ja sitä koskevaa tietoa on mahdollista jakaa viranomaisten välillä. Jaettava tieto ei kuitenkaan olisi varsinaista tiedustelutietoa, eikä yksityiselämän suojan piiriin kuuluvaa viestintää.

Signaalitiedustelulain 3 §:n mukaan signaalien keräämisen tulee perustua käytettäviin hakuehtoihin. Hakuehtojen määrittämisessä ja niiden käytössä tulee huomioida yksityisyydensuoja. Hakuehtoja, jotka liittyvät suoraan tiettyyn fyysiseen henkilöön, saadaan käyttää vain, jos se on toiminnan kannalta erityisen tärkeää. Hakuehdot voivat kuvata niiden toimijoiden, organisaatioiden, alustojen tai teknisten järjestelmien edustuksia, joihin signaalitiedustelun tulee kohdistua. Hakuehdot mahdollistavat teknisesti sen, että olennainen tieto löydetään ja tunnistetaan. Yksittäinen hakuehto voidaan usein liittää tiettyyn viestintäpalveluun, jota kohde käyttää, esimerkiksi tiettyyn matkapuhelinpalveluun tai sähköpostipalveluun.[12] Lain esitöissä[13] todetaan, että nopeasti muuttuva signaaliympäristö edellyttää, että myös hakuehtoja muokataan ja määritetään uusien tietojen karttuessa.

Puolustustiedustelussa harjoitettavaa signaalitiedustelua koskevan asetuksen 3 §:n mukaan FRA:n tulee ilmoittaa puolustustiedustelun valvonnasta vastaavalle elimelle (Statens inspektion för försvarsunderrättelseverksamheten, SIUN) sellaisten hakuehtojen käyttämisestä, jotka on suoraan yhdistettävissä luonnolliseen henkilöön ja joita käytetään signaalitiedustelutoiminnassa.

Tietoliikennetiedustelulla hankittujen tietojen hävittäminen

Signaalitiedustelulain 7 § asettaa FRA:lle tietyissä tilanteissa tietojen hävittämisvelvollisuuden. Lain mukaisesti hankittuja tietoja koskevat tallenteet tai muistiinpanot on välittömästi hävitettävä, jos sisältö koskee yksittäistä luonnollista henkilöä eikä sillä katsota olevan merkitystä 1 §:ssä tarkoitetun toiminnan kannalta. Niin ikään FRA:lla on velvollisuus hävittää

[12] SOU 2024:59, s. 56.
[13] Prop. 2006/07:63, s. 77–78.

tiedot välittömästi, jos tiedot koskevat rippisalaisuutta, lähdesuojaa tai asianajajan ja asiakkaan välistä kommunikointia rikosoikeudellisessa asiassa.

Puolustustiedustelussa harjoitettavaa signaalitiedustelua koskevaa asetusta (Förordning om signalspaning i försvarsunderrättelseverksamhet 2008:923) on muutettu 1.1.2025 voimaan tulleella asetuksella (SFS 2024:427). Muutosasetuksella on täsmennetty tiettyjen signaalitiedustelulaissa tarkoitettujen tallenteiden hävittämisvelvollisuutta. Tallenteet ja muistiinpanot tulee hävittää siten, ettei niitä saada palautettua.

Henkilötietojen käsittelystä FRA:n toiminnassa annetun lain (Lag (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt) 2 luvun 19 §:n mukaan henkilötietoja ei saa käsitellä pidempään kuin on tarpeen käsittelyn tarkoitusten kannalta.

Henkilötietojen käsittelystä FRA:n toiminnassa annetun asetuksen (Förordning (2021:1208) om behandling av personuppgifter vid Försvarets radioanstalt) 3 luvun 1 §:n mukaan FRA:lla saa olla henkilötietoja sisältävää automaattisesti käsiteltyä ja käsittelemätöntä raakadataa, jonka merkitystä tiedustelutoiminnalle ei siis ole vielä arvioitu. Tällaiseen raakadataan kuuluvia henkilötietoja ei kuitenkaan saa käsitellä pidempään kuin yhden vuoden ajan siitä, kun tietojen käsittely on aloitettu.

Ilmoitusvelvollisuus

Signaalitiedustelulain 11 a § edellyttää, että luonnolliselle henkilölle tulee ilmoittaa niin pian kuin mahdollista, ja viimeistään kuukausi puolustustiedustelutehtävän päättymisestä, milloin ja missä tarkoituksessa tiedustelu on toteutettu. Lain 11 b §:n mukaan ilmoituksen antamista voidaan kuitenkin lykätä, jos salassapito estää sen antamisen. Jos ilmoitusta ei ole voitu antaa salassapitosyistä vuoden kuluessa tiedustelutehtävän päättymisestä, sitä ei tarvitse antaa. Ilmoitusta ei myöskään tarvitse antaa, jos tiedustelu on koskenut yksinomaan vieraan valtion olosuhteita tai vieraan valtioiden välisiä suhteita.

Ruotsissa esitetään edellä kuvatun ilmoitusvelvollisuuden poistamista. Esityksessä on huomioitu EIT:n kannanotto Centrum för Rättvisa -tapauksessa. Esitysluonnoksessa[14] todetaan, että salassapidon perusteella FRA ei ole koskaan antanut 11 a §:n perusteella ilmoitusta, eikä ole todennäköistä, että ilmoituksia tulevaisuudessakaan annettaisiin. Esitysluonnoksen mukaan ilmoitusvelvollisuudella ei ole käytännön merkitystä oikeusturvan tai yksityisyyden suojan takaajana. Signaalitiedustelulain 10 a §:n mukainen tarkastusvelvollisuus täyttää tätä tarkoitusta.

5.2.4.2 Norja

Yleistä

Norjan ulkomaan tiedustelupalveluna toimii Etterretningstjenesten (E-tjenesten), jonka tehtävistä ja toimivaltuuksista säädetään laissa tiedustelupalvelusta (Lov om Etterreningstjenesten). Norjan nykyinen tiedustelupalvelulaki on tullut voimaan 2021.

[14] Fö2024/01478, Utkast till lagrådsremiss Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning, s. 124–126.

Norjassa ei ole kotimaan turvallisuuspalvelua, vaan maan sisäisestä kansallisen turvallisuuden ylläpitämisestä vastaa turvallisuuspoliisi Politiets sikkerhetstjeneste (PST). E-tjenestenin ja PST:n välisestä yhteistyöstä on säädetty oma asetuksensa (Instruks om samarbejdet mellom Etteretningstjenesten og Politiets sikkerhetstjeneste).

Tietoliikennetiedustelun hakuehdot

Tiedustelupalvelulain 5 luvun 3 §:n mukaan tiedustelupalvelu voi kerätä raakadataa massana (raw data in bulk), kun se on tarpeen asiaankuuluvan ja riittävän tietopohjan saavuttamiseksi. Tällaiseen raakadataan tehtyjen hakujen tulee täyttää kohdennetun tiedonhankinnan perusedellytykset ja hakuprosessi kirjataan valvontaa varten. Raakadataan tehtäviä hakuja, jotka liittyvät Norjassa oleskelevaan henkilöön, saa suorittaa ainoastaan silloin, kun se on ehdottoman välttämätöntä tiedustelupalvelun 3 luvun 1 §:n mukaisten tehtävien hoitamiseksi. Rajoitus ei koske ulkomaalaisia tai kansalaisuudettomia henkilöitä, jotka toimivat vieraan valtion tai valtiollista toimijaa muistuttavan tahon puolesta.

Tiedustelupalvelulain 7 luvun 5 §:n mukaan tiedustelupalvelu voi suorittaa testikeräystä ja testianalyysejä rajat ylittävästä elektronisesta tietoliikenteestä ja verkosta. Pykälän mukaan testikeräystä ja testianalyysejä saa käyttää yksinomaan valinnan, suodatuksen, tallennuksen, haun, uudelleenkäsittelyn, signaaliympäristön ymmärtämisen ja palveluiden sekä dataformaattien tunnistamisen mahdollistamiseksi, sekä muuhun tekniseen tukeen.

Testikeräys suoritetaan suodattamattoman tietoliikenteen poiminnalla yhdestä tai useammasta tietoliikennevirrasta. Yksi poiminta ei saa ylittää 30 sekuntia, eikä poimintoja saa tehdä useammin kuin kerran tunnissa. Poimintoja ei saa säilyttää pidempään kuin on tarpeen, ja ne on poistettava viimeistään 14 päivän kuluttua. Poiminnat on tallennettava lyhytaikaiseen säilöön, joka on pidettävä erillään niistä säilöistä, jotka on varattu tallennetulle metatiedolle ja tallennetulle sisältötiedolle.

Norjan tiedustelupalvelusta annetun lain 7 luvun 7 §:n mukaan tiedustelupalvelu voi kerätä ja tallentaa metadataa massana (metadata in bulk) sähköisestä viestinnästä, joka kulkee Norjan rajan yli. Lain 7 luvun 6 §:ssä säädetään kuitenkin velvollisuudesta pyrkiä ehkäisemään sellaisen metadatan tallentaminen, joka liittyy Norjassa oleskelevien osapuolten väliseen viestintään. Lain 7 §:n mukaan metatiedolla tarkoitetaan tietoja, jotka kuvaavat muuta dataa tai sisältävät lisätietoja dataan liittyen, kuten tietoja, jotka kuvaavat sisällön muotoa, lähettäjää ja vastaanottajaa tai viestinnän kokoa, sijaintia, ajankohtaa ja kestoa. Sisältötietojen tallentamisen ehkäisemiseksi tiedustelupalvelun on ylläpidettävä luetteloa tallennettavissa olevista metatietotyypeistä ja luettelon tulee olla valvontaviranomaisten saatavilla.

Lain 7 luvun 8 §:n mukaan tallennettuihin metatietoihin on mahdollista tehdä hakuehtojen käyttöön perustuvia hakuja tuomioistuimen luvalla. Hakuja tallennettuihin metatietoihin voi tehdä ainoastaan tähän tehtävään koulutetut ja nimetyt henkilöt. Tallennettujen metatietojen päivitystä, teknistä analyysiä ja vianetsintää saa suorittaa lain 5 §:n mukaan ainoastaan sellaiset tekniset asiantuntijat, jotka eivät työskentele tiedusteluanalyysitehtävissä.

Norjan tiedustelupalvelusta annetun lain 7 luvun 9 §:n mukaan tiedustelupalvelu voi lisäksi tuomioistuimen luvalla kerätä ja tallentaa sisältötietoja ja siihen liittyviä metatietoja sellaisesta tietoliikenteestä, joka ylittää Norjan rajan. Sisältötiedon määritelmänä on, että se on tietoa, joka ei ole metatietoa.

Tietoliikennetiedustelulla hankittujen tietojen hävittäminen

Tekniset parametrit ja käsitellyt testianalyysit, joita ei voida yhdistää yksittäisiin henkilöihin, voidaan säilyttää niin kauan kuin se on tarpeen lain 7 luvun 5 §:n mukaisten testianalyysien tavoitteen saavuttamiseksi.

Tiedustelupalvelusta annetun lain 7 luvun 7 §:n mukaan tallennettu metatieto on poistettava viimeistään 18 kuukauden kuluessa.

Ilmoitusvelvollisuus

Norjan tiedustelupalvelulaissa ei säädetä viranomaiselle yleistä velvollisuutta ilmoittaa siitä, että henkilö on ollut tiedustelun kohteena. Tiedustelumenetelmien käyttöä valvoo tiedusteluvalvontavaliokunta (EOS-utvalget). Tiedusteluvalvontavaliokunnalle on mahdollista tehdä valitus, mikäli epäilee olleensa tiedustelun kohteen tai tietojensa tulleen käsitellyksi lainvastaisesti. EOS-valvontalain (Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste) 8 §:n mukaisesti tiedusteluvalvontavaliokunnalla on kattava pääsy tiedustelupalveluiden tietoihin valvontatehtävässään. Lähtökohtaisesti valituksen johdosta annettavassa lausumassa ei kuitenkaan oteta kantaa siihen, onko henkilö ollut tiedustelun kohteena, sillä kyseessä on salassa pidettävä tieto.

5.2.4.3 Tanska

Yleistä

Tanskassa ulkomaantiedustelusta vastaa puolustusvoimien tiedustelupalvelu FE (Forsvarets Efterretningstjeneste), jonka tehtävistä, toimivaltuuksista ja toiminnan valvonnasta säädetään laissa puolustusvoimien tiedustelupalvelusta (Lov om Forsvarets Efterretningstjeneste, jäljempänä FE-laki). FE-lain muutosesitys on ollut lausuntokierroksella helmikuussa 2025.[15] Puolustusministeriö on huhtikuussa 2025 ilmoittanut, että lakiesityksen antaminen siirtyy seuraavalle vuodelle.[16] Muutosesityksen taustalla on Euroopan ihmisoikeustuomioistuimen ratkaisukäytäntö ja FE-lain päivittäminen vastaamaan tuomioistuimen ratkaisukäytäntöä.

Tietoliikennetiedustelun hakuehdot

Tanskan FE-laissa ei ole erityisiä säännöksiä koskien hakuehtojen määrittämistä ja teknisen analyysin tekemistä signaaliympäristössä tapahtuvien muutosten havaitsemiseksi.

Tietojen hävittäminen

FE-lain 6 §:n 1 momentin mukaan puolustusvoimien tiedustelupalvelun on lähtökohtaisesti poistettava tiedot Tanskassa asuvista luonnollisista tai oikeushenkilöistä, jotka on hankittu 1 §:n 1 momentin mukaisen toiminnan yhteydessä, mikäli viimeisten 15 vuoden aikana ei ole hankittu uutta, samaa asiaa sisällöllisesti koskevaa tietoa, eikä muualla ole toisin säädetty. Pykälän 2 momentin mukaan raakadata tulee poistaa 15 vuoden kuluessa keräysajankohdasta. Tästä voidaan kuitenkin poiketa, mikäli tehtävien suorittaminen edellyttää sitä olennaisista syistä. FE-lain 6 a §:n mukaan kerätyt tiedot on kuitenkin poistettava riippumatta siitä, onko säilytysaika umpeutunut, mikäli asiat tai asiakirjat eivät enää täytä tietojen käsittelyä koskevia ehtoja.

[15] https://hoeringsportalen.dk/Hearing/Details/69633
[16] https://www.ft.dk/samling/20241/almdel/FOU/bilag/127/3012501.pdf

Viranomaisella ei ole velvollisuutta tarkastella tietoja jatkuvasti oma-aloitteisesti sen arvioimiseksi, täyttyvätkö 4 ja 5 §:ssä asetetut edellytykset henkilötietojen käsittelylle edelleen.

Ilmoitusvelvollisuus

FE-laissa ei säädetä viranomaiselle yleistä velvollisuutta ilmoittaa siitä, että henkilö on ollut tiedustelutoiminnan kohteena. Tiedustelupalveluiden toimintaa valvovalle viranomaiselle (Tilsynet med Efterretningstjenesterne, jäljempänä TET) on mahdollista tehdä ilmoitus, mikäli epäilee olleensa tiedustelun kohteena.

5.2.4.4 Saksa

Yleistä

Saksan ulkomaan tiedustelupalveluna toimii Bundesnachrichtendienst (BND), joka vastaa sekä siviili- että sotilaallisia uhkia koskevasta ulkoisesta tiedonhankinnasta. Kotimaan turvallisuuspalvelun tehtävät on jaettu siten, että liittovaltion siviiliturvallisuuspalveluna toimii Bundesamt für Verfassungsschutz (BfV) ja sotilaallisena turvallisuuspalveluna Militärischer Abschirmsdienst (MAD). MAD:n ensisijaisena tehtävänä on havaita ja torjua sellaisia uhkia, jotka kumpuavat Saksan puolustushallinnon sisältä. Kaikkien edellä mainittujen toimijoiden tehtävistä ja toimivaltuuksista säädetään omissa laeissaan, joskin BND:n ja MAD:n toimintaa koskevat lait toimivaltuuksien osalta laajasti viittaavat BfV:n toimintaa koskevaan lakiin, jossa säädetään liittovaltion turvallisuuspalvelun ja osavaltioiden turvallisuuspalveluiden yhteistyöstä (Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz, jäljempänä BfV-laki).

Ulkomaantiedustelupalvelulakia (jäljempänä BND-laki) on uudistettu perustuslakituomioistuimen toukokuussa 2020 antaman päätöksen[17] seurauksena. Uudistettu BND-laki tuli voimaan 1.1.2022. Uudistuksessa huomioitiin erityisesti yksityisyyden suojan sekä lehdistönvapauden toteutuminen ulkomaan tietoliikennetiedustelussa.

Toimivaltuussääntelyn kannalta merkitystä on lisäksi posti- ja telesalaisuuden rajoittamisesta annetulla lailla (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, jäljempänä G10-laki), joka sisältää kaikkia sellaisia tiedustelumenetelmiä koskevan sääntelyn, joilla turvallisuus- ja tiedustelupalvelujen tiedonhankinta puuttuu luottamuksellisen viestin sisältöön.

Tietoliikennetiedustelun hakuehdot

BND-lain 19 §:ssä säädetään strategisesta ulkomaan tietoliikennetiedustelusta. Pykälän 8 momentin mukaan rajoittamaton tietoliikennetiedustelu on kielletty, minkä lisäksi tiedustelu saa kohdistua enintään 30 prosenttiin olemassa olevista tietoliikenneverkoista. Pykälän 5 momentin mukaan tietojen kerääminen saadaan toteuttaa ainoastaan hakuehtojen perusteella. Hakuehtojen on oltava muun muassa ennalta määriteltyjä. Pykälän 7 momentin mukaan tiedustelu ei saa kohdistua saksalaisiin, Saksassa oleviin henkilöihin tai kotimaisiin oikeushenkilöihin.

[17] Bundesverfassungsgericht, 1 BvR 2835/17 (19.5.2020), https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200519_1bvr283517en.html

G10-lain 5 § käsittelee perustuslaissa turvatun viestintäsalaisuuden rajoittamista tietoliikennetiedustelussa. Säännöksen mukaan BND saa parlamentaarisen valvontavaliokunnan luvalla suorittaa tietoliikennetiedustelua, jos tämä on välttämätöntä eräiden uhkien havaitsemiseksi ja estämiseksi. Pykälän 2 momentin mukaan hakuehtoja, jotka johtavat yksittäisten teleliikenneyhteyksien kohdennettuun seurantaan tai koskevat yksityiselämän suojan ydinaluetta ei saa käyttää.

Tietojen hävittäminen

BND-lain 27 §:ssä säädetään kerättyjen tietojen arvioinnista ja tarkastusvelvollisuudesta. Kerätyt tiedot tulee tarkistaa viipymättä ja sen jälkeen säännöllisesti, vähintään seitsemän vuoden välein, sen selvittämiseksi, ovatko ne yksinään tai yhdessä jo olemassa olevien tietojen kanssa tarpeellisia 19 §:n 1 momentissa määriteltyihin tarkoituksiin. Mikäli henkilötiedot eivät ole tarpeellisia näihin tarkoituksiin, ne on viipymättä poistettava.

BND-lain 36 §:n mukaan yksityiselämän ydinaluetta koskevat tiedot, jotka tietoliikennetiedustelun yhteydessä mahdollisesti saadaan, on hävitettävä viipymättä ja poistaminen on dokumentoitava. Tällaisten tietojen kerääminen on kiellettyä.

Ilmoitusvelvollisuus

G10-lain 12 §:ssä säädetään ilmoituksista asianomaisille. Toimenpiteen kohteeksi joutuneelle on ilmoitettava toimenpiteen päättymisen jälkeen. Ilmoitusta ei kuitenkaan tehdä, mikäli ilmoitus vaarantaisi toimenpiteen tarkoituksen tai jos on ennakoitavissa merkittävää haittaa liittovaltion tai osavaltion yleiselle edulle. Mikäli ilmoitusta ei ole tehty 12 kuukauden kuluessa toimenpiteen päättymisestä, tulee ilmoituksen tekemättä jättäminen saattaa G10-komission käsiteltäväksi, joka määrää lykkäyksen jatkoajan.

Laissa ei säädetä tiedusteluviranomaiselle yleistä velvollisuutta ilmoittaa henkilölle, mikäli tämä on ollut tiedustelun kohteena. BfV-lain 15 §:ssä säädetään tietojen antamisesta rekisteröidylle. Viranomainen voi rekisteröidyn pyynnöstä antaa tietoja hänen henkilötiedoistaan, mikäli pyyntö on siinä määrin yksilöity, että siinä viitataan johonkin konkreettiseen tapaukseen ja henkilöllä on erityinen intressi saada häntä koskevat tiedot. Pykälän 2 momentin mukaan tietojen antamisesta voidaan pidättäytyä, mikäli tietojen antaminen vaarantaisi esimerkiksi viranomaisen tehtävien hoitamisen.

5.2.4.5 Alankomaat

Yleistä

Alankomaissa tiedustelutoiminnasta vastaavat yleinen tiedustelu- ja turvallisuuspalvelu Algemene Inlichtingen en Veiligheidsdienst, AIVD) ja sotilaallinen tiedustelu- ja turvallisuuspalvelu (Militaire Inlichtingen- en Veiligheidsdienst, MIVD). Palveluiden toiminnasta säädetään vuoden 2017 laissa tiedustelu- ja turvallisuuspalveluista (Wet op de inlichtingen- en veiligheidsdiensten, 2017, jäljempänä Wiv-laki). Laki korvasi aiemman Wiv-lain vuodelta 2002.

Alankomaissa tiedustelulainsäädännön toimivuutta on arvioitu ja komitea on vuonna 2021 antanut useita suosituksia tiedustelulainsäädännön kehittämiseksi. Heinäkuussa 2024 tuli voimaan väliaikainen laki (Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen), joka

mahdollistaa viranomaisille tehokkaamman toiminnan muuttuneessa turvallisuusympäristössä ja erityisesti valtiollisia kyberuhkia vastaan. Väliaikainen laki on voimassa 1.7.2028 saakka.

Wiv-laista poiketen väliaikainen laki mahdollistaa esimerkiksi yksilöimättömän tietoaineiston (bulk dataset) säilyttämisen Wiv-laissa säädettyä 18 kuukauden määräaikaa pidempään. Wiv-lain 27 artiklan 1 kohdan mukaan yksilöimättömän tietoaineiston tarpeellisuus tulee arvioida mahdollisimman pian ja viimeistään 18 kuukauden kuluessa. Tarpeeton tieto on tämän arvioinnin yhteydessä tuhottava. Väliaikaisen lain 14b ja 14ba artiklojen mukaisesti tarkistamattoman yksilöimättömän tietoaineiston säilyttämisen jatkaminen on mahdollista ministerin päätöksellä. Päätös säilyttämisen jatkamisesta voidaan tehdä vuodeksi kerrallaan, eikä kokonaisenimmäisaikaa ole säädetty. Lain 14 ba artiklan 3 kohdan mukaisesti jatkamispäätöksestä on ilmoitettava tiedustelutoimintaa valvovalle komissiolle (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten CTIVD).

Wiv-lain 25 artiklan 1 kohdan mukaan tiedustelupalveluilla on oikeus kerätä tietoja muun muassa yleisesti saatavilla olevista lähteistä. Tavanomaisiin toimivaltuuksiin kuuluva tiedonhankinta ei edellytä lupaa ministeriltä, eikä hyväksyntää valvontalautakunnalta (Toetsingscommissie Inzet Bevoegdheden, TIB). Ministerin lupaa ei myöskään edellytetä lain 39 artiklan mukaiseen tiedonhankintaan hallintoelimiltä, virkamiehiltä sekä muilta, joiden voidaan katsoa pystyvän toimittamaan tarvittavat tiedot. Valvontalautakunta on riippumaton elin, joka arvioi etukäteen tiedustelutoimivaltuuksien lainmukaisuutta.

Wiv-lain 45 artiklan 1 kohdan nojalla tiedustelupalveluilla on säädettyjen edellytysten täyttyessä oikeus tunkeutua automaattiseen järjestelmään joko käyttämällä teknisiä apuvälineitä, vääriä signaaleja, vääriä avaimia, väärää henkilöllisyyttä tai kolmannen osapuolen automaattisen järjestelmän kautta. Toimivaltuuden käyttäminen on luvanvaraista. Artiklan 5 kohdan mukaan kolmannen osapuolen järjestelmän hyödyntäminen ei kata teknisten laitteiden asentamista.

Ilmoitusvelvollisuus

Wiv-lain 59 artiklan mukaan viranomaisten on arvioitava viiden vuoden kuluttua tiettyjen toimenpiteiden päättymisestä ja sen jälkeen vuosittain, voidaanko toimenpiteestä ilmoittaa sille henkilöille, johon toimipide on kohdistettu. Artiklassa mainitut toimenpiteet kattavat kirjeiden avaamisen, kohdennetun viestinnän seurannan ja asunnossa käymisen. Ilmoitus voidaan kuitenkin jättää tekemättä useilla eri perusteilla, muun muassa toiminnan suojaamiseksi tai mikäli ilmoituksen tekeminen vaarantaisi kansallista turvallisuutta. Tilanteissa, joissa ilmoitusta ei voida tehdä tai sen tekeminen olisi käytännössä mahdotonta, tulee valvontakomissiolle tehdä ilmoitus ja perustella, miksi ilmoitusta ei ole voitu tehdä asianosaiselle.

5.2.4.6 Kybertoimenpiteiden suorittaminen kansainvälisesti

Kansainvälisesti maanpuolustukselle ja kansalliselle turvallisuudelle uhkaa aiheuttavien tietojärjestelmien toimintaan puuttuminen on tyypillisesti ollut toimintaa, josta ei ole ollut juurikaan saatavilla tietoa julkisia lähteistä. Viime vuosina tämä on kuitenkin muuttunut; jotkin maat ovat julkisesti tuoneet esiin mahdollisuuden puuttua maanpuolustusta tai kansallista turvallisuutta uhkaavan tietojärjestelmän toimintaan.

Lainsäädännön tarkkuuden osalta tilanne kuitenkin vaihtelee. Eräät maat ovat säätäneet ulkomaan tiedustelusta vastaavalle viranomaiselle mahdollisuuden suorittaa tiedonhankinnan lisäksi myös muita tarpeellisia toimenpiteitä maanpuolustuksen ja kansallisen turvallisuuden

suojaamiseksi. Näistä valtioista esimerkiksi Yhdistynyt Kuningaskunta on tuonut kansallisessa kyberturvallisuusstrategiassaan julkisesti esiin mahdollisuuden tehdä aktiivisia kybertoimenpiteitä, jossa tuodaan esiin myös toimenpiteiden laillisuusperustaa. Lainsäädännön ollessa verraten epämääräistä, toimenpiteet suoritetaan usean viranomaisen yhteistyönä yhdistämällä näiden toimivaltaa. Yhdistyneessä Kuningaskunnassa toimenpiteiden suorittamiseen osallistuvat ainakin signaalitiedusteluviranomainen GCHQ ja ulkomaan tiedustelupalvelu SIS. Kybertoimenpiteiden suorittaminen perustuu kolmeen lakiin: 1) Intelligence Services Act 1994 (ISA), 2) the Investigatory Powers Act 2016 (IPA) ja 3) the Regulation of Investigatory Powers Act 2000 (RIPA). Laeissa määritellyistä viranomaisista SIS:lle on laissa säädetty mahdollisuus suorittaa tiedonhankinnan lisäksi myös muita toimenpiteitä ulkomailla.

Toista laitaa edustaa esimerkiksi Kanada. Kanadassa on säädetty viestinnän turvallisuuden virastoa koskevassa laissa (Communications Security Establishment Act) virastolle mahdollisuus suorittaa aktiivisia kybertoimia. Lain 19 artiklan mukaan virastolla on mandaatti suorittaa aktiivisia kybertoimenpiteitä maailmanlaajuisen tietoinfrastruktuurin kautta tai sen avulla heikentääkseen, häiritäkseen, vaikuttaakseen, vastatakseen tai puuttuakseen ulkomaisen henkilön, valtion, organisaation tai terroristiryhmän kykyihin, aikomuksiin tai toimintaan siltä osin kuin ne liittyvät kansainvälisiin suhteisiin, puolustukseen tai turvallisuuteen.

Keväällä 2025 Japanin parlamentti hyväksyi lain, jonka nojalla japanilaiset viranomaiset voivat suorittaa aktiivisia kybertoimenpiteitä. Laki antaa poliisille ja itsepuolustusjoukoille mahdollisuuden torjua kyberuhkia myös ennakollisesti ja yhteistyössä liittolaisten kanssa.

Vuonna 2026 Saksassa valmistellaan ulkomaan tiedustelupalvelua koskevaa lainsäädäntöuudistusta, jonka myötä tiedustelupalvelu saisi aiempaa laajempia toimivaltuuksia myös aktiivisiin toimenpiteisiin. Lakiesityksessä ehdotetaan, että Saksan ulkomaan tiedustelupalvelulla olisi oikeus suorittaa aktiivisia toimenpiteitä, kuten haittaohjelmat ja palvelinten lamauttaminen, ulkomailla, jos kyse on kansallisen turvallisuuden uhasta. Lakiehdotuksen toimivaltuudet kattavat myös toimenpiteet muualla kuin kyberympäristössä, kuten sabotaasi-iskut.

Vaikka laajemmin julkisesti ei ole tiedossa, miten laajasti eri valtiot suorittavat aktiivisia kybertoimenpiteitä, edellä kuvattujen esimerkkien nojalla voidaan arvioida, että yhä useampi valtio pyrkii torjumaan kyberuhkia myös oman valtionsa rajojen ulkopuolella. Edellä kuvattujen esimerkkienkin tapauksessa toiminnassa korostetaan kansainväliseen oikeuden asettamia reunaehtoja ja toiminta on vahvasti valvottua.

6 Lausuntopalaute

6.1 Työryhmän mietinnöstä annetut lausunnot

Hallituksen esitysluonnos oli lausuntokierroksella Lausuntopalvelu.fi-palvelun kautta 28.11.2025 –16.1.2026.

Lausuntoa pyydettiin seuraavilta tahoilta: ministeriöt, Aliupseeriliitto, Amnesty International Suomen osasto, Eduskunnan oikeusasiamiehen kanslia, Electronic Frontier Finland - Effi ry, Elinkeinoelämän keskusliitto EK, FiCom ry, Finnish Information Security Cluster (FISC) Kyberala ry, Helsingin hovioikeus, Helsingin käräjäoikeus, Julkisalan koulutettujen neuvottelujärjestö JUKO ry, Korkein oikeus, Oikeuskanslerin virasto, Poliisihallitus, Pääesikunta, Päällystöliitto, Reserviläisliitto, Rajavartiolaitos, Suojelupoliisi, Suomen Erillisverkot Oy, Suomen Reserviupseeriliitto ry, Teknologiateollisuus ry,

Tiedusteluvalvontavaltuutettu, Tietosuojavaltuutetun toimisto, Tasavallan Presidentin kanslia, Liikenne- ja viestintävirasto Traficom, Tulli, Upseeriliitto ry, Varusmiesliitto Ry, Verohallinto, Valtakunnansyyttäjäntoimisto.

Lausuntoja saatiin 41 taholta. Lausunnon antoivat Aliupseeriliitto, Eduskunnan oikeusasiamiehen kanslia, Electronic Frontier Finland - Effi ry, Elinkeinoelämän keskusliitto EK, Eläketurvakeskus, FiCom ry, Finnish Information Security Cluster (FISC) Kyberala ry, Helsingin hovioikeus, Helsingin käräjäoikeus, Keva, Liikenne- ja viestintäministeriö, Miesten hypogonadikuntoutujien järjestö ry, Oikeuskanslerin virasto, Oikeusministeriö, Poliisihallitus, Puolustus- ja Ilmailuteollisuus PIA ry, Pääesikunta, Päällystöliitto, Reserviläisliitto, Rajavartiolaitos, Sisäministeriö, Suojelupoliisi, Suomen Erillisverkot Oy, Suomen Reserviupseeriliitto ry, Syyttäjälaitos, Teknologiateollisuus ry, Tiedusteluvalvontavaltuutettu, Tietosuojavaltuutetun toimisto, Tasavallan Presidentin kanslia, Traficom, työ- ja elinkeinoministeriö, ulkoministeriö, Upseeriliitto ry, valtioneuvoston kanslia, valtiovarainministeriö, Varusmiesliitto ry, Verohallinto, Valtakunnansyyttäjäntoimisto ja ympäristöministeriö. Lisäksi lausunnon antoi kaksi yksityishenkilöä.

Luonnosta koskevat lausunnot ja muut hankkeen valmisteluasiakirjat ovat nähtävillä valtioneuvoston verkkosivustolta tunnuksella PLM007:00/2024.

Lausunnoissa yleisesti pidettiin tärkeänä, että turvallisuusviranomaisilla on nykyisessä turvallisuusympäristössä riittävät toimintamahdollisuudet huomioon ottaen teknologian kiihtyvä kehittyminen.

Lausunnolla olleessa hallituksen esityksen luonnoksessa ehdotettiin puolustushaaroille aiempaa itsenäisemmin osallistua sotilastiedustelutoimintaan. Lisäksi puolustushaarojen käyttöön ehdotettiin tavanomaista tietolähdetoimintaa. Lausunnoissa otettiin kantaa siihen, että nykyisen perustuslain 10 §:n perustelujen mukaisesti tiedustelutoiminta on osoitettu ainoastaan suojelupoliisille ja sotilastiedusteluviranomaisina toimiville pääesikunnalle ja Puolustusvoimien tiedustelulaitokselle. Koska lausunnolla olleessa luonnoksessa ehdotettu muutos herätti enemmän ehkä väärinkäsityksiä puolustushaarojen itsenäisyyden suhteen tiedustelutoiminnassa, jatkovalmistelussa puolustushaaroja koskeva oma pykäläehdotus poistettiin ja tarvittavat muutokset tehtiin voimassa olevan säännöksen muutoksilla.

Vastaavasti lausunnonantajat kiinnittivät huomiota sotilastiedusteluviranomaisesta eronneiden käytännössä Puolustusvoimien eläkeiän saavuttaneiden osallistumiseen sotilastiedustelutoimintaan. Koska Puolustusvoimissa eläkeikä on noussut, reservin yläikärajaa on nostettu ja myös muita virkajärjestelyitä on mahdollisuus tehdä, esitetty säännös osoittautui tarpeettomaksi.

Säännösehdotusta yhteistyötä muiden viranomaisten sekä yritysten ja muiden yhteisöjen kanssa koskevan sääntelyn muutoksia pidettiin perusteltuina ja tarpeellisina.

Luonnoksen 1. lakiehdotuksen 18 a §:n (yhteistoiminta Rajavartiolaitoksen kanssa) esiin nostetiin huomio, ettei perustuslain 10 §:n perusteluiden ja perustuslakivaliokunnan kannanottojen mukaan ole mahdollista antaa tiedusteluviranomaisen asemaa suojelupoliisin, pääesikunnan ja Puolustusvoimien tiedustelulaitoksen lisäksi muille viranomaisille. Lisäksi huomiota kiinnitettiin siihen, että Rajavartiolaitoksen sotilastiedusteluviranomaisen tukemisen rooli voi hämärtää Rajavartiolaitoksen viranomaisroolia. Huomiota kiinnitettiin myös siihen, että rajavartiolain mukaisten Schengenin rajasäännöstöön kytkeytyvien toimenpiteiden osittain tai kokonaan tiedustelutarkoituksessa suorittaminen saattaa olla tarkoitussidonnaisuuden periaatteen ja Schengenin rajasäännöstön noudattamisen näkökulmasta ongelmallista.

Jatkovalmistelussa säännöstä on pyritty selkeyttämään ja perusteluja parantamaan.

Luonnoksen 1. lakiehdotuksen 20 §:n (kansainvälinen yhteistyö) osalta lausunnoissa kiinnitettiin huomiota siihen, että ehdotetun muutoksen myötä ulkomaisen virkamiehen keinovalikoima laajenisi kattamaan myös viestin salaisuuden suojaan kajoavia keinoja. Tätä voidaan pitää laajennuksena siihen, mitä voimassa olevan lain perusteluissa todetaan.

Jatkovalmistelussa perusteluja on pyritty kehittämään. Joka tapauksessa, kuten nykyisin, ulkomainen virkamies toimii sotilastiedustelun ohjauksessa ja valvonnassa, ja sotilastiedusteluviranomainen vastaa toimenpiteiden edellyttämistä luvista ja päätöksistä.

Lausunnonantajat kiinnittivät 1. lakiehdotuksen 33 §:n (teknisestä laitetarkkailusta päättäminen) osalta huomiota siihen, että henkilöön kohdistuvassa teknisessä laitetarkkailussa tuomioistuin kontrollin ulkopuolelle jäisi se, mihin kaikkiin laitteisiin ja ohjelmistoihin toimivaltuus loppujen lopuksi kohdistuisi. Toisaalta jo nykytilassa telekuuntelua voidaan kohdistaa henkilöperusteisesti. Helsingin käräjäoikeus totesi vielä, että muutos ei olennaisesti vaikuta kohdehenkilön oikeusturvaan, sillä tiedustelumenetelmän käyttämisen edellytyksiä arvioidaan tavallisesti suhteessa sen kohteeseen eikä tiettyyn yksittäiseen laitteeseen.

Jo nykyisin esimerkiksi telekuuntelun osalta henkilöön kohdistuvassa telekuuntelussa päätöksen uuden telepäätelaitteen tai teleosoitteen lisäämisestä luvan piiriin tekee tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies. Päätös tehdään aina virkavastuulla. Uudet telepäätelaitteet ja teleosoitteet on lisättävä samaa kohdetta koskevaan uuteen tuomioistuimelle tehtävään vaatimukseen.

Jatkovalmistelussa edellä kuvattu menettely päätettiin saattaa laintasolle. Lisäksi perusteluissa on korostettu sitä, että tiedusteluvalvontavaltuutetun valvonta koskee henkilöperusteisissa tiedustelumenetelmien käytössä myös toimivaltuuden piiriin lisättyjä uusia telepäätelaitteita, teleosoitteita, laitteita ja ohjelmistoja. Vastaavasti sotilastiedusteluvirnaomaisen on ilmoitettava tekemästään lisäämispäätöksestä tiedusteluvalvontavaltuutetulle samassa menettelyssä kuin tehdessään päätöstä tiedustelumenetelmän käytöstä.

Luonnoksen 1. lakiehdotuksen 42 §:n (laitteen menetelmän tai ohjelmiston asentaminen ja poisottaminen) osalta huomiota kiinnitettiin siihen, miten laajasti toimenpiteitä suoritettaisiin, ilmoitetaanko toiminnasta ja miten laillisesti toimivat yritykset ja yhteisöt voisivat pienentää luottamuksellisuuteen liittyviä riskejään. Lisäksi huoli siitä, että Suomessa laillisesti toimivan yrityksen tai yhteisön kyberturvallisuuden taso saattaisi heikentyä.

Säännöksessä tarkoitetuissa toimenpiteissä olisi kyse niistä toimenpiteistä ja siinä laajuudessa, mitä sotilastiedusteluviranomainen voi jo nykyisin lain nojalla tehdä. Näin ollen ei voida pitää todennäköisenä, että vastaisuudessakaan kyberturvallisuuden taso heikentyisi. Sotilastiedusteluviranomaisen tehtävien kannalta on myös keskeistä, että tarvittaville tahoille annetaan tieto esimerkiksi havaituista haavoittuvuuksista. Laitteet, menetelmät ja ohjelmistot ovat sotilastiedusteluviranomaisen jatkuvassa tarkkailussa eikä niitä pääse käyttämään muut tahot. Tämä koskee myös sotilastiedusteluviranomaisen itsensä toteuttamia haavoittuvuuksia. Lisäksi säännöksessä säädetään erikseen myös esimerkiksi ohjelmiston poisottamisesta.

Lausunnoissa kiinnitettiin huomiota myös siihen, että toimenpiteitä voisi suorittaa kotirauhan piirissä. Tämä ei kuitenkaan olisi mahdollista, sillä pykälän 1 momentti kieltää nimenomaisesti, kuten muuallakin laissa, sotilastiedusteluviranomaisen toimenpiteiden tekemisen ja toimivaltuuksien käyttämisen kotirauhan suojaamassa tilassa.

Lausunnoissa nostettiin esiin, että toiminnassa olisi kyse merkittävästä julkisen vallan käytöstä. Kuten hallituksen esityksessä on tuotu säätämisjärjestystä koskevassa osiossa esiin, katsotaan, että kyse ei ole merkittävästä julkisen vallan käytöstä, koska toimintaan ei liity itsenäistä päätöksentekoa ja toimenpiteet tapahtuvat viranomaisen toimivallassa.

Luonnoksen 1. lakiehdotuksen 46 a ja 46 b §:n (yksinomaan tietoverkossa toteutettava peitetoiminta ja siitä päättäminen) huomiota kiinnitettiin siihen, että muutosta tai sen tarvetta ei ole perusteltu hallituksen esityksessä. Jatkovalmistelussa esitetyt muutokset tuotiin esiin.

Lausunnoissa kiinnitettiin huomiota toimivaltuuden kohdentamiseen ja että se vaikuttaisi olevan väljempi kuin mitä voimassa olevassa laissa on. Lausunnolla olleessa versiossa tähän pyrittiin, että kohdentaminen voisi tapahtua sotilastiedustelun toimivallassa olevaan uhkaan liittyen, mutta jatkovalmistelussa päädyttiin ratkaisuun, jossa kohdentaminen perustuu henkilöpiirin rajaamiseen vastaavasti kuin on eräiden muidenkin tiedustelumenetelmien osalta säädetty.

Luonnoksen 1. lakiehdotuksen 61 a §:n (valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu Suomessa) huomiota kiinnitettiin toimivaltuuden laajuuteen ja sen kohdentumiseen ja tietojärjestelmän määrittelyyn lupakäsittelyssä. Säännöksen perusteluja on tarkennettu ja tuotu esiin sitä, että sotilastiedusteluviranomaisella on usein erittäin tarkka lähtötilanne tiedossa, ennen kuin toimivaltuutta ryhdytään käyttämään.

Jatkovalmistelussa on pyritty korostamaan sitä, että tiedustelumenetelmän kohteena ei ole esimerkiksi serverisali kokonaisuutena, vaan sotilastiedusteluviranomainen pystyy osoittamaan varsin suurella tarkkuudella tietyn laitteen, jota valtiollinen toimija Suomessa käyttää. Näin ollen tiedustelumenetelmän kohteena on aluksi tietty laite, jonka toimintaa ja tietoja seuraamalla päästään tarkemmin tietojärjestelmän muihin laitteisiin käsiksi. Tiedonhankinnan piiriin toki voi tulla myös muiden viestintään, mutta tätä tietoa koskee hetihävittämisvelvollisuus.

Jatkovalmistelussa pykälään on lisätty säännös, jossa säädetään menettelystä tilanteessa, jossa tiedustelumenetelmän käytön kohteeksi lisätään uusi laite tai tietojärjestelmän osa. Lisäksi kotimaan tietojärjestelmätiedustelun keskeyttämisestä ehdotetaan säädettäväksi myös tiedustelumenetelmän käytön keskeyttämistä koskevassa pykälässä.

Tarkoitussidonnaisuuden periaatteen mukaisesti toimivaltuudella voitaisiin puuttua ainoastaan valtiollisen toimijan viestintään. Koska kyse on valtiollisen toimijan tietojärjestelmästä, ei voida pitää todennäköisenä, että satunnaiset ulkopuoliset henkilöt käyttäisivät tietojärjestelmää yksityiseen viestintäänsä. Näin ollen viestintää voidaan lähtökohtaisesti pitää valtiollisena viestintänä. Jos tietojärjestelmässä olisi myös muuta viestintää, koskisi sitä hetihävittämissääntely.

Lausunnoissa kiinnitettiin huomiota siihen, että säännös ei yksiselitteisesti koskisi ainoastaan Suomessa olevia tietojärjestelmän osia. Jatkovalmistelussa tähän on kiinnitetty huomiota.

Lausunnoissa tuotiin myös esiin, että toimivaltuus saattaa jopa parantaa oikeusturvaa siinä suhteessa, että tietojärjestelmätiedustelun luvasta päättävällä tuomioistuimella voisi olla paremmin mahdollisuus arvioida tiedustelumenetelmän kokonaisuutta.

Luonnoksen 1. lakiehdotuksen 62 a ja 62 b §n (tietojärjestelmän käytön estäminen tai sen toiminnan haittaaminen vakava vaaran torjumiseksi) osalta lausunnoissa nostettiin esiin huoli siitä, että toimenpiteiden suorittaminen voi aiheuttaa eskalaatiota ja heikentää Suomen ulko- ja turvallisuuspoliittista asemaa. Tämän katsottiin edellyttävät ulko- ja turvallisuuspoliittista

päätöksentekoa ja poikkihallinnollista valmistelua. Edellä todettujen seikkojen olisi hyvä näkyä myös itse pykälässä. Jatkovalmistelussa huomiot todettiin perustelluiksi.

Lausunnoissa huomioitiin myös, että säännöksen suhde varsinaiseen tiedonhankintaan jää säännöstasolla epäselväksi. Jatkovalmistelussa sääntely päätettiin liittää osaksi lain 62 §:ää.

Päätöksenteko toimenpiteiden suorittamisesta aiheutti lausunnonantajissa epäselvyyttä. Lausunnolla olleesta luonnoksesta saattoi saada kuvan, että pääesikunnan tiedustelupäällikkö voisi itsenäisesti päättää kyseisistä toimenpiteistä. Tämä ei ole kuitenkaan ollut tarkoituksena. Jatkovalmistelussa asiaa on selkeytetty säännöstasolla ja perusteluissa.

Osassa lausuntoja esitetyn sääntelyn tavoitteita pidettiin kannatettavina.

Luonnoksen 1. lakiehdotuksen 66 §:n (teknisten tietojen käsittely viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi) osalta kiinnitettiin huomiota siihen, miten tallennettavien tietojen määrä arvioidaan ja kuinka kattavaa tallentaminen on.

Jatkovalmistelussa perusteluja on pyritty selkeyttämään. Viisi prosenttia viestintäverkon osan kapasiteetista perustuisi yksittäisen kuidun tekniseen maksimikapasiteettiin, mikä pysyy vakiona. Järjestelmä johon tieto tallennetaan on toteutettava niin, että järjestelmään voidaan tallentaa ainoastaan viisi prosenttia kyseisestä maksimikapasiteetista per sekunti. Tämän jälkeen tallennettu tieto säilyy 18 kuukauden ajan järjestelmässä, jonka jälkeen se poistuu.

Toimivaltuuden kohteena on aina määritelty Suomen rajan ylittävä viestintäverkon osa, ei Suomen viestintäverkko kokonaisuudessaan. Viestintäverkon osan kapasiteetti ei käytännössä voi muuttua huomaamattomasti, sillä tekniset muutokset näkyvät viestintäverkon osan tietoliikenteessä esimerkiksi tietoliikenne katkoksina. Oletettavaa on, että mahdollisten teknisten muutosten myötä viestintäverkon osa kapasiteetti kasvaa, jolloin järjestelmän määritteet säilyvät ennallaan ja tietoja tallentuu vastaava määrä kuin vanhassa kapasiteetissa. Määrällisesti korkeampi tallentaminen edellyttää järjestelmä muutoksia.

Lausunnoissa nostettiin esiin käsitys, että sotilastiedusteluviranomainen voisi säännöksen nojalla tallennetuista tiedoista poimia yksittäisiä tietoja ja selvittää esimerkiksi lain 104 §:n nojalla tietoa lähteen. Tähän ei kuitenkaan ole mahdollisuutta, sillä tallennettuja tietoja voi käsitellä ainoastaan laissa erikseen säädetyksi ehdotetuissa tapauksissa, eli 67 a §:ssä sekä 68 ja 70 §:ssä säädetyin edellytyksin. Jotta tietoja voisi käsitellä, edellyttää tämä aina tuomioistuimen lupaa. Viime kädessä yksittäiseen tietoon liittyvä henkilö on selvitettävissä ainoastaan varsinaista tietoliikennetiedustelua käyttämällä, mikä edellyttää hakuehtojen käyttöä.

Lausunnoissa kiinnitettiin huomiota, että kielto muodostaa analyysissä tietoa, josta käy ilmi yksittäinen henkilö, ei pitäisi poistaa. Jatkovalmistelussa nimenomainen kielto on palautettu.

Luonnoksen 1. lakiehdotuksen 67 a §:n (tietoliikennetiedustelu hakuehtojen määrittämiseksi) lausunnoissa säännöksen viittausta tietoliikenteen satunnaisuuteen pidettiin epäselvänä. Satunnaisuus päätettiin poistaa jatkovalmistelussa.

Lausunnoissa kiinnitettiin huomiota siihen, että toimivaltuus ei saa mahdollistaa varsinaisen tietoliikennetiedustelun kiertämistä. Jatkovalmistelussa säännöstä on tarkennettu ja säännökseen on kirjattu nimenomaisia rajoitteita esimerkiksi siitä, että toimivaltuuden käytön lopputuloksena ei saa syntyä henkilön yksityiselämää kuvaavaa tietoa taikka viestinnän sisältöä kuvaavaa tietoa.

Lausunnoissa kiinnitettiin huomiota siihen, että tietoliikenteen satunnaisuutta voidaan pitää tulkinnan varaisena. Jatkovalmistelussa tämä päätettiin poistaa, koska joka tapauksessa viestintäverkon osassa liikkuu satunnaista tietoliikennettä, eli täysin tarkkaan ei voida ennakolta tietää, minkä tahon tietoliikennettä viestintäverkon osassa kunakin ajanhetkenä liikkuu. Käytännössä satunnaisuuteen ohjaa myös se, että toimivaltuuden kohteena voi olla 5 prosentti viestintäverkon osan tietoliikenteestä.

Luonnoksen 1. lakiehdotuksen 68 ja 70 §:n osalta otettiin kantaa siihen, että säännöksissä viestin sisältöön menevien hakuehtojen käyttöä ei rajata. Jatkovalmistelussa sääntelyä on tarkennettu ja sisältöön menevien sanallisten hakuehtojen käyttö on sidottu muiden hakuehtojen käyttöön. Muu kuin kielellinen sisältöhakuehtoa (kuten teknistä tietoa) voitaisiin käyttää sellaisenaan.

Lausunnoissa kiinnitettiin huomiota, että muutosta ei ole arvioitu säätämisjärjestysperusteluissa. Jatkovalmistelussa puute on korjattu.

Luonnoksen 1. lakiehdotuksen 78 §:n (tietolähteen turvaaminen) osalta tuotiin esiin, että ehdotus sisältää käsitteitä, joita voidaan pitää tulkinnanvaraisina ja joiden sisältä olisi selvennettävä perusteluissa. Jatkovalmistelussa säännöstä ja sen perusteluja on tarkennettu. Muun muassa avustaminen on vaihdettu rikoslain 17 luvussa käytettyyn termiin järjestää.

Luonnoksen 1. lakiehdotuksen 89 §:n (tiedustelumenetelmän käytöstä ilmoittaminen) osalta kiinnitettiin huomiota siihen, täyttääkö tiedusteluvalvontavaltuutetun suorittama valvonta ja mahdollisuus tehdä tutkimispyyntöjä ja kanteluita aiheutuvan oikeusturvavajeen. Eräät lausunnonantajat kiinnittivät huomiota siihen, että ilmoitusvelvollisuuden kaventamisen sijaan ilmoitusvelvollisuutta pitäisi vahvistaa tai ainakin pitää ennallaan. Toisaalta lausunnoissa todettiin, että asiaa olisi perusteltava vakuuttavammin perusteluissa. Jatkovalmistelussa perusteluja on tarkennettu.

Luonnoksen 1. lakiehdotuksen 96 §:n (viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan avustamisvelvollisuus) osalta tuotiin esiin, että ehdotettu muutos ei saisi johtaa tilanteeseen, jossa yritykset ja yhteisöt joutuisivat luopumaan päästä-päähän salauksesta. Jatkovalmistelussa todettiin, että tällaista sääntelyä ei olla ehdottamassa. Asia tuontiin kuitenkin perusteluissa esiin.

Lausunnoissa tuotiin esiin, että yrityksille avustamisesta suoritettavia korvauksia koskevaa sääntelyä pitäisi kehittää niin, että kaikesta avustamisesta maksettaisiin korvausta vastaavassa laajuudessa kuin mitä on säädetty tietoliikennetiedustelun edellyttämän liityntäpisteen toteuttamisen osalta. Jatkovalmistelussa todettiin, ettei asiaa voida tässä yhteydessä ratkaista, koska asia koskee laajempaa joukkoa viranomaisia kuin pelkästään sotilastiedusteluviranomaista. Esimerkiksi telekuuntelun osalta telekuuntelujärjestelmää käytetään huomattavasti paljon enemmän rikostorjunnassa kuin tiedustelutoiminnassa. Näin ollen asiantilan muuttaminen sotilastiedustelusta annetun lain muuttamista koskevassa hankkeessa ei ole tarkoituksen mukaista.

Lausunnoissa tuotiin esiin, että lausunnolla olleessa luonnoksessa ehdotettu avustamisvelvollisuuden laajennus olisi myös epämääräinen ja laajentaisi säännöksen soveltamista merkittävästi.

Jatkovalmistelussa soveltamisalan todettiin olevan liian laaja, ja esityksessä avustamisvelvollisuus koskisi ainoastaan datakeskuspalvelun tarjoajaa, siten kuin se on määritelty kyberturvallisuuslaissa. Lisäksi esityksessä on vaihdettu termi televerkko

viestintäverkkoon, mitä voidaan pitää paremmin kuvaavana myös sähköisen viestinnän palveluista annetun lain kannalta.

Luonnoksen 1. lakiehdotuksen 99 §:n (korvaus viestinnän välittäjälle ja tietoyhteiskunnan palvelun tarjoajalle) osalta tuotiin esiin, yrityksille avustamisesta suoritettavia korvauksia koskevaa sääntelyä pitäisi kehittää siten, että kaikesta avustamisesta maksettaisiin korvausta vastaavassa laajuudessa kuin mitä on säädetty tietoliikennetiedustelun edellyttämän liityntäpisteen toteuttamisen osalta.

Jatkovalmistelussa todettiin, ettei asiaa voida tässä yhteydessä ratkaista, koska asia koskee laajempaa joukkoa viranomaisia kuin pelkästään sotilastiedusteluviranomaista. Esimerkiksi telekuuntelun osalta telekuuntelujärjestelmää käytetään huomattavasti paljon enemmän rikostorjunnassa kuin tiedustelutoiminnassa. Näin ollen asiantilan muuttaminen sotilastiedustelusta annetun lain muuttamista koskevassa hankkeessa ei ole perusteltua.

Luonnoksen 1. lakiehdotuksen 104 §:n (tietojen saanti yksityiseltä yhteisöltä) osalta lausunnoissa pidettiin ehdotettua muutosta perusteltuna. Lausunnoissa tuotiin kuitenkin esiin käsitys, että ehdotuksella pystyttäisiin kiertämään esimerkiksi telekuuntelua. Ehdotus koskee kuitenkin yksittäisiä tietoja eikä se aseta viestinnän välittäjälle laajoja velvollisuuksia esimerkiksi käsitellä tietoa viranomaisen puolesta. Sääntely lisäksi vastaa sitä, mitä esimerkiksi poliisilaissa on säädetty 4 luvun 3 §:ssä.

Vastaavasti kuin aiemmin on jo tuotu esiin, tietoyhteiskunnan palvelun tarjoaja on jatkovalmistelussa korvattu datakeskuspalvelun tarjoajalla.

Luonnoksen 2. lakiehdotuksen 8 b §:ää (tiedonhankinta yleisesti saatavilla olevista lähteistä) koskevissa lausunnoissa huomiota kiinnitettiin siihen, ettei mahdollisuus käyttää tekaistuja, harhauttavia tai peiteltyjä tietoja yleisesti saatavilla olevissa laillisissa palveluissa saa johtaa siihen, että viranomainen ei maksaisi palvelusta tai muutenkaan aiheuttaisi vahinkoa palveluntarjoajalle. Toisaalta lausunnoissa tuotiin esiin, että suojaamisen olisi tarkoituksen mukaista ulottua jopa tätä pidemmälle, kuten maksun suorittamiseen peitteen turvin.

Lausunnoissa kiinnitettiin huomiota myös sääntelyyn siltä osin, että miten yksittäistä viranomaista koskeva sääntely suhteutuu oikeusjärjestyksen tasolla muita viranomaisia koskevaan sääntelyyn.

Jatkovalmistelussa edellä mainittuja seikkoja on pyritty tuomaan esiin. Joka tapauksessa lausunnoista mahdollisesti esiin noussut kuva siitä, että viranomainen pyrkisi käyttämään kaupallisia palveluita maksamatta, voidaan pitää perusteettomana.

Luonnoksen 2. lakiehdotuksen 36 a §:n (viran haettavaksi julistaminen) osalta tuotiin esiin, että esityksessä olisi huomioitava tarkemmin vastaavan kaltainen sääntely esimerkiksi suojelupoliisin virkojen täytön osalta. Lisäksi viitattiin perustuslakivaliokunnan lausuntoon (PeVL 45/2022 vp.). Jatkovalmistelussa välttämättömyysarviointiin liittyviä seikkoja on tuotu säännöksessä ja sen perusteluissa tarkemmin esille.

Luonnoksessa ollut rikoslain muutos poistettiin tarpeettomana, sillä riittävä sääntely voidaan toteuttaa ainoastaan sotilastiedustelusta annettua lakia muuttamalla.

Lausunnoissa kiinnitettiin huomiota tietojen saantia koskeviin muutosehdotuksiin, joiden osalta todettiin, että valtaosa tieoista, joita muutokset koskisivat, olisi saatavissa jo voimassa olevan

lain nojalla. Lisäksi luonnoksessa olleita muita liitelakeja ja niitä koskevia perusteluja täsmennettiin.

Henkilötietojen käsittelyn osalta lausunnoissa kiinnitettiin huomiota siihen, onko muualla laissa säädetty oikeus salassapitosäännösten estämättä luovuttaa henkilörekisteristään teknisen käyttöyhteyden avulla tai tietojoukkona henkilötietoja Puolustusvoimille oikeutena yhtenevä voimassa olevien sotilastiedusteluviranomaisen tiedonsaantioikeuksien kanssa. Epäselväksi jääkin se, että mitä tarkoitetaan tietojen vertaamisella. Jatkovalmistelussa asiaan pyritty selkeyttämään. Joka tapauksessa sääntely vastaisi sitä, mitä suojelupoliisille on säädetty.

Lisäksi lausunnoissa kiinnitettiin huomiota siihen, että henkilötietojen käsittelyn osalta lausunnolla olleessa luonnoksessa ei juurikaan käsitelty asiaa säätämisjärjestysperusteluissa eikä asiaa koskevaa uudempaa perustuslakivaliokunnan lausuntokäytäntöä huomioitu.

Jatkovalmistelussa edellä kuvatut huomiot on pyritty ottamaan huomioon. Lisäksi jatkovalmistelussa tuotiin esiin tarve sotilastiedustelun virkamiehen turvaamista koskevan sääntelyn kehittämiselle ja telekuuntelun kiirepäätökselle.

6.2 Lainsäädännön arviointineuvoston lausunto

Lainsäädännön arviointineuvosto antoi esitysluonnoksesta lausunnon 4.5.2026 (asianumero VN/13863/2025-VNK-3). Arviointineuvosto katsoi, että hallituksen esitysluonnos noudattaa tyydyttävästi lainvalmistelun vaikutusarviointiohjetta. Arviointineuvosto suosittelee, että esitysluonnosta korjataan neuvoston lausunnon mukaisesti ennen hallituksen esityksen antamista.

Esitysluonnoksen perusteella saa pääosin käsityksen asian taustasta, tavoitteista ja keskeisistä ehdotuksista. Esitysluonnoksessa vaikutuksia on käsitelty useasta näkökulmasta, mutta vaikutusarvioinnin keskeiset johtopäätökset ja vaikutusketjut eivät kaikilta osin käy selkeästi ilmi. Keskeiset kehittämiskohteet liittyvät erityisesti vaikutusten mittaluokan, kohdentumisen ja epävarmuuksien täsmällisempään kuvaamiseen sekä siihen, että vaikutusarviointi jää useissa kohdissa yleisemmälle tasolle kuin nykytilan arviointi.

Arviointineuvosto katsoo, että esitysluonnoksessa vaikutuksia on käsitelty varsin laajasti ja että luonnos kattaa keskeiset vaikutusalueet. Ansiona voidaan pitää myös sitä, ettei vaikutusjakso rajoitu pelkästään sääntelyn tavoiteltujen hyötyjen kuvaamiseen, vaan luonnoksessa tunnistetaan useissa kohdissa myös oikeuksiin puuttumista, teknisiä riskejä, yritystoimintaan kohdistuvia haittoja sekä kansainvälisiin suhteisiin liittyviä jännitteitä.

Arviointineuvosto katsoo, että nykytilan arvioinnin ollessa yksityiskohtainen ja selkeä, jää vaikutusarviointi useissa kohdissa yleisemmälle tasolle; arvioiden painopiste siirtyy usein takaisin muutosten kuvaukseen ja perusteluihin.

Arviointineuvosto katsoo, että esitysluonnoksen yritysvaikutuksia koskevassa jaksossa tunnistetaan useita olennaisia vaikutusmekanismeja. Arviointi kohdistuu muun muassa hallinnollisiin kustannuksiin, avustamisvelvollisuuksiin, tietoturvapoikkeamien käsittelyyn, luottamukseen ja aineettomaan omaisuuteen sekä kyberriskeihin. Arviointi jää kuitenkin suurelta osin laadulliseksi, eikä vaikutusten mittaluokasta esitetä määrällisiä arvioita. Esitysluonnoksessa on tunnistettu myös yrityksille mahdollisesti koituvia hyötyjä, mutta hyötyvaikutusten arviointi jää kuitenkin yleiselle tasolle.

Arviointineuvosto kiinnittää huomiota siihen, että esitysluonnoksessa ei ole erillistä jaksoa julkistaloudellisista vaikutuksista. Taloudelliset vaikutukset tulisi vaikutusarvio-ohjeen mukaan jäsentää vaikutuksina kotitalouksiin, yrityksiin ja julkiseen talouteen.

Arviointineuvosto katsoo, että esitysluonnoksen vaikutukset kansantalouteen ja elinkeinoelämään -jakso on perustellusti lähtenyt siitä, että sotilastiedustelulainsäädännöllä voi olla yrityksille ja kansantaloudelle myös myönteisiä vaikutuksia. Esitysluonnoksessa olisi kuitenkin hyödyllistä kuvata nykyistä täsmällisemmin, millä vaikutusmekanismeilla tällaiset hyödyt voivat välittyä elinkeinoelämään ja kansantalouteen, kuinka merkittävinä niitä pidetään ja mihin tällaiset arviot perustuvat.

Arviointineuvosto pitää myönteisenä, että esitysluonnoksessa tunnistetaan perus- ja ihmisoikeuskytkennät laajasti. Esitysluonnos tunnistaa yksityiselämän suojaan, luottamuksellisen viestin suojaan, oikeusturvaan ja henkilötietojen suojaan liittyviä kysymyksiä. Lisäksi luonnoksessa on laaja erillinen jakso suhteesta perustuslakiin ja säätämisjärjestykseen.

Arviointineuvosto katsoo, että perus- ja ihmisoikeuksia koskevan kokonaisuuden esitystapaa heikentävät toisteisuus ja paikoin pitkät virkkeet. Vaikutusarvioinnissa ja esityksen myöhemmässä perustuslakia ja säätämisjärjestystä koskevassa jaksossa käsitellään osin samoja arvioita ja perusteluja hieman eri sanamuodoin, minkä vuoksi kokonaisuus jää raskaaksi.

Arviointineuvosto katsoo, että viranomaisvaikutuksia on tunnistettu esitysluonnoksessa varsin hyvin. Ehdotukset koskevat muun muassa sotilastiedusteluviranomaisen toimivaltuuksia, Rajavartiolaitoksen avustamisroolia, tiedonvaihtoa eri viranomaisten välillä sekä uusien tehtävien ja teknisten ratkaisujen käyttöönottoa. Vaikutusarviota parantaisi kuitenkin vaikutusten tarkempi erittely viranomaistahoittain. Esitysluonnoksessa olisi perusteltua eritellä ainakin Puolustusvoimien, Rajavartiolaitoksen, tiedusteluvalvontavaltuutetun, tuomioistuinten sekä tietoja luovuttavien muiden viranomaisten työmäärä-, osaamis-, järjestelmä- ja koordinointivaikutuksia nykyistä täsmällisemmin.

Arviointineuvosto pitää myönteisenä, että esitysluonnos tunnistaa tiedonhallintavaikutukset omana vaikutusalueenaan.

Arviointineuvosto katsoo, että esitysluonnoksessa useita toimeenpanoon ja viranomaisten resursointiin liittyviä vaikutuksia kuvataan varsin yleisluonteisesti.

Arviointineuvosto katsoo, että esityksen keskeisin tavoiteltu vaikutus liittyy maanpuolustuksen ja kansallisen turvallisuuden vahvistamiseen. Näitä vaikutuksia koskeva arviointi jää kuitenkin melko yleiselle tasolle, etenkin kun otetaan huomioon, kuinka huolellisesti ehdotettujen muutosten tarvetta on perusteltu esitysluonnoksen nykytilan kuvauksessa. Arvio antaa käsityksen vaikutusten suunnasta, mutta siitä ei kaikilta osin käy riittävän selvästi ilmi, mitä lisähyötyä yksittäisillä muutoksilla arvioidaan saavutettavan nykytilaan verrattuna, kuinka usein nykytilan puutteet käytännössä ilmenevät tai mihin arvio eri turvallisuushyödyistä perustuu. Arviointineuvosto pitää kuitenkin ymmärrettävän**ä,** ettei kaikkia vaikutuksia voida niiden luonteen vuoksi kaikilta osin kuvata täsmällisesti.

Arviointineuvosto katsoo, että esitysluonnoksessa tuodaan laadullisesti esiin sääntelyn mahdolliset myönteiset vaikutukset tietoturvaan ja yhteiskunnan toimintavarmuuteen. Hyötyjen mittaluokka, toteutumisen ehdot ja mahdolliset haittariskit jäävät kuitenkin melko yleiselle tasolle. Vaikutusarviossa olisi hyödyllistä arvioida tarkemmin, kuinka usein uusia

toimivaltuuksia arvioidaan käytettävän ja millaisissa tilanteissa vaikutukset voivat olla merkittäviä.

Arviointineuvosto katsoo, että esitysluonnos tunnistaa rajat ylittäviä vaikutuksia. Tässä vaikutuslajissa olisi kuitenkin hyödyllistä jäsentää tarkemmin vaikutuksia kansainväliseen tiedusteluyhteistyöhön, Suomen suhteisiin muihin valtioihin sekä tilanteisiin, joissa yhteistyö kohdevaltion kanssa ei ole mahdollista. Vaikutuksia tulisi käsitellä tarkemmin myös erilaisten riskien näkökulmasta.

Arviointineuvoston lausunnon perusteella esityksen vaikutusarviointia on täydennetty ja muokattu. Kaikilta osin vaikutuksia tai tarkempaa suuntaa antavaa arviota niistä ei voida antaa, koska tiedot eivät ole julkisia.

7 Säännöskohtaiset perustelut

7.1 Laki sotilastiedustelusta

11 §. *Sotilastiedusteluviranomaiset.* Pykälän 2 momenttia muutettaisiin. Tiedustelutehtäviä suorittaessaan puolustushaarat olisivat nykytilaa vastaavasti edelleen sotilastiedusteluviranomaisen ohjauksen ja valvonnan alaisia. Ehdotuksen myötä Maa-, Meri- ja Ilmavoimat voisivat käyttää tiedustelutehtävän suorittamiseksi voimassa olevassa laissa säädetyn radiosignaalitiedustelun lisäksi tavanomaista, perusmuotoista tietolähdetoimintaa. Puolustushaarat eivät voisi ohjata henkilöä hankkimaan tietoa. Havaintojen ja tietojen toimittaminen perustuisi aina henkilöiden vapaaehtoisuuteen ja tietojen olisi liityttävä sotilastiedusteluviranomaisen tiedustelutehtävään.

Muutoksella mahdollistettaisiin tietojen vastaanottaminen sotilastiedusteluviranomaiselle silloinkin, kun henkilöt esimerkiksi paikallisesti rajan tuntumassa tai ulkomailla liikkuessaan havaitsevat mielestään tavanomaisesta poikkeavaa toimintaa. Perusmuotoisen tietolähdetoiminnan toimivaltuus on merkityksellinen myös tietolähteen kannalta. Koska tietolähteellä on oma-aloitteinen halu kertoa tietämistään toimintaan liittyvistä asioista, olisi perusteltua, että hän voisi lähestyä viranomaista hänelle sopivimpana aikana ja sopivimmassa paikassa.

Puolustushaarojen radiosignaalitiedustelun osalta ei tehtäisi muutoksia ja puolustushaarojen tiedustelusta tältä osin säädettäisiin edelleen lain 60 §:ssä.

15 §. *Tiedustelutoiminnan yhteensovittaminen.* Pykälän 1 momenttia muutettaisiin niin, että viittaus tasavallan presidenttiin vaihdettaisiin tasavallan presidentin kansliaksi. Kokoonpanossa on edustettuna keskeiset korkeimmat virkamiehet eikä alun perinkään ole ollut tarkoitus, että tasavallan presidentti osallistuu koordinaatioon. Jo voimassa olevaa lakia on tulkittu niin, että tasavallan presidentin kanslian edustajan osallistuu kokouksiin, joten säännösteksti saatettaisiin vastaamaan nykytilaa.

18 §. *Yhteistyö muiden viranomaisten sekä yritysten ja muiden yhteisöjen kanssa.* Pykälän 1 momenttiin tehtäisiin tekninen muutos ja säännöksen ensimmäisestä virkkeestä poistettaisiin sana ”tietoja” ja momentin toinen virke, joka viittaa henkilötietojen käsittelyä koskevaan lakiin Puolustusvoimissa. Viittaus henkilötietojen käsittelystä Puolustusvoimissa annettuun lakiin on jo lain 2 §:ssä, joten 18 §:n 1 momentin viittausta voidaan pitää tarpeettomana.

Pykälän 2 momenttiin tehtäisiin muutos, joka koskisi haittaohjelmia. Muutoksen myötä lain 74 § kumottaisiin. Nykytilassa säännös on sitonut tietojen luovuttamisen tiedustelun menetelmien

ja järjestelmien kehittämiseksi, eli tietojen luovuttaminen haittaohjelmista on sidottu tiedustelun tarpeeseen. Tätä voidaan pitää tarpeettomana rajauksena, koska haittaohjelmatietojen luovuttamisen olisi tapahduttava mahdollisimman matalalla kynnyksellä. Luovuttaminen olisi edelleen sidottu sotilastiedusteluviranomaisen tehtävään.

Säännöksen jälkimmäisessä osassa tietojen luovuttaminen olisi sidottu tarpeellisuuteen maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi. Tämä tarkoittaisi sitä, että tietojen luovutuksella voitaisiin parantaa Suomen maanpuolustusta tai kansallista turvallisuutta, ja tiedonluovutuksella olisi oltava liityntä näihin etuihin.

Kyberympäristön merkitys yhteiskunnassa ja sitä kautta maanpuolustuksessa ja kansallisessa turvallisuudessa on jatkanut kasvuaan entisestään. Teknologian kehityksen myötä myös kehittyneet niin kutsutut APT-toimijat kehittävät toimintatapojaan edelleen. Etenkin näiden toimijoiden haittaohjelmia koskevien tietojen luovuttaminen on voitava tapahtua yhteiskunnan toiminnan kannalta kriittisille toimijoille mahdollisimman matalalla kynnyksellä. On myös huomattava, että haittaohjelmaa koskeva tieto ei perusoikeuksien kannalta kuulu luottamuksellisen viestin alaan.

Säännöksen viittaus tiedon luovuttamiseen, jos se on tarpeen maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi, tarkoittaisi myös tilanteita, joissa sotilastiedusteluviranomaisen toimenpiteestä voisi syntyä riski maanpuolustukselle tai kansalliselle turvallisuudelle. Esimerkiksi tilanteessa, jossa sotilastiedusteluviranomaisen toimenpide aiheuttaisi kohteena olevan toimijan eskalatorisia toimenpiteitä, esimerkiksi kyberhyökkäyksen suomalaisia teleoperaattoreita vastaan, sotilastiedusteluviranomaisen olisi tarkoituksenmukaista ilmoittaa riskistä Suomen kriittisestä viestintäinfrastruktuurista vastaaville toimijoille. Vastaava voisi tulla kyseeseen myös muiden kriittisten toimijoiden osalta. Ilmoittamisella varmistettaisiin se, että kriittisestä infrastruktuurista vastaavat toimijat pystyisivät omin toimenpitein varautumaan ja käynnistämään omat toimenpiteensä haitallisen toiminnan ehkäisemiseksi.

Vastaavasti, jos sotilastiedusteluviranomainen käyttäisi esimerkiksi havaitsemaansa laitteen tai ohjelmiston haavoittuvuutta taikka asentaisi takaportin kohteena olevaan järjestelmään, sotilastiedusteluvirnaomaisen olisi tarkoituksenmukaista ilmoittaa asiasta laitteen tai tietojärjestelmän haltijalle, jos se on mahdollista ja jos haavoittuvuudesta tai sotilastiedusteluviranomaisen omasta toimenpiteestä voi aiheutua vaaraa maanpuolustukselle tai kansalliselle turvallisuudelle.

Pykälän 3 momenttiin tehtäisiin niin kutsutun palomuurisääntelyn uudistamisesta johtuvat pykäläviittausten muutokset (laki sotilastiedustelusta annetun lain muuttamisesta 169/2026).)

Pykälän 4 momenttiin, jossa säädetään asetuksenantovaltuudesta, ei tehtäisi muutoksia.

18 a §. *Yhteistoiminta Rajavartiolaitoksen kanssa*. Pykälä olisi uusi. Pykälässä säädettäisiin Rajavartiolaitoksen mahdollisuudesta avustaa sotilastiedusteluviranomaista tiedustelutehtävän suorittamisessa osallistumalla tiedustelumenetelmien käyttöön. Sotilastiedusteluviranomaisen ja Rajavartiolaitoksen väliseen yhteistoimintaan sovelletaan lähtökohtaisesti sotilastiedustelusta annetun lain 18 §:ää, mutta käytännön toiminnassa, erityisesti tiedustelumenetelmien käyttöön liittyvissä yksittäistapauksissa, on kuitenkin havaittu olevan Rajavartiolaitoksen tuelle laajempia tarpeita. Kyse olisi siis lyhytaikaisesta, yksittäisten tiedustelutehtävään liittyvien tehtävien tai toimenpiteiden lyhytaikaisesta suorittamisesta ja ne tapahtuisivat aina sotilastiedusteluviranomaisen pyynnöstä ja toimivallassa. Pyyntö voisi olla tietyissä tilanteissa

ennalta tehty tai se voisi tapahtua nopeampaa reagointia vaativissa tilanteissa viranomaisten välisten päivystysjärjestelyjen kautta.

Sotilastiedusteluviranomaisen toimenpiteiden on aina oltava puolustettavia suhteessa tiedonhankinnan merkittävyyteen. Myös Rajavartiolaitokselle tehtävää yksittäistä toimenpidettä koskevaa pyyntöä olisi siten aina arvioitava sillä tavoiteltavaan päämäärään nähden. Tiedonhankintatoimenpiteiden mitoittamiseen vaikuttaisi esimerkiksi se, kuinka oleellinen merkitys tietyllä yksittäisellä toimenpiteellä on uhkaan liittyvien tietojen hankinnan kannalta eikä toimenpiteellä saisi puuttua kenenkään oikeuksiin enempää kuin on välttämätöntä tiedustelun käytön tarkoituksen saavuttamiseksi.

Pykälän 1 momentissa säädettäisiin, että lain 18 §:n lisäksi Rajavartiolaitos voisi avustaa pykälässä lueteltujen tiedustelumenetelmien käytössä. Tiedustelumenetelmään liittyvällä yksittäisellä toimenpiteellä tarkoitettaisiin esimerkiksi menetelmän käyttöön liittyvää teknistä asennustoimenpidettä taikka henkilöön tai henkilöryhmään tilapäisesti kohdistuvaa tarkkailua. Luettelo olisi tyhjentävä ja koskisi ensisijaisesti vain niitä tiedustelumenetelmiä, joista päätöksen voi lain mukaan tehdä tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies. Tällaisia tiedustelumenetelmiä olisivat tarkkailu ja suunnitelmallinen tarkkailu, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen laitetarkkailu, teleosoitteen tai telepäätelaiteen yksilöintitietojen hankkiminen, laitteen sekä menetelmän tai ohjelmiston asentaminen ja poisottaminen sekä paikkatiedustelu ja jäljentäminen. Rajavartiolaitos voisi kuitenkin avustaa teknisessä kuuntelussa, katselussa ja seurannassa, teknisessä laitetarkkailussa sekä paikkatiedustelussa ja jäljentämisessä myös silloin, kun tiedustelumenetelmän käyttöön liittyvän luvan on antanut tuomioistuin. Kyseeseen tulisi siis joukko tiedustelumenetelmiä, joiden käyttö sekä siihen liittyvät yksittäiset toimenpiteet vastaisivat toteutukseltaan lähinnä Rajavartiolaitoksen omissa tehtävissään käyttämiä salaisia tiedonhankintakeinoja ja joissa sillä jo olisi vastaavaa käytännön kokemusta yksittäisen tehtävän tai toimenpiteen suorittamisesta. Rajavartiolaitoksen toimenpiteissä ei olisi kuitenkaan kyse tiedustelutoiminnasta, sillä toimenpiteellä saatujen tietojen käsittely ja analysointi olisi aina sotilastiedusteluviranomaisella. Toiminta tapahtuisi sotilastiedusteluviranomaisen toimivallassa, ohjauksessa ja valvonnassa.

Luetelluista toimivaltuuksista tekninen kuuntelu, tekninen laitetarkkailu ja jäljentäminen voivat kohdistua viestin sisältöön. Toimenpiteen jälkeen tiedot ohjautuisivat tai siirrettäisiin suoraan sotilastiedusteluviranomaiselle. Viestin sisältöön menevien tiedustelumenetelmien osalta on usein kyse tilanteesta, jossa tehdään asennustoimenpide ja tiedot ohjautuvat suoraan sotilastiedusteluviranomaiselle.

Tekninen laitetarkkailukin voi kohdistua viestin suojaan, mutta käytännössä Rajavartiolaitoksen alueellisessa toimivallassa kyse olisi teknisen laitteen, kuten tallennusvälineen, sisältämien tietojen kopioinnista ja kopion toimittamisesta sotilastiedusteluviranomaiselle. Näin ollen Rajavartiolaitos ei pystyisi perehtymään viestin sisältöön, mikä ei ole myöskään toimenpiteiden tarkoitus. Jäljentämisessäkin on kyse teknisestä toimenpiteestä.

Sotilastiedusteluviranomaisella olisi kuitenkin siitä riippumatta velvollisuus järjestää tehtäviä tai toimenpiteitä suorittavalle Rajavartiolaitoksen henkilöstölle tiedustelumenetelmiin liittyvien erityispiirteiden koulutusta. Sotilastiedusteluviranomainen vastaisi niin ikään tiedustelumenetelmää koskevasta päätöksestä tai luvasta, sekä 89 §:n mukaisesta ilmoitusvelvollisuudesta.

Rajavartiolaitoksen suorittamien toimenpiteiden luonne vaihtelee tiedustelumenetelmä kohtaisesti. Joissain tilanteissa välttämättömässä toimenpiteessä saattaa olla kyse laitteen,

menetelmän tai ohjelmiston asentamisesta, kun taas esimerkiksi tekninen kuuntelu saattaa edellyttää myös kohteen seuraamista tietyn matkan päästä. Sotilastiedustelusta annetun lain yleisten periaatteiden mukaisesti toimenpiteiden olisi täytettävä esimerkiksi suhteellisuusperiaate sekä vähimmän haitan periaate.

Toimenpiteiden suorittaminen olisi sidottu välttämättömyyteen. Tällä tarkoitettaisiin sitä, että sotilastiedusteluviranomainen ei ehtisi paikalle käynnistämään tiedustelumenetelmän käyttöä. Tästä esimerkkinä olisi tilanne, jossa sotilastiedustelun kohde saapuu raja-alueelle eikä suunnitelmallista tarkkailua pystytä aloittamaan, ellei raja-alueella oleva rajamies aloittaisi sitä.

Välttämättömyydellä tarkoitettaisiin myös sitä, että Rajavartiolaitos voisi suorittaa toimenpidettä ainoastaan välttämättömän ajan, eli sotilastiedusteluviranomaisen olisi otettava tiedustelumenetelmän käyttö itselleen mahdollisimman pian.

Pykälän 1 momentissa säädettäisiin lisäksi, että Rajavartiolaitoksen olisi sotilastiedusteluviranomaisen pyynnöstä ilman aiheetonta viivytystä keskeytettävä tässä momentissa tarkoitettu toimenpide, eli käytännössä heti, kun se olisi mahdollista esimerkiksi vaarantamatta menetelmän käytön tarkoitusta. Keskeytystä koskeva pyyntö voisi tulla kyseeseen esimerkiksi tilanteessa, jossa tuomioistuin toteaisi, ettei sotilastiedusteluviranomaisen tiedustelumenetelmää koskevalle kiirepäätökselle olisi ollut lupaan oikeuttavia perusteita. Pyyntö keskeytyksestä voitaisiin tehdä myös Rajavartiolaitoksen ilmoituksen perusteella, mikäli Rajavartiolaitos arvioisi, ettei sillä kyseisellä hetkellä olisi, esimerkiksi omista lakisääteisistä tehtävistään johtuen, mahdollisuuksia pyydetyn toimenpiteen suorittamiseen tai sen jatkamiseen taikka sotilastiedusteluviranomainen toteaisi, että sillä olisi itsellä mahdollisuus toteuttaa pyydetty toimenpide. Toimenpiteen suorittamisen tarpeellisuutta olisi arvioitava koko aika.

Ehdotettavan 2 momentin mukaan Rajavartiolaitos voisi tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen pyynnöstä suorittaa Rajavartiolaitokselle säädetyn tehtävän yhteydessä rajavartiolain (578/2005) 28 §:ssä tarkoitettuja toimenpiteitä, jotka olisivat välttämättömiä sotilastiedustelutehtävän kannalta, silloin kun sotilastiedusteluviranomaisella ei olisi toimivaltuutta yksittäisen tehtävän suorittamiseen, Kyse olisi siis Rajavartiolaitoksen antamasta avusta sotilastiedusteluviranomaiselle, joka olisi eräänlainen virka-avun ja yhteistoiminnan välimuoto, joka edesauttaisi muun muassa viranomaisten järkevää ja tehokkaampaa resurssien käyttöä. Rajavartiolaitos käyttäisi erityisosaamistaan ja sotilastiedusteluviranomainen voisi saadun tiedon avulla toimia tehokkaammin omalla erityisosaamisalueellaan.

Toimenpiteitä voisi momentin perusteella toteuttaa sotilastiedusteluviranomaisen tiedustelutehtävän edellyttämässä laajuudessa ja niille asetettaisiin välttämättömyysedellytys. Välttämättömyyttä olisi arvioitava suoritettavien 1 momentissa tarkoitettujen toimenpiteiden kannalta, mutta myös sen kannalta, ehtisikö sotilastiedusteluviranomainen itse paikalle suorittamaan tiedustelumenetelmien käyttöä.

On huomattava, että Rajavartiolaitoksella olisi jo käsitys siitä, kenet kannattaa ottaa tarkempaan rajatarkastukseen. Oletettavaa on, että myös Rajavartiolaitoksen tehtävien näkökulmasta on perusteltua tarkastaa kyseinen henkilö, vaikka ensisijainen tarve vaikuttaisikin olevan sotilastiedustelullinen.

Rajavartiolain 28 §:ssä säädetään rajavalvontaa koskevista toimivaltuuksista. Pykälän 1 momentin mukaan rajavartiomiehellä on Schengenin rajasäännöstössä tarkoitetun rajavalvonnan suorittamiseksi oikeus ilman rikosepäilyä suorittaa momentin 1–11 kohdissa

lueteltuja toimenpiteitä Schengenin rajasäännöstön edellyttämässä laajuudessa. Schengenin rajasäännöstön johdanto-osan 6 kohdan mukaan rajavalvonnan olisi autettava torjumaan laitonta maahanmuuttoa ja ihmiskauppaa ja ehkäisemään jäsenvaltioiden sisäiseen turvallisuuteen, yleiseen järjestykseen, kansanterveyteen ja kansainvälisiin suhteisiin kohdistuvat uhkat.

Rajavalvonnassa rajatarkastus voi vähimmäistarkastuksena yksinkertaisimmillaan olla henkilöllisyyden ja matkustusasiakirjojen tarkastamista sekä muiden maahantuloedellytysten täyttymisen varmistamista esimerkiksi kyselemällä matkan tarkoituksesta sekä sen varmistamista, että henkilöllä on riittävät varat ilmoitetun oleskelunsa ajalle. Sotilastiedustelutehtävän edellyttämällä laajuudella tarkoitettaisiin rajavartiolain 28 §:ssä säädettyjen toimenpiteiden, kuten esimerkiksi perusteellisemman tarkastuksen, toteuttamista laajemmin kuin esimerkiksi rajavalvonnassa olisi yksittäistapauksessa muuten tarpeen. Momentti ei rajoittaisi Rajavartiolaitoksen osallistumista ainoastaan rajavalvonnan yhteydessä toteutettaviin tehtäviin. Tarkoituksenmukaista olisi, että Rajavartiolaitos voisi sotilastiedusteluviranomaisen pyynnöstä toteuttaa 28 §:ssä tarkoitettuja toimenpiteitä myös muiden tehtäviensä yhteydessä esimerkiksi silloin, kun se suorittaa vesiliikenteen valvontaa tai alustarkastuksia. Toimenpiteissä voisi esimerkiksi olla kyse henkilön hallussa olevien asiakirjojen, tämän mukana olevien tavaroiden tai hänen käyttämänsä kulkuneuvon tarkastaminen tai siihen kohdistettava etsintä, tai henkilön matkustusasiakirjojen jäljentäminen esimerkiksi valokuvaamalla.

Toteutettavien toimenpiteiden tulisi aina olla välttämättömiä sotilastiedusteluviranomaisen tiedustelutehtävän kannalta. Välttämättömyyttä arvioitaessa tulisi ottaa huomioon, olisiko pyydetty toimenpide välttämätön tiedustelutehtävän kannalta ja olisiko välttämätöntä, että sen suorittaisi Rajavartiolaitos, jotta sotilastiedusteluviranomaisen tehtävien suorittaminen onnistuisi. Rajaylitystilanne voi olla ainoa hetki, jolloin sotilastiedustelun kohteen halussa olevaa omaisuutta voitaisiin tutkia, olisi kyse sitten asiakirjoista, tietotekniikasta tai aineista. Välttämättömyys voisi tarkoittaa esimerkiksi sitä, ettei sotilastiedusteluviranomaisen pyytämää toimenpidettä olisi mahdollista toteuttaa muussa yhteydessä tai, ettei sotilastiedusteluviranomainen voisi esimerkiksi asian kiireellisyyden vuoksi lähtökohtaisesti toteuttaa sitä itse. Rajavartiolaitos voisi lisäksi aina kieltäytyä pyydetyn toimenpiteen toteuttamisesta, mikäli se arvioisi, ettei sillä olisi sen toteuttamiseen tarvittavia edellytyksiä tai se voisi vaarantaa Rajavartiolaitoksen omien lakisääteisten tehtävien suorittamista. Rajavartiolaitoksen yhteistoiminnan sotilastiedusteluviranomaisten kanssa tulisi alueellisesti kohdentua rajavartiolain 4 §:n mukaisesti.

Pykälän 2 momentissa säädettäisiin lisäksi, että toimenpiteen kohteena oleva henkilö olisi velvollinen olemaan läsnä toimenpiteitä suoritettaessa enintään 12 tuntia kerrallaan ja toimenpiteen suorittamisesta päättäisi rajanylityspaikan esimies tai vähintään luutnantin arvoinen rajavartiomies. Koska momentissa viitattaisiin rajavartiolain 28 §:ssä tarkoitettuihin toimenpiteisiin, joiden toteuttamiseksi Rajavartiolaitokselle on säädetty enintään 12 tunnin aika, olisi tarkoituksenmukaista säätää läsnäolovelvollisuus saman mittaiseksi. Toimenpiteistä voisi päättää rajanylityspaikan esimiehenä toimiva rajavartiomies sekä vähintään luutnantin arvoinen rajavartiomies, joilla katsotaan olevan koulutuksen ja kokemuksensa puolesta riittävä tietotaito päätöksen tekemiseen.

Ehdotettu pykälän 3 momentti sisältäisi oikeuden 2 momentissa säädetyissä tilanteissa käyttää vääriä, harhauttavia tai peiteltyjä tietoja 2 momentissa tarkoitettujen toimenpiteiden suorittamiseksi silloin, kun se olisi välttämätöntä toimenpiteen paljastumisen estämiseksi. Sotilastiedusteluviranomaisen tiedustelutehtävän suorittaminen ja tiedonhankinta sekä siinä käytettävät keinot ja menetelmät olisi kyettävä tarvittaessa suojaamaan niiden paljastumisen

estämiseksi myös silloin kun Rajavartiolaitos oman tehtävänsä yhteydessä suorittaisi yksittäisiä toimenpiteitä. Väärien, harhauttavien tai peiteltyjen tietojen käyttämisen tarkoituksena olisi siis tarve olla paljastamatta tiedonhankinnan kohteelle, että rajavalvonnassa käytettävää toimivaltuutta vastaavaa toimivaltuutta käytetäänkin kokonaan tai osittain tiedustelutarkoituksessa. Rajavartiolaitos ei silloin olisi velvollinen esimerkiksi ilmoittamaan toimenpiteen kohteelle rajatarkastuksen laajuuteen vaikuttavaa tosiasiallista syytä. Päätöksen suojaamisesta voisi tehdä rajanylityspaikan esimiehenä toimiva rajavartiomies sekä vähintään luutnantin arvoinen rajavartiomies, joilla katsotaan olevan koulutuksen ja kokemuksensa puolesta riittävä tietotaito päätöksen tekemiseen.

Pykälän 4 momentin mukaan Rajavartiolaitoksen olisi luovutettava tässä pykälässä tarkoitetulla toimenpiteellä saadut tallenteet ja asiakirjat käsittelemättöminä sotilastiedusteluviranomaiselle, sekä hävitettävä toimenpiteen suorittamisessa syntyneet tallenteet ja asiakirjat.

Koska Rajavartiolaitos voisi suorittaa tässä pykälässä tarkoitettuja tehtäviä Rajavartiolaitokselle säädetyn tehtävän yhteydessä hävitysvelvollisuus ei luonnollisesti koskisi sellaisia tallenteita ja asiakirjoja, joita Rajavartiolaitos tarvitsisi oman tehtävänsä suorittamiseksi, vaikka ne voisivat kuulua myös sotilastiedusteluviranomaiselle luovutettaviin tallenteisiin ja asiakirjoihin. Kumpikin viranomainen olisi silloin vastuussa tietojen säilyttämisestä ja niiden hävittämisestä oman sääntelynsä mukaisesti.

Rajavartiolaitoksella olisi kuitenkin aina oikeus kirjata omaan rekisteriinsä perustiedot tässä pykälässä tarkoitetun toimenpiteen ajankohdasta ja paikasta sekä suoritetusta toimenpiteestä tai tiedon sen suorittamatta jättämisestä.

20 §. *Kansainvälinen yhteistyö.* Pykälän 3 momenttia muutettaisiin. Säännöksestä poistettaisiin viittaus tiettyjen tiedustelumenetelmien käyttöön. Viittauksen poiston myötä ulkomainen toimivaltainen viranomainen voisi osallistua minkä tahansa tiedustelumenetelmän käyttöön yhteistoiminnassa sotilastiedusteluviranomaisen virkamiehen kanssa.

Ulkomaisen virkamiehen itsenäistä oikeutta toimia Suomessa ei ehdoteta laajennettavaksi. Ulkomaisen toimivaltaisen virkamiehen oikeus osallistua tiedustelumenetelmien käyttöön Suomen alueella olisi edelleen sidottu yhteistoimintaan sotilastiedusteluviranomaisen kanssa. Ulkomaisella virkamiehellä ei edelleenkään olisi itsenäistä päätösvaltaa tai itsenäistä oikeutta käyttää tiedustelumenetelmiä Suomessa eikä aikaisemmin jo voimassa olevan lain sekä sotilastiedustelusta annetun lain hallituksen esityksessä tarkemmin kuvattua toimintamallia, jossa sotilastiedusteluviranomainen on kokonaisvastuussa tiedusteluoperaation ja yksittäisen siinä käytettävän menetelmän lainmukaisuudesta sekä ohjaamisesta ja valvonnasta, olla muuttamassa.

Ulkomainen toimivaltainen virkamies toimisi edelleen menetelmän käytön osalta ennemmin avustavassa roolissa, vaikka säännösehdotuksessa käytettäisiinkin termiä osallistua. Kaikki säännöksen tarkoittamat toimet tapahtuisivat sotilastiedusteluviranomaisen virkamiehen ohjauksessa ja valvonnassa. Muutoksen tarkoituksena olisi varmistaa, että sotilastiedusteluviranomaisen ja ulkomaalaisen tiedustelu- tai turvallisuuspalvelun yhteisoperaation aikana, olisi operaation käytössä kaikki se tekninen ja taktinen osaaminen sekä resurssit, joita ulkomaalaisella tiedustelu- tai turvallisuuspalvelulla on yksittäisen tiedustelumenetelmän toteuttamiseksi. Menetelmän käyttöön osallistuminen on tarpeen erityisesti esimerkiksi sellaisten tele- ja tietoverkkotiedustelun menetelmien teknisen toteutuksen osalta, joihin sotilastiedusteluviranomaisella ei o teknisen kehityksen nopeuden tai tekniikan erityislaatuisuuden vuoksi ole joko koulutusta, muuta osaamista tai resursseja, eikä

edellä mainittuja kykyjä ole hankittavissa tiedustelutehtävän vaatiman toteutusaikataulun puitteissa.

Osallistumista sotilastiedustelun virkamiehen kanssa olisi arvioitava tiedustelumenetelmäkohtaisesti. Esimerkiksi tietoliikennetiedustelussa osallistuminen voisi tapahtua sotilastiedusteluviranomaisen virkamiehen välittömässä läheisyydessä ja neuvoen sotilastiedusteluviranomaisen virkamiestä tietojen analysoinnissa ja tarkempien hakuehtojen määrittämisessä.

Toisaalta esimerkiksi peitetoiminnassa sen luonteen vuoksi sotilastiedustelun virkamies ei voi kaikissa tilanteissa olla ulkomaisen peitemiehen välittömässä läheisyydessä. Näin ollen ulkomainen peitemies pystyisi hoitamaan tehtäväänsä sinänsä itsenäisesti, mutta hänen olisi noudatettava sotilastiedusteluviranomaisen antamia ohjeita, määräyksiä ja muita rajoituksia.

Kolmantena esimerkkinä voidaan nostaa myös telekuuntelu, jossa osallistuminen voisi tarkoittaa esimerkiksi sellaisten laitteistojen ja menetelmien hyödyntämistä, joita sotilastiedusteluviranomaisella ei ole käytössään. Näissä tilanteissa vieraan valtion virkamies voisi esimerkiksi tehdä varsinaisen tiedonhankinnan teknisen toimenpiteen, mutta hankittujen tietojen analysointi tapahtuisi sotilastiedusteluviranomaisen toimesta tai yhteistyössä sotilastiedusteluviranomaisen kanssa.

Kaikkien edellä kuvattujen esimerkkien kannalta keskeistä on se, että toiminnan on tapahduttava Suomen kansallisten etujen mukaisesti, sotilastiedustelun tehtäviin liittyen tai kansallisen turvallisuuden suojaamiseksi. Joka tapauksessa säännöksen tarkoittamassa toiminnassa ulkomaisella virkamiehellä ei ole itsenäistä toimivaltaa käyttää tiedonhankintaa Suomen alueella. Jos ulkomainen virkamies toimisi toisin kuin säännöksessä on todettu, syyllistyisi hän rikokseen.

Säännöksen kannalta keskeistä on, että ulkomainen virkamies on velvollinen noudattamaan sotilastiedusteluviranomaisen hänelle antamia määräyksiä, rajoituksia ja ohjeita. Jos ulkomainen virkamies ei noudata näitä, hän voisi syyllistyä rikoslaissa rikokseksi säädettyyn rikokseen, kuten vakoiluun tai luvattomaan tiedustelutoimintaan. Ulkomaisen virkamiehen virkavastuusta on säädetty erikseen lain 21 §:ssä. Lisäksi on huomattava, että jos ulkomainen virkamies toimii vastoin lain 20 §:n 3 momentissa säädettyä tai ulkomainen tiedustelu- tai turvallisuuspalvelu toimii Suomen alueella omavaltaisesti, on kyse rikollisesta toiminnasta.

Sotilastiedusteluviranomaisella olisi esitetyn muutoksen mukaisesti erityinen selonottovelvollisuus toiminnasta aiheutuvista riskeistä, perustuslain suojaamien perus- ja ihmisoikeuksien sekä sotilastiedustelusta annetun lain yleisten periaatteiden toteutumisesta ennen kuin sotilastiedusteluviranomainen tekee päätöksen ulkomaisen toimivaltaisen virkamiehen osallistumisesta tiedustelumenetelmien käyttöön.

Sotilastiedusteluviranomaisen olisi lisäksi informoitava yhteistyötä tekevää tiedustelu- tai turvallisuuspalvelua yhteistoimintaan liittyvistä ulkomaisen virkamiehen virkavastuusta, ja ohjaus ja valvonta olisi järjestettävä tavalla, jolla voidaan varmistaa ulkomaisen virkamiehen toiminnan lainmukaisuus riittävällä tavalla.

Kansainvälisen yhteistyön valvonta kuuluu tiedusteluvalvontavaltuutetun toimivaltaan vastaavasti kuin muukin sotilastiedustelutoiminta.

33 §. *Teknisestä laitetarkkailusta päättäminen.* Pykälän 3 momentin 2 kohtaan lisättäisiin viittaus teknistä laitetta tai ohjelmistoa käyttävästä henkilöstä. Kuten useat muutkin tiedustelumenetelmät, olisi teknistä laitetarkkailuakin voitava kohdentaa henkilöperusteisesti.

Kun teknisen laitetarkkailun lupa kohdistuisi henkilöön, lupa käsittäisi luvan kohteena olevan henkilön hallussa olevan tai hänen oletettavasti muuten käyttämän laitteen tai ohjelmiston. Teknisen laitetarkkailun lupa ei olisi laite- tai ohjelmistokohtainen, vaan lupa käsittäisi kaikki luvan kohteena olevan henkilön hallussa olevat ja käyttämät laitteet ja ohjelmistot. Luvan hakijan tulisi pystyä osoittamaan perusteet sille, että tietty luvan kohteena oleva henkilö on osallisena sotilastiedustelun kohteena olevaa toimintaa tai kansallista turvallisuutta vakavasti uhkaavaa toimintaa. Henkilöön kohdistuvassa teknisessä laitetarkkailussa tiedonhankinta voisikin olla liitännäinen muihin tiedustelumenetelmiin. Kun tuomioistuimen luvassa määritelty toimenpiteen kohteena oleva henkilö ottaisi käyttöönsä tai hänen oletettaisiin ottaneen käyttöönsä uusia laitteita tai ohjelmistoja taikka ilmenisi, että hänen hallussaan on laite tai hän käyttää ohjelmistoa, tiedusteluviranomainen voisi kohdistaa toimenpiteen näihin laitteisiin ja ohjelmistoihin. Lisättäessä uusia laitteita ja ohjelmistoja luvan piiriin, myös näiden kohdalla olisi tehtävä viranomaisen päätös ja ilmoitus tiedusteluvaltuutetulle.

Pykälän 4 momentin mukaan, kuten muiden henkilöön kohdistuvien tiedustelumenetelmien osalta, tiedustelumenetelmän käytön aikana tehtäisiin viranomaisen päätös uuden laitteen tai ohjelmiston lisäämisestä menetelmän käytön kohteeksi. Kun tekniseen laitetarkkailuun mahdollisesti haetaan uutta lupaa tuomioistuimelta, olisi tunnistetut laitteet ja ohjelmistot ilmoitettava vaatimukseen vastaavasti, miten nykyisin toimitaan henkilöön kohdistuvien tiedustelumenetelmien osalta.

36 §. *Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättäminen.* Pykälän 1 momenttiin lisättäisiin mahdollisuus kiirepäätökseen vastaavasti, mitä on säädetty esimerkiksi telekuuntelusta (38 §) ja varsinaisen tietoliikennetiedustelun (69 ja 71 §) osalta. Kiiremenettelyä voidaan pitää poikkeuksellisena, sillä tuomioistuimessa on toimiva päivystysjärjestelmä.

Jos kiireellisessä tilanteessa tehdyn päätöksen yhteydessä tuomioistuin katsoo, että edellytyksiä toimenpiteelle ei ole ollut, tiedustelumenetelmän käyttö olisi lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot olisi heti hävitettävä.

Kiirepäätösasia tulisi saattaa tuomioistuimen käsiteltäväksi siitä huolimatta, että telekuuntelu tai muun vastaavan tietojen hankkimisen käyttäminen lopetetaan 24 tunnin kuluessa sen käytön aloittamisesta. Muuten hyvin lyhytaikaisella tiedonhankinnalla voitaisiin kiertää päätöksentekomenettelylle asetettuja vaatimuksia. Asian saattaminen tällaisissakin tapauksissa tuomioistuimen käsiteltäväksi edistää toimimista lainmukaisesti. Tämä koskisi muitakin tilanteita, joissa sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies voi väliaikaisesti päättää tiedustelumenetelmän käytöstä.

Pykälän 4 momentin mukaan, kuten muiden henkilöön kohdistuvien tiedustelumenetelmien osalta, tiedustelumenetelmän käytön aikana tehtäisiin viranomaisen päätös uuden laitteen tai ohjelmiston lisäämisestä menetelmän käytön kohteeksi. Kun tekniseen laitetarkkailuun mahdollisesti haetaan uutta lupaa tuomioistuimelta, olisi tunnistetut laitteet ja ohjelmistot ilmoitettava vaatimukseen vastaavasti, miten nykyisin toimitaan henkilöön kohdistuvien tiedustelumenetelmien osalta.

42 §. *Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen.* Pykälän 1 momenttiin tehtäisiin muutos lisäämällä lueteltujen tiedustelumenetelmien listaan valtiolliseen

toimijaan kohdistuva tietojärjestelmätiedustelu Suomessa ja ulkomaan tietojärjestelmätiedustelu.

Pykälän 2 momentti olisi uusi. Sen mukaan tiedusteluviranomainen voisi pyytää viranomaisen ulkopuolista tekemään asennus- tai poistamistoimenpiteen pykälässä tarkoitettujen päämäärien saavuttamiseksi. Säännöksen tilanteissa olisi kyse toimenpiteistä, joita sotilastiedusteluviranomainen ei pysty itse suorittamaan käsillä olevassa tilanteessa, vaikka viranomaisella olisikin toimivalta tähän. Selvää on se, että viranomaisen olisi lähtökohtaisesti tehtävä pykälän 1 momentissa tarkoitetut toimenpiteet itsenäisesti ja ainoastaan välttämättömissä tapauksissa viranomainen voisi tukeutua ulkopuolisen tahon apuun. Välttämättömyysvaatimus tarkoittaisi lähtökohtaisesti sitä, että voitaisiin osoittaa, että tiedustelumenetelmän käyttö, johon esimerkiksi asentaminen liittyy, ei ole mahdollista tai ainakin vaatii oleellisesti enemmän voimavaroja tai viivyttää tiedonhankintaa kohtuuttomasti huomioon ottaen uhkan vakavuus.

Säännöksen mukainen toiminta perustuisi viranomaisen esittämään pyyntöön, josta pyynnön vastaanottajalla on oikeus kieltäytyä. Vastauksen olisi oltava vapaaehtoisesti annettu ennen toimenpiteeseen ryhtymistä ja että pyynnön vastaanottaja on ymmärtänyt sen merkityksen. Vastauksen olisi oltava aidosti vapaaehtoinen. Pyynnön esittäjä ei saisi käyttää taivuttelua tai muuta johdattelua, jotta vastaus olisi halutunlainen. Tarkoituksenmukaista olisi, että tiedusteluviranomainen tuo esiin suostumusperusteisuuden, mutta johtopäätösten tekeminen toimenpiteiden suorittamisesta olisi jätettävä asianomaiselle henkilölle. Avustajalle olisi myös tuotava ilmi hänelle mahdollisesti aiheutuvat vaikutukset. Lähtökohtaisesti kyse olisi virnaomaisena toimivallassa tapahtuvasta toiminnasta, johon viranomaisella oli itselläkin oikeus. Näin ollen viranomaisen avustaminen ei voisi olla sinänsä irtisanomisperuste. Jos avustaja toimisia vastoin hänelle annettuja tarkkoja ohjeita, voisi tämä luonnollisesti johtaa viime kädessä irtisanomiseen.

Säännöksessä tarkoitettu toimenpide olisi rajattu sotilastiedusteluviranomaisen osoittamaan tarkoin rajattuun kohteeseen ja toimenpiteen olisi tapahduttava sotilastiedusteluviranomaisen ohjeistuksen mukaisesti. Sotilastiedusteluviranomaisen olisi voitava luottaa avustajan toimivan ohjeistuksen mukaisesti jo toiminnan paljastumisriskin vuoksi. Lievimmillään esimerkiksi laitteiston asentamisessa avustaminen voisi tarkoittaa esimerkiksi sitä, että avustaja vie tietyn laitteiston sisältävän laatikon tiettyyn määrättyyn paikkaan, johon hänellä on pääsy.

Pykälässä tarkoitetuissa toimenpiteissä on kyse niin kutsutusta sivutoimivaltuudesta, eli se liittyy kiinteästi käytettävään tiedustelumenetelmään ja siihen, miten kulloistakin tiedustelumenetelmän käyttöä on rajattu. Esimerkiksi, jos kyse on teknisestä kuuntelusta, kyse voi olla mikrofonin asentamisesta tiettyyn tilaan.

Jos kyse olisi teknisestä laitetarkkailusta, kyse voisi olla seurantaohjelmiston asentamisesta tiettyyn laitteeseen tai ohjelmistoon. Teknisessä laitetarkkailussa lupavaatimuksessa on tarkoin yksilöitävä kohteena oleva laite tai ohjelmisto, joten nyt käsiteltävänä olevassa säännöksen perusteella ei voida asentaa esimerkiksi teleoperaattoreiden tiloihin laitteistoja, jotka mahdollistaisivat massavalvonnan. Tähän ei myöskään ole olemassa toimivaltuutta.

Asennus- ja poistotoimenpiteiden olisi näin ollen kohdistuttava vain yksilöityyn ja rajattuun laitteeseen, menetelmään tai ohjelmistoon tiedustelumenetelmän mukaisesti. Toimenpiteitä ei voitaisi ulottaa esimerkiksi teleyrityksen keskeisiin hallinta-, valvonta- tai muihin ydinjärjestelmiin muutoin kuin poikkeuksellisesti ja erityisen painavin perustein, ja silloinkin mahdollisimman rajoitetusti. Lisäksi toimenpiteet olisi suunniteltava siten, etteivät ne aiheuta esimerkiksi teleyrityksen valvonta- ja häiriönhallintajärjestelmissä poikkeamahavaintoja tai

automaattisia suojaamistoimenpiteitä. Tämä on välttämätöntä sekä käyttövarmuuden että operatiivisen turvallisuuden kannalta. Etenkin sotilastiedusteluviranomaisen operaatioturvallisuus ohjaa toteuttamaan toimenpiteet niin, ettei kohdejärjestelmän hallinnoija havaitse toimenpiteitä.

Lisäksi tällä on merkitystä mahdollisen vahingonkorvauksen suhteen. Jos avustaja toimisi tarkasti sotilastiedusteluviranomaisen ohjeistuksen mukaan, olisi kyse viranomaisen vastuulla tapahtuvasta toiminnasta, eli mahdollinen vahingonkorvausvastuu kohdistuu viranomaiseen. Tilanne vastaisi sitä, että viranomainen itse kävisi suorittamassa toimenpiteen, josta aiheutuisi mahdollisesti ennakoimattomia vahinkoja.

Käytännössä, jos avustajaa on ohjeistettu laittamaan USB-tikku, jota kautta teknisen laitetarkkailun mahdollistava ohjelmisto asentuu. kiinni laitteeseen, tapahtuisi tämä selkeästi viranomaisen toimivallassa, ja jos asennuksesta tai teknisestä laitetarkkailusta aiheutuisi vahinkoja jopa sivulliselle, vastaisi viranomainen tästä vastaavasti kuin jos viranomainen itse olisi asennuksen tehnyt.

Jos avustaja toimisi oman harkintansa mukaisesti saadun ohjeistuksen ulkopuolella, vastaisi avustaja mahdollisista vahingoista itse. Tilanne vastaisi pitkälti sitä, että ohjattu tietolähde annetun tiedonhankintatehtävän ohessa aiheuttaisi vahinkoja tai tekisi rikoksia.

Joka tapauksessa toimenpiteen suorittamisessa korostuvat ennen kaikkea tarkka suunnittelu, avustajan tarkka ohjeistaminen sekä riskiarviointi. Luonnollisesti toimintaa ohjaa myös sotilastiedustelutoiminnan salassa pitäminen sekä vahva luottamus avustajaan.

Asentamisen mahdollistavan tiedustelumenetelmän käytön osalta siitä säädettyjen edellytyksien olisi täytyttävä erikseen – luonnollisesti niiden osalta olisi noudatettava säädettyä päätöksentekomenettelyä lupineen. Säännöksessä tarkoitettua henkilöä ei saisi käyttää viranomaisille annettujen toimivaltuuksien käyttöä koskevien rajoitusten kiertämiseen. Avustajan käytöstä olisi tehtävä selkoa tiedustelumenetelmän käyttöä koskevassa päätöksessä. Joka tapauksessa sotilastiedusteluviranomaisen olisi tehtävä päätös pykälässä tarkoitetusta toiminnasta ja ilmoitettava siitä tiedusteluvalvontavaltuutetulle. Lisäksi tiedusteluvalvontavaltuutettu valvoo toimivaltansa mukaisesti toimintaa.

Lisäksi toimenpiteen olisi perustuttava viranomaisen asianmukaisesti tekemään tiedustelumenetelmän käyttöpäätökseen. Selvää on se, että säännöksen nojalla viranomainen ei voisi pyytää henkilöä asentelemaan summittaisesti pykälässä tarkoitettuja laitteita, menetelmiä tai ohjelmistoja oletuksella, että ne voisivat joskus tulla käytettäviksi.

Edellä todetun takia kyse on yksittäistapauksellisesta toiminnasta. Näin ollen viranomaisen esittämä pyyntö ja siihen annettu vastaus eivät voi olla luonteeltaan pysyviä, vaan kyse olisi aina yksittäisen toimenpiteen suorittamisesta.

Säännöksen toiminta tapahtuisi viranomaisen toimivallassa sen ohjauksessa ja valvonnassa. Toimenpiteissä olisi aina kyse toimenpiteistä, jotka ovat viranomaiselle lain mukaan mahdollisia. Avustaja ei toteuttaisi tiedonhankintaa, vaan esimerkiksi laitteen tekninen hallinta, sen toiminnan ohjaaminen, tallenteiden tarkastaminen ja arviointi säilyisivät toimivaltaisella viranomaisella. Suoritettavia toimenpiteitä ei voida katsoa merkittäväksi julkisen vallan käytöksi.

Pykälän 1 momentin rajoituksia sovellettaisiin myös viranomaisen ulkopuolisen suorittamiin toimenpiteisiin, joten asentamis- ja poisottamistoimenpiteet eivät saisi tapahtua pysyväisluonteiseen asumiseen käytettävässä tilassa.

Edellä todetusta johtuisi myös se, ettei avustaja voi suorittaa toimenpidettä pysyväisluonteiseen asumiseen käytettävässä tilassa, kuten on pykälän 1 momentissa nimenomaisesti säädetty.

Säännöksen kannalta keskeistä on myös laitteen, menetelmän tai ohjelmiston poisottaminen. Poisottamista olisi arvioitava välttämättömyyden kannalta, eli laite, menetelmä tai ohjelmisto voisi olla asennettuna vain välttämättömän ajan. Esimerkiksi asennetun ohjelmiston kannalta mahdollinen tietoturvariski kohteena olevalle laitteistolle olisi jäätävä mahdollisimman vähäiseksi.

Pykälän 3 momentti olisi uusi. Pykälän 1 momentin mukaisesti asentamisessa, käyttöön ottamisessa ja poistamisessa viranomaisella olisi oikeus salaa mennä kohteeseen tai tietojärjestelmään sekä kiertää, purkaa tai muulla vastaavalla tavalla tilapäisesti ohittaa kohteen tai tietojärjestelmän suojaus tai haitata sitä. Salaa tietojärjestelmään meneminen ja esimerkiksi tietojärjestelmän suojauksen ohittaminen saattaa edellyttää tarvittavan ohjelmiston vaivihkaista ujuttamista etäyhteydellä ulkopuolisia tietojärjestelmiä ja laitteistoja käyttäen. Luonnollisesti toiminnassa on vältettävä vahingon tuottamista käytetyille järjestelmille ja laitteistoille sekä vältettävä ulkopuolisten tietojärjestelmien ja laitteistojen paljastumista kohteelle.

Uuden säännöksen mukaan sotilastiedusteluviranomainen voisi salaa käyttää myös ulkopuolisia laitteita ja tietojärjestelmiä. Säännös rajaisi asentamisen ja poisottamisen sekä tiedonvälityksen tietoteknisiin menetelmiin, eli sotilastiedusteluviranomaisen virkamies ei tekisi fyysisesti laitteelle tai tietojärjestelmälle mitään, vaan kyse olisi nimenomaan menetelmän tai ohjelmiston asentamisesta ja poisottamisesta tietoteknisin menetelmin etänä.

Esimerkiksi sotilastiedustelun kohde voisi itse käyttää tällaista ulkopuolista laitetta tai tietojärjestelmää, jolloin sotilastiedusteluviranomaisella olisi mahdollisuus päästä kiinni kohteeseen tuon ulkopuolisen laitteen tai tietojärjestelmän välityksellä. Tällainen tilanne voisi olla käsillä, mikäli sotilastiedustelun kohde hyödyntäisi esimerkiksi kahvilan tai kauppakeskuksen verkkoa, jolloin sotilastiedusteluviranomaisen olisi luontevin hyödyntää samaista verkkoa tarvittavien toimenpiteiden suorittamiseksi sotilastiedustelun kohteen laitteistossa.

Ottaen huomioon säännöksen tavoite, laitteiston, menetelmän ja ohjelmiston asentaminen ja poisottaminen sekä tiedonvälittäminen ei käytännössä voisi tapahtua esimerkiksi teleyrityksen kriittisissä tuotantoympäristöissä. Tässäkin tapauksessa kyse olisi varsin paljon resursseja vievästä toimenpiteestä, minkä lisäksi toimenpide ei saisi näkyä mitenkään varsinaiselle kohteelle. Tämä aiheuttaa suurehkon riskin siitä, että järjestelmän toiminta häiriintyisi siten, että se herättää kohteena olevan toimijan mielenkiinnon.

Edellä todetun lisäksi on huomattava, että lain yleisiä periaatteita sovelletaan myös pykälässä tarkoitettuihin toimenpiteisiin, jotka ovat kiinteässä liitoksessa varsinaisen tiedustelumenetelmän käyttöön. Näin ollen esimerkiksi jo vähimmän haitan periaate johtaa siihen, ettei laajempien tietoverkkokokonaisuuksien tai tietojärjestelmäkokonaisuuksien hyödyntäminen tulisi käytännössä kyseeseen. Lisäksi suhteellisuusperiaate johtaa siihen, että suoritettavien toimenpiteiden olisi oltava suhteellisia käytettävään tiedustelumenetelmään ja tiedustelutehtävän päämääriin nähden. Periaatteiden näkökulmasta edellä tarkoitetussa esimerkissä teleyrityksen kriittinen tuotantoympäristön käyttäminen säännöksessä tarkoitettuun toimintaa voidaan katsoa käytännössä teoreettiseksi vaihtoehdoksi.

Asentamisen ja poisottamisen olisi pääsääntöisesti tapahduttava mahdollisimman lähellä kohdetta, kuten edellä kuvatussa tapauksessa kahvilan yleisesti jaetun langattoman verkon välityksellä. Jos kyse olisi fyysistä asentamista tai poisottamista koskevista toimenpiteistä, sovellettavaksi tulisi pykälä 1 momentti tai 2 momentti.

Säännös rajaisi toimenpiteet yksittäisiin laitteisiin tai tietojärjestelmän osaan. Näin ollen sotilastiedusteluviranomaisen olisi pystyttävä yksilöimään laite tai tietojärjestelmän osa, mitä kautta menetelmä tai ohjelmisto pystyttäisiin asentamaan kohteeseen. Toimenpiteitä ei olisi tarkoituksenmukaista ulottaa esimerkiksi teleyrityksen keskeisiin hallinta-, valvonta- tai muihin ydinjärjestelmiin muutoin kuin poikkeuksellisesti ja erityisen painavin perustein, ja silloinkin mahdollisimman rajoitetusti.

Tarkoitetuissa toimenpiteissä ei myöskään ole kyse siitä, että esimerkiksi laitteen valmistajan olisi asennettava myymiinsä laitteisiin valmiiksi tiedustelumenetelmien käytön mahdollistava ohjelmisto tai menetelmä.

Säännöksen mukainen toiminta edellyttäisi välttämättömyyttä. Tässä tapauksessa kyse olisi sen arvioimisesta, voisiko sotilastiedusteluviranomainen päästä haluamaansa tavoitteeseen omin toimin käyttämättä ulkopuolisia laitteita tai tietojärjestelmiä. Mikäli omat toimet olisivat mahdottomia tai vaatisivat poikkeuksellisen paljon resursseja, täyttyisi säännöksessä tarkoitettu välttämättömyys. Välttämättömyyttä olisi arvioitava myös asennuksessa tai poisottamisessa taikka tiedonsiirtämisessä käytettävän laitteen tai tietojärjestelmän osan kannalta. Esimerkiksi yleisen, avoimen jaetun verkon käyttäminen voi tulla kyseeseen matalammalla kynnyksellä, kun taas merkittävämmän, vahvasti suojatun laitteen tai tietojärjestelmän osan käyttäminen toimenpiteen suorittamisessa tulisi kyseeseen harvemmin. Jälkimmäisessä tilanteessa olisi arvioitava sitä, pystyttäisiinkö toimenpide suorittamaan vähemmän resursseja vaativaa tai mahdollisesti vähemmän vahinkoa aiheuttavan laitteen tai tietojärjestelmän osan välityksellä.

Arvioinnissa olisi huomioitava myös toimenpiteen kohteena olevan laitteen tai tietojärjestelmän osan merkitys kokonaisuudessaan. Esimerkiksi yksittäisen laitteen häiriö voi aiheuttaa merkittäviäkin seurannaisvaikutuksia, jos kyse on teleyrityksen hallinnoiman viestintäverkon kannalta keskeisestä laitteesta. Säännöksen soveltaminen tällaisten laitteiden osalta olisi erittäin harvinaista. Sotilastiedustelutoiminnan yleisistä periaatteista ja salassa pidosta johtuen yksittäisten laitteiden tai tietojärjestelmien osan kautta kulkeva tietomäärä pyritään pitämään mahdollisimman havaitsemattomana.

Säännöksessä viitattu tilapäisyys tarkoittaisi sitä, että menetelmän tai ohjelmiston asentamisessa ja poisottamisessa ja tiedon siirtämisessä ei voitaisi käyttää vakituisesti samoja laitteita ja tietojärjestelmiä. Tarkoituksen mukaista myös operatiivisesta näkökulmasta on, että mahdollisuuksien mukaan menetelmä tai ohjelmisto ujutetaan kohteeseen useita eri reittejä samanaikaisesti käyttäen.

Lisäksi luonnollisesti, sotilastiedusteluviranomaisen toiminnan luonteen takia, asentaminen ja poisottaminen sekä tiedonsiirto pyritään tekemään mahdollisimman vaivihkaisesti. Näin ollen, vaikka toiminnassa käytettäisiin ulkopuolisia laitteita ja tietojärjestelmiä, jäljet pyritään peittämään mahdollisimman perusteellisesti. Toiminnassa ei ole myöskään kyse siitä, että välittäjänä toimivaan laitteeseen tai tietojärjestelmään tehtäisiin erityisiä muutoksia.

Säännöksen mukaisesti toiminnassa ei saisi aiheuttaa vähäistä suurempaa haittaa käytettävälle laitteelle tai tietojärjestelmälle. Säännöksen tarkoittamassa toiminnassa on kyse ennen kaikkea tietoliikenteen välittämisestä menetelmän tai ohjelmiston asentamiseksi tai poisottamiseksi ja toisaalta tiedonsiirtämisestä kohde laitteesta tai järjestelmästä sotilastiedustelulle. Näin ollen

tarpeellisessa vähäisessä haitassa olisi kyse lähinnä hetkellisestä tietoliikenneliittymän käytön lisääntymisestä ja tätä kautta liittymän haltijan käyttämien sähköisten palveluiden mahdollisesta hetkellisestä hidastumisesta. Ulkopuolisen tietojärjestelmän käyttö voisi näkyä järjestelmän käytön tilapäisenä hetkellisenä kasvuna.

Haitan arvioinnissa olisi nimenomaisesti huomioitava mahdolliset suorituskykyvaikutukset, kuten viive ja kapasiteetti, omistajalle palvelutasosopimusten rikkomisesta aiheutuvat seuraamukset, ylimääräinen häiriönselvitystyö, palautustoimet ja mainehaitta. Esimerkiksi teleyritysympäristössä liikenteen hidastuminen tai palvelun laadun heikkeneminen ovat tyypillisesti vähäistä suurempaa haittaa.

Edellä todetut seikat olisi otettava huomioon säännöksen toimenpiteitä suunniteltaessa, vaikka säännöksessä kyse ei olekaan suurimuotoisesta toiminnasta yksittäisen tietoliikenneyhteyden osalta. Joka tapauksessa, koska toimenpiteissä ei ole kyse esimerkiksi teleyrityksen kriittiseen tuotantoympäristöön kohdistuvista toimenpiteistä ja asennettavat menetelmät ja ohjelmistot ovat lähtökohtaisesti huomaamattomia ja tiedon siirtäminen pyritään tekemään huomaamattomasti, edellä kuvatut merkittävät vaikutukset voidaan arvioida käytännössä teoreettisiksi. Viimeksi mainittu edellyttäisi suurien datamäärien siirtämistä yksittäisten liittymien kautta.

Mikäli vastoin edellä kuvattua, säännöksen toiminnasta aiheutuisi tarpeetonta haittaa, olisi sotilastiedusteluviranomainen velvollinen korvaamaan vahingon ja haitan. Toiminnan luonteen takia henkilö tai yhteisö, jonka laitetta tai tietojärjestelmää käytetään, ei saa tietoa sotilastiedusteluviranomaisen toiminnasta. Toisaalta lähtökohtaisesti henkilön tai yhteisön ei pitäisi tällaista edes havaita. Jos henkilö tai yhteisö epäilisi, että laitetta tai tietojärjestelmää olisi käytetty säännöksessä tarkoitetulla tavalla ja taholle olisi aiheutunut vähäistä suurempaa haittaa sotilastiedusteluviranomaisen toiminnasta, voisi henkilö tai yhteisö tehdä tiedusteluvalvontavaltuutetulle tutkimispyynnön.

Itsestään selvää on se, että edellä kuvatussa toiminnassa ei voida hankkia välittävänä olevasta laitteesta tai tietojärjestelmästä taikka näiden tuottamasta tiedosta tietoa. Tällöin olisi kyse tiedonhankinnasta, mitä käsiteltävänä oleva säännös ei kata. Toimiessaan edellä tarkoitetulla tavalla, sotilastiedusteluviranomainen syyllistyisi rikolliseen toimintaan, jos tarvittavia tiedustelumenetelmän käyttöä koskevia lupia ei ole.

Momentin lopussa säädettäisiin informatiivisesti, että sotilastiedusteluviranomainen olisi velvollinen korvaamaan aiheuttamansa vähäistä suuremman haitan tai vahingon. Vahingonkorvauksesta ja vahingonkorvauksiin liittyvästä prosessista säädetään vahingonkorvauslaissa.

43 §. *Peitetoiminta.* Pykälästä kumottaisiin 3 momentti. Momentti koskee peitetoimintaa tietoverkoissa, josta säädettäisiin ehdotetussa 46 a §:ssä ja siitä päättämisestä 46 b §:ssä. Tämän takia momentti olisi tarpeeton.

Muilta osin pykälä säilyisi ennallaan ja siihen liittyvä oikeustila säilyisi ennallaan.

44 §. *Peitetoimintaa koskeva suunnitelma.* Pykälä ja sen otsikko muutettaisiin koskemaan ainoastaan peitetoimintaa koskevaa suunnitelmaa. Peitetoimintaa koskeva päätöksenteko perustuu aina esitykseen, jonka on sisällettävä peitetoiminnasta päätöstä koskevat seikat. Esitys perustuu myös aina suunnitelmaan, joka on päätöksentekoasiakirjojen liitteenä, joten erillisestä esityksestä säätämistä voidaan pitää turhana.

45 §. *Peitetoiminnasta päättäminen.* Pykälän 1 momentista poistettaisiin viittaus tehtävään määrättyyn tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies, joka käytännössä on päättänyt peitetoiminnasta tietoverkossa. Viittaus olisi turha, koska esityksessä ehdotetaan säädettäväksi nimenomaisesta toimivaltuudesta, joka koskisi yksinomaan tietoverkossa toteutettavaa peitetoimintaa.

Pykälän 4 momentista poistettaisiin viittaus peitetoiminnan lopettamiseen. Lopettamisesta nimenomaisesti säätämistä voidaan pitää turhana, sillä kuten muidenkin tiedustelumenetelmien osalta, tiedustelumenetelmän käyttö on lopetettava, jos edellytyksiä sille ei enää ole.

46 a §. *Yksinomaan tietoverkossa toteutettava peitetoiminta.* Lakiin lisättäisiin uusi pykälä, jossa säädettäisiin uudesta yksinomaan tietoverkossa toteutettavan peitetoiminnan toimivaltuudesta. Toimivaltuudesta säätäminen erikseen varsinaisesti peitetoiminnasta on perusteltua sen matalamman käyttökynnyksen takia. Sotilastiedustelun kohteena olevia uhkia käsitellään taajaan myös tietoverkoissa, ja uhista tarkemman tiedon hankkiminen edellyttää usein kanssakäymistä esimerkiksi keskusteluun osallistuvien kanssa. Lisäksi sotilastiedustelun kannalta on aina turvallisempaa hankkia tietoa kotimaasta kuin mennä kohdevaltioon paikan päälle. Menetelmällä olisi myös merkitystä uusien kohteiden löytämisessä.

Pykälän 1 momentissa säädettäisiin ainoastaan tietoverkoissa toteutettavan peitetoiminnan määritelmästä. Yleisesti peitetoiminnalla tarkoitetaan tiettyyn henkilöön tai tämän toimintaan kohdistuvaa suunnitelmallista tiedonhankintaa käyttämällä soluttautumista, jossa tiedonhankinnan edellyttämän luottamuksen hankkimiseksi tai tiedonhankinnan paljastumisen estämiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka valmistetaan tai käytetään vääriä asiakirjoja. Määritelmäsäännös ei edellyttäisi, että kohteena oleva henkilö tai henkilöryhmä kyettäisiin nimeämään tai yksilöimään esimerkiksi ominaisuuksiltaan, vaan riittävää olisi, että henkilö tai henkilöryhmä voitaisiin yksilöidä erimerkiksi harjoitetun toiminnan kautta. Koska peitetoiminnan eräänä tavoitteena on selvittää kohteena olevaan toimintaan liittyviä rakenteita ja siinä toimivia henkilöitä, olisi perusteetonta, että tällaisen selvittämistyön edellytyksenä olisi tieto esimerkiksi henkilön nimestä.

Määritelmällisesti peitetoiminta yksinomaan tietoverkoissa vastaisi sitä, mitä lain 43 §:ssä säädetään normaalista peitetoiminnasta ja mitä 43 §:n 3 momentissa säädetään peitetoiminnasta tietoverkoissa.

Pykälän 2 momentissa säädettäisiin toimivaltuuden erityisestä edellytyksestä. Edellytys vastaisi sitä, mitä voimassaolevan lain 42 §:n 3 momentissa säädetään. Yksinomaan tietoverkoissa tapahtuva peitetoiminta olisi mahdollista, jos sillä voitaisiin olettaa olevan erittäin tärkeä merkitys tiedustelutehtävän kannalta.

Pykälän 3 momentissa säädettäisiin yksinomaan tietoverkossa tehtävää peitetoimintaa koskevasta suunnitelmasta. Sen olisi sisällettävä päätöksenteon ja peitetoiminnan toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaa olisi tarpeen mukaan tarkistettava.

46 b §. *Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättäminen.* Pykälässä säädettäisiin päätöksenteosta. Päätöksenteko vastaisi sitä, miten aiemmin on päätetty lain 45 §:n nojalla peitetoiminnasta tietoverkossa.

Pykälän 1 momentin mukana päätöksen tekisi tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies. Päätöksentekotaso vastaisi sitä, mitä nykyisin noudatetaan lain 45 §:ssä säädetyssä peitetoiminnassa tietoverkossa.

Pykälän 2 momentin mukaan päätös voisi olla voimassa enintään kuusi kuukautta kerrallaan. Pykälän 3 momentin mukaan päätös olisi tehtävä kirjallisesti.

Pykälän 4 momentissa olisi säädetty päätöksessä mainittavat seikat. Päätöksessä mainittava seikat vastaisivat sitä, mitä lain 45 §:ssä on säädetty. Toimivaltuus kohdistuisi ennen kaikkea uhkaan liittyvään toimintaan, jota olisi määritelty tarkemmin tiedustelutehtävässä. Lisäksi tietoverkossa toimittaessa voi olla käytännössä mahdotonta määrittää tietty kohdehenkilö, koska henkilöitä voi ilmaantua esimerkiksi keskusteluun nopeassa tahdissa ja toisaalta he voivat poistua keskustelusta yhtä nopeasti. Tiedustelutehtävässä olisi kuitenkin pystyttävä rajaamaan kohteena olevaa toimintaa mahdollisimman tarkasti eikä peitetoiminta tietoverkossa voisi olla täysin kohdentumatonta.

51 §. *Tietolähdetoiminta.* Pykälän 3 momentti jaettaisiin uusiksi 3 ja 4 momenteiksi. Voimassa olevaa 3 momenttia voidaan pitää soveltajan kannalta epäselvänä. Muutoksella on vaikutuksia myös ulkomailla toteutettavan tiedustelun osalta.

Uusi 3 momentti koskisi tietolähteen ohjatussa käytössä sovellettavaa kieltoa hankkia tietoja sellaisella tavalla, joka edellyttäisi viranomaiselle kuuluvien toimivaltuuksien käyttöä. Käytännössä tämä on tarkoittanut sitä, että tietolähde ei voi hankkia sellaisia tietoja, joihin hänelle ei ole pääsyä. Jos tietolähteelle on myönnetty oikeus käyttää tietyssä tietojärjestelmässä tietyssä kansiossa olevia tietoja, tietolähde voi toimittaa ainoastaan näitä tietoja tiedusteluviranomaiselle. Tietolähteellä ei kuitenkaan ole oikeutta mennä hankkimaan tietoja eri käyttäjäoikeuksilla olevan henkilön käyttämistä tiedoista, mikä tarkoittaisi jo viranomaistoimivaltuuksien käyttöä.

Muutoksen myötä edellä tarkoitettu sääntö tuotaisiin selkeämmin esiin ja siitä säädettäisiin omassa momentissaan.

Pykälän uudessa 4 momentissa säädettäisiin selontekemisestä tietolähteen oikeuksista ja velvollisuuksista sekä tietolähteen turvallisuuteen liittyvistä seikoista. Momentti sisältäisi voimassa olevan lain 3 momentissa säädetyt muut asiat kuin mitä olisi uudessa 3 momentissa. Näiltä osin muutos ei vaikuttaisi voimassa olevaan oikeustilaan.

Voimassa olevan pykälän 4 ja 5 momentit siirtyisivät ehdotetun muutoksen myötä uudeksi 5 ja 6 momentiksi.

53 §. *Tietolähteen ohjatusta käytöstä päättäminen.* Pykälän 1 momenttiin tehtäisiin muutos. Muutoksen myötä myös tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies voisi tehdä päätöksen tietolähteen ohjatusta käytöstä. Muutos vastaisi sitä, mitä poliisilain 5 a luvussa on säädetty suojelupoliisin tietolähteen ohjatusta käytöstä päättämisestä.

Muutos on tarpeellinen, sillä päätöksentekijätaso laskettaisiin lähempänä operatiivista toimintaa olevalle tasolle. Näin tietolähteen ohjatussa käytössä pystyttäisiin reagoimaan nopeammin muuttuviin tilanteisiin. Alemman tasoisella lähempänä operatiivista toimintaa olevalla päätöksentekijällä voidaan myös arvioida olevan paremmat tiedot itse toiminnasta päätöksenteon tueksi.

55 §. *Paikkatiedustelusta päättäminen.* Pykälän 3 momenttiin tehtäisiin muutos. Muutoksen myötä paikkatiedustelusta ajoneuvoon päättäisi tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

Ajoneuvo on paikka, johon ei ole yleistä pääsyä paikkatiedustelun ajankohtana, mutta jonka ei ole perusteltua saada normaalitilanteessa vastaavanlaista suojaa kuin esimerkiksi lukittu toimisto. Päätöksentekoa koskevalla muutoksella päätöstä ajoneuvoon kohdistuvasta paikkatiedustelusta ei tarvitsisi tehdä tuomioistuimessa. Päätöksenteko vastaisi sitä, mitä pakkokeinolaissa on säädetty paikanetsinnästä.

Säännöksen soveltamisessa on kuitenkin otettava huomioon tilanteet, joissa ajoneuvoa käytetään pysyväisluonteiseen asumiseen.

55 a §. *Näytteenotto paikkatiedustelussa.* Pykälä olisi uusi. Säännöksen mukaan sotilastiedusteluviranomaisella olisi oikeus paikkatiedustelussa ottaa aineesta, omaisuudesta tai esineestä näyte, jos se on tarpeen tiedustelutehtävän suorittamiseksi. Säännöksen myötä sotilastiedusteluviranomainen voisi ottaa tiedustelumenetelmän käytön yhteydessä paikan päällä näyteitä esimerkiksi aineesta, jonka voidaan olettaa liittyvän tiedustelutehtävän kohteena olevaan toimintaan.

56 a §. *Aineen, omaisuuden tai esineen tilapäinen haltuunotto.* Sotilastiedustelun kohteina ovat lain 4 §:n mukaan muun muassa sotilaallinen toiminta, Suomen maanpuolustukseen kohdistuva tiedustelutoiminta ja vieraan valtion toiminta tai muu sellainen toiminta, joka vakavasti uhkaa Suomen maanpuolustusta tai vaarantaa yhteiskunnan elintärkeitä toimintoja. On ilmeistä, että edellä tarkoitetun toiminnan saadessa uusia muotoja vallitsevassa maailmanpoliittisessa tilanteessa, esimerkiksi paikkatiedustelun yhteydessä voi löytyä sellaisia aineita, joita mahdollisesti voidaan käyttää räjähteiden valmistukseen tai esimerkiksi myrkyllisiä kemikaaleja. Löydettyä ainetta ei kuitenkaan voida yleensä tunnistaa tai sen vaarallisuutta arvioida pelkästään ulkoisten tunnusmerkkien perusteella. Ulkomaiseen tiedustelutoimintaan liittyen kyse voisi olla tilanteesta, jossa löydettyihin asiakirjoihin olisi kirjoitettu tekstiä ihmissilmälle näkymättömällä kemiallisella aineella, ja tekstiä saadaan näkyviin ainoastaan toista ainetta käyttämällä.

Vaikka tilanteissa lähtökohtaisesti voidaan olettaa olevan jonkin rikostunnusmerkistön täyttävästä toiminnasta, esimerkiksi aineen laadusta ei voida varmistua ennen tarkempia testejä. Jos pykälän toimivaltuudella hankittu tieto esimerkiksi räjähteessä käytettävästä aineesta varmistuisi, tieto voitaisiin luovuttaa niin kutsutun palomuurisääntelyn mukaisesti rikostorjuntaviranomaiselle.

Tiedustelutoiminnan luonteen vuoksi toimivaltuuden käytössä tarkoitettu haltuunotto olisi tilapäistä. Jotta sotilastiedusteluviranomaisen toiminta pysyisi salassa, olisi haltuunoton oltava mahdollisimman lyhytkestoista ja haltuun otettava aine, esine tai omaisuus olisi palautettava mahdollisimman pian alkuperäiselle paikalleen.

61 a §. *Valtiollisen toimijan tietojärjestelmään kohdistuva tiedustelu kotimaassa.* Pykälässä säädettäisiin uudesta kotimaassa tapahtuvasta tietojärjestelmätiedustelusta, joka kohdistuisi valtiolliseen toimijaan. Valtiollinen toimija on määritelty laissa vieraan valtion tunnistetuksi viranomaiseksi tai sellaiseen rinnastuvaksi toimijaksi sekä tarkoitetun tahon palveluksessa olevaksi tai sen määräyksessä ja ohjauksessa toimivaksi tahoksi.

Tietojärjestelmällä tarkoitettaisiin tietojenkäsittelylaitteista, tiedonsiirtolaitteista, tietoa käsittelevistä ohjelmista ja tietojen käsittelysäännöistä muodostuvaa kokonaisuutta. Tietojärjestelmä voi muodostua useiden eri laitteiden ja ohjelmistojen tai näiden osien muodostamasta maantieteellisesti ja loogisesti hajautetusta kokonaisuudesta. Tietojärjestelmä voi kattaa osia, jotka kuuluvat samanaikaisesti johonkin toiseen tietojärjestelmään.

Pykälässä tarkoitettu tietojärjestelmätiedustelu sisältäisi teknisesti telekuuntelua ja televalvontaa sekä teknistä laitetarkkailua vastaavat menetelmät ja niiden yhdistelmät, joilla saataisiin hankkia tietoa tietojärjestelmässä kulkevasta viestistä, sinne tallennetusta viestistä ja tietojärjestelmän muuten sisältämistä tiedoista. Toimivaltuus mahdollistaisi tietojärjestelmien sisäisen liikenteen tarkastelun. Tällaista sisäistä liikennettä ovat esimerkiksi tekninen viestinvaihto valtiollisen toimijan käyttämän käyttöliittymän ja sen taustalla toimivan tiedontallennusalustan välillä sekä viestiliikenne valtiollisen toimijan hallinnoiman tietojärjestelmän eri käyttäjien välillä. Tietojärjestelmän osien välisen teknisen kontrolliliikenteen tarkkailu mahdollistaisi myös kokonaiskuvan luomisen tietojärjestelmän sisäisestä toiminnasta, sen sisältämistä tiedoista ja sen muodostamasta uhkasta. Toimivaltuuden kohteen voisi muodostaa esimerkiksi päätelaite, päätelaitteessa käytettävä käyttöliittymä ja viestintäohjelmisto, päätelaitteen tietoliikenneyhteys sekä valtiollisen toimijan käyttämät reitittimet, serverit ja tallennuspalvelut (pilvipalvelut), siltä osin kuin valtiollinen toimija hallinnoi niitä.

Valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvassa tiedustelussa yhdisteltäisiin nykyisiä toimivaltuuksia tietyiltä osin. Esimerkiksi laitteeseen tallennettuun tietoon ja ohjelmistoon kohdistuvilta osin kyse olisi teknisen laitetarkkailun kaltaisesta toimenpiteestä ja kun tieto liikkuisi päätelaitteelta pilvipalveluun, kyse olisi telekuuntelun kaltaisesti toimenpiteestä, jos tietoa hankittaisiin esimerkiksi tietojärjestelmän yleiseen viestintäverkkoon liittävästä reitittimestä.

Lähtökohtaisesti valtiollisen toimijan hallinnoimaan tietojärjestelmään on käyttöoikeus ainoastaan niillä, joille valtiollinen toimija on sen myöntänyt. Näin ollen tietojärjestelmän tiedustelu ei kohdistuisi satunnaiseen joukkoon ihmisiä, vaan niihin, joille valtiollinen toimija on myöntänyt käyttöoikeuden, kuten työntekijöilleen.

Toimivaltuuden käytön kohteena ei olisi myöskään ulkopuolinen tietojärjestelmä, kuten sosiaalisen median alusta, vaan nimenomaisesti valtiollisen toimijan omassa käytössä oleva tietojärjestelmä ja sen käyttäminen. Toki valtiollisen toimijan hallinnoiman tietojärjestelmän kautta voidaan esimerkiksi sosiaalisen median palveluun tuottaa tietoa, josta voitaisiin hankkia tietoa siltä osin kuin sitä tuotetaan valtiollisen toimijan tietojärjestelmässä. Kun tieto on toimitettu sosiaalisen median palveluun, tieto olisi hankittava muulla sopivalla tiedustelumenetelmällä kuin valtiolliseen toimijaan kohdistuvalla tietojärjestelmätiedustelulla kotimaassa eihän kyse ole enää sosiaalisen median alustan osalta valtiollisen toimija tietojärjestelmästä. Tähän ohjaa myös lain periaatesäännökset.

Pykälän 1 momentin mukaan pykälässä tarkoitetulla valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvalla tiedustelulla tarkoitettaisiin tiedonhankintaa valtiollisen toimijan Suomen alueella hallinnoimien tai käyttämien tietojärjestelmien siitä osasta, joka toteuttaa tai edesauttaa tiedustelutehtävän kohteena olevaa toimintaa tai joka tallentaa tai välittää tiedustelutehtävän kohteena olevaan toimintaan liittyviä tietoja. Säännös rajaisi pykälässä tarkoitetun tietojärjestelmätiedustelun kattamaan ne osat tietojärjestelmästä, jotka sijaitsevat Suomessa. Hallinnoimisella tarkoitettaisiin sitä, että valtiollisella toimijalla on käyttöoikeus tiettyyn laitteeseen tai ohjelmistoon ja toimija pystyy päättämään käyttöoikeuden rajoissa laitteen tai ohjelmiston käytöstä. Esimerkiksi pilvipalveluun tallennettavan tiedon osalta hallinnointi kattaa sen osan, johon valtiollinen toimija voi tallentaa tietoja, ei koko pilvipalvelua.

Käyttäminen kattaisi myös tilanteet, joissa esimerkiksi valtioon attribuoitu APT-toimija on kaapannut jonkin tietojärjestelmän osan käyttöönsä ja suorittaa haitallisia kybertoimia kaappauksen kohteena olevan tietojärjestelmän osasta. Tältä osin menetelmän käyttö kohdistuisi ja rajautuisi vain ”murrettuun” tai muutoin APT-toimijan käyttämään

tietojärjestelmän osaan ja valtiollisen toimijan toimintaan tähän liittyen. Ylimääräinen tieto hävitettäisiin hävittämistä koskevien säännösten mukaisesti ja huomioon otettaisiin tiedustelukiellot. Jo toimivaltuuden käyttöä valmisteltaessa otettaisiin huomioon, miten vältettäisiin ylimääräisen tiedon havaitseminen ja varmistettaisiin ylimääräisen tiedon tehokas poisto, jos sitä ennakoimattomasti joutuisi tiedonhankinnan kohteeksi.

Toimivaltuuden osalta olisi myös huomioitava valtiollisen toimijan määritelmä, joka kattaisi myös valtiollisen toimijan ohjauksessa olevat toimijat. Valtiollisen toimijan sijaistoimija saattaisi käyttää jonkin tietojärjestelmän osaa ja valtiollisen toimijan ohjauksessa suorittaa haitallisia toimia Suomen maanpuolustusta tai kansallista turvallisuutta vastaan.

Teknisesti pykälän tietojärjestelmätiedustelu kohdistuisi toistensa kanssa tietyssä sotilaallisessa toiminnassa tai kansallista turvallisuutta vakavasti uhkaavassa tarkoituksessa kommunikoivien laitteiden ja virtuaalisten järjestelmien muodostamaan loogiseen kokonaisuuteen, jolloin lupaa ei edellytettäisi vaadittavan erikseen jokaiseen sellaiseen laitteeseen tai ohjelmistoon, joka kuuluu kokonaisuuteen, tai laitteita yhdistävään tietoliikenneyhteyteen.

Pykälän tarkoittamassa tietojärjestelmätiedustelussa ei olisi kyse yksittäisten henkilöiden tai laitteiden tiedustelusta, vaan tietojärjestelmä on usein muuttuva kokonaisuus. Tämän takia tiedustelun kohteena voi olla myös ne valtiollisen toimijan uudet laitteet ja käyttäjät, jotka eivät olleet osana tietojärjestelmää tai sen käyttöä tiedonhankinnan alkaessa. Luonnollisesti henkilöt ja laitteet voivat tulla tiedustelumenetelmän käytön kohteeksi vain siltä osin kuin ne liittyvät teknisesti tietojärjestelmään. Mikäli järjestelmän käyttäjän telepäätelaitteesta olisi tarkoitus saada myös muilta osin tietoja, olisi kyse toisen tiedustelumenetelmän käytöstä.

Tietoa voitaisiin hankkia joko kokonaisesta tietojärjestelmästä tai jostain tietojärjestelmän sellaisesta loogisesta tai fyysisestä osasta, joka toteuttaa tietojärjestelmän jotakin toiminnallisuutta tai joka muutoin voidaan määrittää tietojärjestelmässä omaksi osakseen perustuen tietojärjestelmän käyttäjään tai tietojärjestelmän osan perustellusti oletettuun tietosisältöön. Tiedonhankintaa voitaisiin kohdistaa esimerkiksi:

1) kyberuhkatoimijan rakentamaan ja käyttämään tietoverkkoinfrastruktuuriin siihen kuuluvine palvelimineen, kaapattuine laitteineen ja tietoliikenneyhteyksineen;
2) tiettyyn käyttäjätiliin tiedostonjakopalvelussa;
3) tietyn henkilöryhmän tai organisaation yksityiskäytössä olevaan viestintäpalveluun;
4) päätelaitteen tiedot, jotka se on tallentanut eri sovellusten kautta pilvipalveluun;
5) palveluntarjoajan virtualisoituna ylläpitämä palvelun ja sen tietosisältö, mutta ei muut samassa fyysisessä palvelimessa sijaitsevat tietosisällöt, jotka ovat muiden toimijoiden hallinnassa;
6) abstraktit tietovarannot, kuten tietyt virtuaalivaluuttatransaktiot.

Toimivaltuus mahdollistaisi sotilastiedusteluviranomaiselle aiempaa ennakoivamman tietojärjestelmien tiedustelun ja uhkien tunnistamisen. Tämä mahdollistaisi sen, että sotilastiedusteluviranomainen pystyisi tunnistetuissa tietojärjestelmissä etsimään hankittavaa tietoa sekä tunnistamaan uusia tietojärjestelmiä, jotka ovat osana sotilaallista toimintaa tai kansalliselle turvallisuudelle vakavaa uhkaa aiheuttavaa toimintaa.

Tiedon hankkiminen tietojärjestelmään saapuvasta tai siitä lähtevästä viestistä puolestaan mahdollistaisi tiedustelun tietojärjestelmän toimintaan suhteessa sen kyberympäristöön, eli esimerkiksi siihen, miten tietojärjestelmä toteuttaa kyberuhkatoimijan käskyjä tai millaisen uhkan se muutoin muodostaa.

Tietojärjestelmän kokonaisuus rajautuu esimerkiksi kohteena olevien laitteiden välisen kommunikoinnin ja käyttöoikeuksien perusteella. Kokonaisuudessa olevat laitteet kommunikoivat muiden tietojärjestelmän kokonaisuuteen kuuluvien laitteiden välillä ja käytettävillä laitteilla ja ohjelmistoilla on käyttöoikeuksia tiettyihin laitteisiin ja muihin ohjelmistoihin. Esimerkiksi näiden tietojen ja hankittujen tietojen pohjalta myös esimerkiksi datakeskuksen palvelimista pystytään rajaamaan tietojärjestelmän kokonaisuuteen kuuluva tallennustila tai serverikaappi, jota käytetään tietojärjestelmässä. Tietojärjestelmätiedustelu ei edellytä laajojen ennalta määräämättömien tietoliikennevirtojen tai tietomassojen läpikäyntiä, joten näin ollen toiminnassa ei ole kyse tietoliikennetiedustelua vastaavasta toiminnasta, jossa tiedonhankinta perustuisi kohdetta kuvaavien hakuehtojen käyttöön.

Selvää on se, että tietojärjestelmätiedustelu ei kohdistuisi kaikkeen datakeskuksessa olevaan tietoon, kuten ennalta määräämättömien yksityisten tallentamiin tietoihin. Toimivaltuuden käyttö ei kohdistuisi ennalta määräämättömästi kaikkeen mahdolliseen tietoon, vaan rajautuisi niihin osiin, joita valtiollinen toimija käyttää tietojärjestelmän infrastruktuurin mukaisesti. Yksinkertaisimmillaan tietojärjestelmän tietoja päästäisiin käsittelemään täysin vastaavassa laajuudessa kuin mihin tietojärjestelmän yksittäisellä käyttäjällä on mahdollisuus. Näin ollen esimerkiksi pilvipalvelun osalta ei päästä katsomaan muita tietoja kuin mitä yksittäinen käyttäjä pääsee katsomaan ja käsittelemään.

Luonnollisesti, koska tietomäärät voivat olla isoja, voitaisiin tietoja käsitellä automatisoidusti ja manuaalisesti, kuten muutakin tietoa.

Perusoikeuksien ja ihmisoikeuksien kunnioittamisen periaate ohjaa siihen, että tiedonhankinta on tarkkaan kohdistettava valtiolliseen toimijan tietoon ja tietovarantoihin. Jos on epäselvää, kohdistuuko tiedonhankinta tietovarantoon, jossa olisi pääsääntöisesti yksityisten henkilöiden tietoja, sotilastiedusteluviranomaisella olisi korostunut selonotto- ja perusteluvelvollisuus.

Pykälän 2 momentti sisältäisi rajauksen tietojärjestelmän tiedusteluun. Koska tietojärjestelmissä voi olla kyse laajoistakin laitteiden ja ohjelmistojen kokonaisuudesta, tietojärjestelmätiedustelua voitaisiin käyttää ainoastaan siinä laajuudessa kuin on välttämätöntä tiedustelutehtävän kohteena olevan toiminnan kannalta. Toisin sanoen tietojärjestelmän ensimmäiseksi havaitusta pisteestä voitaisiin siirtyä tietojärjestelmän muihinkin laitteisiin ja ohjelmistoihin, jos ne liittyisivät tiedustelutehtävään ja tietojärjestelmän kokonaisuuteen. Toisaalta muista tietojärjestelmän osista ei saisi hankkia tietoa, koska se laajentaisi tiedon hankinnan muuhun kuin välttämättömään.

Päätöksentekoa koskevassa pykälässä säädettäisiin erikseen uuden telepäätelaiteen, teleosoitteen, laitteen tai ohjelmiston lisäämistä koskevasta päätöksenteosta. Koska lisäämisestä tehtäisiin oma päätöksensä, myös tiedusteluvalvontavaltuutettu pystyy valvomaan tehokkaasti toimintaa.

Selvää on se, että muita tietojärjestelmän tietoja kuin niitä, jotka liittyvät tiedustelutehtävän kohteena olevaan valtiolliseen toimijaan, ei saisi hankkia. Jos tällaisia tietoja tulisi tiedustelumenetelmän kohteeksi, olisi ne hävitettävä hävittämistä koskevien säännösten mukaisesti. Lisäksi esityksessä ehdotetaan muutettavaksi lain 85 §:ää, jonka myötä säännöksessä tarkoitettu tietojärjestelmätiedustelu olisi keskeytettävä, jos se kohdistuisi väärin. Toimivaltuutta koskisi myös pöytäkirjaamisvelvollisuus sekä tallenteiden ja asiakirjojen tarkastamisvelvollisuus vastaavasti kuin muilla tiedustelumenetelmillä hankittuja tietoja.

Toimivaltuuden käyttöä rajaisivat myös tiedustelukiellot ja katselu- ja kuuntelukiellot sekä lain yleiset periaatteet.

61 b §. *Valtiolliseen toimijan tietojärjestelmään kohdistuvasta tiedustelusta kotimaassa päättäminen.* Pykälässä säädettäisiin päätöksenteosta. Päätöksenteko vastaisi niitä tiedustelumenetelmiä, joita tietojärjestelmätiedustelussa teknisesti yhdistetään, eli esimerkiksi telekuuntelua ja televalvontaa.

Pykälän 1 momentin mukaan tuomioistuimelle vaatimuksen tekisi tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

Pykälän 2 momentin mukaan luvan voimassaoloaika olisi enintään 6 kuukautta.

Pykälän 3 momentissa olisi säädetty vaatimuksessa ja päätöksessä mainittavista seikoista. Momentin 1 kohdassa toimenpiteen perusteena olevalla tiedustelutehtävällä tarkoitettaisiin 10 §:n 6 kohdassa tarkoitettua tiedustelutehtävää. Tiedustelutehtävä olisi tiedustelumenetelmän käytön perusteena, kuten muidenkin tiedustelumenetelmien osalta. Vaatimuksessa ja päätöksessä tulisi ilmetä toimenpiteen tavoite, mihin tiedustelumenetelmän käytöllä pyrittäisiin. Toimivaltuuden käytön tavoite olisi määriteltävä riittävällä tarkkuudella.

Momentin 2 kohdan mukaan vaatimuksessa ja päätöksessä olisi määriteltävä toimenpiteen kohteena oleva valtiollinen toimija ja sen käyttämä tietojärjestelmä. Valtiollinen toimija olisi pystyttävä nimeämään määritelmän mukaisesti. Kyse voi olla Suomen alueella toimivasta valtion viranomaisesta tai tämän ohjauksessa ja määräyksessä toimivasta tahosta. Joka tapauksessa valtiollinen liitäntä olisi tuotava esiin ja perusteltava se.

Kohdan mukaisesti vaatimuksessa olisi määriteltävä mahdollisimman tarkkaan järjestelmäkokonaisuus siten, että tuomioistuimen on mahdollista yksiselitteisesti ymmärtää ja valvoa, millaiseen tietojärjestelmäkokonaisuuteen ja kenen hallintaoikeuden tai käytön piiriin toiminta kohdistuu.

Järjestelmän kuvaaminen voisi tapahtua esimerkiksi kuvaamalla kohteena olevan tietojärjestelmän looginen kokonaisuus. Loogisella kokonaisuudella tarkoitettaisiin abstraktia, teknologianeutraalia kuvausta siitä, miten tietojärjestelmän osat toimivat yhdessä. Looginen kokonaisuus ei kerro sitä, millä laitteilla tai ohjelmointikielillä järjestelmän on toteutettu, vaan miten tieto kulkee, mitä toimintoja järjestelmä tarjoaa ja miten eri osat liittyvät toisiinsa. Tietojärjestelmän looginen taso vastaa kysymykseen, miten järjestelmän toiminnallisuus on järjestetty ilman fyysisiä yksityiskohtia. Luvassa määritetyn loogisen kokonaisuuden rajoissa tietojärjestelmätiedustelua voitaisiin kohdistaa laitteisiin, ohjelmistoihin ja tiedonsiirtokanaviin.

Usein sotilastiedusteluviranomaisella saattaa olla tiedossa esimerkiksi jokin laite, joka liittyy tietojärjestelmän loogiseen kokonaisuuteen. Tämä laite olisi tuota esiin tuomioistuimelle esitettävässä vaatimuksessa. Tiedossa olevan laitteen kautta tietojärjestelmästä saadaan tietoa, ja hankittujen tietojen perusteella tietojärjestelmästä saadaan parempi käsitys ja järjestelmän muista osista ja niiden kautta voidaan hankkia tietoa.

Toimivaltuudessa ei olisi kyse yksittäisen henkilön käyttämistä laitteista tai teleosoitteista, vaan toisiinsa fyysisesti tai loogisesti liitoksissa olevasta kokonaisuudesta. Tämän takia vaatimuksessa ja luvassa olisi määriteltävä käytettävä tietojärjestelmä riittävällä tarkkuudella. Kyse voisi olla esimerkiksi asiahallintajärjestelmästä, johon järjestelmän käyttäjän syöttämät tiedot näkyvät laitteen näytöllä, mutta tallennus tapahtuu pilvipalveluun.

Toimivaltuus kattaisi myös ne uudet käyttäjät, laitteet ja laitteistot, jotka tulevat osaksi tai yhdistyvät tietojärjestelmään. Tämän takia vaatimuksessa ja luvassa ei voitaisi määritellä tietojärjestelmää laite- tai teleosoitekohtaisesti.

Momentin 3 kohta olisi päätöksenteon kannalta keskeinen. Vaatimukseen ja päätökseen olisi sisällytettävä ne tosiseikat, joihin kotimaan tietojärjestelmätiedustelun edellytykset ja kohdistaminen perustuisivat. Tosiseikkojen esittäminen tuomioistuimelle velvoittaa tiedusteluviranomaisen esittämään ja perustelemaan ne tosiseikat, joiden perusteella tuomioistuimella olisi tosiasiallinen mahdollisuus huolelliseen lupaharkintaan ja tuomioistuin voisi tehdä tiedustelumenetelmän käytön edellytysten täyttymisestä omat johtopäätöksensä.

Mainituissa edellytyksissä olisi kyse 12 §:n tiedustelumenetelmien yleisistä edellytyksistä ja toimivaltuutta koskevassa 61 a §:ssä mainituista edellytyksistä. Lisäksi vaatimuksessa ja päätöksessä olisi esitettävä riittävät tosiseikat tiedustelutehtävästä ja sen pohjana olevasta lain 4 §:ssä tarkoitetusta sotilastiedustelun kohteena olevasta valtiollisesta toimijasta.

Lupaa haettaessa ja päätöstä perusteltaessa erityisen tärkeässä asemassa ovat sotilastiedustelun yleiset periaatteet. Suhteellisuusperiaatteen kannalta tärkeässä asemassa olisi erityisesti se, kuinka vakavasta toiminnan ilmenemismuodosta olisi kysymys.

Kohdassa tarkoitettujen tietojen olisi oltava riittävää ja oikean sisältöistä. Tuomioistuin voisi varmistua tiedon riittävyydestä kyselyoikeuttaan käyttämällä. Lisäksi hakija toimii tosiseikastoa esittäessään virkavastuun alaisena ja vastaa esittämiensä perusteiden oikeellisuudesta. Tuomioistuimen harkinta voi perustua vain siihen, että hakija kertoo – asioiden korkeasta salaisuusasteesta huolimatta – tuomioistuimelle avoimesti ja oikeasisältöisesti siitä toiminnasta, josta tietoja halutaan tiedustelumenetelmiä käyttämällä hankkia sekä kohteesta.

Momentin 4 kohdan mukaan vaatimukseen ja päätökseen olisi sisällytettävä luvan voimassaoloaika kellonajan tarkkuudella.

Momentin 5 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava Suomessa toteutettavan valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelun suorittamista johtava ja valvova virkamies.

Momentin 6 kohdan mukaan vaatimukseen tai päätökseen tulisi sisällyttää mahdolliset rajoitukset ja ehdot. Tuomioistuin voisi asettaa päätöksessään tiedustelumenetelmän käytölle rajoituksia ja käytön ehtoja. Jos tällaisia rajoituksia ja ehtoja olisi tiedossa jo vaatimusta laadittaessa, vaatimuksen esittäjän tulisi harkita niiden kirjaamista jo itse vaatimukseen.

62 §. *Ulkomaan tietojärjestelmätiedustelu.* Pykälän 2 momenttia muutettaisiin. Muutoksen myötä toimivaltuutta saisi käyttää myös muut sotilastiedusteluviranomaiset kuin Puolustusvoimien tiedustelulaitos. Sotilastiedustelutoiminnan kehityksen myötä on havaittu tarve, että sotilastiedusteluviranomaisella yleisesti on tarve ulkomaan tietojärjestelmätiedustelun käyttöön.

Pykälään lisättäisiin uusi 4 momentti. Sen mukaan sotilastiedusteluviranomainen voisi tehdä tarvittavia tietoteknisiä toimenpiteitä Suomen ulkopuolelle olevassa tietojärjestelmässä, jos tietojärjestelmällä tai sen kautta aiheutettaisiin Suomen maanpuolustukselle tai kansalliselle turvallisuudelle vakavaa uhkaa. Tietotekniset toimenpiteet voisivat koskea esimerkiksi toimia, joilla pyritään estämään järjestelmän toiminta kokonaan tai osittain tai haittaamaan tietojärjestelmän käyttöä.

Toimenpiteillä tarkoitettaisiin tietoteknisiä menetelmiä, joten säännöksen nojalla fyysisiin, kineettisiin vaikuttamisen toimenpiteisiin ryhtyminen ei olisi mahdollista. On huomattava, että tietojärjestelmän kautta saatetaan toteuttaa fyysisessä maailmassa tapahtuvia suoritteita, kuten toiminnanohjausjärjestelmässä on kyse.

Säännöksen käyttöala olisi myös lain soveltamisalan ja ulkomaan tietojärjestelmätiedustelua koskevan sääntelyn mukaisesti sidottu sotilastiedustelutoimintaan, joten pelkästään estäviin toimenpiteisiin ryhtyminen ei olisi säännöksen nojalla mahdollista. Näin ollen säännöksen käyttäminen edellyttäisi käytännössä sitä, että kyse on ollut ensisijaisesti tiedonhankinnasta. Käytännössä tilanne voisi tulla kyseeseen esimerkiksi, jos tiedustelu kohdistuisi tietojärjestelmään, jota sittemmin käytettäisiin säännöksessä kuvattuun vakavasti uhkaavaan toimintaan tai sen mahdollistamiseen. Toimivaltuutta voitaisiin käyttää myös, jos olisi viitteitä Suomen maanpuolustusta tai kansallista turvallisuutta vakavasti vaarantavasta toiminnasta, jonka nojalla käynnistettäisiin tiedusteluoperaatio, jonka myötä vakavaa vaaraa aiheuttavaan tietojärjestelmään voitaisiin kohdistaa tarvittaessa säännöksessä tarkoitettuja toimenpiteitä.

Toimenpiteiden voidaan arvioida kohdistuvan tarkasti käytännössä aina, sillä kohteena oleva tietojärjestelmä on jo sotilastiedustelun kohteena.

Koska kyse on toisen valtion alueella suoritettavista toimenpiteistä, toimenpiteen arvioinnissa olisi otettava huomioon kansainvälinen oikeus ja sen asettamat reunaehdot. Kansainvälistä oikeutta kyberympäristössä on käsitelty tämän esityksen yleisperusteluissa.

Säännöksessä tarkoitetulla suhteellisuudella tarkoitettaisiin sitä, että toimenpiteen olisi kohdistuttava tarkasti vakavasti uhkaavaan toimintaan eikä sillä saisi aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä toimenpiteen suorittamiseksi. Ennen toimenpiteen suorittamisesta olisi tehtävä sen vaikutusten tarkka arviointi.

Toimenpiteiden vaikutusten olisi oltava myös väliaikaisia ja ne olisi lopetettava heti, kun uhkan aiheutuminen saadaan estettyä.

Säännöksessä tarkoitetulla välttämättömyydellä tarkoitettaisiin sitä, että vaarantavaa toimintaa ei voida estää tai lopettaa muilla keinoin taikka muiden keinojen käyttö edellyttäisi merkittävien resurssien käyttämistä. Kuten aiemmin tässä esityksessä on tuotu ilmi, Suomi katsoo, että kansainvälinen oikeus soveltuu kyberympäristössä täysimääräisesti. Näin ollen välttämättömyyttä olisi arvioitava myös kansainvälisen oikeuden kontekstissa, ja ensisijaisesti olisi arvioitava muiden keinojen, kuten diplomatian ja retorsion mahdollisuutta. Vihamieliseen toimintaan voidaan reagoida myös pyytämällä toisen valtion CERT-yksikköä puuttumaan valtionsa alueella tapahtuvaan toimintaan. Viime kädessä kyseessä voi olla vetoaminen valtiovastuusääntöjen mukaiseen kansainvälisoikeudelliseen välttämättömyyteen (niin kutsuttu plea of necessity).

On myös huomattava, että kansainvälisen oikeuden mukaan valtiolla on oikeus suojata itseään oikeudettomalta toiminnalta, ja suvereniteetin loukkauksiin voidaan vastata kansainvälisen oikeuden sallimin keinoin. On tarkoituksenmukaista, että jokaisella itsenäisellä valtiolla on käytössään monipuolinen keinovalikoimia varautua ja vastata erilaisiin sitä koskeviin uhkiin sekä normaali- että poikkeusoloissa. Tällainen kokonaisuus vahvistaa valtion kykyä suojata suvereniteettiaan, ylläpitää yhteiskunnan elintärkeitä toimintoja ja reagoida oikea-aikaisesti sekä oikeasuhtaisesti tilanteisiin, jotka voivat horjuttaa sen turvallisuutta tai toimintakykyä.

Koska säännöksessä tarkoitetut toimenpiteet voivat tietyissä tilanteissa sisältää merkittäviäkin ulko- ja turvallisuuspoliittisia vaikutuksia, olisi toimenpiteitä käsiteltävä lain 15 §:ssä tarkoitetussa menettelyssä. Toimenpiteet edellyttävät myös ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteisen kokouksen valmistelevaa käsittelyä. Vaikka operatiivisen päätöksen tekisikin pääesikunnan tiedustelupäällikkö, ulko- ja turvallisuuspoliittinen päätöksenteko olisi tehtävä ennen tätä.

Selvää on, että momentissa tarkoitetut toimenpiteet eivät saisi ylittää kansainvälisoikeudellisen aseellisen voimankäytön kynnystä, ja toimivaltuutta saisi käyttää ainoastaan Suomen maanpuolustukselle tai kansalliselle turvallisuuden vakavaa uhkaa aiheuttavan tietojärjestelmän käytön estämiseen ja haittaamiseen.

Tavanomaisena esimerkkinä vakavaa uhkaa maanpuolustukselle ja kansalliselle turvallisuudelle aiheuttavasta toiminnasta on APT-toimijat. APT-toimijat (Advanced Persistent Threat) ovat pitkäkestoisia, huomaamattomia ja usein valtiollisesti tuettuja kyberuhkaryhmiä, jotka kohdistavat hyökkäyksiä yhteiskunnan kannalta merkittäviin kohteisiin, kuten hallintoon, kriittiseen infrastruktuuriin ja yrityksiin. Ne toimivat erityisen järjestelmällisesti: tunkeutuvat, pysyvät piilossa ja varastavat tietoa tai häiritsevät toimintaa pitkällä aikavälillä. Useita APT-toimijoita on jo attribuoitu liittyviksi tiettyyn valtioon.

APT-toimijat joutuvat rakentamaan toiminnalleen infrastruktuurin (esimerkiksi palvelimia, tietoliikenneyhteyksiä ja tietojärjestelmiä), joka toteutetaan usein varsinaisen omistajan tai haltijan tietämättä esimerkiksi haittaohjelmia ja haavoittuvuuksia hyödyntäen, Jotta varsinainen kyberhyökkäys toteutuisi, infrastruktuuria ohjataan komentopalvelimilta.

Sotilastiedustelu voi jo nykyisin seurata toimivaltansa nojalla APT-toimijoita, mutta niiden toimintaa pystytään ainoastaan seuraamaan ja niistä saatua tietoa pystytään luovuttamaan muille viranomaisille. APT-toimijoiden toiminnan seurauksia voidaan ehkäistä Suomen alueella, mutta tämä ei varsinaisesti estä toimintaa ja torjuntatoimenpiteet aiheuttavat kustannuksia.

Säännös ei mahdollista sotilastiedusteluviranomaisen hyökkäyksellisiä toimenpiteitä. Säännöksen nojalla ei voida toteuttaa esimerkiksi tuhoavia toimenpiteitä tietyn valtion kriittiseen infrastruktuuriin, jotta tietyn valtion yhteiskunnan toiminta häiriintyisi.

Vaikka säännöksessä ei voida katsoa olevan kyse lain 3 §:ssä tarkoitetusta tiedonhankinnasta, tarkoituksenmukaisuus näkökohtien mukaisesti olisi perusteltua säätää toimintamahdollisuudesta tiedonhankintatoimivaltuuden yhteydessä. Säännöksen tilanteissa sotilastiedusteluviranomainen on jo kohteessa ja sotilastiedusteluviranomaisella on mahdollisuus toimia säännöksessä tarkoitetuissa tilanteissa.

Sotilastiedusteluviranomainen on ainut viranomainen, jolla on toimivalta ja toimivaltuus hankkia tietoa ulkomaan tietojärjestelmistä. Lisäksi osana Puolustusvoimia, sotilastiedusteluviranomaisella on osaaminen valtakunnan alueellisen koskemattomuuden turvaamisesta ja siihen liittyvästä strategisesta, operatiivisesta ja taktisesta suunnittelusta.

63 §. *Ulkomaan tietojärjestelmätiedustelusta päättäminen.* Pykälään lisättäisiin uusi 3 momentti, jolloin nykinen 3 momentti siirtyisi uudeksi 4 momentiksi. Pykälässä säädettäisiin edellä 62 §:n 4 momenttia koskevasta päätöksenteosta.

Ulko- ja turvallisuuspoliittisesti herkällä alueella olisi toimenpidettä koskevassa päätöksenteossa aina huomioitava ulko- ja turvallisuuspoliittisten näkökantojen lisäksi kansallinen lainsäädäntö ja kansainvälinen oikeus. Edellä tarkoitetut näkökannat olisi valmisteltava poikkihallinnollisesti lain 15 §:ssä säädetyssä menettelyssä. Päätös olisi käsiteltävä myös valmistelevasti TP-UTVA:ssa.

Ehdotetun 62 §:n 4 momentin toimivaltuuden käytöstä päätettäessä olisi aina huomioitava toimenpiteen oikeasuhtaisuus sisältäen vaikutukset kohteelle, mahdollinen eskalaation riski sekä mahdolliset Suomeen kohdistuvat vastatoimet ja niiden vaikutukset.

Keskeinen osa toimenpiteet vaikutusten arvioinnissa on myös operaatioturvallisuudella. Jos toimenpidettä ei voida suorittaa operaatioturvallisesti, toimenpide jää tekemättä. Päätöksenteossa olisi myös aina huomioitava toimenpiteen vaatimat resurssit ja suhteuttaa niitä realistisesti odotettavissa oleviin hyötyihin.

Momentin mukaisesti päätöksen tekisi pääesikunnan tiedustelupäällikkö. Päätös edellyttäisi aina asian käsittelyä valmistelevasti lain 15 §:n 2 momentin mukaisesti ja TP-UTVA:ssa. Toimeenpanevan päätöksen operaatiosta tekisi tämän jälkeen operatiivisesta toiminnasta vastaava taho, eli sotilastiedusteluviranomainen. Menettelyä voidaan pitää tarkoituksen mukaisena myös ulkopoliittisten herkkyyksien vuoksi.

Ehdotetun 62 §:n 4 momentin toimenpiteiden suorittaminen edellyttää tarkkaa operatiivista ja poliittista arviointia. Päätöksenteon kannalta keskeistä on määritellä toimenpiteen kohde, eli tietojärjestelmä (tietojenkäsittelylaitteiden, tiedonsiirtolaitteiden ja tietoja käsittelevien ohjelmistojen muodostama yhteen toimiva kokonaisuus), johon toimenpiteitä kohdistetaan. Lähtökohtana on, että sotilastiedusteluviranomaisella on jo tarkka kuva kohteena olevasta tietojärjestelmästä.

Keskeistä on myös arvioida tietojärjestelmän tai sen kautta aiheutuvaa vakavaa uhkaa. Vakavaksi uhkaksi katsotaan toiminnot, jotka on määritelty lain 4 §:ssä. Arviossa olisi kiinnitettävä huomiota siihen, miten akuutti uhkan konkretisoituminen on. Jos toinen valtio haluaa kohdistaa Suomeen haitallisia toimenpiteitä, vaatii tämä toimenpiteen suorittajalta valmistelevia toimenpiteitä. Keskeistä olisikin sen arviointi, missä vaiheessa voidaan riittävän korkealla todennäköisyydellä todeta, että toimenpiteet tulevat kohdistumaan Suomeen. Tämä voidaan todeta esimerkiksi silloin, kun tietojärjestelmään syötetään Suomea koskevia tietoja tai Suomessa olevia kohteita.

Toimenpiteet edellyttävät myös tarkkaa suunnittelua, jotta haluttu lopputulos saadaan aikaiseksi. Toimenpiteiden suorittamista tulee myös valvoa niin oikeudellisesti kuin operatiivisesti.

Edellä kuvatut ja muut näkökohdat olisi arvioitava lain 15 §:ssä tarkoitetussa menettelyssä sekä TP-UTVA:ssa, jotka voisivat ilmaista oman käsityksensä niistä.

64 §. *Ulkomailla tapahtuva sotilastiedustelu.* Pykälän 1 momenttiin lisättäisiin viittaus tietolähdetoimintaa koskevan 51 §:ään ja sen 3 momenttiin. Lisäyksen myötä ulkomailla tapahtuvassa tietolähdetoiminnassa ei tarvitsisi soveltaa kieltoa hankkia tietoja viranomaistoimivaltuuksilla.

Voimassa olevien säännösten takia epäselvyyttä on aiheuttanut se, onko kiellossa käyttää viranomaistoimivaltuuksia kyse suomalaisen viranomaisten vai kohdevaltion viranomaisten toimivaltuuksista. Joissain valtioissa viranomaisten toimivaltuudet saattavat olla erittäin laajoja, minkä takia voi jäädä epäselväksi se, käyttääkö tietolähde viranomaistoimivaltuuksia vai ei.

Uuden viittauksen myötä poikkeamisessa olisi kuitenkin oltava kyse välttämättömyydestä.

Pykälän 2 momentti jaettaisiin kahteen momenttiin. Uuden muotoilun myötä 2 momentissa käsiteltäisiin päätöksentekoa, ja 3 momentti käsittelisi virkamiehen suostumusta.

Pykälän 2 momentin mukaan pääesikunnan tiedustelupäällikkö päättäisi ulkomailla tapahtuvasta sotilastiedustelusta ja siellä sallituista tiedustelumenetelmistä. Voimassa olevan säännöksen mukaan selvää ei ole ollut se, päättääkö pääesikunnan tiedustelupäällikkö myös

yksittäisten tiedustelumenetelmien käytöstä ulkomailla. Tämä on saattanut luoda käytännön ongelman ulkomailla toteuttavien tiedusteluoperaatioiden suorittamisessa, jos yksittäisen tiedustelumenetelmän käyttö edellyttää pääesikunnan tiedustelupäällikön tekemää päätöstä.

Ehdotetun muutoksen myötä pääesikunnan tiedustelupäällikkö tekisi päätöksen ulkomailla tapahtuvasta sotilastiedustelusta (tiedusteluoperaatiosta) ja siinä käytettävistä tiedustelumenetelmistä, eli mitkä tiedustelumenetelmät ovat sallittuja kyseisessä operaatiossa. Päätöksen mukaista tiedustelumenetelmän käyttöä koskevan päätöksen voisi tehdä tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies, joka on lähempänä käytännön toimintaa. Muutos selkeyttäisi oikeustilaa ja virkamiehen oikeusturva parantuisi.

Ulkomailla tapahtuvaan tiedusteluun liittyvien ulkopoliittisten herkkyyksien takia päätöksenteossa olisi otettava huomioon tiedustelun painopisteet sekä 15 §:n sääntely ja sitä kautta tulleet mahdolliset suuntaviivat.

Pykälän uudessa 3 momentissa säädettäisiin ulkomailla tapahtuvaan sotilastiedusteluun osallistuvan sotilastiedusteluviranomaisen virkamiehen suostumuksesta. Säännös vastaisi nykytilaa, joka on säädetty eduskunnan myötävaikutuksella. Ulkomaille lähtemisen edellytyksenä olisi edelleen aina suostumus.

Ehdotettujen muutosten myötä voimassa olevan pykälän 3 momentti siirtyisi uudeksi 4 momentiksi.

66 §. *Teknisten tietojen käsittely viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi.* Pykälässä säädettäisiin voimassa olevan lain teknisten tietojen käsittelyn lisäksi teknisten tietojen käsittelystä tietoliikenteen reitittymisen ja muutosten seuraamiseksi. Tämän takia pykälän otsikkokin muutettaisiin vastaamaan sisällöllisesti uutta pykälämuotoilua.

Voimassa olevan 66 §:n 1 momentissa teknisten tietojen käsittely on sidottu hetkellisyyteen, jota on käytännössä pidetty vaikeana toteuttaa eikä sitä ole pidetty tarkoituksenmukaisena. Toimivaltuuden nojalla saatava tieto on lain 10 §:n 11 kohdan mukaisesti muita kuin viestin sisältöön kuuluvia tietoliikenteen tietoja. Näitä tietoja voivat olla muun muassa IP-osoiteavaruudet, erilaiset protokollat ja laitenumerot. Vaikka sinänsä esimerkiksi IP-osoite voi yksilöidä yksittäisen henkilön, toimivaltuuden nojalla ei voida tarkemmin ryhtyä selvittämään IP-osoitteen käyttäjää tai tämän viestintää eikä tietoja voida käyttää muussa tarkoituksessa kuin teknisessä analyysissä. Vaikka hankittu tieto olisi sinänsä henkilötietoa, ei henkilötietoa voida toimivaltuuden nojalla kuitenkaan yhdistää yksittäiseen luonnolliseen henkilöön tai organisaatioon. Tämän takia hetkellisyyden poistamisen ei voida katsoa johtavan siihen, että teknisten tietojen käsittelyn voitaisiin katsoa olevan niin kutsuttua massavalvontaa.

Pykälän tarkoittamaa toimivaltuutta käytettäessä voidaan tarvittaessa käyttää myös tietoliikenteen teknisiin tietoihin kohdistuvia hakuehtoja, jotta saatavan tiedon määrää voidaan jo heti alkuvaiheessa rajata mahdollisimman olennaiseen. Toimivaltuuden tarkoituksena on tunnistaa olennaiset viestintäverkon osat, joten teknisten tietojen käsittelyä kannalta tietoja rajataan olennaisesti esimerkiksi tietyn maantieteellisen alueen IP-osoiteavaruuksilla. Tästä ei ole kuitenkaan tarpeen säätää erikseen toimivaltuuden luonteen takia.

Vaikka pykälästä poistuisi viittaus hetkellisyyteen ja pykälässä ehdotetaan uutta käyttötarkoitusta tietoliikenteen teknisten tietojen käsittelylle, toiminta on edelleen tarkkaan valvottua niin sisäisesti kuin ulkoisesti. Ulkoisessa valvonnassa korostuu tiedusteluvalvontavaltuutetun rooli.

Pykälästä poistettaisiin myös automaattisen tietojen käsittelyn avulla tehtyyn analyysiin. Todettua voidaan pitää turhana, sillä käytännössä aina analyysi toteutetaan automaattisen tietojen käsittelyn avulla. Toisaalta voi tulla tilanteita, joissa analyysiä jouduttaisiin tekemään tai rikastamaan manuaalisesti. Joka tapauksessa käytettävät tiedot ovat tietoliikenteen teknisiä tietoja eikä niiden taustalla olevia henkilöitä voida selvittää teknisten tietojen käsittelyn avulla.

Pykälän 1 momentin 1 kodassa säädettäisiin teknisten tietojen käsittelystä viestintäverkon osan tunnistamiseksi. Kohta vastaisi käytännössä voimassa olevan lain 66 §:n 1 momentin säännöstä. Teknisten tietojen käsittelyllä tarkoitetaan tietoliikenteen teknisten tietojen käsittelyä 68 ja 70 §:ssä säädettyjen tietoliikennetiedustelutoimivaltuuksien käyttämiseksi olennaisten viestintäverkon osien tunnistamiseksi. Toimivaltuudella pyritään tunnistamaan ne Suomen rajan ylittävän viestintäverkon osat, kuten kuidut ja kuitujen aallonpituudet, joissa kulkee sotilastiedustelun kohteena olevan toimijan tietoliikennettä. Toimivaltuudella ei voida hankkia muuta kuin tietoliikenteen teknisiä tietoja ja vain analyysin tuottamiseksi viestintäverkon osan tunnistamiseksi. Viestin sisältötietoja ei voida käyttää.

Pykälän 1 momentin 2 kohta olisi uusi. Kohdan perusteella tietoliikenteen teknisiä tietoja voitaisiin seurata ja analysoida sen selvittämiseksi, reitittyykö tietoliikenne uudella tavalla tai onko tietoliikenteessä yleisesti tapahtunut joitain muutoksia. Toimivaltuudella pystyttäisiin havaitsemaan fyysiseen viestintäverkkoon liittyviä muutoksia, kuten viestintäverkon osan teknisen kapasiteetin nousu, sekä tietoliikenteen liikkumisessa tapahtuvia loogisen tason muutoksia.

Tietoliikenteessä ja etenkin internet-verkon toiminnassa keskeisenä ominaisuutena on tiedon mahdollisimman tehokas kulku lähettäjältä vastaanottajalle. Tämän takia esimerkiksi yksittäinen sähköpostiviesti pilkkoutuu useiksi tietoliikennepaketeiksi, joista jokainen kulkee yksittäisen paketin kannalta tehokkainta reittiä lähettäjältä vastaanottajalle. Tämä tarkoittaa sitä, että sotilastiedustelun kohteena olevan toimijan tietoliikenteen reitittyminen voi muuttua hyvinkin nopeasti. Nyt käsiteltävänä olevan säännöksen nojalla reitittymistä voitaisiin seurata.

Kohdassa viitatulla tietoliikenteen muutosten seuraamisella tarkoitettaisiin yleisemmin tietoliikenteen ja viestintäverkon muutosten seuraamista tietoliikenteen teknisten tietojen avulla. Viestintäverkoissa voi tapahtua teknisiä muutoksia ja uusia laitteistoja otetaan käyttöön. Tällä voi olla olennaista merkitystä tietoliikennetiedustelujärjestelmän toiminnan kannalta ja tietoliikennetiedustelussa tarvittavien laitteistojen ja teknisten asetusten ja säätöjen kannalta. Saatujen analyysien perusteella voitaisiin esimerkiksi tehostaa laitteistohankintoja ja kohdentaa niitä asianmukaisesti sekä tehdä tietoliikennetiedustelun järjestelmiin tarvittavia muutoksia.

Pykälän 2 momentissa säädettäisiin voimassa olevaa lakia vastaavasti, että teknisten tietojen käsittelyssä ei saisi muodostaa tietoa, josta voidaan tunnistaa yksittäinen luonnollinen henkilö. Säännös olisi informatiivinen. Pykälä itsessään koskee tietoliikenteen teknisten tietojen käsittelyä, eikä siitä ole luettavissa henkilösidonnaisuutta. Lain periaatesäännöksissä on säädetty tarkoitussidonnaisuuden periaatteesta ja perustuslain 2 §:n 3 momentti edellyttää julkista valtaa tarkoin noudattamaan lakia. Jos analyysiä tuotettaisiin yksittäisen henkilön tunnistamiseksi, rikkoisi viranomainen ilmankin säännöstä virkavelvollisuuksiaan ja syyllistyisi todennäköisesti rikokseen.

Pykälän 3 momentin mukaan pykälässä tarkoitettuja teknisten tietojen käsittelyssä käsiteltäviä teknisiä tietoja voitaisiin tallentaa 18 kuukauden ajaksi. Säännöksen mukaan tallennettavien tietojen määrä ei saisi ylittää 5 prosenttia kohteena olevan Suomen rajan ylittävän viestintäverkon osan kapasiteetista, eli tietoliikenteen määrästä, jonka viestintäverkon osa voi enimmillään teknisesti kuljettaa. Esimerkin omaisesti, jos viestintäverkon osan tekninen

kapasiteetti on 100 per yksi sekunti, teknisisiä tietoja voitaisiin tallentaa 5 per yksi sekunti. Käytännössä tallennettavat tekniset tiedot ovat satunnaisia teknisiä tietoja.

Säännöksessä annettaisiin sotilastiedusteluviranomaiselle myös oikeus tallentaa kerättyjä teknisiä tietoja enintään 18 kuukauden ajaksi. Tallennetut tiedot tuhoutuisivat 18 kuukauden päästä tallennuksen hetkestä sekunnin tarkkuudella.

Tallennettuja tietoja voitaisiin käyttää esimerkiksi pykälän 1 momentin 1 ja 2 kohdassa tarkoitettujen analyysien tukena tai ehdotetun 67 a §:n hakuehtojen määrittämiseen sekä 68 ja 70 §:ssä säädettyjen varsinaisten tietoliikennetiedustelun toimivaltuuksien yhteydessä. Luonnollisesti edellä viitatuissa pykälissä tarkoitettuja toimivaltuuksia käytettäessä nyt käsiteltävien tietojen käyttö edellyttää asianmukaista tuomioistuimen lupaa, josta on säädetty 67 b §:ssä sekä 69 ja 71 §:ssä. Tallennettuja tietoliikenteen teknisiä tietoja ei voida käyttää itsenäisesti tiedustelutehtävän suorittamiseen, jollei tähän ole saatu asianmukaista lupaa.

Teknisten tietojen tallentaminen ja käyttäminen edellyttävät tietojärjestelmää ja menettelyjä, jotka takaavat sen, ettei tallennettuja tietoja pysty käyttämään muuhun kuin tarkoitettuun tarkoitukseen tai ilman asianmukaista tuomioistuimen lupaa. Tämä edellyttää tarkkaa pääsynhallintaa ja valvontaa.

Pykälän 4 momentissa säädettäisiin teknisten tietojen käsittelyssä viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi saadun tiedon hävittämisesti. Säännöksen mukaan tiedot olisi hävitettävä 18 kuukauden kuluttua niiden tallentamisesta. Kyse olisi nimenomaisesti niistä tietoliikenteen teknisistä tiedoista, jotka olisi tallennettu pykälän 3 momentin mukaan, ei niistä, jotka ovat osana tilastollista analyysia tai jotka ovat päätyneet jatkokäsittelyyn ehdotetun 67 a §:n tai 68 tai 70 §:n tiedustelumenetelmien kautta.

On huomattava, että sotilastiedusteluviranomainen ei voi käyttää tässä tarkoitettuja tietoja muussa yhteydessä, ellei tuomioistuin ole myöntänyt lupaa sellaiselle toimivaltuudelle, jolla tässä tarkoitettuja tietoja saa käyttää. Näin ollen sotilastiedusteluviranomainen ei voi selvittää esimerkiksi tiettyä välitystietoa käyttäneen henkilöllisyyttä sotilastiedustelusta annetun lain 104 §:n avulla, ellei välitystietoa ole saatu varsinaisella tietoliikennetiedustelulla (lain 68 ja 70 §). Sotilastiedusteluviranomainen voisi siis selvittää välitystietoa käyttäneen henkilöllisyyden 104 §:n kautta, jos välitystieto olisi tullut hakuehtojen mukaisen tietoliikenteeseen kohdistuvan tiedonhankinnan yhteydessä.

67 §. *Teknisten tietojen käsittelystä päättäminen viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi.* Pykälään tehtäisiin edellä 66 §:ään ehdotetuista muutoksista johtuvan muutokset. Pykälän otsikossa viitattaisiin 66 §:n mukaisesti viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamisesta päättämiseen.

Pykälän 1 momenttiin tehtäisiin muutos 66 §:ään ehdotettujen muutosten takia. Momentissa viitattaisiin viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseen.

Lisäksi tuomioistuimelle vaatimuksen tekevä virkamies muutettaisiin aiemmasta Puolustusvoimien tiedustelulaitoksesta sotilastiedusteluviranomaiseksi. Sotilastiedusteluviranomaisen organisaation takia ei ole tarkoituksenmukaista, että vaatimuksen esittäjän olisi oltava nimenomaisesti Puolustusvoimien tiedustelulaitoksen virkamies, vaan vaatimuksen esittäjä voisi olla myös Pääesikunnan tiedusteluosaston virkamies. Olennaista olisi edelleen se, että virkamies on tähän tehtävään määrätty tiedustelumenetelmien käyttöön

erityisesti perehtynyt sotilaslakimies tai tiedustelumenetelmien käyttöön erityisesti perehtynyt muu virkamies.

Pykälän 2 momentissa säädetty luvan voimassaoloaika olisi kuusi kuukautta aiemman kolmen kuukauden sijaan. Kolmen kuukauden määräaikaa on pidetty perusteettoman lyhyenä ajanjaksona ottaen huomioon sen, että toimivaltuuden käytöllä ei hankita muuta kuin tietoliikenteen teknistä tietoa teknisen analyysin suorittamiseksi. Enimmillään kuuden kuukauden määräaika olisi myös yhteneväinen varsinaisen tietoliikennetiedustelun määräaikojen kanssa, joista säädetään lain 69 ja 71 §:ssä.

Luvan voimassaoloaika alkaisi kulua luvan antopäivästä tai päätöksen tekopäivästä lähtien.

Säännöksen mukaan lupa voisi koskea myös todettua luvan antopäivää tai päätöksen tekoa edeltävää aikaa, joka voisi olla kuutta kuukautta pidempi. Teknisten tietojen käsittelyssä voitaisiin käyttää ehdotetun 66 §:n 3 momentissa tarkoitettuja tallennettuja teknisiä tietoja.

Pykälän 3 momentin 1 kohtaan tehtäisiin ehdotetuista 66 §:n muutoksista johtuva muutos. Voimassa olevan 1 kohdan maantieteellisen alueen tai verkkoalueen lisäksi kohtaan lisättäisiin kohde, jonka tietoliikenteen reitittymistä tai muutosta seurataan. Kohteilla tarkoitettaisiin sotilastiedustelun kohteena olevaa toimijaa, jonka tietoliikenteen reitittymisestä tai muutoksista olisi hankittava tietoa. Tämä voi edellyttää rajaavien hakuehtojen käyttöä, jotta kohteen tietoliikenteessä tapahtuvia teknisiä muutoksia voitaisiin seurata. Luonnollisesti vaatimuksessa olisi tehtävä selkoa siitä, miten kohteen tietoliikenteen teknisiä muutoksia seurattaisiin ja mitä tietoja seurannan mahdollistamiseksi on käytössä.

Pykälän 3 momentin 2 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava viestintäverkon osat, joista tietoa haetaan. Kohtaan ei esitetä muutoksia.

Pykälän 3 momentin 3 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava käsittelyä johtava ja valvonta tiedustelumenetelmien käyttöön erityiseesti perehtynyt virkamies. Kohtaan ei esitetä muutoksia.

Pykälän 3 momentin 4 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava suunnitelma käsittelyn toteuttamisesta. Suunnitelman laatimista olisi sovellettava myös momentin 1 kohdan muutokseen, eli tietoliikenteen reitittymisen ja muutosten seurantaan. Näin ollen suunnitelmassa olisi tehtävä selkoa siitä, miten seuranta tullaan tarkemmin ottaen toteuttamaan.

67 a §. *Tietoliikennetiedustelu hakuehtojen määrittämiseksi.* Pykälä olisi uusi. Pykälässä säädettäisiin mahdollisimman kohdennetussa tietoliikennetiedustelussa tarpeellisten uusien hakuehtojen määrittämisestä. Termillä määrittäminen viitattaisiin siihen, että sinänsä sotilastiedustelun kohteet pysyvät voimassa olevan lain mukaisesti samana, mutta esimerkiksi kohteiden viestintäverkossa käyttämä teknologia ja viestinnän keinot saattavat muuttua. Etenkin vallitsevassa turvallisuuspoliittisessa tilanteessa teknologian kehityssykli on nopeutunut ja uutta teknologiaa ja uusia menetelmiä pyritään ottamaan käyttöön aiempaa nopeampaan tahtiin. Sotilastiedustelun kohteena olevat toimijat muuttavat alituiseen toimintaansa ja kehittävät uusia toimintatapoja.

Uuden toimivaltuuden tarkoituksena on riittävän erottelukykyisten hakuehtojen määrittäminen. Nykytilassa kaikissa tilanteissa uusien hakuehtojen määrittäminen tapahtuu käytännössä varsinaisen tietoliikennetiedustelun yhteydessä, mutta kohteena olevan toimijan vaihtaessa viestintään käytettävää teknistä menetelmää, voi tiedon saaminen kohteesta lakata yllättäenkin.

Toimivaltuuden käyttö olisi sidottu välttämättömyyteen. Välttämättömyyden määritelmän mukaisesti uusien hakuehtojen määrittämisen olisi toisin sanoen oltava käytännössä mahdotonta muilla keinoin, sen olisi vaadittava oleellisesti enemmän voimavaroja tai muiden keinojen käyttö viivyttäisi tiedonhankintaa kohtuuttomasti. Esimerkiksi tilanteessa, jossa kohteena olevan toimijan tietoliikenteestä ei enää yllättäen saada hankittua tietoa käytetyillä hakuehdoilla tietäen kuitenkin kohteen viestivän edelleen vakituiseen. Näin ollen voidaan olettaa kohteen ottaneen käyttöön uuden viestinnän keinon, jonka takia käytössä olisi oltava uuteen viestinnän keinoon kohdistuvia hakuehtoja. Tilanteessa tieto toki voitaisiin hankkia muilla tiedustelumenetelmillä, mutta esimerkiksi tiedustelumenetelmien käyttöä ulkomailla ei voida pitää realistisena vaihtoehtona jo pelkästään virkamiesten hengen ja terveyden suojaamisen, saati tiedusteluoperaatioon käytettävien resurssien ja ajan kannalta.

Pykälän 1 momentin mukaan Puolustusvoimien tiedustelulaitos voisi kerätä tietoliikennettä ja tallentaa sitä määrittääkseen sotilastiedustelun kohteita koskevia hakuehtoja. Viestintäverkon osassa liikkuva tietoliikenne on satunnaista, eli uusien hakuehtojen määrittämistä ei pyritä ensivaiheessa kohdistamaan tiettyyn tietoliikenteeseen. Tietoliikennevirrassa kulkee siis satunnaista tietoliikennettä.

Hakuehtojen määrittämisessä kohteena on tietoliikenteen tavuvirta, josta kohteena olevaan toimijaan liittyvän tietoliikenteen säännönmukaisuuden tai teknisten ominaispiirteiden perusteella pyrittäisiin määrittämään uusia hakuehtoja. Toimivaltuuden käytössä tietoliikennettä ei saatettaisi muotoon, josta analyytikko voisi lukea varsinaisen semanttisen viestin, vaan toiminnassa pyritään määrittämään sitä, mistä tietoliikenteessä (kokonaisvaltainen tavuvirta sisältäen kaikki protokollakerrokset) on ylipäätään kysymys. Tämä voi vaatia tietoliikenteen tarkastelua tavujen tasolla, riippumatta siitä, mikä protokollapinon rakenne on.

Jos analyysikyky rajoitetaan vain alempien tietoliikennekerrosten otsikkotietoihin (kuten IP-osoite) jo tunnettuihin seikkoihin, heikentyy mahdollisuudet muodostaa ymmärrys tai johtopäätökset tietoliikenteen luonteesta. Tässä yhteydessä on hyvä myös ymmärtää, että tietoliikenteen luonteella ei tarkoiteta ihmisten välisen kommunikaation puhuttua tai kirjoitettua merkityssisältöä, vaan sitä mitä tietoliikenteessä siirretään, minkä toimijoiden tai järjestelmien välillä ja millä teknisillä menetelmillä ja tunnuspiirteillä.

Ennalta tunnistamattoman liikenteen kohdalla ei ole lähtökohtaista tietoa esimerkiksi siitä, missä kohden tavuvirtaa jokin tuntematon protokollakerros alkaa tai mihin se loppuu; selvittäminen vaatii tutkimustyötä tietoliikenteen tavutasolla, esimerkiksi tietoliikenteen toistumakuvioiden havaitsemiseksi. Tämä voi joissakin tapauksissa olla myös edellytys sille, että voidaan tunnistaa se, onko kyseessä kohteen liikenne vai ei.

Toinen tärkeä näkökulma on myös tietoliikenteen tunnistusten arviointi: mikäli ei ole kykyä tarkastella tietoliikennettä sellaisenaan (raakana), ei ole välttämättä edellytyksiä arvioida, onko jokin protokollatunnistus tai kohdeosuma oikea vai niin kutsuttu väärä positiivinen.

Kuten aiemmin tässä hallituksen esityksessä on kuvattu, hakuehtoja voivat olla muun muassa kohteen käyttämät tietoliikenteen tekniset tiedot ja erilaiset protokollat, joilla viestintää välitetään lähettäjältä vastaanottajalle. Esimerkiksi uusia viestintäohjelmistoja kehitettäessä usein myös kehitetään uusi protokollia. Taajaan käytetty viestintäsovellus WhatsApp käyttää muokattua versiota XMPP-protokollasta ja salaukseen käytetään Signal Protocol -salausprotokollaa, kun taas viestintäsovellus Telegram käyttää omaa salaus- ja viestintäprotokollaa MTProto. Nämä protokollat voivat olla nykyisin hakuehtona, mutta uusia vastaavaan käyttötarkoitukseen käytettäviä protokollia kehitetään alituiseen eikä niistä välttämättä ole tarkempaa tietoa ennen kuin protokollaa käyttää laaja käyttäjäjoukko. Etenkin

valtiolliset toimijat pyrkivät kehittämään viestintäänsä niin, ettei käytettävä teknologia tule laajan käyttäjäjoukon käytettäväksi.

Momentissa tarkoitetun määrittämisen tarkoituksena olisi löytää esimerkiksi edellä kuvattuja uusia protokollia ja muita hakuehtoina käytettäviä tietoja, joilla tietoliikennetiedustelu voitaisiin kohdistaa sotilastiedustelun kohteeseen ja vain välttämättömään tietoon.

Toimivaltuuden kannalta ei ole merkitystä sillä, onko tietoliikenne salattu. Myös salattu tietoliikenne kulkee tietoliikenteessä bitti- ja tavuvirtana, jonka toistuvaiskuvioita tulkitsemalla voidaan määrittää uusia hakuehtoja. Tavuvirtaa tutkittaessa pyritään muodostamaan merkityksiä, joiden avulla voidaan havaita tiedustelun näkökulmasta hyödynnettävissä olevaa tietoa. Vaikka liikenne on salattua, se ei sulje pois merkityksien muodostamista.

Toimivaltuus ei koske viestin sisältöä eli viestin semanttisen merkityssisällön selvittämistä, vaan tietoa haetaan esimerkiksi niin kutsutussa hyötykuormassa havaittavissa olevista ominaispiirteistä.

Hakuehtojen määrittämisessä pyritään myös tunnistamaan tietoliikenteen säännönmukaisuuden tai ominaispiirteen mukaisesta tietoliikenteestä esimerkiksi se, miten lähettäjä ja vastaanottaja näkyvät esimerkiksi tunnistetussa uudessa protokollassa.

Uusien hakuehtojen määrittämisen myötä hakuehdoista pystyttäisiin kehittämään tarkempia ja tätä kautta myös puututtaisiin vähemmän tiedustelun kannalta tarpeettomaan tietoliikenteeseen ja sen sisältöön. Lisäksi tietoliikennetiedustelun voidaan arvioida olevan tehokkaampaa, koska kohteen tietoliikenteestä voitaisiin hankkia tietoa aiempaa saumattomammin.

Pykälän 2 momentin mukaan hakuehtojen määrittämisessä ei saisi hyödyntää viestin merkityssisällössä olevia tietoja. Säännöksellä suojattaisiin viestin merkityksellistä sisältöä eikä sen selvittäminen ole muutenkaan toimivaltuuden tarkoituksena. Lisäksi säännöksen toimivaltuudella ei voitaisi selvittää tietyn henkilön toimintaa. Kuten 1 momentissa todetaan, hakuehtojen määrittämisessä on kyse nimenomaan tiedustelun kohteen tietoliikenteeseen osuvien hakuehtojen määrittämisestä, ei kohteen viestinnän tai muun, esimerkiksi yksityiselämän, selvittämisestä. Viestinnän selvittämisessä on kyse lain 68 ja 70 §:ssä tarkoitetun toimivaltuuden käyttämisestä.

Osaltaan viestin merkityssisältöön puuttumista estäisi se, että aiemmin tässä esityksessä esiin tuodusti tietoliikenne koostuu tietoliikennepaketeista. Näin ollen yksittäisessä paketissa oleva viestin merkityksellinen sisältö jää usein vähäiseksi; yksittäisestä tietoliikennepaketista ei ole käytännössä koskaan mahdollista selvittää järkevää kielellistä merkitystä, jollei tietoliikennepaketteja yhdistetä riittävään moneen muuhun samaan viestintätapahtumaan liittyvään tietoliikennepakettiin.

Vaikka sinänsä hankittavat tiedot voivat olla henkilötietoja, pelkästään tämän tiedon ei voida katsoa olevan merkittävää puuttumista henkilön yksityisyyteen. Esimerkiksi IP-osoite rajaa internetverkkoon yhteydessä olevan laitteen tiettyyn laitteeseen, mutta se ei itsessään kerro laitteen käyttäjästä vielä yhtään mitään. Vastaavasti käytettävät protokollat tai niiden joukko ei vielä itsessään kerro mitään viestinnän sisällöstä tai protokollien käyttäjästä muuta, kuin että kyseinen käyttäjä käyttää näitä protokollia. Se, että tiedetään tietyn toimijan käyttävän tiettyjä protokollia viestinnässään, edellyttää jo muuta tiedustelutietoa kuin hakuehtojen määrittämisessä syntyvää tietoa.

Momentissa säädettäisiin lisäksi nimenomaisesti, ettei hakuehtojen määrittämisen tuloksena saa syntyä viestin sisältöä kuvaavaa tietoa taikka tietoa, josta voidaan tehdä henkilön yksityiselämää koskevia päätelmiä. Näin ollen lopputuloksessa ei saisi näkyä esimerkiksi se, sisälsikö jokin viesti liitetiedoston tai mikä oli viestin semanttinen sisältö. Lisäksi lopputuloksessa ei saisi näkyä se, kuka viesti kenen kanssa ja milloin. Toimivaltuudessa on kyse nimenomaisesti siitä, että pystytään tunnistamaan kohteeseen liittyviä teknisiä määritteitä ja kohteen tietoliikenteen teknistä kehikkoa, johon lisättävillä tarkemmilla tiedoilla varsinainen tietoliikennetiedustelu kohdistuu välttämättömään.

Pykälän 3 momentissa säädettäisiin hakuehtojen määrittämisessä käytettävän tietoliikenteen määrästä. Hakuehtojen määrittäminen voisi kohdistua Suomen rajan ylittävään viestintäverkon osaan. Kerättävän tietoliikenteen määrä, josta hakuehtoja voitaisiin määrittää, ei saisi ylittää 5 prosenttia kohteena olevan viestintäverkon osan kapasiteetista. Kapasiteetilla viitattaisiin viestintäverkon osan tekniseen maksimikapasiteettiin. Hakuehtojen määrittämisessä tietoliikenteen määrää olisi siis rajattu fyysisesti tiettyyn Suomen rajan ylittävään viestintäverkon osaan sekä teknisesti tiettyyn määrään viestintäverkon osassa liikkuvasta tietoliikenteestä. Jos Suomen rajan ylittävän viestintäverkon osan tekninen kapasiteetti olisi 100 per sekunti, hakuehtoja voitaisiin määrittää 5 per sekunti osasta tietoliikennettä.

Käytännössä hakuehtojen määrittämisessä käytettävä tietojärjestelmän tekniset määritteet rajaisivat tiedon keruun tiettyyn datamäärään per sekunti, ei prosenttiosuuteen. Näin ollen, jos kohteen olevan viestintäverkon osan kapasiteetti kasvaisi yllättäen, toimivaltuuden kohteeksi joutuisi edelleen aiemmin määritetty datamäärä, mikä olisi siis matalampi kuin 5 prosenttia. Käytännössä, jos viestintäverkon osan tekninen kapasiteetti kasvaisi, edellyttäisi se teknisiä muutostöitä viestintäverkossa, mikä pystyttäisiin havaitsemaan toimivaltuuden käytön aikana.

Erona edellä 66 §:ssä säädettävään teknisten tietojen käsittelyyn on se, että teknisiä tietoja voidaan kerätä ja tallentaa koko viestintäverkon osan tietoliikenteestä. Tallennettavien teknisten tietojen yhteismäärä ei saa ylittää viittä prosenttia Suomen rajan ylittävän viestintäverkon osan teknisestä kapasiteetista.

Nyt käsiteltävässä hakuehtojen määrittämisessä toimivaltuuden kohteena voi olla 5 prosenttia Suomen rajan ylittävän viestintäverkon osan teknisestä kapasiteetista ja käsittelyyn päätyvä 5 prosenttia tietoliikennettä voidaan myös tallentaa. Eli, jos viestintäverkon osan tekninen kapasiteetti on 100 per sekunti, niin uusia hakuehtoja voidaan määrittää tietoliikenteen määrästä, mikä vastaa 5 per sekunti. Näin ollen tallennukseen voi mennä 5 per sekunti kohteena olevan viestintäverkon osan tietoliikennettä, josta on myös määritetty uusia hakuehtoja.

Toimivaltuuden nojalla hankittavat tiedot olisivat viestin merkityssisällön ulkopuolisia tietoja eikä sillä voitaisi näin ollen puuttua merkittävästi yksityiselämän suojaan. Hankittavien tietojen perusteella ei voitaisi tunnistaa yksittäisiä henkilöitä eikä niitä voitaisi säännöksen toimivaltuuden käytöllä yhdistellä tavalla, joista pystyttäisiin tunnistamaan yksittäinen henkilö. Edellä todettu olisi myös jo tarkoitussidonnaisuuden vastaista.

Pykälän 4 momentissa säädettäisiin hakuehtojen määrittämisessä käytettävien tietojen tallennusajasta. Säännöksen mukaan kerätty ja tallennettu tietoliikenne olisi hävitettävä viimeistään 12 kuukauden kuluttua keräyshetkestä. Näin ollen tallennettu tietoliikenne hävitettäisiin sekunnin tarkkuudella 12 kuukauden kuluttua sen tallentamisesta.

Säilytettävien tietojen rajaus ei luonnollisestikaan koskisi määritettyjä hakuehtoja, vaan määritettyjä hakuehtoja voitaisiin käyttää niin pitkään kuin niillä pystyttäisiin hankkimaan kohteesta tietoa varsinaisessa tietoliikennetiedustelussa.

Hakuehtojen määrittämisessä historiatiedolla on hakuehdon tarkkuuden kannalta merkittävä rooli. Uusien hakuehtojen määrittämisen prosessissa havaittuja mahdollisia uusia hakuehtoja ja sen tarkkuutta voidaan arvioida vertaamalla sitä aiemmin kerättyyn tietoliikenteeseen. Säännöksessä tarkoitettua säilytysaikaa voidaan pitää riittävänä edellä tarkoitettujen tavoitteiden saavuttamiseksi.

On myös edelleen korostettava, että pykälässä tarkoitetussa toiminnassa ei ole tarkoitus hankkia tietoa viestin merkityssisällöstä tai seurata kohteena olevan toimijan liikkeitä, vaan kyse on nimenomaan kohteeseen liittyvien mahdollisimman tarkkojen hakuehtojen määrittämisestä. Jos edellä tarkoitetusti toimittaisiin, kyseessä olisi varsinainen tietoliikennetiedustelu, johon olisi hankittava laissa tarkoitettu lupa.

Esimerkiksi aiemmin tässä esityksessä esimerkkinä käytettyä protokollapinoa voitaisiin verrata aiemmin 12 kuukauden aikana saatuihin tietoihin ja tätä kautta varmistua siitä, että hakuehdoksi määritetty protokollapino kohdistuu oikeaan kohteeseen. Tallennusaikaa voidaan pitää välttämättömänä ja kohtuullisena ottaen huomioon tietoliikenteen alati muuttuvan luonteen sekä teknologian ja menetelmien kehittyminen.

On huomattava, että sotilastiedusteluviranomainen ei voi käyttää tässä tarkoitettuja tietoja muussa yhteydessä, ellei tuomioistuin ole myöntänyt lupaa sellaiselle toimivaltuudelle, jolla tässä tarkoitettuja tallennettuja tietoja saisi käyttää. Näin ollen sotilastiedusteluviranomainen ei voi selvittää esimerkiksi tiettyä välitystietoa käyttäneen henkilöllisyyttä sotilastiedustelusta annetun lain 104 §:n avulla tai viestin sisältöä, ellei tietoa ole saatu varsinaisella tietoliikennetiedustelulla (lain 68 ja 70 §). Näin ollen muu tieto, kuin tuomioistuimen luvan mukaisia hakuehtoja vastaava tieto ei joutuisi tiedonhankinnan kohteeksi.

Tietoliikenteen tallentaminen ja siihen pääsy edellyttävät uutta tietojärjestelmää, johon tallennettuihin tietoihin pääsy edellyttää tuomioistuimen lupaa. Tietojen käyttö on tarkkaan kirjattava ja sitä on tarkasti valvottava niin sisäisesti kuin ulkoisesti.

Momentin mukaan tallennettuja tietoja voisi käyttää pykälän 1 momentissa tarkoitetussa hakuehtojen määrittämisessä, mutta myös jäljempänä säädettyyn tarkoitukseen. Viimeksi mainitulla viitattaisiin lain 68 ja 70 §:ssä säädettyyn varsinaiseen tietoliikennetiedusteluun.

Pykälän 5 momentin mukaan hakuehtojen määrittämisessä voitaisiin käyttää 66 §:n 3 momentissa tarkoitettuja tallennettuja tietoliikenteen teknisiä tietoja. Käytännössä kyse olisi tietojen vertailusta ja käyttökelpoisen hakuehdon muodostamisesta sekä tunnistetun hakuehdon vertaamisesta tekniseen historiatietoon.

67 b §. *Hakuehtojen määrittämisestä päättäminen.* Pykälän 1 momentin mukaan päätöksen hakuehtojen määrittämisestä tekisi tuomioistuin tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta. Päätöksenteko vastaisi sitä, mitä teknisten tietojen käsittelystä on jo nykyisin säädetty. Uudessa toimivaltuudessa olisi kyse tietoliikenteen käsittelystä sen teknisemmässä muodossa, joten uutta toimivaltuutta koskeva päätöksentekokin vastaisi teknisten tietojen käsittelystä säädettyä päätöksentekoa.

Pykälän 2 momentissa säädettäisiin luvan voimassaoloajaksi enintään kuusi kuukautta luvan antopäivästä tai päätöksen tekopäivästä alkaen.

Säännöksen mukaan lupa voisi koskea myös todettua luvan antopäivää tai päätöksen tekoa edeltävää aikaa, joka voisi olla kuutta kuukautta pidempi. Käytännössä tämä tarkoittaisi

tilannetta, jossa käytettäisiin hakuehtojen määrittämisessä ehdotetun 66 §:n 2 momentissa tarkoitettuja tallennettuja teknisiä tietoja tai 67 a §:n 4 momentissa tarkoitettuja tietoja.

Pykälän 3 momentissa olisi säädetty vaatimuksessa ja päätöksessä mainittavat seikat. Momentin 1 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava tiedustelutehtävä, jota varten hakuehtoja määritetään ja sitä koskevat tosiseikat. Tiedustelutehtävällä tarkoitetaan lain 10 §:n mukaan pääesikunnan tiedustelupäällikön sotilastiedusteluviranomaiselle antamaa toimeksiantoa tiedustelutiedon hankkimiseksi 4 §:ssä tarkoitetusta sotilastiedustelun kohteesta, joka perustuu ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteisen kokouksen valmistelevasti käsittelemiin painopisteisiin tai 14 §:ssä tarkoitettuun tietopyyntöön. Tiedustelutehtävän kuvauksessa yksilöitäisiin suurempi kokonaisuus, jota koskevia hakuehtoja olisi määritettävä tietoliikennetiedustelun tarkoituksenmukaiseksi käyttämiseksi.

Momentin 2 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava tosiseikat siitä, mihin hakuehtojen määrittämisen välttämättömyys perustuisi. Tosiseikkoina voitaisiin mainita esimerkiksi se, että saatujen havaintojen perusteella käytettävät hakuehdot eivät enää tuota vastaavanlaista tietoa, mitä niillä on aiemmin saatu, mutta kuitenkin saatujen kokemusten nojalla voidaan todeta, että viestintä todennäköisesti toteutetaan toisella tavalla eikä käytössä olevilla hakuehdoilla viestintään päästä käsiksi.

Toisaalta vaatimuksessa ja päätöksessä olisi tehtävä selkoa siitä, miksi hakuehtoja ei voida määrittää esimerkiksi varsinaista tietoliikennetiedustelua käyttäen. Vaatimuksessa voitaisiin myös esittää arvio siitä, päästäisiinkö hakuehtojen määrittämisellä parempaan ja kohdennetumpaan tietoliikennetiedusteluun.

Momentin 3 kohdan mukaan vaatimuksessa ja päätöksessä on mainittava kohteen tietoliikenteen oletettu säännönmukaisuus tai ominaispiirre, jonka perusteella hakuehtoja määritetään ja perustelut sille.

Tämän esityksen yleisperusteluissa on käsitelty tietojärjestelmien tuottamaa tietoliikennevirtaa tarkemmin. Tietojärjestelmissä käytetään useita eri ohjelmia tuottamaan tietojärjestelmän yksittäisiä ja yhteisiä toiminnallisuuksia. Etenkin hajautetuissa tietojärjestelmissä tietojärjestelmän toiminta edellyttää fyysisesti eri paikoissa olevien laitteistojen välistä viestintää, jotta tietojärjestelmä kokonaisuudessaan toimii halutulla tavalla.

Jotta sähköinen viestintä ohjautuisi haluttuun määränpäähän tarkoitetulla tavalla, vaatii tietoliikenne säännöstöjä, eli protokollia. Protokollat muun muassa pilkkovat tiedoston tiettyyn muotoon ja salaavat tietoliikenteen tietyllä tavalla. Tämä näkyy tietoliikennevirrassa tiettynä säännönmukaisuutena tai ominaispiirteenä. Säännönmukaisuuksia ja ominaispiirteitä voidaan tunnistaa esimerkiksi protokollapinossa käytettävän yksittäisen protokollan toiminnan ominaispiirteestä, mutta varsinaista hakuehtoa ei voida kohdistaa tämän perusteella.

Jo pelkästään edellä kuvatut tietojärjestelmän toimintaan keskeisesti vaikuttavat seikat tuottavat tietojärjestelmän tietoliikenteeseen säännönmukaisuuksia ja ominaispiirteitä. Kohdan mukainen säännönmukaisuus tai ominaispiirre voi olla tiedossa jo kohteena olevasta tietojärjestelmästä, mutta tiedossa on, että vastaavaa tietojärjestelmää käyttää myös esimerkiksi toinen valtion viranomainen tai tietoa olisi hankittava pääjärjestelmän alajärjestelmästä, joka järjestelmien yhteen toimivuuden vuoksi käyttää ainakin pitkälti vastaavia protokollia ja tekniikoita kuin itse pääjärjestelmä. Tässä vaiheessa ei kuitenkaan ole vielä tiedossa se, miten esimerkiksi viestin lähettäjä ja vastaanottaja määrittyvät tietojärjestelmässä, mistä syystä tarkempaa hakuehtoa ei voida määrittää vielä tässä vaiheessa.

Toisaalta säännönmukaisuus voi olla peräisin myös reaalimaailmasta. Tiedossa voi olla esimerkiksi, että tietyllä alueella järjestetään sotilaallinen harjoitus ja harjoituksessa tiettynä ajankohtana lähetetään viestejä. Jos tarkempia hakuehtoja ei ole tiedossa, uusien hakuehtoja voitaisiin määrittää harjoitusalueen tietoliikenteestä.

Ominaispiirrettä vastaavan tietoliikenteen löytäminen edellyttää usein manuaalista työtä, jotta säännönmukaisuutta tai ominaispiirrettä vastaava tietoliikenne löydetään. Tietoliikenteen tavuvirrasta hakuehtojen määrittäminen ei edellytä tietoliikenteen purkamista muotoon, josta ilman merkittävää tietoteknistä osaamista oleva henkilö voisi selvittää viestin sisällön.

Momentin 4 kohdan mukaan vaatimuksessa ja päätöksessä olisi ilmoitettava ne Suomen rajan ylittävät viestintäverkon osat, kuten kaapeleiden kuidut, joihin tietoliikennetiedustelua hakuehtojen määrittämiseksi kohdennettaisiin.

Momentin 5 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava suunnitelma hakuehtojen määrittämisestä. Suunnitelmassa olisi tehtävä tarkemmin selkoa esimerkiksi siitä, että miten hakuehtojen määrittäminen toteutettaisiin ja minkälaisin keinoin. Suunnitelmassa olisi myös kuvattava sitä, miten tarkempaan käsittelyyn päätyisi mahdollisimman vähän viestinnän merkityksellistä sisältöä ja miten yksityisyyden suojasta huolehditaan mahdollisimman pitkälle.

Momentin 6 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava luvan voimassaoloaika kellonajan tarkkuudella ja 7 kohdan mukaan olisi mainittava toimintaa johtava ja valvova Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies.

Momentin 8 kohdan mukaan tuomioistuin voisi asettaa päätöksessään tietoliikennetiedustelulle rajoituksia ja ehtoja. Jos tällaisia rajoituksia ja ehtoja olisi tiedossa jo vaatimusta laadittaessa, niin ne olisi syytä kirjata jo vaatimukseen. Rajoituksia ja ehtoja voitaisiin asettaa esimerkiksi sille, kuinka Puolustusvoimien tiedustelulaitos saa muodostaa hakuehtoja niiden hakuehtojen luokkien puitteissa, joihin tuomioistuin myöntää luvan tai miten paljon Puolustusvoimien tiedustelulaitos voi tallentaa tietoliikennettä.

68 §. *Valtiolliseen toimijaan kohdistuva tietoliikennetiedustelu.* Pykälää ja sen otsikkoa muutettaisiin siten, että pykälässä ei viitattaisi valtiollisen toimijan tietoliikenteeseen, vaan valtiolliseen toimijaan kohdistuvaan tietoliikennetiedusteluun. Käytäntö on osoittanut, että valtiollisen toimijan tietoliikenne ei liiku tietyissä valikoiduissa kuiduissa, vaan muun tietoliikenteen seassa. Ehdotettu uusi muotoilu vastaisi paremmin nykytilaa tietoliikenteen liikkumisesta.

Valtiolliseen toimijaan kohdistuva tietoliikennetiedustelu voisi perustua edelleen hakuehtojen käyttöön.

Pykälän 2 momenttia ei muutettaisi. Säännöksen mukaan Puolustusvoimien tiedustelulaitos voi käsitellä tietoliikenteestä hankittua tietoa automaattisesti ja manuaalisesti.

Pykälän 3 momenttia muutettaisiin. Muutoksen myötä poistettaisiin täydellinen kielto käyttää Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja hakuehtona. Poiston voidaan katsoa olevan välttämätön, sillä valtiollinen toimija voi olla myös Suomessa tai saapua kesken tiedonhankinnan Suomeen. Etenkin tilanteessa, jossa valtiollinen toimija on ollut Suomen rajan

ulkopuolella ja saapuu ehkä jopa yllättäen Suomeen, olisi valtiolliseen toimijaan kohdistuvaa tietoliikennetiedustelua pystyttävä jatkamaan.

Säännös ei mahdollistaisi esimerkiksi telekuuntelua koskevan sääntelyn kiertämistä Säännöksen soveltamisen kannalta keskeistä on se, että kohteeseen olisi mahdollisimman pian kohdistettava muita tiedustelumenetelmiä, kuten telekuuntelua. Tähän ohjaavat jo sotilastiedustelun yleiset periaatteet, kuten suhteellisuusperiaate. Lisäksi esimerkiksi telekuuntelulla saadaan joka tapauksessa enemmän ja tarkempaa tietoa kohteen viestinnästä kuin tietoliikennetiedustelulla. Kohteeseen pyrittäisiinkin kohdentamaan muita tiedustelumenetelmiä mahdollisimman pian kohteen tarkemman olinpaikan selvittyä. Tätä periaatetta ilmennettäisiin säännöksessä viittauksella tilapäisyyteen.

Esimerkiksi tilanteessa, jossa vieraan valtion asevoimien erikoisjoukko on valtiollisen toimijan tietoliikennetiedustelun kohteena ja joukko saapuu todelliset tarkoitusperät peittäen Suomeen, tarkemman tiedon saaminen joukosta edellyttää kohdennetumpien tiedustelumenetelmien käyttöä. Tietoliikennetiedustelulla voitaisiin saada ensi vaiheessa merkittävää tietoa kohdennetumpien tiedustelumenetelmien käytölle Suomessa.

Pykälän uuden 4 momentin mukaan pykälässä tarkoitetussa tiedonhankinnassa voitaisiin käyttää 66 §:n 3 momentissa tarkoitettuja tallennettuja tietoliikenteen teknisiä tietoja ja 67 a §:n 3 momentissa tarkoitettua tallennettua tietoliikennettä. Muutoksen myötä kohteesta saataisiin aiempaa tarkempaa tietoa ja tiedustelumenetelmää pystyttäisiin kohdentamaan edelleen aiempaa tarkemmin. Tietojen käyttö edellyttäisi 69 §:n mukaista lupaa, jossa olisi määritetty hakuehdot, joita vastaavia tietoja voitaisiin hakea tallennetuista tiedoista.

69 §. *Valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta päättäminen.* Pykälän 2 momenttia muutettaisiin. Luvan voimassaoloaika olisi edelleen voimassa olevan lain mukaisesti kuusi kuukautta, mutta ajanjakso alkaisi luvan antopäivästä tai päätöksen tekopäivästä alkaen.

Säännöksen mukaan lupa voisi koskea myös tietoja, jotka on tallennettu ehdotetun 66 §:n 3 momentin ja 67 a §:n 3 momentin perusteella.

70 §. *Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu.* Pykälän 2 momenttia muutettaisiin. Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta poistettaisiin ehdoton kielto käyttää Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja (voimassa olevan pykälän 2 momentti). Kiellon poistamisen myötä myös Suomessa oleskeleva sotilaalliseen tai kansalliselle turvallisuudelle vakavaan uhkaan osallistuva henkilö voisi tilapäisesti olla tietoliikennetiedustelun kohteena.

Tiedustelun kohteena on toiminta, johon voi myös olennaisesti liittyä Suomessa oleskelevat henkilöt. Etenkin tilanteessa, jossa sotilaalliseen tai kansallista turvallisuutta vakavasti uhkaavaan toimintaan liittyvä henkilö saapuu yllättäen Suomeen tietoliikennetiedustelun käytön aikana, voi aluksi olla tarve jatkaa tietoliikennetiedustelua, kunnes voidaan siirtyä käyttämään kohdennetumpia tiedustelumenetelmiä, kuten telekuuntelua. Kohdennetumpiin tiedustelumenetelmiin siirtymistä edellyttää jo pykälän 1 momentissa todettu muun kuin valtiollisen toimija tietoliikenteeseen kohdistuvan tiedustelun viimesijaisuus, jota on arvioitava myös tietoliikennetiedustelun käytön aikana. Toisaalta esimerkiksi tilanteessa, jossa vieraan valtion asevoimien henkilöstöä tai tiedusteluviranomaisia on soluttautunut Suomeen, tietoliikennetiedustelulla voitaisiin havaita tämä, jos henkilö olisi yhteydessä rajan yli toimeksiantajaansa. Tämän jälkeen Suomessa olevaa telepäätelaitetta tai teleosoitetta voitaisiin

seurata tietoliikennetiedustelulla, kunnes tarkemmin kohdennettuja tiedustelumenetelmiä pystyttäisiin käyttämään.

Suomen sisäiseksi tietoliikenteeksi katsottavan tietoliikennetiedustelun kielto säilyisi muuttumattomana.

Pykälän 3 momentti muutettaisiin. Momentin mukaan muun kuin valtiollisen toimijan tietoliikenteen tiedustelussa voitaisiin käyttää myös viestin sisältöön kohdistuvia hakuehtoja.

Hakuehdon määritelmän (10 §:n 1 kohta) mukaan hakuehdolla tarkoitetaan tietoa, jonka perusteella tietoliikennetiedustelulla viestintäverkon osasta mahdollisimman rajatusti ja täsmällisesti valitaan tietoliikennetiedustelun kohteena oleva tietoliikenne ja puuttuminen luottamuksellisen viestin salaisuuden suojaan rajautuu tiedustelun tarkoituksen kannalta välttämättömään. Nykytilassa pelkästään esimerkiksi tietoliikenteen teknisten tietojen käyttämisen voidaan katsoa tuottavan usein liian laajoja hakutuloksia; hankittuja tietoja voitaisiin jo ensivaiheessa rajata semanttisessa sisällössä olevan hakuehdon avulla.

Hakuehto, joka voisi kohdistua myös viestin semanttiseen sisältöön, voidaan arvioida johtavan tarkempaan tiedon hankintaan tietoliikenteestä. Tämä parantaisi yksityisyyden suojaa tarkemman ja kohdennetumman tiedonhankinnan myötä sekä vastaisi paremmin lain määritelmää hakuehdosta. Selvänä voidaan pitää sitä, että pelkän puhutun kielen ilmaisun käyttö hakuehtona tuottaisi useimmiten vieläkin laajempia tuloksia, mitä ei voida pitää myöskään operatiiviselta kannalta järkevänä. Kielellisiä hakuehtoja, kuten puhutun kielen ilmaisuja, käytettäisiinkin yhdessä tietoliikenteen teknisten tietojen kanssa mahdollisimman kohdennetun tiedon hankkimiseksi.

Viestin sisältöön menevien hakuehtojen kiellon poistolla on myös operatiivinen merkitys. Nykytilassa hakuehtona voidaan käyttää tietoliikenteen teknisiä tietoja. Tekninen tieto voi olla myös viestin sisällössä, esimerkiksi edelleen lähetettyjen sähköpostiviestien ketjussa. Nykytilassa teknisen hakuehdon voidaan katsoa kohdistuvan sinänsä oikein erottelemalla tietoliikennevirrasta hakuehtoa vastaavaa tietoliikennettä, mutta erottelua ei voida tehdä sen välillä, onko hakuehto viestin semanttisessa sisällössä vai ei. Tämän takia tiedusteluviranomainen perehdyttyään hakuehtoa vastaavaan tietoliikenteeseen joutuu hävittämisvelvollisuuksien nojalla poistamaan tiedon, jossa hakuehto esiintyy, mutta hakuehtoa vastaava tieto on viestin sisällössä, esimerkiksi edelleen lähetetyssä sähköpostiviestissä. Hakuehtoa vastaava tieto voi olla myös tietoliikenteessä muutoin viestin sisällöksi katsottavissa tiedoissa, kuten pilvipalvelimeen tallennettavassa yhteystietoluettelossa.

Nyt ehdotetun muutoksen myötä jatkokäsittelyyn päätyvää tietoa voitaisiin karsia jo hakuehtojen käytön vaiheessa, jolloin tiettyjä esimerkiksi puhutun kielen ilmaisuja käyttämällä hankittava tietomäärä olisi jo lähtökohtaisesti suppeampaa ja paremmin kohdistetumpaa. Näin ollen nykytilassa osa hakuehtojen mukaisesta tietoliikenteen jatkokäsittelystä siirtyisi osaksi vaihetta, jossa tietoliikenteestä suodatetaan hakuehtojen avulla tietoliikennettä. Näin ollen sotilastiedusteluviranomaisen jatkokäsittelyyn päätyy aiempaa vähemmän tietoa.

Semanttisessa sisällössä olevien tietojen käyttö hakuehtona olisi perusteltava tuomioistuimelle tehtävässä hakemuksessa 71 §:n 3 momentin 5 kohdan mukaisesti. Perustelussa voitaisiin tuoda esiin esimerkiksi se, minkälaisia havaintoja kohteen tietoliikenteestä on tehty aiemmin, esimerkiksi käyttääkö kohde joitain tiettyjä sanoja tai sanontoja taikka erityistä kieltä viestiessään toiminnassaan.

Pykälän 4 momentti pysyisi vastaavana kuin nykytilassa.

Pykälän 5 momentti olisi uusi. Sen mukaan muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvassa tiedustelussa voitaisiin käyttää myös 66 §:n 3 momentissa tarkoitettuja teknisiä tietoja sekä 67 a §:n 3 momentin nojalla hakuehtojen määrittämisessä käytettyä tietoliikennettä. Jotta tietoja voitaisiin käyttää, edellyttäisi tämä 71 §:ssä säädettyä lupaa. Tallennettujen tietojen käyttö perustuisi luvassa todettujen hakuehtojen käyttämiseen.

71 §. *Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta päättäminen.* Pykälän 2 momenttia muutettaisiin. Luvan voimassaoloaika olisi edelleen voimassa olevan lain mukaisesti kuusi kuukautta, mutta ajanjakso alkaisi luvan antopäivästä tai päätöksen tekopäivästä alkaen.

Säännöksen mukaan lupa voisi koskea myös todettua luvan antopäivää tai päätöksen tekoa edeltävää aikaa, joka voisi olla kuutta kuukautta pidempi. Käytännössä tämä tarkoittaisi tilannetta, jossa käytettäisiin tietoliikenteen tiedustelussa ehdotetun 66 §:n 3 momentin ja 67 a §:n 3 momentin perusteella tallennettuja tietoja.

74 §. *Haitallista tietokoneohjelmaa koskevien tietojen luovuttaminen yrityksille ja yhteisöille.* Pykälä kumottaisiin tarpeettomana. Haitallista tietokoneohjelmaa koskevien tietojen luovuttaminen olisi mahdollista 18 §:n 2 momenttiin ehdotetun muutoksen perusteella.

77 §. *Tiedustelumenetelmää käyttävän virkamiehen turvaaminen.* Pykälän 1 momentissa säädetään tiedustelumenetelmää käyttävän virkamiehen turvaamisesta. Turvaaminen voi tapahtua asentamalla varustamalla säännöksessä mainittuja tiedustelumenetelmiä käyttävä virkamies kuuntelu tai katselun mahdollistavilla laitteilla. Säännös koskee siis virkamiehen päällä olevia laitteita.

Edellä todetun lisäksi virkamiehen turvaaminen voisi tapahtua myös asentamalla kuuntelun ja katselun mahdollistava laite virkamiehen käyttämään tilaan. Tämä osaltaan laskisi virkamiehen paljastumisen riskiä, koska vaatteissa olevat laitteet saattavat tietyissä tilanteissa paljastua verraten helpostikin. Lisäksi tilassa olevat laitteet mahdollistavat laajemman tilannekuvan saamisen itse tilanteesta, koska tilaa voidaan valvoa kokonaisvaltaisemmin. Näin ollen esimerkiksi voidaan varmistua siitä, ettei tiedustelumenetelmää käyttävän virkamiehen selän takaa hyökätä virkamiehen kimppuun.

Pykälän 2 momenttiin ei tehtäisi muutoksia. Kuuntelu ja katselu saataisiin tallentaa, mutta tallenteet on hävitettävä heti sen jälkeen, kun niitä ei tarvita virkamiehen turvaamiseen. Jos niitä on kuitenkin tarpeen säilyttää asiaan osallisen oikeusturvaan liittyvistä syistä, tallenteet saadaan säilyttää ja niitä saadaan käyttää tässä tarkoituksessa. Tällöin tallenteet on hävitettävä, kun asia on lainvoimaisesti ratkaistu tai jätetty sillensä.

Selvää on se, ettei pykälä mahdollista tiedustelumenetelmiä koskevien säännösten kiertämistä.

78 a §. *Tietolähteen hengen ja terveyden turvaaminen.* Pykälä olisi uusi. Siihen siirrettäisiin voimassa olevan lain 78 §:n 5 momentti, jonka mukaan pääesikunnan tiedustelupäällikön päätöksellä tietolähteelle voitaisiin antaa yksittäistapauksessa muun muassa käytettäväksi vääriä asiakirjoja, jos se on välttämätöntä tietolähteen hengen ja terveyden suojaamiseksi. Tältä oikeustilaa ei olisi tarkoitus muuttaa.

Säännös koskisi tilanteita, joissa mainittuja tietoja ja asiakirjoja käytettäisiin tietolähteen hengen ja terveyden suojaamiseksi muussa tilanteessa kuin tietolähteen tuomiseksi Suomeen.

Pykälän 2 momentti olisi uutta sääntelyä. Lakiin lisättäisiin säännöstä, jonka myötä sotilastiedusteluviranomaisella olisi myös mahdollisuus järjestää tietolähde muulla tavalla Suomen rajan yli. Kyse ei olisi kaikissa tapauksissa normaalista rajaylityspaikan kautta tapahtuvasta maahantulosta, vaan tarvittaessa tietolähteen saapumisesta Suomeen vaivihkaisesti. Säännös kattaisi myös tilanteet, joissa tietolähde järjestettäisiin Suomeen käyttämällä 1 momentissa tarkoitettuja vääriä tietoja ja asiakirjoja.

Rikoslain 17 luvun 8 §:ssä säädetään laittoman maahantulon järjestämisestä. Esimerkiksi pykälän 1 momentin 2 kohdan mukaan laittoman maahantulon järjestämisestä on tuomittava henkilö, joka tuo tai yrittää tuoda Suomeen tai Suomen kautta muuhun maahan ulkomaalaisen, jonka maahantuloasiakirja on väärä, väärennetty, myönnetty toiselle henkilölle taikka saatu viranomaiselta asiakirjan myöntämisen kannalta merkityksellisen totuudenvastaisen tai harhaanjohtavan tiedon avulla, lahjomalla viranomainen tai virkamiehen väkivaltaisella vastustamisella. Viittaus rikoslain pykälään selkeyttäisi myös sääntelyä säännöksessä jo nykyisin säädettyjen väärien asiakirjojen ja tietojen käytön osalta. Ehdotettu viittaus poistaisi selkeästi rikosoikeudellisen vastuun säännöksen tarkoittamissa tilanteissa.

Nyt käsiteltävänä olevassa säännösehdotuksessa tarkoitetulla järjestämisellä tarkoitettaisiin sitä, mitä rikoslain 17 luvun 8 §:ssä tarkoitetaan. Näin ollen sotilastiedusteluviranomainen voisi esimerkiksi 1) tuoda Suomeen tai Suomen kautta muuhun maahan ulkomaalaisen, jolla ei ole maahantuloon vaadittavaa matkustusasiakirjaa, viisumia, oleskelulupaa tai matkustusasiakirjaa rinnastettavaa muuta asiakirjaa, 2) tuoda Suomeen tai Suomen kautta muuhun maahan ulkomaalaisen, jonka maahantuloasiakirja on väärä, väärennetty tai myönnetty toiselle henkilölle tai 3) järjestää tai välittää edellä tarkoitetulle ulkomaalaiselle kuljetuksen Suomeen.

Lähtökohtaisesti sotilastiedusteluviranomaisen on mahdollisuuksiensa mukaan pyrittävä suojaamaan tietolähdettä. Normaalitapauksessa kyse on siitä, että tietolähdettä ei pyydetä hankkimaan tietoa tavalla, joka saattaa hänet selkeästi hengen ja terveyden vaaraan. Tilanteet saattavat kuitenkin muuttua nopeasti ja riippuen siitä, minkälaiseen tietoon tietolähteellä on pääsy, hengen ja terveyden vaarantumisen uhka voi olla todellinen.

Nyt käsiteltävänä olevassa tilanteessa esimerkiksi kohdevaltiossa korkeassa yhteiskunnallisessa asemassa oleva henkilö on jakanut merkittäviä salassa pidettäviä tietoja sotilastiedusteluviranomaiselle. Jossain vaiheessa pitkähkön yhteistyön aikana tietolähteelle syntyy vahva epäilys, että kohdevaltion viranomaset ovat ryhtyneet seuraamaan hänen toimiaan. Tilanteen tarkempi seuraaminen vahvistaa havainnon oikeaksi. Yleisesti on tiedossa, että kohdevaltion viranomaiset kiduttavat vankeja, ja oletettavaa on, että myös tässä tapauksessa tietolähdettä tultaisiin kiduttamaan jopa kuolemaan asti. Saatujen tietojen perusteella tietolähteelle valmistetaan vääriä asiakirjoja ja tehdään vääriä rekisterimerkintöjä tarvittaviin viranomaisrekistereihin. Valmistettujen asiakirjojen ja rekisterimerkintöjen avulla tietolähde pääsee Suomen rajan yli rajanylityspaikalta ja edelleen kolmanteen valtioon kyseisen valtion toimivaltaisen viranomaisen avustuksella.

Toisaalta tilanne voi olla kohdevaltiossa se, että maasta poistuminen on tarkoin valvottua. Maasta poistuminen saattaa edellyttää kohdevaltion viranomaisilta erillisiä asiakirjoja. Tilanteessa, jossa tietolähde on kohdemaassa esimerkiksi hyvin tunnettu henkilö tai ainakin viranomaisten keskuudessa hyvin tunnettu, väärennetyt asiakirjat eivät välttämättä riitä tietolähteen hengen ja terveyden suojaamiseksi. Näin ollen tietolähteen hengen ja terveyden suojaaminen saattaisi edellyttää sitä, että Suomen rajan ylittäminen tapahtuisi muualta kuin virallisen rajanylityspaikan kautta.

Tilanteessa, jossa on saatu vahvoja varmistettuja tietoja tietolähteen paljastumisesta kohdevaltion viranomaisille, sotilastiedusteluviranomainen voisi valmistella suunnitelman, jonka avulla tietolähde pääsisi Suomen rajan yli. Suunnitelmassa voitaisiin osoittaa kartasta maastoreitti, jota seuraamalla tietolähde pystyisi ylittämään Suomen maarajan. Suunnitelma voisi sisältää myös tietoja siitä, milloin maaraja on ylitettävissä niin, etteivät muut viranomaiset havaitse sitä.

Rikoslain 17 luvun 8 §:n 2 momentin mukaan laittoman maahantulon järjestämisenä ei pidetä tekoa, jota erityisesti huomioon ottaen tekijän humanitaariset tai läheisiin perhesuhteisiin liittyvät vaikuttimet sekä ulkomaalaisen turvallisuuteen vaikuttavat olot hänen kotimaassaan tai vakinaisessa asuinmaassaan on pidettävä kokonaisuutena ottaen hyväksyttävistä syistä tehtynä. Nyt käsiteltävänä olevan säännösehdotuksen tilanteissa edellä tarkoitettu rikoslain säännös tulisi varmasti sovellettavaksi, mutta sääntelyn selkeyden vuoksi nimenomainen rikoksen pois sulkemista voidaan pitää tarkoituksenmukaisena.

Soveltamisen voidaan arvioida olevan poikkeuksellista. Mahdollisuus myös poikkeavan maahantulon järjestämiseen voidaan katsoa parantavan tietolähteen luottamusta suomalaiseen sotilastiedusteluun sekä suomalaiseen yhteiskuntaan. Käytännössä myös tietolähteen on oltava erittäin luotettava ja hänen toimittamiensa tietojen on oltava merkityksellisiä, jotta säännöksen soveltaminen tulisi kyseeseen.

Säännöksen soveltamisen edellytyksenä on välttämättömyys. Välttämättömyys edellyttäisi sitä, että tietolähteen turvaamista ei voida käytännössä suorittaa muilla keinoin tai se vaatisi huomattavia resursseja. Lisäksi tietolähteen hengen ja terveyden suojaamisen tarve on voitava arvioida todelliseksi.

Arvion olisi oltava laaja-alainen ja pohjauduttava varmistettuihin tietoihin. Ylätason arvio kohdemaasta voitaisiin tehdä esimerkiksi yleisesti saatavilla olevien tietojen perusteella, kuten sen perusteella, että yleisesti on tiedossa kohdevaltion viranomaisten syyllistyvän vankien kiduttamiseen tai muuten epäinhimilliseen kohteluun. Tarkemman arvion olisi pohjauduttava varmennettuihin tietoihin esimerkiksi siitä, että tietolähteen on haivattu joutuneen paikallisten viranomaisten tarkkailun kohteeksi. Pelkkä tarkkailun havaitseminen ei useinkaan olisi välttämättä riittävää, vaan kohdevaltion viranomaisen olisi myös tehtävä muita konkreettisempia toimia, kuten kotietsintöjä tai puhuttamisia, ennen kuin välttämättömyyden voitaisiin katsoa kokonaisarvion osalta täyttyvän.

Ehdotuksessa tarkoitetut tilanteet ovat erittäin sensitiivisiä, mikä osaltaan tarkoittaa sitä, että tietoa ei voida aina jakaa muille viranomaisille. Toisaalta ehdotuksen tapaukset voivat olla myös ulko- ja turvallisuuspoliittisesti herkkiä, jolloin ulko- ja turvallisuuspoliittisella johdolla olisi oltava tarvittava tieto.

Tietolähde voisi hakea Suomesta turvapaikkaa, jolloin hän kävisi läpi normaalin turvapaikanhakijaa koskevan prosessin. Suomea voitaisiin myös käyttää kauttakulkumaana kolmanteen maahan.

Pykälän 3 momentissa säädettäisiin tietolähteen oikeudesta käyttää 1 momentissa tarkoitettuja tietoja, rekisterimerkintöjä ja asiakirjoja pykälän 2 momentissa tarkoitetuissa tilanteissa. Pykälän 2 momentissa olisi säädetty sotilastiedusteluviranomaisen oikeudesta järjestää tietolähde maahan, mutta tämä ei poista tietolähteen mahdollista rikosoikeudellista vastuuta.

Säännös koskisi etenkin tilanteita, joissa tietolähde saapuisi maahan sotilastiedusteluviranomaisen antamia ja tekemiä vääriä rekisterimerkintöjä, tietoja ja

asiakirjoja käyttämällä tai sotilastiedusteluviranomaisen avustamana muuta kuin virallista rajanylityspaikkaa käyttäen. Ensimmäisessä tilanteessa on kyse rikoslain 17 luvun 7 §:n 1 kohdassa tarkoitetusta tilanteesta, jossa tietolähde ylittää tai ryittää ylittää Suomen rajan ilman siihen oikeuttavaa matkustusasiakirjaa, viisumia, oleskelulupaa tai matkustusasiakirjaan rinnastettavaa muuta asiakirjaa. Nyt käsiteltävänä olevan säännösehdotuksen myötä tietolähde voisi käyttää rajaylityksen yhteydessä sotilastiedustelun tekemiä ja valmistamia vääriä tietoja, rekisterimerkintöjä ja asiakirjoja syyllistymättä rikokseen.

Jälkimmäisessä tapauksessa olisi kyse rikoslain 17 luvun 7 §:n 1 kohdan tarkoittamista tilanteista, joissa tietolähde ylittää tai yrittää ylittää Suomen rajan muualta kuin luvallisesta maahantulo- tai maastalähtöpaikasta. Pykälän 2 momentissa olisi säädetty sotilastiedusteluviranomaisen oikeudesta järjestää tietolähde Suomeen rikoslain 17 luvun 8 §:n estämättä. Näin ollen pykälän 2 momentin tilanteissa tietolähde ei syyllistyisi valtiorajarikokseen, kun hän ylittäisi Suomen rajan muualta kuin luvallisesta maahantulopaikasta.

Säännöksessä tarkoitetut toimet voivat täyttää myös muuta 7 §:n 1 momentissa mainitut tekomuodot; momentin 2 kohdan mukaan se, joka muuten rikkoo rajan ylittämisestä annettuja säännöksiä voi syyllistyä valtiorajarikokseen ja momentin 3 kohdan mukaan se, joka oleskelee tai liikkuu rajavyöhykkeellä tai ryhtyy siellä kiellettyyn toimeen rajavartiolain 51 §:n vastaisesti tai ilman mainitun lain 52 §:ssä edellytettyä lupaa, voi syyllistyä valtiorajarikokseen. Säännöksessä tarkoitettu tietolähde saattaa joutua odottamaan esimerkiksi sotilastiedusteluviranomaisen noutoa rajavyöhykkeellä esimerkiksi ilman rajavartiolain 52 §:ssä tarkoitettua lupaa.

Pykälässä tarkoitettu tietolähteen saapuminen Suomeen saattaa täyttää myös muun rikoksen tunnusmerkistön. Etenkin väärän asiakirjan käyttämisellä tietolähde voisi syyllistyä esimerkiksi rikoslain 16 luvun 7 §:ssä tarkoitettuun rekisterimerkintärikokseen tai rikoslain 16 luvun 5 §:ssä tarkoitettuun väärän henkilötiedon antamiseen. Edellä tarkoitettujen säännösten voidaan katsoa sisältävän sääntelyä, jonka nojalla nyt käsiteltävinä olevissa tilanteissa tietolähde ei syyllistyisi rikokseen.

82 §. *Tiedustelukiellot.* Pykälän 1 momenttiin lisättäisiin tiedustelumenetelmistä tekninen laitetarkkailu ja valtiolliseen toimijaan Suomessa kohdistuva tietojärjestelmätiedustelu. Ehdotettujen muutosten myötä 1 momentin kielto kohdistaa momentissa mainittuja tiedustelumenetelmiä erityisiin ammattiryhmiin laajenisi. Tekninen laitetarkkailu voi kohdistua myös tallennettuun viestintään ja uusi toimivaltuus, valtiolliseen toimijaan Suomessa kohdistuva tietojärjestelmätiedustelun, voi vastaavasti kohdistua viestintään.

Vastaavasti pykälän 2 momenttiin lisättäisiin edellä mainitut tiedustelumenetelmät vastaavista syistä.

85 §. *Tiedustelumenetelmän käytön keskeyttäminen.* Pykälää muutettaisiin. Jo voimassa olevassa pykälässä on säädetty kattavasti tiettyjen tiedustelumenetelmien käytön keskeyttämisestä, mutta säännöstä on tarpeen kehittää. Pykälässä on kyse lähinnä selventävästä säännöksestä; sotilastiedustelusta annettua lakia on jo nykyisellään tulkittu niin, että telekuuntelu ja televalvonta on keskeytettävä niin pian kuin mahdollista siltä osin, jos tiedonhankinta kohdistuu muuhun kohteena olevalta henkilöltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin. Kuuntelulla saatu tallenteet ja televalvonnalla saadut tiedot sekä saatuja tietoja koskevat muistiinpanot on heti hävitettävä.

Pykälän 1 momentissa säädettäisiin, että telekuuntelun tai televalvonnan kohdistuessa muuhun kuin luvan kohteena olevalta henkilöltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin taikka että teknisen kuuntelun kohteena oleva henkilö ei oleskele kuunneltavassa tilassa tai muussa paikassa, tiedustelumenetelmän käyttö on tältä osin keskeytettävä niin pian kuin mahdollista sekä tällaiset kuuntelulla saadut tallenteet ja televalvonnalla saadut tiedot sekä tällaisilla tiedustelumenetelmillä saatuja tietoja koskevat muistiinpanot on hävitettävä heti. Säännös vastaisi voimassa olevaa momentti sillä erotuksella, että siihen lisättäisiin televalvonta.

Pykälän 2 momentti koskisi radiosignaalitiedustelua. Säännös vastaisi voimassa olevan pykälän 2 momenttia. Radiosignaalitiedustelua koskevan pykälän mukaan radiosignaalitiedustelulla ei saa hankkia tietoa muun kuin valtiollisen toimijan viestin sisällöstä. Radiosignaalitiedustelun luonteen vuoksi sen kohteeksi saattaisi joutua luottamuksellisen viestin suojaa nauttivaa viestintää. Tässä käsiteltävänä olevan momentin mukaan tällainen viesti ja sitä koskevat muistiinpanot olisi hävitettävä heti. Keskeyttäminen ei tässä tapauksessa tarkoittaisi kaiken radiosignaalitiedustelun keskeyttämistä vaan radiosignaalitiedustelu olisi tältä osin kohdennettava uudelleen niin, ettei ilmi tullutta muun kuin valtiollisen toimijan viestintää enää päätyisi radiosignaalitiedustelun piiriin.

Pykälän 3 momentin mukaan velvollisuus keskeyttämiseen sekä tallenteiden ja muistiinpanojen hävittämiseen koskisi myös teknistä laitetarkkailua. Tekninen laitetarkkailu ei voi kohdistua välitettävänä olevaan viestiin. Jos kävisi ilmi, että tekninen laitetarkkailu kohdistuisi luottamukselliseen viestiin, johon olisi sovellettava lain 4 luvussa säädettyä telekuuntelua, televalvontaa tai muuta teknistä tarkkailua kuin teknistä laitetarkkailua, olisi tekninen laitetarkkailu tältä osin keskeytettävä ja tältä osin saadut tiedot sekä tietoja koskevat muistiinpanot hävitettävä heti.

Säännöstä voidaan pitää keskeisenä ehdotetun teknisen laitetarkkailun muutoksen takia, minkä myötä tekninen laitetarkkailu voisi kohdistua myös henkilöperusteisesti. Sinänsä henkilöperusteista kohdentamista on jo voimassa olevassa säännöksessä, jossa todetaan, että jos käy ilmi, että lain 32 §:n 4 momentissa tarkoitettu henkilö ei enää käytä teknisen laitetarkkailun kohteena olevaa laitetta tai ohjelmistoa, on tekninen laitetarkkailu keskeytettävä.

Pykälän 4 momentin mukaan vastaavasti valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu Suomessa olisi keskeytettävä siltä osin, kuin sen havaitaan kohdistuvan laitteeseen, tiedonsiirtolaitteeseen tai tietoja käsittelevään ohjelmistoon, joka ei kuulu luvan kohteena olevaan tietojärjestelmään. Saadut tiedot ja tallenteet sekä näitä koskevat muistiinpanot olisi hävitettävä heti.

Pykälän 5 momentissa säädettäisiin voimassa olevan pykälän 4 ja 5 momenttia vastaavasti paikkatiedustelun keskeyttämisestä. Ehdotettuun momenttiin yhdistettäisiin paikkatiedustelun keskeyttämistä koskevat voimassa olevan pykälän 4 ja 5 momentti.

86 §. *Tietoliikennetiedustelulla hankittujen tietojen hävittäminen.* Pykälän 1 momenttiin lisättäisiin uusi kohta, jonka mukaan tieto olisi hävitettävä, jos on käynyt ilmi, että tietoa ei tarvita maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi. Säännöksen tarkoittama hävittämisvelvollisuus koskisi niin ollen tietoa, joka on epäolennaista maanpuolustuksen tai kansallisen turvallisuuden suojaamisen kannalta.

Tietoliikennetiedustelulla saatu tieto voi joissain tapauksissa koskea jotain muuta tietoliikennetiedustelun kohteena olevaa maanpuolustusta koskevaa uhkaa tai kansallista turvallisuutta vakavasti uhkaavaa toimintaa kuin sitä, mitä varten lupa tietoliikennetiedusteluun on myönnetty. Kyse voisi olla esimerkiksi siitä, että lupa tietoliikennetiedusteluun on

myönnetty tiedon hankkimiseksi sotilaallisesta uhkasta, mutta luvan nojalla toteutetun tietoliikennetiedustelun avulla saadaan varsinaisen kohteen tietoliikenteen ohella tai sijasta tietoa muusta sellaisesta toiminnasta, joka vakavasti vaaraan Suomen elintärkeitä toimintoja. Jos tällaisella luvallisen tietoliikennetiedustelun oheistuotteena saadulla tiedolla on merkitystä maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi, ei velvollisuutta sen hävittämiseen olisi.

Säännös vastaisi sitä, mitä suojelupoliisin hävittämisvelvollisuudesta on säädetty tietoliikennetiedustelusta siviilitiedustelussa annetun lain 15 §:ssä.

Pykälä säilyy edellä tarkoitetusta tekniseksi katsottava ja säännöstä selkeyttävästä lisäyksestä huolimatta soveltamisen osalta nykytilan kaltaisena; sotilastiedusteluviranomainen ei saisi edelleenkään säilöä sen tehtävien kannalta tarpeetonta tietoa. Hankittu tieto on aktiivisesti tarkastettava ja hävitettävä viipymättä.

Pykälässä säädetty ei koskisi 66 §:n 2 momentin ja 67 a §:n 4 momentin perusteella tallennettuja tietoja.

89 §. *Tiedustelumenetelmän käytöstä ilmoittaminen.* Voimassa olevaa pykälää ei voida pitää säännösteknisesti tarkoituksenmukaisena. Tämän takia pykälän säännökset hajautettaisiin uusiin 89 a §:ään ja 89 b §:ään. Pykälän 1 momentissa säilyisi ennallaan ja voimassa olevan pykälän 7 momentti siirtyisi pykälän 2 momentiksi.

Pykälään esitetään lisättäväksi uusi säännös. Uudessa 3 momentissa säädettäisiin ilmoituksen tekemisestä tilanteissa, joihin sovelletaan pakkokeinolain 10 luvun 60 §:n 3 momenttia. Näissä tilanteissa ilmoituksen lykkäämistä tai ilmoituksen tekemättä jättämistä voisi vaatia tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies. Tarve johtuu siitä, että voimassa olevassa sotilastiedustelusta annetussa laissa, toisin kuin esimerkiksi poliisilain 5 luvun 58 §:n 5 momentissa ja poliisilain 5 a luvussa, ei ole mainintaa siitä, että pakkokeinolakia voidaan soveltaa soveltuvin osin. Tämän takia viitattu pykälä tulisi sovellettavaksi sotilastiedustelusta annetun lain osalta sellaisenaan sanamuotonsa mukaisesti, jolloin lykkäystä tai ilmoittamatta jättämistä vaativana tahona olisi oltava pidättämiseen oikeutettu virkamies.

Säännöksen viittaus aloitettuun esitutkintaan tarkoittaisi nimenomaan esitutkintaa kohteena olevan henkilön osalta liittyessään tiedustelun kohteen olevaan toimintaan.

Voimassa olevan pykälän 8 momentti, joka koskee valtiolliselle toimijalle ilmoittamista, siirtyisi pykälän 4 momentiksi.

89 a §. *Muun kuin valtiollisen toimijan tietoliikennetiedustelusta ilmoittaminen.* Pykälä olisi uusi. Säännöksessä säädettäisiin muuhun kuin valtiolliseen toimijaan kohdistuvan tietoliikennetiedustelun lähtökohtaisesta ilmoittamatta jättämisestä. Laajemmasta ilmoittamatta jättämisestä säädettäisiin valtiollisen toimijan osalta ehdotetun 89 §:n 4 momentissa, joka vastaa voimassa olevan lain 89 §:n 8 momenttia.

Tietoliikennetiedustelu poikkeaa menetelmänä esimerkiksi telekuuntelusta eikä se ole tiedustelumenetelmänä yhtä intensiivinen kohteen kannalta kuin telekuuntelu. Tietoliikennetiedustelua rajataan fyysisesti kohdistamalla se tiettyyn Suomen rajan ylittävään viestintäverkon osaan. Kuten edellä on jo todettu, tietoliikenne kulkee kulloisenkin tilanteen mukaan tehokkainta reittiä pitkin viestintäverkon osissa ja tämän takia voidaan sanoa, että

tietoliikennetiedustelujärjestelmän kohteeksi joutuu satunnaista tietoliikennettä. Tiedustelun kannalta merkittävää tietoa saadaan kuitenkin myös muusta kuin varsinaisesta viestin sisällöstä.

Tietoliikennetiedustelu on lähtökohtaisesti tarkoitettu Suomen raja ulkopuolelta tulevien uhkien tiedusteluun. Tämän lähtökohdankin takia käytännössä on mahdotonta selvittää henkilötasolla ulkomailta tulevan tietoliikenteen alkuperäistä lähettäjää tai tämän asuinpaikkaa; käytännössä ilmoituksen tekeminen on mahdotonta. Lisäksi ei voida olettaa, että sotilastiedusteluviranomainen pitäisi kattavaa rekisteriä tahoista, joille olisi ilmoitettava tilanteessa, jossa he sattuisivat saapumaan Suomeen.

Tietoliikennetiedustelun lopullinen kohdentaminen perustuu hakuehtoihin ja hakuehtojenluokkiin. Etenkin hakuehtojen luokat muodostuvat laajoista kohteeseen kohdistuvista hakuehdoista. Tietoliikennetiedustelu ei kohdistu tiettyyn henkilöön vaan uhkaan. Tämän takia ei voida puhua samalla tavalla yksityiselämään ja yksityisen viestin suojaan puuttuvasta toiminnasta tai intensiteetiltään vastaavasta tiedonhankinnasta kuin esimerkiksi perinteisessä telekuuntelussa.

Kuten aiemmin on todettu, EIT on hyväksynyt tiedustelujärjestelmät, joissa lähtökohtaista ilmoitusvelvollisuutta ei ole. EIT on ratkaisuissaan todennut, että etenkin tietoliikennetiedustelun osalta ilmoittaminen on käytännössä mahdotonta ja riittävänä voidaan pitää sitä, jos henkilö voi saattaa asiansa selvitettäväksi muilla keinoilla. Tämä saattaa olla myös henkilön kannalta tehokkaampi vaihtoehto.

Ilmoitusvelvollisuuden tarkoitus on se, että kohteena oleva henkilö voi turvautua tarvittaviin oikeussuojakeinoihin ja saattaa viranomaisen toiminnan lainmukaisuuden tutkittavaksi. Lähtökohtaisesti salaisessa tiedustelutoiminnassa esitetty muutos ilmoitusvelvollisuuteen ei kuitenkaan supista tosiasiallisesti henkilöiden oikeutta saada asiaansa tutkittavaksi, sillä jokaisella on tiedustelutoiminnan valvonnasta annetun lain 12 §:n perusteella, jos ainakin epäilee, oikeus pyytää tiedusteluvalvontavaltuutettua tutkimaan häneen kohdistuneen mahdollisen tiedustelumenetelmän käytön lainmukaisuuden. Lisäksi mainitun lain 11 §:n mukaan jokainen, joka katsoo, että tiedustelutoiminnassa on rikottu hänen oikeuksiaan tai menetelty muutoin lainvastaisesti, voi kannella tiedusteluvalvontavaltuutetun valvontavaltaan kuuluvassa asiassa. Ilmoitusvelvollisuuden osalta todettakoon, että EIT on hyväksynyt myös lähtökohtaisen ilmoittamattajättämisen, jos henkilöillä on käytössään vastaavia keinoja, kuten ulkopuolinen valvova taho, mitä kautta hän voi päästä vastaavaan lopputulokseen kuin ilmoitusvelvollisuuden kautta.

Muilta osin voimassa olevan säännöksen mukaisesti tietoliikennetiedustelujärjestelmään tullut viestinä poistettaisiin hävittämisvelvollisuuksien mukaisesti eikä näin ollen lähtökohtaista ilmoitusvelvollisuutta syntyisi. Tästä säädettäisiin nimenomaisesti 4 momentissa.

Näin ollen, koska sotilastiedustelun kohteena voi olla esimerkiksi vieraan valtion asevoimiin liittyvä yksityinen yhteisö, henkilöllä ei ole sinänsä merkitystä, vaan tietoliikennetiedustelun kohteena on organisaatio; tietoliikennetiedustelun luonteen takia kohteena ei ylipäänsä useinkaan voida katsoa olevan selvästi eroteltavissa olevia henkilöllisiä kohteita.

Pykälän 2 momentin mukaan ilmoitus olisi tehtävä, jos tietoliikennetiedustelussa on selvitetty tai selvinnyt 82 §:n 1 momentissa tarkoitettujen tahojen todistamiskiellon tai todistamattajättämisoikeuden alaista tietoa. Säännös koskee muun muassa pappeja ja toimittajia.

Säännöksessä mainittujen tahojen viestintää ja käsittelemiä tietoja voidaan pitää erityisen luottamuksellisina. Jos säännöksessä mainittu taho osallistuu tiedustelumenetelmän käytön kohteena olevaan toimintaan, ilmoittamisvelvollisuutta ei kuitenkaan olisi.

Ilmoitusvelvollisuutta ei kuitenkaan olisi, jos momentin viittauksen mukaisesti tieto olisi hävitetty 81 tai 86 §:n perusteella. Luonnollisesti, jos tieto on hävitetty tarpeettomana, ei myöskään ilmoitusvelvollisuutta voi syntyä. Säännös vastaisi voimassa olevan lain 86 §:n 2 momenttia.

89 b §. *Ilmoituksen tekeminen, lykkääminen ja tekemättä jättäminen.* Pykälä olisi uusi. Aineellisten muutosten lisäksi pykälään siirrettäisiin voimassa olevasta 89 §:stä eräitä säännöksiä lain systematiikan selkeyttämiseksi.

Pykälän 1 momentin mukaan ilmoitus olisi tehtävä viipymättä kirjallisesi sen jälkeen, kun 89 §:ssä ja 89 a §:ssä tarkoitetun tiedustelumenetelmän käytön tarkoitus on saavutettu. Ilmoitus olisi kuitenkin tehtävä edellä viitatuissa pykälissä tarkoitetulle henkilölle viimeistään vuoden kuluttua tiedustelumenetelmän käytön lopettamisesta. Säännös vastaisi voimassa olevan 89 §:n 1 momenttia.

Pykälän 2 momentin mukaan ilmoitusvelvollisuus konkretisoituisi vasta silloin, kun tiedustelumenetelmän kohteena olleen henkilöllisyys olisi selvinnyt. Luonnollisesti ilmoituksen tekeminen ilman tietoa henkilöllisyydestä on käytännössä mahdotonta.

Lisäksi olisi tiedettävä henkilön Suomessa oleva asuinpaikka. Henkilöllisyyden tietäminen ei yksinään riitä kirjallisen ilmoituksen tekemiseen, vaan henkilöllä olisi oltava tiedossa oleva asuinpaikka tai muu osoite, jonne ilmoitus voidaan toimittaa. Vasta edellä mainittujen kahden tiedon selvittyä ilmoitus voidaan toimittaa.

Jos henkilöllisyydeltään tunnettu tiedustelumenetelmien käytön kohteen asuinpaikka ei olisi tiedossa, sotilastiedusteluviranomaiselta ei edellytettäisi kovin laajoja toimenpiteitä pelkästään ilmoituksen tekemiseksi. Vastaavasti henkilöllisyydeltään tuntemattoman kohteen selvittäminen ei edellyttäisi laajoja selvittämistoimenpiteitä. Laajojen selvitysten tekeminen ilmoituksen takia saattaisi vaarantaa henkilön yksityisyyden suojaa tarpeettomasti.

Pykälän 2 momentinkin osalta on huomattava, että jokainen, joka epäilee joutuneensa tiedustelumenetelmän käytön kohteeksi, voi saattaa asiansa selvitettäväksi tiedusteluvalvontavaltuutetulle.

Pykälän 3 momentin mukaan kohteelle ilmoittamisesta olisi samalla annettava kirjallisesti tieto luvan myöntäneelle tuomioistuimelle. Lupaa edellyttävän tiedustelumenetelmän kohteelle ilmoittaminen olisi siten saatettava myös Helsingin käräjäoikeuden tietoon. Säännös vastaisi voimassa olevan 89 §:n 5 momenttia.

Pykälän 4 momentin mukaan tuomioistuin voisi pääesikunnan tiedustelupäällikön taikka tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta päättää, että ilmoitusta kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedustelumenetelmän käytön turvaamiseksi, Suomen sotilaallisen maanpuolustuksen turvaamiseksi tai kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saataisiin tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä sotilaallisen maanpuolustuksen turvaamiseksi tai kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoituksen lykkäämisestä tai kokonaan tekemättä jättämisestä

päättäisi tuomioistuin, vaikka kysymys olisi sellaisesta tiedustelumenetelmästä, josta on päättänyt tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

Ehdotuksen mukaisesti ilmoitusta voitaisiin lykätä enintään kahdeksi vuodeksi kerrallaan. Uuden lykkäyksen myöntäminen tulisi olla poikkeuksellista. Toistuvan ilmoittamisen lykkäämisen sijaan tulisi hakea kokonaan ilmoittamatta jättämistä, jos edellytykset ovat olemassa, koska esimerkiksi kymmenen vuoden kuluttua tehtävällä ilmoituksella ei käytännössä ole merkitystä kohteelle. Lykkäämistä ja uudelleen lykkäämistä tulisi hakea ennen määräajan päättymistä. Lykkäämisen mahdollistavana perusteena olisi ensinnäkin käynnissä olevan tiedustelumenetelmän käytön turvaaminen. Tiedonhankinta voisi liittyvä mihin tahansa vireillä olevaan tiedusteluoperaatioon, myös siviilitiedusteluoperaatioon.

Lykkääminen olisi mahdollista myös maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi. Tämä tarkoittaisi sitä, että käsillä olisi oltava maanpuolustukseen, valtioon tai yhteiskuntaan kohdistuva uhka. Kuitenkin esimerkiksi yksityishenkilöihin kohdistuvat väkivallanteot voisivat kuulua maanpuolustuksen tai kansallisen turvallisuuden piiriin, jos ne laajuudeltaan tai merkitykseltään olisivat maanpuolustuksen tai kansallisen turvallisuuden kannalta merkittäviä ja voisivat siten muodostaa vakavan uhan sille. Lisäksi lykkääminen olisi mahdollista hengen tai terveyden suojaamiseksi. Lykkäämisen kynnyksenä olisi, että se on perusteltua. Kynnys lykkäämiselle ei siis olisi kovin korkea. Säännös vastaisi voimassa olevan lain 89 §:n 6 momenttia.

Pykälän 5 momentissa säädettäisiin ilmoituksen tekemättä jättämisestä. Säännös erotettaisiin omaksi momentikseen voimassa olevan 89 §:n 6 momentista. Säännös vastaisi voimassa olevaan säännöstä tältä osin.

Momentin mukaan ilmoitus saataisiin jättää tuomioistuimen päätöksellä kokonaan tekemättä vain silloin, jos se on välttämätöntä maanpuolustuksen turvaamiseksi tai kansallisen turvallisuuden varmistamiseksi taikka hangen tai terveyden suojaamiseksi. Kynnys olisi näin ollen korkea.

Pykälän 6 momentissa olisi viittaussäännös tuomioistuinmenettelyyn. Mikäli tuomioistuin ei myöntäisi lykkäystä tai ei hyväksyisi ilmoituksen kokonaan tekemättä jättämistä, saisi vaatimuksen esittäjä kannella päätöksestä Helsingin hovioikeudelle siten kuin jäljempänä 113 §:ssä säädetään.

91 §. *Muussa kuin virkasuhteessa olevan toimivaltuudet.* Voimassa oleva sääntely koskee ainoastaan asevelvollisuuslain mukaisessa kertausharjoituksessa olevia riittävän koulutuksen saaneita reserviläisiä. Lisäksi tiedustelumenetelmien käyttö on rajattu radiosignaalitiedusteluun, ulkomaan tietojärjestelmätiedusteluun, teknisten tietojen käsittelyyn sekä tietoliikennetiedustelun kohdentamiseen. Pykälään muutettaisiin niin, että sotilastiedustelutoiminnassa voitaisiin aiempaa laajemmin käyttää asevelvollisuuslain mukaisessa palveluksessa olevia sekä vapaaehtoiseen maanpuolustukseen osallistuvia henkilöitä. Lisäksi edellä tarkoitetuilla henkilöillä olisi mahdollisuus käyttää aiempaa laajemmin tiedustelumenetelmiä. Selvää on kuitenkin se, ettei asevelvollisuuslain mukaisessa palveluksessa olevia tai vapaaehtoiseen harjoitukseen osallistuvia henkilöitä voida käyttää henkilöstöpulan korjaamiseen, vaan palvelukselle tai vapaaehtoiselle harjoitukselle on oltava puolustusvoimallinen syy. Erityisiä syitä voisivat olla esimerkiksi Suomessa harvinaisten kielten osaaminen ja muu erityisosaaminen tietyn asiakokonaisuuden osalta.

Säännöksessä tarkoitetuissa tilanteissa olisi kyse niin kutsutusta harmaasta vaiheesta, jolloin maanpuolustukseen ja kansalliseen turvallisuuteen kohdistuu lievempiä laaja-alaisen vaikuttamisen toimenpiteitä ja mahdollista sotilaallista operaatiota valmistellaan. Sotilastiedustelun näkökulmasta tämä tarkoittaa sitä, että organisaatiota on kasvatettava nopealla aikajänteellä ja tekijöitä tarvitaan enemmän, hyvässä tapahtumien kehityskulussa lyhytaikaisesti.

Pykälän 1 momentissa viitattaisiin ensinnäkin asevelvollisuuslain mukaiseen palvelukseen. Tällä tarkoitetaan varusmiespalveluksen lisäksi kertausharjoitusta, ylimääräistä palvelusta ja liikekannallepanoa. Palvelukseen määrättyä voitaisiin käyttää sotilastiedustelun tehtävissä jäljempänä säädetyin rajauksin.

Momenttiin lisättäisiin myös mahdollisuus käyttää vapaaehtoisesta maanpuolustuksesta annetun lain 18 ja 19 §:ssä tarkoitettuun vapaaehtoisessa harjoituksessa olevia henkilöitä. Sanotun lain 18 § koskee Puolustusvoimien järjestämiä vapaaehtoisia harjoituksia.

Lain 19 §:n koskee Puolustusvoimien järjestämien vapaaehtoisten harjoitusten erityistehtäviä. Pykälän tarkoittamiin harjoituksiin voivat osallistua myös muut kuin 18 §:ssä tarkoitetun henkilöt, kunhan he ovat terveydeltään ja muilta henkilökohtaisilta ominaisuuksiltaan siihen sopiva. Säännöksen mukaan edellytyksenä ei ole varusmiespalveluksen suorittaminen tai reserviin kuuluminen. Vapaaehtoisten harjoitusten kautta sotilastiedusteluun on mahdollista osallistaa aiempaa laajemmin yhteiskunnan eri osa-alueilta osaamista sotilastiedustelutoimintaan.

Asevelvollisuuslain mukaisessa palveluksessa olevalta ja vapaaehtoiseen maanpuolustukseen osallistuvalta edellytettäisiin riittävää koulutusta määriteltyihin tehtäviin. Sotilastiedusteluviranomainen määrittäisi riittävän koulutuksen ja kokemuksen kyseessä olevaan tehtävään. Luonnollisesti tiedustelun kokonaisuudessa toimittaessa vaativampiin tehtäviin siirtyminen edellyttää kokemusta eikä käytettävissä olevia toimivaltuuksia voida käyttää täysimääräisesti ennen riittävää kokemusta sekä tiedollisia ja taidollisia valmiuksia. Erityistä huomiota olisi kiinnitettävä tietoturvallisuuteen ja henkilötietojen käsittelyyn.

Säännöksessä tarkoitettujen sotilastiedustelun tehtäviä suorittava saisi käyttää tässä laissa tarkoitettuja toimivaltuuksia ainoastaan sotilastiedusteluviranomaisen palveluksessa olevan virkamiehen ohjauksessa ja valvonnassa. Näin ollen ensisijainen vastuu säännöksessä tarkoitettujen henkilöiden toiminnasta olisi ohjaavalla ja valvovalla virkamiehellä, joka määrittää tehtävän ja mahdollisesti käytettävän toimivaltuuden.

Säännöksessä tarkoitettu riittävän koulutuksen saanut henkilö voisi käyttää 4 luvussa tarkoitettuja tiedustelumenetelmiä lukuun ottamatta ohjattua tietolähdetoimintaa, peitetoimintaa ja valeostoa tiedustelutehtävän suorittamiseksi. Vaikka säännös antaa sinänsä laajat toimivaltuudet, edellyttää niiden käyttö aina riittävää koulutusta ja kokemusta. Toimivaltuuksien käyttävien piiriä rajaa myös tiedustelutoiminnan vaivihkainen luonne, jonka ohjaa tarkkaan harkintaa mitä tietoja ja mitä keinoja tehtävää toteuttavalla henkilöllä on käytössään. Arviointiin vaikuttaa aina koulutus, tiedot ja taidot sekä luotettavuus. Säännöksessä tarkoitetut henkilöt eivät saisi koskaan itsenäisesti päättää, mitä tiedustelumenetelmiä ja missä laajuudessa niitä voitaisiin käyttää. Lisäksi toimintaan vaikuttaa aina sotilaallinen organisoituminen.

Asevelvollisuuslain mukaisessa palveluksessa tai vapaaehtoisesta maanpuolustuksesta annetun lain 18 ja 19 §:ssä tarkoitetussa vapaaehtoisessa harjoituksessa olevat puolustusvoimista annetun lain 47 §:n perusteella sotilastiedusteluviranomaisen palveluksesta eronneet henkilöt

voisivat käyttää kaikkia 4 luvussa tarkoitettuja tiedustelumenetelmiä sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa. Erityisenä vaatimuksena on myös, että he olisivat tiedustelumenetelmien käyttöön erityisesti perehtyneitä.

Pykälän 2 momentissa säädettäisiin sotilastiedusteluvirnaomaisen palveluksesta eronneiden 1 momentissa tarkoitetussa palveluksessa tai harjoituksessa olevien toimivaltuuksista.

Säännös koskisi myös Puolustusvoimista annetun lain 47 §:ssä tarkoitetun eroamisiän saavuttaneita. Esimerkiksi eroamisiän saavuttaneilla sotilastiedusteluviranomaisessa toimineilla henkilöillä on parhaimmillaan useiden vuosikymmenien kokemus ja osaaminen sotilastiedustelutoiminnasta. Lisäksi heillä saattaa olla osaamista, mitä nuoremmilla sukupolvilla ei vielä ole. Näin myös säännöksessä tarkoitettuja henkilöitä voitaisiin käyttää tarvittaessa maanpuolustuksen ja kansallisen turvallisuuden suojaamisessa.

Eroamisikää Puolustusvoimien palveluksesta on nostettu viime aikoina taajaan. On myös huomattava, että reserviläisten yläikärajaa on nostettu 65 ikävuoteen lailla 1346/2025, joka on tullut voimaan 1.1.2026 alkaen asevelvollisuuslain muutoksella. Samassa yhteydessä vapaaehtoisen maanpuolustuksen harjoitukseen osallistuvilta poistettiin yläikäraja kokonaan.

Palvelukseen tai harjoitukseen osallistuvan henkilön osaaminen arvioitaisiin tapauskohtaisesti huomioiden hänen kokemuksensa.

Tiedustelumenetelmien käyttö tapahtuisi aina sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa.

93 §. *Muussa kuin virkasuhteessa olevan virkavastuu.* Pykälän otsikko muutettaisiin kuvaamaan tarkemmin henkilöitä, jotka voivat osallistua sotilastiedustelutoimintaan. Voimassa oleva säännös koskee ainoastaan asevelvollisuuslain mukaisessa palveluksessa olevia.

Pykälän 1 momentin mukaan virkavastuu laajennettaisiin kattamaan myös ehdotetussa 91 §:ssä tarkoitetut vapaaehtoisesta maanpuolustuksesta annetun lain 18 ja 19 §:n tilanteet. Virkavastuu koskisi siis myös muita kuin asevelvollisia.

Pykälän 2 momentissa virkavastuu laajennettaisiin koskemana myös muita kuin virkasuhteessa olevia. Virkavastuu on laajempi kuin työsopimussuhteen nojalla syntyvä vastuu. Toimittaessa merkittävää julkista valtaa sisältävissä tehtävissä, virkavastuun olisi katettava myös sopimussuhteiset henkilöt.

94 §. *Muussa kuin virkasuhteessa olevan vahingonkorvausvastuu.* Pykälän otsikko muutettaisiin vastaamaan uusia säännöksiä. Säännös olisi informatiivinen.

Pykälän 1 momentissa viitattaisiin henkilöön, joka lain mukaista tehtävää suorittaessaan aiheuttaa vahinkoa. Henkilöllä tarkoitettaisiin muussa kuin virkasuhteessa olevaan henkilöä, kuten asevelvollisuuslain mukaisessa palveluksessa olevaa.

Asevelvollisuuslain nojalla annetun tai muun vastaavan määräyksen perusteella valtion palveluksessa olevalla henkilöllä on vahingonkorvauslain 4 luvun 2 §:n 2 momentin mukaan sama vastuu kuin virkamiehellä ja työntekijällä. Sotilas on velvollinen korvaamaan vahingosta määrän, joka harkitaan kohtuulliseksi ottamalla huomioon vahingon suuruus, teon laatu, vahingon aiheuttajan asema, vahingon kärsineen tarve sekä muut olosuhteet. Erityisasemassa ovat pykälän 3 momentin mukaan ne sotilaat, jotka ovat tuottaneet vahingon ollessaan vastuussa sotaväen aluksesta tai ilma-aluksesta. Edellä sanottu merkitsee myös mahdollisuutta

vahingonkorvauksen sovitteluun huomioon ottaen muun muassa vahingon suuruus, teon laatu ja vahingon aiheuttajan asema. Jos hänen viakseen jää vain lievä tuottamus, ei vahingonkorvausta tuomita. Tahallisen rikoksen ollessa kyseessä pääsääntönä on täyden korvauksen tuomitseminen. Valtion oikeus regressioon vahingonaiheuttajalta on 4 luvun 3 §:n mukaan niin ikään rajoitettu. Valtion isännänvastuun ulottaminen myös 87 ja 88 §:ssä tarkoitetuissa tehtävissä oleviin henkilöihin edellyttää säännöksen ottamista tähän lakiin. Vahingonkorvauslakia ei näin ollen tarvitsisi muuttaa.

Säännös kattaisi myös tilanteet, joissa sotilastiedusteluviranomaisen ulkopuolinen henkilö avustaisi tiedustelumenetelmän käytön edellyttämän laitteen, menetelmän tai ohjelmiston asentamisessa tai poisottamisessa.

Vahingonkorvauslain 3 luvun säännösten perusteella työnantaja on velvollinen korvaamaan vahingon, jonka työntekijä virheellään tai laiminlyönnillään työssään kolmannelle aiheuttaa (1 §:n 1 momentti). Jos joku suorittaa viranomaisen määräyksestä laissa määrättyä tehtävää olematta itsenäinen yrittäjä ja tätä tehtävää suorittaessaan virheellään tai laiminlyönnillään aiheuttaa vahinkoa, on se, jonka lukuun tehtävä suoritetaan, velvollinen korvaamaan vahingon (1 §:n 3 momentti). Esimerkiksi varusmiestä on pidetty julkisoikeudellisessa oikeussuhteessa olevana työnsuorittajana, josta julkisyhteisö voi joutua vahingonkorvausvastuuseen. Viitatut vahingonkorvauslain säännökset laajentavat siis viranomaisen isännänvastuuta.

Pykälän 2 momentissa säädettäisiin vapaaehtoisesta maanpuolustuksesta annetun lain 18 ja 19 §:ssä tarkoitettuun vapaaehtoiseen harjoitukseen osallistuvan korvausvastuusta. Korvausvastuuseen sovellettaisiin vahingonkorvauslain 4 luvun säännöksiä asevelvollisen korvausvastuusta. Säännös olisi aineellinen, sillä vahingonkorvauslaissa ei säädetä vapaaehtoiseen maanpuolustukseen osallistuvien henkilöiden vahingonkorvausvastuusta. Säännös vastasisi sitä, mitä vapaaehtoisesta maanpuolustuksesta annetussa laissa säädetään vahingonkorvausvastuusta.

96 §. *Viestinnän välittäjän ja datakeskuspalvelun tarjoajan avustamisvelvollisuus.* Pykälään ehdotetaan muutosta, jonka mukaan siinä jatkossa viitattaisiin teleyrityksen ja yhteisötilaajan sijaan sähköisen viestinnän palveluista annetun lain 3 §:n 36 kohdassa tarkoitettuun viestinnän välittäjään. Viestinnän välittäjällä tarkoitetaan myös sellaista muuta tahoa, joka välittää sähköistä viestintää muutoin kuin henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiin.

Lisäksi avustamisvelvollisuus koskisi datakeskuspalvelun tarjoajia. Datakeskuspalvelu on määritelty kyberturvallisuuslain 2 §:n 2 kohdassa ja sillä tarkoitetaan palvelua, joka käsittää rakenteita tai rakenteiden ryhmiä, jotka on tarkoitettu datan tallennus-, käsittely- ja siirtopalveluja tarjoavien tietoteknisten laitteiden ja verkkolaitteiden keskitettyyn ylläpitoon, yhteenliittämiseen ja ohjaukseen yhdessä kaikkien tarvittavien sähkönjakeluun ja toimintaolosuhteiden säätelyyn tarkoitettujen laitteiden ja infrastruktuurin kanssa. Velvollisuus koskisi edellä tarkoitettua palvelua tarjoavaa tahoa.

Pykälän 1 momentissa mainittaisiin myös uusi tiedustelumenetelmä, valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu kotimaassa. Viestinnän välittäjän ja datakeskuspalvelun tarjoajan olisi avustettava sotilastiedusteluviranomaista vastaavasti kuin esimerkiksi telekuuntelussa.

Pykälän 2 momentin mukaan sotilastiedusteluviranomaisella sekä toimenpiteen suorittajalla ja avustavalla henkilöstöllä olisi oikeus telekuuntelua varten tarpeellisen yhteyden kytkemiseksi päästä myös muihin kuin viestinnän välittäjän hallinnassa oleviin tiloihin, ei kuitenkaan

vakituiseen asumiseen käytettyihin tiloihin. Toimenpiteestä päättäisi erityisesti tiedustelumenetelmien käyttöön erityisesti virkamies.

Momentissa viitattaisiin myös datakeskuspalvelun tuottajaan vastaavasti, mitä on viitattu viestintäpalvelun tarjoajan osalta.

97 §. *Tiedonsiirtäjän velvollisuus myötävaikuttaa tietoliikennetiedustelun edellyttämän liityntäpisteen rakentamiseen ja ylläpitämiseen.* Pykälän 2 momenttia muutettaisiin. Muutoksen myötä sotilastiedusteluviranomainen voisi tehdä tietoliikennetiedustelun edellyttämän liityntäpisteen ilman tiedonsiirtäjän myötävaikutusta, jos se olisi tiedustelun suojaamisen kannalta välttämätöntä. Toimenpide kohdistuisi käytännössä tiedonsiirtäjiin, jotka eivät ole myötämielisiä ja voivat olla esimerkiksi vieraan valtiollisen toimijan hallinnassa.

Säännöksessä käytettävällä termillä tiedustelu viitattaisiin yleisesti tietoliikennetiedustelua käyttäviin tiedusteluviranomaisiin, eli sotilastiedusteluviranomaiseen ja suojelupoliisiin. Sotilastiedusteluviranomainen toimii teknisenä toteuttajana tietoliikennetiedustelussa suojelupoliisille. Teknisen toteuttamisen yhtenä osa-alueena on liityntäpisteen toteuttaminen, joten liityntäpiste olisi voitava tehdä tarvittaessa salassa myös suojelupoliisin tarpeiden mukaisesti.

Käytännössä on havaittu tilanteita, joissa yleisen viestintäverkon toiminnan kannalta vähäisenä pidettävä tiedonsiirtäjää saattaa hallinnoida tiettyä viestintäverkon osaa. Tiedonsiirtäjä on kuitenkin toimija, johon ei voida saada yhteyttä tai toimija toimii valtiollisen toimijan ohjauksessa. Itsestään selvää on, ettei tällaisissa tilanteissa liityntäpistettä voida toteuttaa tiedonsiirtäjän myötävaikutuksella.

Selvää on se, että liityntäpisteen rakentaminen ei saa aiheuttaa tarpeetonta haittaa yleiselle viestintäverkolle. Tähän ohjaavat jo lain yleiset periaatteet ja toiminnan paljastumisen riski. Esimerkiksi Suomen yleisen viestintäverkon kannalta keskeinen toimija ei voisi olla säännöksen tarkoittamien toimenpiteiden kohteena käytännössä koskaan, sillä toimenpiteistä saattaisi aiheutua merkittävää haittaa ja tätä kautta sotilastiedusteluviranomaisen toiminta saattaisi paljastua.

Liityntäpiste olisi edelleen lähtökohtaisesti toteutettava tiedonsiirtäjän myötävaikutuksella ja lähtökohtaisesti 2 momentin tarkoittamissa tilanteissa tiedonsiirtäjällä olisi oikeus olla paikalla mahdollisuuksien mukaan liityntäpistettä toteutettaessa. Sotilastiedusteluviranomaisen olisi aina liityntäpistettä salassa toteuttaessaan tarkoin harkittava toimenpiteen välttämättömyys niin operatiivisesti kuin oikeudellisestikin.

99 §. *Korvaus viestinnän välittäjälle ja datakeskuspalvelun tarjoajalle.* Pykälään tehtäisiin vastaavat 97 §:ään ehdotetuista muutoksista johtuvat muutokset korvauksen saajiin.

101 §. *Muutoksenhaku korvauspäätökseen.* Pykälä vastaisi käytännössä sitä, mitä voimassa olevassa laissa säädetään muutoksenhausta korvauspäätökseen. Pykälän 1 momenttiin tehtäisiin 97 §:ään ehdotetuista muutoksista johtuvat muutokset.

Pykälän 2 momentissa olisi informatiivinen viittaus hallintolakiin ja oikeudenkäynnistä hallintoasioissa annettuun lakiin oikaisuvaatimuksen ja valitusoikeuden osalta.

Pykälän 3 momentti vastaisi voimassa olevan pykälän 4 momenttia. Momentissa säädettäisiin Liikenne- ja viestintäviraston oikeudesta tulla kuulluksi, mikäli korvausasiaa käsitellään hallinto-oikeudessa.

104 §. *Tietojen saanti yksityiseltä yhteisöltä*. Pykälän 2 momenttia muutettaisiin vastaamaan sitä, mitä muualla esimerkiksi rikostorjunnan osalta säädetään. Tietopyyntöjen kohteena voisi jatkossa olla tietoyhteiskunnan palvelun tarjoaja säännöksessä nykyisin mainitun yhteisötilaajan sijasta. Tietoyhteiskunnan palvelulla tarkoitetaan sähköisen viestinnän palveluista annetun lain 3 §:n 29 kohdassa tarkoitettuja tietoyhteiskunnan palveluita kuten sähköisenä etäpalveluna vastaanottajan henkilökohtaisesta pyynnöstä tavallisesti korvausta vastaan toimitettavaa palvelua. Tietoyhteiskunnan palvelun tarjoajalla tarkoitettaisiin vastaavasti palvelun tarjoajaa, joka tarjoaa sähköisen viestinnän palveluista annetun lain 3 §:n 29 kohdassa tarkoitettuja tietoyhteiskunnan palveluita. Tällaisia voisivat olla esimerkiksi pilvipalveluiden tai erilaisten datakeskuspalveluiden tarjoajat tai muut digitaalisen infrastruktuurin tarjoajat, kuten verkossa toimivat markkinapaikat tai hakukoneet, taikka erilaiset verkkoyhteisöalustat.

Ehdotettujen muutosten taustalla ovat toimintaympäristön muutokset, erityisesti yhteiskunnan digitalisaatio ja siihen liittyvä teknologinen kehitys, joiden seurauksena nykyinen sääntely ei enää kaikilta osin vastaa käytännön tarpeisiin. Uusi muotoilu kattaisi aiempaa laajemman joukon erilaisia toimijoita sekä kaikki palvelun tarjoamiseen osallistuvat eri toimijat, joilta sotilastiedusteluviranomainen voisi saada tietoja tehtäviensä suorittamiseksi. Palveluketjuun voi liittyä useampia eri palvelun tarjoajia, joilla on eri tehtäviä ja rooli palvelun tuottamisessa, vaikka palvelun tarjoaja ei itsessään välitä viestintää.

Tiedot, joiden pohjalta säännöksessä tarkoitettu tietopyyntö voidaan tehdä, on jo sotilastiedusteluviranomaisen hallussa ja hankittuna esimerkiksi toisella tiedustelumenetelmällä. Pyynnön kohteena voisi näin ollen olla esimerkiksi se, kuka käytti tiettyä IP-osoitetta tiettynä ajankohtana. Säännöksen tarkoituksena ei ole murtaa päästä-päähän salausta.

Lisäksi 2 momenttia muutettaisiin siten, että siitä kävisi selvästi ilmi, että sotilastiedusteluviranomaisella olisi oikeus saada palvelun käyttäjän tai tilaajan tunnistamiseksi tarpeelliset tiedot. Käyttäjällä tarkoitettaisiin sähköisen viestinnän palveluista annetun lain 3 §:n 7 kohdan mukaisesti luonnollista henkilöä, joka palvelun tilaajana tai muuten käyttää viestintäpalvelua tai lisäarvopalvelua. Tilaajalla tarkoitettaisiin puolestaan kyseisen lain 3 §:n 30 kohdan mukaisesti oikeushenkilöä ja luonnollista henkilöä, joka on muuta kuin teletoimintaa varten tehnyt sopimuksen viestintäpalvelun tai lisäarvopalvelun toimittamisesta. Sotilastiedusteluviranomainen voisi tietopyynnön nojalla saada sellaiset tarpeelliset tiedot, joiden avulla käyttäjän tai tilaajan tunnistaminen olisi mahdollista.

Pykälässä säädetty tiedonsaantioikeus koskisi jatkossakin tietoja, jotka ovat tarpeen tiedustelutehtävän suorittamiseksi.

Hallintovaliokunta on mietinnössään HaVM 1/2024 vp, sekä aiemmissa kannanotoissaan (HaVL 37/2022 vp, HaVM 42/2022, HaVM 3/2023 vp) pitänyt esimerkiksi salaisten tiedonhankintakeinojen osalta perusteltuna, että säännöksiä uudistetaan yhdenmukaisesti ja että sääntely on mahdollisimman samansisältöistä. Asiallisesti samojen keinojen sääntelyssä ei valiokunnan näkemyksen mukaan ole tarkoituksenmukaista olla perusteettomia eroja. Esimerkiksi salaisten tiedonhankintakeinojen yhdenmukainen sääntely on keskeistä toimivan viranomaisyhteistyön näkökulmasta. Selkeä ja johdonmukainen sääntely lisää paitsi käsittelyn tehokkuutta myös kohteiden yhdenvertaista kohtelua. Vastaavalla tavalla tulisi sääntelyn samansisältöisyys ottaa huomioon myös eri viranomaisten oikeuksissa tiedonsaantiin, sekä tietyin edellytyksin myös oikeuksiin jakaa ja välittää saamaansa tietoa toisille viranomaisille.

Pykälän 2 momentin muutoksien osalta ei ole kyse tilanteesta, jossa palveluita tarjoavat yritykset tai yhteisöt joutuisivat luopumaan päästä-päähän salauksesta taikka helpottamaan tai

mahdollistamaan sotilastiedusteluviranomaisten pääsyä järjestelmiinsä tai palveluihinsa yleisesti.

Pykälään lisättäisiin uusia 3 momentti. Momentissa säädettäisiin nimenomaisesti, että tiedot voisi saada viipymättä ja maksutta, jollei laissa toisin säädetä.

111 §. *Tallenteiden tutkiminen.* Pykälän 1 momenttia muutettaisiin. Voimassa olevassa sääntelyssä tiedustelumenetelmien käytössä kertyneitä tallenteita saa tutkia muiden ohella sotilastiedusteluviranomaisen tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies. Selvyyden vuoksi momenttia muutettaisiin tältä osin siten, että tallenteita saa tutkia sotilastiedusteluviranomaisen tehtävään määrätty virkamies, mikä vastaa paremmin käytännön toimintaa sotilastiedusteluviranomaisessa.

Voimassa olevassa säännöksessä sotilastiedusteluviranomaisessa päätöksen tallenteiden tutkimiseen oikeutetusta henkilöstä voi tehdä ainoastaan pääesikunnan tiedustelupäällikkö. Käytännössä päätöksentekotaso on todettu liian korkeaksi ja myös tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen olisi voitava tehdä vastaavia päätöksiä. Ehdotetulla muutoksella päätöksen voisi tehdä siis käytännön toimintaa lähempänä olevat virkamiehet, joilla on perehtyneisyys kyseiseen tehtävään, ja päätöksentekotaso vastaisi paremmin sitä, mitä se on esimerkiksi tiedustelumenetelmien käyttämisestä päättämisen osalta. Tältä osin säännös vastaisi sitä, mitä poliisilain 5 a luvussa säädetään tallenteiden tutkimisesta.

Muilta osin pykälään ei tehtäisi muutoksia.

7.2 Laki puolustusvoimista

8 b §. *Tiedonhankinta yleisesti saatavilla olevista lähteistä.* Pykälä olisi uusi. Pykälässä säädettäisiin Puolustusvoimia koskevasta oikeudesta hankkia tietoja yleisesti saatavilla olevista lähteistä. Tiedonhankintaa voisi näin ollen tehdä sotilastiedusteluviranomaisen lisäksi myös esimerkiksi Puolustusvoimien tutkimuslaitos ja Puolustusvoimien kyberpuolustuksesta vastaavat toimijat.

Yleisesti saatavilla olevilla lähteillä tarkoitettaisiin perinteisten avointen lähteiden, kuten sanomalehtien ja perinteisten uutispalveluiden, lisäksi digitaalisia palveluita, jotka saattavat edellyttää kirjautumista tai profiilin luomista. Näitä digitaalisia palveluita olisivat muun muassa sosiaalinen media (Facebook ja TikTok) ja rekisteröitymistä edellyttävät tietopalvelut, kuten Jane’s Information Service. Nimenomaan rekisteröitymisen, vastaavan muun profiilin luominen tai tietojen luovuttaminen olisi keskeinen ero perinteisiin avointen lähteiden tiedusteluun verrattuna. Se, missä perinteisesti avointen lähteiden tiedon on katsottu olevan saatavilla kenelle vaan ilman tietojen luovuttamista, yleisesti saatavilla olevissa lähteissä saatetaan joutua luovuttamaan joitain tietoja. Edellä mainituista tiedon lähteistä voidaan käyttää nimitystä rajattu avoin tietolähde.

Yleisesti saatavilla olevien lähteiden määritelmä olisi kuitenkin siinä mielessä löyhä ja sitä olisi arvioitava aina sitä vasten, mikä on ollut tietojen saataville saattaneen tahon tarkoitus, esimerkiksi saada julkaistulle tiedolle mahdollisimman paljon näkyvyyttä vai kontrolloiko taho tietohiin pääsyä tarkasti. Esimerkiksi useat tietopalvelut edellyttävät rekisteröitymistä, mutta sitä, kuka rekisteröityy, ei välttämättä kontrolloida mitenkään ja rekisteröityminen hyväksytään automaattisesti.

Toisaalta joissain digitaalisissa palveluissa tarkoituksena on nimenomaisesti ehkäistä käyttäjän tunnistamista, kuten Tor-verkossa. Näissä palveluissa voidaan olettaa olevan myös Puolustusvoimien tehtävien kannalta olennaista tietoaineistoa. Palveluita saatetaan myös käyttää tietovuotoihin, jotka saattavat tarjota jopa merkittävää tietoa esimerkiksi sotilastiedustelulle.

Se, voidaanko esimerkiksi sosiaalisen median ryhmää pitää säännöksen tarkoittamana yleisesti saatavilla olevana lähteenä, riippuu kulloisestakin tilanteesta. Oikeuskirjallisuudessa rajanvedosta on käytetty karkeana esimerkkinä, että viestin ollessa suunnattu vain kavereille tai osalle heistä, eivät he vielä muodosta yleisöä, sillä edellytyksellä, että kavereita on vain muutama. Kaveripiirin ollessa laaja, esimerkiksi satoja henkilöitä, muodostaa joukko jo yleisön. Lähtökohtana olisikin pidettävä sitä, voidaanko ryhmän jäsenistön katsoa muodostuvan tiiviistä ystäväpiiristä vai onko kyse kokonaisuudesta, jossa jäsenillä ei ole toisiinsa tiivistä kaikki ryhmän jäsenet kattavaa sosiaalista suhdetta. Jos ryhmässä olisi kyse tiiviin ystäväpiirin ryhmästä, olisi ryhmän jäsenyys peruutettava tai vaihtoehtoisesti sosiaalisen median tili olisi siirrettävä esimerkiksi sotilastiedusteluviranomaiselle, jotta tämä voisi tarvittaessa hankkia tietoja tiedustelumenetelmillä.

Yleisesti saatavilla olevista lähteistä hankittu tieto on lähteistä saatavaa yleistä tietoa. Säännöksen tarkoittamassa tiedonhankinnassa tiedontuottajalla tai viestin lähettäjä ei ole merkitystä, ainoastaan viestissä olevalla tiedolla. Jos esimerkiksi sosiaalisen median alustalla ryhdyttäisiin seuraamaan tiettyä henkilöä tai ryhmän jäsentä, kyseessä ei välttämättä olisi enää yleisistä lähteistä hankittavasta tiedosta vaan esimerkiksi toimivaltuutena sotilastiedusteluviranomaiselle tai rikostorjuntaviranomaiselle säädetystä suunnitelmallisesta tarkkailusta. Tilanteessa arviointiin vaikuttaisi toki se, onko kyse julkisuuden henkilöstä ja missä roolissa henkilö osallistuu keskusteluun tai päivitysten tekemiseen.

Lähtökohtaisesti säännöksessä tarkoitetussa tiedon hankinnassa olisi aina kyse sisällöstä ja sisällön seuraamisesta. Sisällön seuraamisen kautta toki voi toistua tietyt tahot tiedontuottajana, mutta itse tiedonhankinta ei ole tässä tapauksessa tapahtunut tiedontuottajan perusteella.

Pykälän tarkoittamassa tiedonhankinnassa voi syntyä tarve henkilötietojen tallentamiselle. Tallentamisessa ja käsittelyssä olisi noudatettava henkilötietojen käsittelystä Puolustusvoimissa annettua lakia.

Pykälän 1 momentissa säädettäisiin Puolustusvoimien toimivaltuudesta hankkia ja käsitellä tietoa yleisesti saatavilla olleista lähteistä. Tiedon hankinnan olisi kuitenkin liityttävä Puolustusvoimien tehtäviin, joten se ei voisi kohdistua mihin tahansa tietoon.

Pykälän 2 momentissa säädettäisiin oikeudesta käyttää teknisiä menetelmiä 1 momentissa säädetyn tiedon hankinnan toteuttamisessa. Säännös ei rajaisi tiedonhankinnan keinoja, vaan tietoa voitaisiin hankkia myös automatisoidusti. Näin ollen tiedonhankinta voisi tapahtua yksittäisen virkamiehen toimesta lehteä selaamalla tai tietoteknisin menetelmin algoritmia käyttäen. Vastaavasti tieto voitaisiin tallentaa käyttämällä kopiokonetta tai tallentamalla se tietokoneen ohjelmistoa käyttäen tietokoneen kovalevylle.

Pykälän 3 momentissa säädettäisiin yleisesti saatavilla olevien lähteiden tiedonhankinnan suojaamisesta, eli niin kutsutun kevyen peitteen käytöstä. Tarve tarkoitetulle peitteelle Puolustusvoimien muussa kuin sotilastiedustelutoiminnassa liittyy siihen, ettei Puolustusvoimien toiminta paljastuisi mahdollisen tietomurron yhteydessä. Esimerkiksi Puolustusvoimien tutkimustoiminta saattaa vaarantua, jos maanpuolustukselle uhkaa aiheuttava toimija saa tietoonsa, mihin aiheisiin Puolustusvoimien tutkimustoimintaa suunnataan.

Säännöksen tapauksessa kyse olisi tekaistujen tietojen antamisesta rekisteröitymisen yhteydessä tai profiilia luotaessa. Säännöksessä tarkoitetussa suojaamisessa olisi kiinnitettävä huomiota siihen, kuinka luotettavaa rekisteröitymistä tai profiilia palvelu edellyttää. Jos esimerkiksi keskustelupalstalle rekisteröitymisessä edellytetään ainoastaan nimen ja joidenkin osoitetietojen antamista sekä nimimerkin keksimistä, eikä tietoja tarkasteta sen kummemmin, kyseessä olisi säännöksessä tarkoitettu suojaaminen. Jos taas rekisteröityminen edellyttää maksutietojen antamista ja vahvaa tunnistautumista pankkitunnuksilla, kyse ei ole enää säännöksessä tarkoitetusta yleisesti saatavilla olevien lähteiden tiedonhankinnan suojaamisesta.

Rekisteröitymisessä käytettävä kevyt peite saattaa edellyttää esimerkiksi sähköpostiosoitteen luomista. Tällä voi olla merkitystä rekisteröitymisen lisäksi käyttäjätunnuksen tai profiilin ylläpidon kannalta. Sähköpostiosoitteen luomiseen pätisi samat periaatteet kuin edellä kuvattuihin palveluihin liityttäessä. Sähköpostiosoitetta ei saisi käyttää muuhun kuin kevytpeitteen luomiseen ja siihen liittyvien viestien vastaanottamiseen. Sähköpostin kautta ei voisi käydä keskustelua toisen henkilön kanssa, tai jos näin kävisi, olisi keskustelu päätettävä ilman aiheetonta viivytystä.

Selvää on se, että yleisesti saatavilla olevien lähteiden tiedonhankinnassa ei saisi ryhtyä suoraan kanssakäymiseen muiden esimerkiksi keskustelupalstalla tai sosiaalisen median ryhmässä olevien henkilöiden kanssa. Keskustelu ja keskusteluun osallistumisessa voidaan pääsääntöisesti katsoa olevan kyse rikostorjunnassa ja tiedustelutoiminnassa käytettävästä peitellystä tiedonhankinnasta. Toki voi syntyä tilanteita, joissa keskustelupalstalla tai ryhmässä pysyminen edellyttää aktiivisuutta. Tällöin viestinnän olisi oltava yleisellä tasolla eikä se saisi johtaa pidempään kommunikoitiin toisen ryhmän jäsenen kanssa.

Säännöksen tarkoitettu suojaaminen olisi tarkoituksenmukaista järjestää niin, että mahdollisimman pitkälle käytettäisiin pysyviä kevyt peitteitä, joiden käyttäjä toki voi vaihtua tilanteen mukaan. Tämä osaltaan helpottaa toiminnan laillisuusvalvontaa ja kevytpeitteiden käytön organisointia.

Esimerkiksi sosiaalisen median ryhmiä on monenlaisia. Karkeasti voidaan puhua julkisista, suljetuista ja salaisista ryhmistä. Ensimmäiseen näistä voi liittyä kuka vain ilman kummempia ryhmään pääsyprosesseja.

Suljetuissa ryhmissä ryhmään pääsy edellyttää ryhmään pääsyyn hyväksymistä. Nyt käsiteltävänä olevan säännöksen kannalta tämä tarkoittaisi sitä, että jos ryhmään pääsyn edellytyksenä on ainoastaan pyynnön esittäminen, ryhmä on selkeästi säännöksen tarkoittama yleisesti saatavilla oleva lähde. Jos ryhmään pääsy edellyttäisi vastaamista yksityiskohtaisiin kyselyihin henkilöstä itsestään, lähenisi toiminta jo tiedustelumenetelmien käyttöä, jolloin ryhmään pääsyä ei enää voitaisi katsoa yleisesti saatavilla olevien lähteiden tiedonhankinnaksi. Toisaalta, jos ryhmään pääsyn edellytyksenä olisi yleiseen kyselyyn vastaaminen esimerkiksi tiettyä asiaa koskevista mielipiteistä, kyse olisi pykälässä tarkoitetusta tiedonhankinnasta ja kevyt peitteen käytöstä.

Kolmantena ryhmätyyppinä voidaan mainita salaiset ryhmät, jotka eivät näy yleisesti käyttäjille ja edellyttävät pääsääntöisesti kutsua ryhmän ylläpitäjältä. Jos kutsu tällaiseen ryhmään tulisi, voitaisiin siihen liittyä. Ryhmän ylläpitäjän tai kutsun lähettäjän kanssa ei kuitenkaan saisi ryhtyä kanssakäymiseen. Käytännössä tilanteessa olisi pykälässä tarkoitetun toiminnan kannalta kutsun hyväksymisestä. Toki salaiseen ryhmäänkin pääsyn edellytyksenä voi olla kyselyyn vastaaminen, joka olisi mahdollista kevyt peitteen rajoissa, mutta vastausten olisi oltava yleisellä tasolla eikä ne saisi johtaa kanssakäymiseen ylläpitäjän tai ryhmänjäsenten kanssa.

Erilaisia teknisiä menetelmiä Puolustusvoimien tietoliikenteen ja tietoturvan suojaamiseksi, kuten VPN-palvelut, ei katsottaisi säännöksessä tarkoitetuksi suojaamiseksi.

Pykälän 4 momentin mukaan pääesikunta päättäisin niistä Puolustusvoimien hallintoyksiköistä, jotka voisivat käyttää 3 momentissa tarkoitettua yleisesti saatavilla olevien lähteiden suojaamista. Kaikilla Puolustusvoimien hallintoyksiköillä on tarve hankkia tietoa yleisesti saatavilla olevista lähteistä eikä säännös estäisi tätä. Kaikilla Puolustusvoimien hallintoyksiköillä ei kuitenkaan olisi tarvetta käyttää tiedon hankinnassaan suojaamista. joten nämä hallintoyksiköt voitaisiin määritellä tarkemmin pääesikunnan päätöksellä. Päätöksenmukaisilla hallintoyksiköillä olisi oltava perusteltu tarve toimintansa suojaamiseksi. Esimerkiksi voidaan arvioida, että kaikilla varusmieskoulutusta antavilla yksiköillä ei ole tarvetta yleisesti saatavilla olevien lähteiden tiedonhankinnan suojaamiseen.

Keskeistä on, että suojaamisen käyttö on keskitettyä tiettyihin Puolustusvoimien hallintoyksiköihin.

Pykälän 5 momentissa säädettäisiin suojaamisen käytöstä vastaavasta virkamiehestä, joka olisi 4 momentissa tarkoitetussa päätöksessä tarkoitetun Puolustusvoimien hallintoyksilön päällikkö. Päällikkö vastaisi myös suojaamisen käytöstä hallintoyksikössään. Yleisesti pykälässä tarkoitettujen toimenpiteiden laillisuutta valvottaisiin osana Puolustusvoimien laillisuusvalvontaa.

8 c §. *Yleisesti saatavilla olevista lähteistä hankitun tiedon hävittäminen.* Pykälässä säädettäisiin 8 b §:ssä tarkoitetun tiedonhankinnan aikana saatujen tallenteiden ja asiakirjojen tarkastamisesta ja tietojen hävittämisestä. Selvyyden vuoksi 1 momentissa todettaisiin tiedonkäsittelyä koskeva pääsääntö, että viranomaisen tulee hävittää viipymättä sellaiset tiedot, joita ei tehtävien suorittamiseksi tarvita.

Pykälän 2 momentissa olisi informatiivinen viittaus henkilötietojen käsittelystä Puolustusvoimissa annettuun lakiin.

36 a §. *Viran haettavaksi julkistaminen.* Pykälään lisättäisiin uusi 3 momentti. Pykälän 3 momentin mukaan täytettäessä muu kuin 1 tai 2 momentissa tarkoitettu virka tai virkasuhde hakumenettelyssä Puolustusvoimat voisi jättää ilmoittamatta virkaan tai virkasuhdetta hakeneiden nimet ja nimitetyn nimen muille hakijoille, jos haettavan tehtävän luonne sitä välttämättä edellyttää. Välttämättömyydellä tarkoitettaisiin viimesijaisuutta, jolloin Puolustusvoimien olisi harkittava tehtävän täytön yhteydessä viran tai virkasuhteen täyttämisen tapaa viraston henkilöstö- ja organisaatioturvallisuuden, tehtävään liittyvien uhkien, sotilastiedustelun suojaamisen tai muun erittäin tärkeän yleisen tai yksityisen edun näkökulmasta ja punnittava välttämättömyys -edellytyksen täyttymistä. Lähtökohtana on, että avoin viranhaku olisi edelleen pääsääntö, ja virkojen ja virkasuhteiden täyttö haettavaksi julistamatta olisi poikkeusmenettely.

Puolustusvoimien tiettyjen virkojen erityiseen luonteeseen kuuluu maanpuolustuksen erityisosaaminen, kansallisen turvallisuuden suojaaminen, sotilastiedustelu sekä rikostorjunnan salaiset tiedonhankintakeinot ja salaiset pakkokeinot. Virkamiehen tehtävän laadun mukaan on henkilöllisyyttä suojattava tehokkaasti ja pidettävä se salassa alusta lukien.

Esimerkiksi keskeiset sotilastiedusteluun liittyvät tehtävät, joissa virkamiehen henkilöllisyyttä on suojattava tehokkaasti jo rekrytointivaiheessa liittyvät sotilastiedustelun operatiivisiin tehtäviin ja niiden tukitehtäviin sekä tietojen analyysitehtäviin. Operatiivisessa toiminnassa esimerkiksi tietolähteiden suojaamisen kannalta on ensiarvoisen tärkeää, että tietolähdettä ei

voida tunnistaa sotilastiedustelun virkamiehen kautta. Esimerkiksi sotilastiedustelun operatiivisen toiminnan tukitehtäviin sisältyvät muun muassa operatiivisten lakimiesten sekä operaatioihin liittyvät teknologia-, talous- ja henkilöstöhallinnon tehtävät.

Yksi keskeinen elementti Puolustusvoimien toiminnan kokonaisuudessa on pääsy tietoon virassa tai virkasuhteessa ja tiedon kumuloituminen. Puolustusvoimien tehtäviä suorittavat ja tietoja omaavat virkamiehet voivat olla vieraiden valtioiden tiedonhankinnan ja vaikuttamisyritysten kohde. Virkamiehiä on suojattava painostukselta, kiristykseltä, väkivallan uhalta ja värväysyrityksiltä. Henkilöllisyyden paljastuminen merkitsee, että virkamies ei voi toimia tehtävässä värväysyritysten, hengen tai terveyden vaaran ja tehtävän suorittamisen vaarantumisen vuoksi. Puolustusvoimien hallinto- ja teknologiatehtävissä toimivien henkilöllisyyksien suojaamista arvioitaisiin samoin perustein kuin suojataan esimerkiksi sotilastiedustelun operatiivisen tai analyysitehtävissä toimivien henkilöllisyyksiä.

Arvioitaessa 3 momentissa tarkoitettua välttämättömyyttä, olisi huomioon otettava Puolustusvoimien henkilöstö- ja organisaatioturvallisuus, täytettävä tehtävä ja siihen liittyvät uhat sekä muu erittäin tärkeä yleinen tai yksityinen etu.

Viran tai virkasuhteen täyttämisestä olisi ilmoitettava hakijoille toimittamalla nimityspäätös tiedoksi. Tällöin olisi ilmoitettava täytettävänä ollut virka tai virkasuhde, päätöksen tehnyt viranomainen sekä nimityspäivä. Menettelyllä turvataan muutoksenhakuoikeuden käyttämisen mahdollisuutta. Muutoksenhakuoikeuden turvaaminen virkaan nimittämistä koskeviin päätöksiin mahdollistaa nimityspäätöksen jälkikäteisen muuttamisen valituksen seurauksena ja edistää osaltaan hakijoiden tasa-arvoa ja yhdenvertaisuutta. Julkisen hakumenettelyn kohdalla ei voida poissulkea mahdollisuutta, että hakijana voi olla toimintansa salassa pitävä valtiollinen toimija, jolloin muiden hakijoiden tai valitun tietojen leviäminen on riski.

Puolustusvoimien virkoja ja virkasuhteista täytettäessä lähtökohtana säilyisi edelleen avoin viranhaku.

Säännöksellä ei olisi vaikutusta julkisuuslain soveltamiseen. Tietopyyntö arvioitaisiin julkisuuslain mukaan.

7.3 Rikoslaki

7 §. *Valtionrajarikos*. Pykälän 2 momentin mukaan valtionrajanrikoksesta ei tuomittaisi ulkomaalaista, joka on tehnyt valtionrajarikoksen sotilastiedustelusta annetun lain 78 §:n 5 momentin perusteella. Kyse on tilanteista, joissa Suomea avustanut henkilö joutuu hengen ja terveyden vaaraan lähtömaassaan ja henkilön hengen ja terveyden suojaamiseksi on välttämätöntä saada kyseinen henkilö pois lähtömaastaan. Tilanteissa kohtuussyistä ja selvyyden vuoksi olisi aihetta säätää erikseen valtionrajarikosta koskevasta syytevapaudesta.

Poistamalla edellä viitatuilta osin teon rangaistavuus, henkilö ei syyllistyisi sotilastiedusteluviranomaisen hänelle sotilastiedustelusta annetun lain 78 §:n 5 momentin perusteella antamien väärien asiakirjojen käytöllä rikoslain 17 luvun 7 §:ssä tarkoitettuun tekoon. Toisaalta henkilö voitaisiin joutua järjestämään asian sensitiivisyyden vuoksi Suomen rajan yli muuten kuin virallisen rajaylityspaikan kautta.

Tilanteissa henkilö saattaa jäädä Suomeen, mikä edellyttäisi normaaleja maahanmuuttoprosesseja tai turvapaikanhakua, mutta tilanteissa Suomi saattaisi olla myös vain kauttakulkumaa, josta henkilö siirretään kolmanteen valtioon.

7.4 Laki Finanssivalvonnasta

71 d §. *Oikeus luovuttaa tietoja suojelupoliisille ja sotilastiedusteluviranomaiselle.* Pykälän 1 momenttiin lisättäisiin viittaus sotilastiedusteluviranomaiseen. Lisäyksen myötä sotilastiedusteluviranomaisella olisi toimialallaan vastaavat oikeudet saada tietoja Finanssivalvonnalta kuin suojelupoliisilla omalla toimialallaan.

Säännöksen mukaan Finanssivalvonnalla olisi oikeus luovuttaa salassapitosäännösten estämättä pyynnöstä tietoja sotilastiedusteluviranomaiselle, jos tiedot olisivat välttämättömiä tiedustelutehtävän kannalta. Tiedustelutehtävällä tarkoitetaan sotilastiedustelusta annetun lain 10 §:n 9 kohdan mukaan pääesikunnan tiedustelupäällikön sotilastiedusteluviranomaiselle antamaa toimeksiantoa tiedustelutiedon hankkimiseksi 4 §:ssä tarkoitetusta sotilastiedustelun kohteesta, joka perustuu ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteisen kokouksen valmistelevasti käsittelemiin painopisteisiin tai 14 §:ssä tarkoitettuun tietopyyntöön.

Ehdotetussa säännöksessä ei luovutettavia tietosisältöjä voida luetella kattavasti, joten tietojen luovutus olisi sidottu välttämättömyyskriteeriin.

Pykälän 2 momenttiin esitettäisiin vastaava muutosta, jonka mukaan Finanssivalvonnalla olisi oikeus luovuttaa salassapitosäännösten estämättä oma-aloitteisesti sotilastiedusteluviranomaiselle Finanssivalvonnan hallussa olevia tietoja liittyen rahanpesuun tai terrorismin rahoittamiseen, pakotesääntelyn kiertämiseen tai muihin epätavallisiin liiketoimiin liittyvistä järjestelyistä, joilla varoja siirretään kolmansiin maihin ja toimien epäillään liittyvän sotilaalliseen toimintaan tai niillä vaarannettavan kansallista turvallisuutta, jos tiedot ovat tarpeellisia sotilastiedusteluviranomaisen toimialaan kuuluvien sotilaallisen toiminnan ja kansallisen turvallisuuden suojaamiseksi sitä vakavasti uhkaavalta toiminnalta.

Lisäksi ehdotettaisiin, että pykälän 1 ja 2 momentissa tarkoitettujen tietojen luovuttamiseen sovelletaan lain 71 §:n 5 momenttia, jossa säädetään niistä tilanteista, jolloin Finanssivalvonta ei saa luovuttaa tietoja, ellei se ole saanut suostumusta tietojen luovuttamiseen.

7.5 Laki harmaan talouden selvitysyksiköstä

6 §. *Velvoitteidenhoitoselvityksen käyttötarkoitus.* Pykälän 39 kohtaa muutettaisiin vaihtamalla piste puolipisteeksi.

Pykälään lisättäisiin uusi 40 kohta. Sen mukaan velvoitteidenhoitoselvitys voitaisiin laatia tukemaan sotilastiedustelusta annetussa laissa tarkoitettua sotilastiedustelua. Ehdotettu muutos koskisi sotilastiedustelusta annetun lain 3 §:ssä säädetty sotilastiedustelun tarkoitusta annettavista selvityksistä. Ehdotettu muutos uudeksi 40 kohdaksi mahdollistaa jatkossa velvoitehoitoselvityksen laatimisen tukemaan sotilastiedusteluviranomaisen toimintaa. Sotilaallisia ja kansalliseen turvallisuuteen kohdistuvia uhkia voidaan itsessään pitää niin vakavina, että velvoitteidenhoitoselvityksiä tulisi voida laatia tukemaan sotilastiedusteluviranomaisen tehtävien hoitamiseksi.

Harmaan talouden yksiköstä annetun lain 7 §:n mukaan selvitysyksiköllä on oikeus saada salassapitovelvollisuuden estämättä viranomaiselta ne velvoitteidenhoitoselvityksen laatimiseksi välttämättömät tiedot, jotka velvoitteidenhoitoselvitystä pyytävä viranomainen on oikeutettu saamaan selvityspyynnössä kuvattua käyttötarkoitusta varten. Osana Puolustusvoimia sotilastiedusteluviranomaisen oikeudesta saada tietoja viranomaisilta säädetään puolustusvoimista annetun lain 17 §:ssä. Säännöksen mukaan Puolustusvoimilla on

oikeus saada viranomaiselta sekä julkista tehtävää hoitamaan asetetulta yhteisöltä laissa säädetyn tehtävän suorittamiseksi välttämättömät tiedot ja asiakirjat salassapitovelvollisuuden estämättä, jollei sellaisen tiedon tai asiakirjan antamista Puolustusvoimille tai tietojen käyttöä todisteena ole laissa kielletty tai rajoitettu.

Kun sotilastiedusteluviranomaisen tehtäviin ja kansallisen turvallisuuden suojaamiseen liittyviin tiedollisiin toimivaltuuksiin sovellettava sääntely hajautuu eri säädöksiin, sääntelyn yhdellä kertaa tapahtuva täsmentäminen olisi käytännössä hyvin vaikeasti toteutettavissa. Sotilastiedusteluviranomaisen tehtävät ja kansallisen turvallisuuden suojaaminen on siviili- ja sotilastiedusteluviranomaisen tietojen saannin perusteeksi sinällään varsin väljä, että tietojen saannin peruste on perusteltua kytkeä kiinteämmin siviili- ja sotilastiedustelun tarkoitukseen sekä tiedustelulaeissa määriteltyihin siviili- ja sotilastiedustelun kohteisiin. Tämän vuoksi on perusteltua, että sotilastiedusteluviranomaiseen liittyviä tiedollisia toimivaltuuksia koskevat säännökset kytketään sotilastiedustelusta annetun lain 4 §:ssä tarkoitettuun uhkaavaan toimintaan silloin, kun tällainen kytkentä ilmenee muusta asiayhteydestä. Sotilastiedustelusta annetussa laissa, ottaen huomioon Puolustusvoimista annetun lain 17 §:n, tiedollisten toimivaltuuksien osalta kytkennän voi katsoa ilmenevän asiayhteydestä ja sotilastiedustelusta annetun lain 104 §:ssä kytkentä on todettu myös nimenomaisesti.

Käytettäessä tietojen luovuttamisen perusteena sotilastiedustelun tiedustelutehtävää edellytetään sääntelyltä siten yksityiskohtaisuutta, että henkilötietojen suojaan liittyvät käyttötarkoitussidonnaisuus ja tarpeellisuusvaatimus täyttyvät. Sotilastiedustelusta annetun lain 4 §:ssä luetellut kohteet ovat luonteelta sotilaallisia, jolloin uhka katsotaan aina vakavaksi, tai uhkia, jotka vakavasti uhkaavat kansallista turvallisuutta.

Velvoitteidenhoitoselvityksen tarkoituksena on oikean ja riittävän kokonaiskuvan antaminen organisaatiosta sekä sen julkisoikeudellisten velvoitteiden hoitamisesta viranomaisten rekistereissä olevien tietojen perusteella. Velvoitteidenhoitoselvityksessä kuvataan myös organisaation välittömät ja välilliset organisaatio- ja organisaatiohenkilökytkennät. Tämän kaltaisen ajantasaisen ja kattavan kokonaiskuvan saaminen organisaatiosta on ensisijaisen tärkeää, kun selvitetään sellaisten taloudellisten toimijoiden taustoja, joiden epäillään liittyvän kansallista turvallisuutta vaarantavaan toimintaan. Velvoitteidenhoitoselvitykset olisivat myös tärkeitä selvitettäessä yritysjärjestelyitä, joiden epäillään liittyvän vieraan valtion vaikuttamistoimintaan.

7.6 Tuloverolaki

92 b §. *Todistelupalkkiot, vihjepalkkiot ja tietolähdetoiminnasta maksettavat palkkiot***.** Luonnollisen henkilön saaman tulon veronalaisuudesta säädetään tuloverolaissa. Suomen verojärjestelmä perustuu laajaan tulokäsitteeseen, jonka mukaan veronalaista tuloa ovat verovelvollisen rahana tai rahanarvoisena etuutena saamat tulot, jos niitä ei ole erikseen säädetty verovapaiksi.

Pykälän *3 kohdan* mukaan veronalaista tuloa ei ole viranomaisen maksama palkkio sotilastiedustelusta annetussa laissa (590/2019) ja poliisilaissa (872/2011) tarkoitetulle tietolähteelle tiedustelutehtävien hoitamiseksi merkityksellisten tietojen hankkimisesta sekä rikostorjunnasta Rajavartiolaitoksessa annetussa laissa (108/2018) tarkoitetulle tietolähteelle rajaturvallisuuden ylläpitämiseen liittyvien tehtävien hoitamiseksi merkityksellisten tietojen hankkimisesta.

Kohtaan lisättäisiin uudeksi verottoman palkkion saajaksi tiedusteluviranomaista avustanut henkilö. Tilanteissa olisi kyse esimerkiksi ehdotetun sotilastiedustelusta annetun lain 42 §:n 2

momentissa tarkoitetusta avustamisesta. On tärkeää, että kyseisten toimenpiteiden avustamisessa auttaneiden henkilöllisyys ei paljastu verotuksen yhteydessä. Palkkion verovapautta puoltaa myös se, että avustajalle maksettavat palkkiot olisivat varsin satunnaisia ja vähäisiä.

7.7 Rajavartiolaki

3 §. *Rajavartiolaitoksen tehtävät.* Pykälän 3 momenttiin lisättäisiin säännös Rajavartiolaitoksen osallistumisesta sotilastiedusteluun. Rajavartiolaitoksen osallistumisesta sotilastiedusteluun säädettäisiin tarkemmin ehdotettavassa 25 a §:ssä ja toimivaltuuksista sotilastiedustelusta annettuun lakiin ehdotetussa 18 a §:ssä.

25 a §. *Rajavartiolaitoksen osallistuminen sotilastiedusteluun.* Pykälä olisi uusi. Pykälässä säädettäisiin Rajavartiolaitoksen osallistumisesta sotilastiedusteluun.

Pykälän 1 momentissa säädettäisiin, että Rajavartiolaitos osallistuisi pyynnöstä sotilastiedusteluun hankkimalla tietoja ja tekemällä toimenpiteitä sotilastiedusteluviranomaisten tiedustelutehtävien tukemiseksi. Tehtävä olisi Rajavartiolaitokselle uusi.

Sotilastiedustelusta annetun lain 3 §:n mukaan sotilastiedustelun tarkoituksena on hankkia ja käsitellä tietoa ylimmän valtiojohdon päätöksenteon tukemiseksi ja Puolustusvoimien pykälässä erikseen lueteltujen tehtävien suorittamiseksi Suomeen kohdistuvasta tai Suomen turvallisuusympäristön kannalta merkityksellisestä sotilaallisesta toiminnasta, vieraan valtion toiminnasta tai muusta sellaisesta toiminnasta, joka vakavasti uhkaa Suomen maanpuolustusta tai vaarantaa yhteiskunnan elintärkeitä toimintoja.

Rajavartiolaitos osallistuisi sotilastiedusteluun tukemalla sotilastiedusteluviranomaista tämän pyynnöstä tiedustelutehtävään liittyvän yksittäisen toimenpiteen suorittamisessa. Sotilastiedustelusta annetun lain 10 §:n 9 kohdan määritelmäsäännöksen mukaan tiedustelutehtävällä tarkoitetaan pääesikunnan tiedustelupäällikön sotilastiedusteluviranomaiselle antamaa toimeksiantoa tiedustelutiedon hankkimiseksi sotilastiedustelun kohteesta, joka perustuu ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteisen kokouksen valmistelevasti käsittelemiin painopisteisiin tai niiden mukaiseen tietopyyntöön. Sääntelyllä ei olisi tarkoitus muuttaa nykyisten tiedusteluviranomaisten asemaa, eikä Rajavartiolaitos olisi tehtävässään sotilastiedusteluviranomainen. Kyse olisi lyhytaikaisesta, yksittäisten tiedustelutehtävään liittyvien tehtävien tai toimenpiteiden suorittamisesta ja ne tapahtuisivat aina sotilastiedusteluviranomaisen pyynnöstä. Pyyntö voisi olla tietyissä tilanteissa ennalta tehty tai se voisi tapahtua nopeampaa reagointia vaativissa tilanteissa viranomaisten välisten päivystysjärjestelyjen kautta.

Pykälän 2 momentti sisältäisi informatiivisen viittauksen siitä, että Rajavartiolaitoksen toimivaltuuksista sotilastiedusteluun osallistumisessa säädettäisiin sotilastiedustelusta annetussa laissa.

7.8 Laki henkilötietojen käsittelystä Rajavartiolaitoksessa

32 §. *Henkilötietojen luovuttaminen toiselle rikosasioiden tietosuojalaissa tarkoitetulle toimivaltaiselle viranomaiselle.* Pykälään lisättäisiin uusi 2 momentti, jossa säädettäisiin radioteknisen valvonnan tietojen luovuttamisesta salassapitosäännösten estämättä Puolustusvoimille sotilastiedustelusta annetussa laissa säädettyjä tehtäviä varten. Kyse olisi

henkilötiedoista ja muista tiedoista, joita Rajavartiolaitos käsittelee lain 15 b §:n mukaisesti radioteknisen valvonnan suorittamiseksi rajavartiolain 29 a–29 c §:ssä säädetyin edellytyksin. Radiotekniselläl valvonnalla tarkoitetaan rajavartiolain 29 a §:n 1 momentin mukaan muulla teknisellä laitteella kuin tutkalla tapahtuvaa radiotaajuisten sähkömagneettisten aaltojen ja radiolaitteiden havaitsemista, tunnistamista, paikantamista, yksilöintiä ja seurantaa sähkömagneettisten aaltojen ominaisuuksien avulla. Rajavartiolain 29 b §:ssä säädetään sähköisen viestinnän tietojen käsittelystä radioteknisessä valvonnassa ja 29 c §:ssä radioteknisen valvonnan tietojen käsittelystä ja hävittämisestä.

7.9 Laki henkilötietojen käsittelystä Puolustusvoimissa

37 a §. *Sotilastiedusteluviranomaisen oikeus ylläpitää henkilörekisteriään.* Pykälä olisi uusi. Säännöksien tarkoituksena olisi edistää tietosuojaa ja varmistaa, että sotilastiedusteluviranomaisen rekisteriin tallettamat tiedot ovat oikeita ja ajantasaisia. Koska sotilastiedusteluviranomaisen henkilörekisteri sisältää maanpuolustusta ja kansallisen turvallisuuden suojaamista varten käsiteltäviä tietoja, kohdistuu siihen erityisiä tietoturva- ja tietosuojariskejä ja erityisen vakava laittoman tiedustelutoiminnan uhka. Niiden hallitsemiseksi rekisteri on luokiteltu korkean tietoturvallisuuden tasolle, jonka vuoksi siitä ei ole automatisoituja yhteyksiä ulos. Tämän vuoksi myöskään tietojen päivittämistä ei voida tehdä samalla tavalla kuin alemman tietoturvallisuustason järjestelmissä, joihin tietoja voidaan päivittää tekemällä rekisteröityihin henkilöihin kohdistuvia suoria kyselyjä. Keskeinen vaatimus on, ettei alemman tietosuojan rekisteriin siirry kyselyn yhteydessä korkeamman tietosuojatason järjestelmästä tietoa. Tämän vuoksi tiedon päivittäminen korkean tietoturvatason rekisteriin on toteutettava siten, että luovuttavaan rekisteriin ei muodostu loki- tai muuta tietojoukkoa siitä, mitä tietoja on päivitetty sotilastiedusteluviranomaisen henkilörekisteriin. Sotilastiedusteluviranomaisen tiedonhankinnan kohteiden tai intressien paljastuminen ulkopuolisille tai kohteille itselleen voisi vaarantaa maanpuolustuksen tai kansallisen turvallisuuden.

Esitettyjä säännöksiä ei voida pitää yksityisyyden suojan kannalta erityisen merkittävänä, sillä vertailun mahdollistaminen ei laajentaisi tietosisältöä, johon sotilastiedusteluvirnaomaisella on jo tällä hetkellä oikeus. Säännös selventäisi ja tekisi lainsäädäntöä tarkkarajaisemmaksi siltä osin kuin sotilastiedusteluviranomaisella on oikeus saada tarpeellisia henkilötietoja tehtäviensä suorittamiseksi ja rekisterinsä ylläpitämiseksi teknisen käyttöyhteyden avulla tai tietojoukkona. Säännöksellä ei siten muutettaisi nykyistä oikeustilaa, mutta huomioitaisiin teknisen kehityksen vaatimukset tietosuojalle ja rekisterin oikeellisuudelle.

Pykälän 1 momentissa kytkettäisiin oikeus suorittaa vertailu lainmukaisiin tiedonsaanti- tai luovutusoikeuksiin. Säännöksessä toistettaisiin selkeyden vuoksi, että sotilastiedusteluviranomaisella olisi oikeus saada tietoja tehtäviensä suorittamiseksi salassapitosäännösten estämättä. Luovuttavasta rekisteristä kerättyä laajempaa tietojoukkoa verrattaisiin automaattisessa käsittelyssä sotilastiedusteluviranomaisen rekisterin henkilötietoihin. Henkilörekistereitä ei suoraan yhdistettäisi toisiinsa, vaan niitä verrattaisiin erillisellä teknisellä alustalla. Riittävä vertailutietojoukko arvioitaisiin tapauskohtaisesti. Se voisi kohdistua esimerkiksi rekisterin muutostietoihin, tiettyyn otantaan tai koko rekisterin sisältöön. Säännöksen tulkinnassa ja soveltamisessa olisi yksittäistapauksessa aina otettava huomioon myös henkilötietojen käsittelyn perusperiaatteet.

Ennen tietojen siirron aloittamista selvitettäisiin, miten tarvittavat vertailu- ja muut tiedot voidaan teknisesti poimia eri rekistereistä ja tietojärjestelmistä ja yhdistää sähköiseen muotoon niin, että tietosisältö täyttää vertailun tarpeet, eikä tietojen poimiminen ja yhdistäminen

aiheuttaisi tarpeetonta lisätyötä ja kustannuksia tiedon luovuttavalle taholle. Samalla minimoitaisiin ylimääräisten tietojen käsittelyn tarve.

Pykälän 1 momentissa säädettäisiin myös tietojen hävittämisvelvollisuudesta. Vertailutietojen analysoinnin ja käsittelyn jälkeen tarpeettomat vertailutiedot tulisi poistaa välittömästi sotilastiedusteluviranomaisen tietovarannoista. Käytännössä tietoja verrattaisiin tietoturvallisessa ympäristössä, jonka jälkeen aiheettomiksi osoittautuvat tiedot välittömästi hävitettäisiin. Pykälässä jaettaisiin selkeyden vuoksi henkilötietojen käsittelyä tarkemmin osiin. Henkilötietojen käsittelyllä tarkoitetaan lähtökohtaisesti kaikkia henkilötietojen käsittelyyn liittyviä toimia. Tässä yhteydessä mainittaisiin erillisenä kynnyksenä henkilötietojen tallentaminen. Jako ilmentäisi sitä, ettei sotilastiedusteluviranomaisen rekisteriin tulisi vertailun seurauksena päätyä henkilöitä, joiden osalta laissa säädetyt edellytykset eivät ole täyttyneet.

Pykälän 2 momentissa olisi kyse niiden henkilötietojen tuomisesta vertailua varten sotilastiedusteluviranomaisen tietojärjestelmän erilliseen osaan, joiden alkuperäiseksi tai muuksi kuin alkuperäiseksi käyttötarkoitukseksi on säädetty maanpuolustus tai kansallinen turvallisuus. Tietojen käsittely tapahtuisi kokonaisuudessaan korkean tietoturvatason tietojärjestelmässä ilman tarpeetonta tietojen siirtoa alemman tietoturvatason järjestelmiin, mikä olennaisesti korottaisi tietoturvallisuutta. Menettely olisi tarpeellinen myös edellä kuvattujen tietoturvavaatimusten johdosta.

Säännöksen tarkoitus olisi mahdollistaa tietojen käyttö niissä tilanteissa, joissa tarve samojen tietojen käsittelyyn on toistuva. Tämän johdosta toisin kuin 1 momentissa tietoja ei olisi poistettava välittömästi vertaamisen jälkeen, mikäli tiedossa olisi että vertailua jouduttaisiin tekemään toistuvasti. Kerätty tietojoukko olisi kuitenkin poistettava heti, kun tietojen käsittelyn tarkoitus on saavutettu. Tietojoukolla tarkoitettaisiin tässä yhteydessä tarkemmin määrittelemätöntä käyttötarkoituksensa perusteella rajautuvaa ryhmää, joka voisi olla esimerkiksi rekisteri, rekisterin osa, tietokanta tai koontitieto. Säännöksessä ei määriteltäisi erikseen vertailtavia henkilötietoluokkia. Kyseeseen voisi siten tulla myös erityiset henkilötietoryhmät. Menettelyä tulisi soveltaa ainoastaan niissä tilanteissa, joissa katsotaan olevan välttämätöntä siirtää laajempi tietojoukko toisesta tietojärjestelmästä tietyssä määritellyssä tarkoituksessa tapahtuvan henkilötietojen käsittelyn mahdollistamiseksi. Kerättyjä tietoja tulisi säilyttää erillään muista tiedoista. Käytännössä tämä tarkoittaisi, että tietoja tulisi säilyttää tietojärjestelmän osassa, johon pääsyoikeus on erityisesti rajattu. Kyseisiä tietoja käytettäisiin maanpuolustukseen ja kansallisen turvallisuuden suojaamiseksi, joka olisi joko tietojen alkuperäinen käyttötarkoitus tai niille säädetty muu kuin alkuperäinen käyttötarkoitus.

8 Voimaantulo

Ehdotetaan, että lait tulevat voimaan mahdollisimman pian.

9 Suhde muihin esityksiin

Esityksen antamisen aikaan eduskunnassa on käsittelyssä hallituksen esitys eduskunnalle laiksi perustuslain 10 §:n muuttamisesta (HE 50/2026). Nyt käsiteltävänä oleva esitys ei liity mainittuun hallituksen esitykseen ja esitys voidaan käsitellä voimassa olevan perustuslain mukaisessa järjestyksessä.

Esitykseen liittyy sisäministeriössä valmisteltavana oleva hallituksen esitys eduskunnalle siviilitiedustelulainsäädännön muuttamisesta. Valmisteltavassa esityksessä siviilitiedustelua koskevaan lainsäädäntöön tehtäisiin vastaavat muutokset, mitä käsiteltävänä olevassa

hallituksen esityksessä ehdotetaan. Hallituksen esitys on tarkoitus saattaa eduskunnan käsiteltäväksi syysistuntokaudella 2026. Hallituksen esitykset edellyttävät yhteensovittamista eduskunnassa.

10 Suhde perustuslakiin ja säätämisjärjestys

10.1 Yleiset lähtökohdat

Esitykseen sisältyy sääntelyä, joka on merkityksellistä perustuslaissa säädettyjen perusoikeuksien kannalta; sotilastiedustelutoiminnassa käytettävillä toimivaltuuksilla puututaan yksilön perusoikeuksiin. Perustuslain kannalta merkityksellisimpiä ovat säännösehdotukset, joilla annetaan viranomaisille uusia yksilöön kohdistuvia toimivaltuuksia tai joilla muuten rajoitettaisiin yksilön oikeuksia tai toimintavapautta.

Vaikka tiedustelumenetelmien käytöllä puututtaisiin joihinkin perusoikeuksiin, kuten perustuslain 10 §:n 1 momentissa säädettyyn yksityiselämän suojaan, pyritään sotilastiedustelusta annetun lain soveltamisella kuitenkin suojaamaan ja turvaamaan muita perusoikeuksia, kuten perustuslain 7 §:ssä turvattua oikeutta elämään ja henkilökohtaiseen turvallisuuteen sekä perustuslain 1 luvussa säädettyjä valtiojärjestyksen perusteita, kuten valtion itsemääräämisoikeutta.

Ihmisten kollektiivinen turvallisuus samoin kuin yhteiskunnan elintärkeät toiminnot ja järjestäytynyt yhteiskuntaelämä ovat niin tärkeitä suojeluintressejä, että tiedustelusääntelylle on olemassa painava yhteiskunnallinen tarve ja perusoikeusjärjestelmän kannalta hyväksyttävä peruste.

Hyväksyttävänä perusteena pidetään myös kansallista turvallisuutta, jota koskien perustuslakivaliokunta on ottanut kantaa viimeaikaisessa lausuntokäytännössään. Viimeaikaisessa lausuntokäytännössä perustuslakivaliokunta on todennut, että valtion tulee pyrkiä takaamaan kansallinen turvallisuus sekä yleinen järjestys kaikissa olosuhteissa (PeVL 16/2022 vp, kappale 10). Perusoikeuksien välisessä intressipunninnassa on lisäksi otettava huomioon ehdotettujen toimien taustalla olevat intressit etenkin, jos toimet voivat ääritapauksessa palautua jopa henkilökohtaisen turvallisuuden perusoikeuteen (PeVL 37/2022 vp, kappale 8 ja siinä viitatut PeVL 16/2022 vp, kappale 5, ks. myös PeVL 5/1999 vp, s. 2 /II, ks. myös esim. PeVL 36/2020 vp, s. 3, PeVL 15/2018 vp, s. 8).

Tiedustelumenetelmien valtiosääntöoikeudellisessa arvioinnissa voidaan perustuslakivaliokunnan mielestä (PeVL 36/2018 vp.) osin tukeutua rikostorjunnan salaisia tiedonhankintakeinoja ja salaisia pakkokeinoja koskevaan valiokunnan käytäntöön (esim. PeVL 32/2013 vp, PeVL 67/2010 vp, PeVL 66/2010 vp, PeVL 5/1999 vp). Samalla on kuitenkin oikeudellisesti eroteltava ne seikat, jotka oikeuttavat sääntelyn eroavaisuuden. Salaisia tiedonhankintakeinoja ja salaisia pakkokeinoja koskeva käytäntö ei perustuslakivaliokunnan käsityksen mukaan siten ole sellaisenaan ja varauksitta sovellettavissa tiedustelun tiedonhankintamenetelmiä koskevaa lainsäädäntöä valtiosääntöoikeudellisesti arvioitaessa. Tiedustelumenetelmiä on arvioitava menetelmäkohtaisesti vastaavia salaisia tiedonhankintamenetelmiä ja salaisia pakkokeinoja koskeva perustuslakivaliokunnan käytäntö huomioon ottaen siten, että tiedustelutoiminnan erityinen luonne otetaan asianmukaisesti huomioon. Perustuslakivaliokunta painottaa, että yksityiselämän ja henkilötietojen suoja tulee suhteuttaa toisiin perus- ja ihmisoikeuksiin sekä muihin painaviin yhteiskunnallisiin intresseihin (PeVL 14/2018 vp, s. 6 ja PeVL 5/1999 vp, s. 2/II).

Sotilastiedustelusta annettu laki tuli voimaan 1.6.2019. Lain mukaan sotilastiedustelussa voidaan hankkia tietoa ainoastaan laissa tyhjentävästi luetelluista kohteista, jotka on säädetty mahdollisimman yksilöidysti tiedustelutoiminnan erityispiirteet huomioon ottaen. Sotilastiedustelun kohteet ovat useimmiten valtioita tai muita julkisyhteisöjä, jotka jäävät perussoikeussuojan ulkopuolelle (HE 309/1993 vp, PeVL 9/2015 vp ja PeVL 4/2018); perusoikeudet suojaavat luonnollisia henkilöitä. Myös tiedustelumenetelmistä on säädetty mahdollisimman tarkkarajaisesti ja täsmällisesti.

Tässä hallituksen esityksessä ehdotetuilla muutoksilla on tarkoitus säätää eräiden tiedustelumenetelmien osalta tarkennuksista, joiden myötä tiedustelutoiminta voitaisiin kohdentaa ja kohdistuisi teknologian kehittyessä entistä paremmin tarkoitettuun kohteeseen aiempaa tehokkaammin. Lisäksi muutoksilla otettaisiin huomioon turvallisuusympäristössä tapahtuneet muutokset. Näiden lähtökohtien edistämisellä voidaan katsoa olevan perusoikeusmyönteisiä vaikutuksia.

Ehdotuksessa sotilastiedustelua koskevan lain muuttamista koskevat säännökset määrittäisivät viranomaisen toimivaltuudet mahdollisimman tarkasti ja siten, että valtuuksien käyttö olisi sallittu vain tehtävien edellyttämässä laajuudessa.

Ehdotetun lain mukaiset valtuudet puuttua kansalaisten perusoikeuksiin kuuluisivat vain virkavastuulla toimiville virkamiehille, jotka olisivat vastuussa myös heitä pyynnöstä avustavien henkilöiden toimista.

Toimivaltuuksia koskevia säännösehdotuksia on tarkasteltava kokonaisuutena voimassa olevan lain kanssa, etenkin sotilastiedustelutoimintaa rajoittavia yleisiä periaatteita vasten. Sotilastiedustelusta annetussa laissa säädetään yksityiskohtaisesti toimintaa koskevista, toiminnan läpileikkaavista periaatteista. Näitä ovat perusoikeuksien ja ihmisoikeuksien kunnioittaminen (5 §), suhteellisuusperiaate (6 §), vähimmän haitan periaate (7 §), tarkoitussidonnaisuuden periaate (8 §) ja syrjivän tiedustelutoiminnan kielto.

Sovellettavista periaatteista laajimpana voidaan nähdä perusoikeuksien ja ihmisoikeuksien kunnioittaminen. Sen mukaan sotilastiedusteluviranomaisen on kunnioitettava perusoikeuksia ja ihmisoikeuksia sekä toimivaltuuksia käyttäessään valittava perusteltavissa olevista vaihtoehdoista se, joka parhaiten edistää näiden oikeuksien toteutumista.

Suhteellisuusperiaate ohjaa sotilastiedustelu toimenpiteitä niin, että niiden on oltava puolustettavia suhteessa tiedon hankinnalla saatavien tietojen tärkeyteen, tiedustelutehtävän kiireellisuuteen, tavoiteltavaan sotilastiedustelun päämäärään, sotilastiedustelun kohteeseen, muille tiedustelutoimenpiteen käytöstä aiheutuvaan oikeuksien rajoittamiseen sekä muihin asiaan vaikuttaviin seikkoihin. Lisäksi toimenpiteellä tulee olla riittävät tosiasialliset mahdollisuudet saavuttaa sotilastiedustelun hyväksyttävät päämäärät.

Vähimmän haitan periaatteen mukaan sotilastiedustelun toimivaltuuden käytöllä ei kenenkään oikeuksiin saa puuttua enempää eikä kenellekään saa aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi. Tiedon hankkimisessa ei saa puuttua luottamuksellisen viestin salaisuuteen muuten kuin mahdollisimman kohdennetusti ja rajoitetusti.

Tarkoitussidonnaisuuden perusteella toimivaltuuksia saadaan käyttää vain laissa säädettyyn tarkoitukseen.

Syrjivän tiedustelutoiminnan kiellon mukaan sotilastiedustelun toimenpiteen kohdentaminen ei saa ilman hyväksyttävää perustetta perustua henkilöiden ikään, sukupuoleen, alkuperään, kansalaisuuteen, asuinpaikkaan, kieleen, uskontoon, vakaumukseen, mielipiteeseen, poliittiseen toimintaan, ammattiyhdistystoimintaan, perhesuhteisiin, terveydentilaan, vammaisuuteen, seksuaaliseen suuntautumiseen tai muuhun henkilöön liittyvään syyhyn. Voidaan katsoa, että periaate osaltaan takaa objektiivista kohdentamista sotilastiedustelun laissa määritettyyn kohteeseen.

Edellä kuvattujen periaatteiden tarkoituksen voidaan nähdä harkintavallan rajoittajina ja mielivallan ehkäisijöinä ja näin parantavan yksilön oikeusturvaa.

Lakiehdotuksia on arvioitava perustuslain 10 §:n lisäksi perustuslain 8 §:ssä säädetyn laillisuusperiaatteen, 15 §:ssä säädetyn omaisuuden suojan, 21 §:ssä säädetyn oikeusturvan sekä vastuuta virkatoimista koskevan 118 §:n ja hallintotehtävän antamista muulle kuin viranomaiselle koskevan 124 §:n kannalta.

Lakiehdotuksia tulee lisäksi tarkastella perusoikeuksien yleisten rajoitusedellytysten kannalta (HE 1/1998 vp, PeVM 25/1994 vp).

10.2 Laki sotilastiedustelusta

10.2.1 Sotilastiedustelua rajaavat yleiset periaatteet

Sotilastiedustelusta annetussa laissa säädetään yksityiskohtaisesti toimintaa koskevista, toiminnan läpileikkaavista periaatteista. Näitä ovat perusoikeuksien ja ihmisoikeuksien kunnioittaminen (5 §), suhteellisuusperiaate (6 §), vähimmän haitan periaate (7 §), tarkoitussidonnaisuuden periaate (8 §) ja syrjivän tiedustelutoiminnan kielto.

Sovellettavat periaatteista laajimpana voidaan nähdä perusoikeuksien ja ihmisoikeuksien kunnioittaminen. Sen mukaan sotilastiedusteluviranomaisen on kunnioitettava perusoikeuksia ja ihmisoikeuksia sekä toimivaltuuksia käyttäessään valittava perusteltavissa olevista vaihtoehdoista se, joka parhaiten edistää näiden oikeuksien toteutumista.

Suhteellisuusperiaate ohjaa sotilastiedustelu toimenpiteitä niin, että niiden on oltava puolustettavia suhteessa tiedon hankinnalla saatavien tietojen tärkeyteen, tiedustelutehtävän kiireellisuuteen, tavoiteltavaan sotilastiedustelun päämäärään, sotilastiedustelun kohteeseen, muille tiedustelutoimenpiteen käytöstä aiheutuvaan oikeuksien rajoittamiseen sekä muihin asiaan vaikuttaviin seikkoihin. Lisäksi toimenpiteellä tulee olla riittävät tosiasialliset mahdollisuudet saavuttaa sotilastiedustelun hyväksyttävät päämäärät.

Vähimmän haitan periaatteen mukaan sotilastiedustelun toimivaltuuden käytöllä ei kenenkään oikeuksiin saa puuttua enempää eikä kenellekään saa aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi. Tiedon hankkimisessa ei saa puuttua luottamuksellisen viestin salaisuuteen muuten kuin mahdollisimman kohdennetusti ja rajoitetusti.

Tarkoitussidonnaisuuden perusteella toimivaltuuksia saadaan käyttää vain laissa säädettyyn tarkoitukseen.

Syrjivän tiedustelutoiminnan kiellon mukaan sotilastiedustelun toimenpiteen kohdentaminen ei saa ilman hyväksyttävää perustetta perustua henkilöiden ikään, sukupuoleen, alkuperään, kansalaisuuteen, asuinpaikkaan, kieleen, uskontoon, vakaumukseen, mielipiteeseen, poliittiseen

toimintaan, ammattiyhdistystoimintaan, perhesuhteisiin, terveydentilaan, vammaisuuteen, seksuaaliseen suuntautumiseen tai muuhun henkilöön liittyvään syyhyn. Voidaan katsoa, että periaate osaltaan takaa objektiivista kohdentamista sotilastiedustelun laissa määritettyyn kohteeseen.

Edellä kuvattujen periaatteiden tarkoituksen voidaan nähdä harkintavallan rajoittajina ja mielivallan ehkäisijöinä ja näin parantavan yksilön oikeusturvaa.

Sotilastiedustelun kohdentamista ja rajoitusmekanismeja on käsitelty aiemmin yleisperustelujen kappaleessa 2.2.1.

10.2.2 Tietoliikennetiedustelu

10.2.2.1 Yleistä

Perustuslain 10 §:ssä säädetään yksityiselämän suojasta. Säännös turvaa jokaiselle oikeuden luottamukselliseen viestintään ilman, että ulkopuoliset saavat oikeudettomasti tiedon hänen lähettämiensä tai hänelle osoitettujen luottamuksellisten viestien sisällöstä. Tämä merkitsee esimerkiksi suojaa kirjeiden tai muiden suljettujen viestien avaamista tai hävittämistä sekä puhelujen kuuntelemista tai nauhoittamista vastaan.

Sääntely ei suojaa ainoastaan viestin lähettäjää, vaan kysymyksessä on viestinnän molempien osapuolten perusoikeus. Viestin sisällön lisäksi perustuslain säännökset suojaavat myös viestin lähettäjän ja vastaanottajan tunnistamistietoja sekä muita tietoja, joilla voi olla merkitystä viestin luottamuksellisuuden säilymiselle.

Perustuslain 10 §:n 4 momentin mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Säännöksessä säädetyt mahdollisuudet rajoittaa luottamuksellisen viestin suojaa on katsottu perusoikeusuudistuksen yhteydessä tyhjentäväksi luetteloksi (HE 309/1993 vp, s. 54).

Säännös ei suojaa tavallisen kuuloetäisyydellä käytävän, aistihavainnoin kuultavissa olevan keskustelun sisältöä, mutta perinteisesti luottamukselliseksi tarkoitetun keskustelun kuunteleminen teknisin apuvälinein merkitsee rajoitusta luottamuksellisen viestin salaisuuden suojaan (HE 309/1993 vp, s. 53, PeVL 11/2005 vp, s. 4, PeVL 36/2002 vp, s. 6, PeVL 2/1996 vp, PeVL 5/1999 vp, s. 4).

Perustuslakivaliokunta on lausuntokäytännössään (PeVL 26/2025 vp. s. 5) korostanut säännöksen soveltamisrajoituksista, että tiedonhankinta kansallista turvallisuutta uhkaavasta toiminnasta voitaisiin 10 §:n 4 momentin perusteella osoittaa vain kansallisesta turvallisuudesta huolehtivien viranomaisten tehtäväksi, joita tällä hetkellä ovat Puolustusvoimat ja suojelupoliisi.

Toiseksi rajoitusedellytys koskisi vain tiedon hankkimista sellaisesta toiminnasta, joka on sotilaallista tai luonteensa takia voi muodostua vakavaksi uhkaksi kansalliselle turvallisuudelle.

Kolmanneksi lailla tulee säätää tyhjentävästi toimivaltuuksien kohdentumisesta sotilaalliseen toimintaan tai kansallista turvallisuutta vakavasti uhkaavaan toimintaan.

Neljänneksi perustuslain 10 §:n 4 momentin sääntely ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa.

Välttämättömyys-kriteeri tarkoittaa valiokunnan mukaan (PeVL 26/2025 vp, kohta 15), että luottamuksellisen viestin salaisuuteen kohdistunut rajoitus on sallittu vain, jos tiedonhankinta ei ole mahdollista vähemmän puuttuvin keinoin, ja että tiedon hankkimisessa puututaan luottamuksellisen viestin salaisuuteen mahdollisimman kohdennetusti ja rajoitetusti. Valtiosääntöoikeudellisen tulkinnan lähtökohtana valiokunta on tähdentänyt myös sitä, että perustuslaista johtuu tarve yhtäältä tulkita kansallisen turvallisuuden käsitettä suppeasti sekä toisaalta asettaa uhan vakavuusaste korkealle.

Perustuslakivaliokunnan mukaan (PeVL 26/2025 vp, kohta 15) rajoitusperusteeseen vetoavalla on myös velvollisuus esittää riittävät perustelut sille, että jokin toiminta voi muodostua vakavaksi uhaksi kansalliselle turvallisuudelle. Välttämättömyysvaatimuksen täyttymiseksi ei perustuslakivaliokunnan mielestä riitä, että tiedon hankkimisen luottamuksellisista viesteistä voidaan yleisesti katsoa edistävän kansallista turvallisuutta (PeVM 4/2018 vp, s. 8–9).

Perusoikeussäännökset suojaavat luonnollisia henkilöitä ja oikeushenkilöitä välillisesti. Valtio ja muut julkisyhteisöt jäävät perusoikeussuojan ulkopuolelle (HE 309/1993 vp, PeVL 9/2015 vp ja PeVL 4/2018). Vieraan valtion viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa. Tällaisen viestinnän havaitsemiseksi on kuitenkin välttämätöntä puuttua luottamuksellisen viestinnän suojaan. Viestintä ammattitoiminnassa voi toiminnan luonteen ja viestinnän osapuolten viestien taltiointia koskevan tietoisuuden vuoksi jäädä luottamuksellisen viestin salaisuuden suojan ulkopuolelle, vaikka tällaisessa viestinnässä voitaisiinkin sinänsä välittää myös luottamuksellisia viestejä henkilöiden välillä (liikenteen ohjauksessa syntyvä puhe- ja viestiliikenne; PeVL 62/2010 vp).

EIT:n ratkaisukäytännössä tietoliikennetyyppisten toimivaltuuksien tiedonkäsittelyssä puuttumisen syvyys yksityiselämän suojaan voidaan jakaa neljään tasoon (Big Brother Watch kohta 325 ja Centrum för Rättvisa kohta 239). Ensimmäisessä vaiheessa on kyse tietoliikenteen keräyksestä ja sen tallentamisesta, toisessa vaiheessa tietoliikenteeseen kohdistetaan hakuehtoja tietoliikenteen suodattamiseksi olennaiseen, kolmannessa vaiheessa jäljelle jäävään tietoon perehdytään ja neljännessä, viimeisessä vaiheessa analysoitua tietoa käytetään ja jaetaan sitä tarvitseville. EIT katsoo, että tietoliikenteen keräys ei vielä itsessään puutu syvällisesti henkilön yksityisyyden suojaan, kun taas puuttuminen on syvintä viranomaisen tutustuessa viestintään ja laatiessa saamiensa tietojen pohjalta raportin. Vastaavasti viranomaisen virkamiehen tutustuessa suodatettuun aineistoon, edellyttää tämä kaikista vahvinta valvontaa ja muita oikeusturvan takeita. Edellä todettu ei kuitenkaan poistane vaatimusta siitä, että myös viranomaisen mahdollisuudesta päästä keräämään tietoliikennettä on säädettävä.

Todettakoon vielä, että perustuslakivaliokunta on todennut nimenomaisesti, että viestin sisältö ei menetä perustuslain suojaa pelkästään sen perusteella, että esimerkiksi telekuuntelun avulla on saatu tieto siitä (PeVL 99/2022 vp, kappale 12).

Nyt käsiteltävänä olevaan esityksen 66, 67 a, 68 ja 70 § puuttuvat luottamuksellisen viestin suojaan. Säännöksiä on arvioitava perustuslain 10 §:n 4 momentin kannalta.

10.2.2.2 Teknisten tietojen käsittely

Suhde välitystietoon

Esityksen 1. lakiehdotuksen 66 §:n mukaan teknisiä tietoja voidaan käsitellä 1) tilastollista analyysiä varten tietoliikennetiedustelun kohdentamiseksi viestintäverkon osaan ja 2) tietoliikenteen reitittymisen ja muutosten seuraamiseksi. Sotilastiedustelusta annetun lain 10 §:n 11 kohdan mukaan teknisellä tiedolla tarkoitetaan muita kuin viestin sisältöön kuuluvia tietoliikenteen tietoja.

Perustuslain 10 §:n säännökset suojaavat viestin lähettäjän ja vastaanottajan tunnistamistietoja sekä muita tietoja, joilla voi olla merkitystä viestin luottamuksellisuuden säilymiselle. Viestinnän välitystiedot kuuluvat perustuslain 10 §:n 2 momentin luottamuksellisen viestin salaisuuden suojan piiriin (HE 309/1993 vp, s. 53).

Arvioitavan sääntelyn kannalta on merkityksellistä, että perustuslakivaliokunnan aiemmassa vakiintuneessa käytännössä viestin tunnistamistietojen on katsottu jäävän luottamuksellisen viestin salaisuutta suojaavan perusoikeuden ydinalueen ulkopuolelle (ks. esim. PeVL 33/2013 vp, s. 3, PeVL 6/2012 vp, s. 3—4, PeVL 29/2008 vp, s. 2, PeVL 3/2008 vp, s. 2). Tämä on merkinnyt, ettei perustuslain nykyiseen 10 §:n 4 momenttiin sisältyvää erityistä lakivarausta ole sellaisenaan sovellettu välitystietojen salaisuuden rajoittamiseen. Välitystietojen salaisuuden suojaan puuttuvan sääntelyn on kuitenkin valiokunnan käytännön mukaan tullut täyttää perusoikeuksien rajoittamisen yleiset edellytykset (PeVL 62/2010 vp, s. 4/II, PeVL 23/2006 vp, s. 2—3). Siten on ollut esimerkiksi mahdollista säätää televalvontatoimivaltuudesta myös tilanteessa, jossa ei välttämättä ole ollut kyse perustuslain nykyisen 10 §:n 4 momentissa tarkoitetusta yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavista rikoksista (PeVL 33/2013 vp, s. 3). Tunnistamistietojen saamista on pidetty mahdollisena myös joissakin tilanteissa, joissa ei ole ollut kyse perustuslain nykyisen 10 §:n 4 momentin mukaisista rajoitusperusteista (PeVL 62/2010 vp, s. 4/II).

Sittemmin perustuslakivaliokunta on tarkistanut käytäntöään, koska sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat kuitenkin olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen (PeVL 18/2014 vp, s. 6/II).

Perustuslakivaltiokunta on katsonut (PeVL 15/2024 vp. kohta 12–13) Rajavartiolaitoksen radioteknisen valvonnan osalta lausuntokäytännössään radiolaitteen yksilöinnin mahdolliseksi, jos viestinnän tietoja ei käytetä radiolaitteen omistajan tai haltijan tunnistamiseksi. Yksilöinnin on tapahduttava käytännössä automaattisesti teknisin menetelmin, ja sen avulla olisi mahdollista rajata tarpeettomia kohteita pois radioteknisen valvonnan piiristä. Lausunnon kohteena ollut radiotekninen valvonta voi kohdistua teknisen laitteiston sensorien toiminta-alueella rajoittamattomaan joukkoon radiolaitteita. Perustuslakivaliokunta katsoi, että sääntelyä oli arvioitava perusoikeuksien yleisten rajoitusedellytysten kautta.

Nyt käsiteltävänä olevan säännösehdotuksen mukaan teknisten tietojen käsittely kohdistuu tietoliikenteen teknisiin tietoihin, eli muuhun kuin viestin sisältöön kuuluviin tietoihin. Perustuslain kannalta kyse on käytännössä viestinnän välitystiedoista sekä erilaisten sähköistä viestintää välittävien laitteiden teknisistä tiedoista ja muista viimeksi mainittuihin rinnastuvista teknisistä tiedoista. Tietoja voidaan käsitellä ainoastaan säännöksessä tarkasti mainittuihin tarkoituksiin, joita ovat tilastollinen analyysi tietoliikennetiedustelun kohdentamiseksi viestintäverkon osaan sekä tietoliikenteen reitittymisen ja muutosten seuraaminen. Kyse on teknisestä kohdentamisesta toimintaympäristössä ja tietoliikennetiedustelujärjestelmän teknisestä kehittämisestä tietoja analysoimalla Tietoliikenteen teknisiä tietoja ei käsitellä sotilastiedustelun kohteiden tai henkilöiden tunnistamiseksi, vaan kyse on teknisestä

kohdentamisesta toimintaympäristössä ja tietoliikennetiedustelujärjestelmän teknisestä kehittämisestä tietoja analysoimalla.

Sen lisäksi, mitä sotilastiedustelusta annetussa laissa erikseen säädetään toimintaa koskevista yleisistä periaatteista (kuten tarkoitussidonnaisuuden periaate), säännöksessä olisi nimenomaisesti säädetty, ettei teknisten tietojen käsittelyssä voi syntyä analyysi (tietoja yhdistelemällä), josta voidaan suoraan tunnistaa yksittäinen henkilö. Vaikka tekniset tiedot saattavat sisältää myös henkilötiedoksi katsottavia tietoja, niiden luonteella henkilötietona ei ole säännösehdotuksen kannalta merkitystä säännösehdotuksessa tarkoitetussa toiminnassa eikä niitä saisi muutenkaan käyttää muuhun kuin säännöksessä tarkkaan säädettyihin tarkoituksiin, ainoastaan teknisenä tietona. Henkilötietojen käsittelystä säädetään erikseen henkilötietojen käsittelystä Puolustusvoimissa annetussa laissa.

Tietoliikenteen keräyksen kesto teknisten tietojen käsittelyssä

Nyt käsiteltävänä olevan esityksen 1. lakiehdotuksen 66 §:ssä voimassa olevaa pykälää esitetään muutettavaksi niin, että säännöksestä poistettaisiin tietoliikenteen keräyksen hetkellisyyttä koskeva rajaus.

Perustuslakivaltiokunta katsoi sotilastiedustelusta annettua lakia koskevassa lausunnossaan (PeVL 36/2018 vp. s. 22–23), että lakiehdotuksen 63 §:n (voimassa oleva 66 §) sanamuoto vaikuttaa perustuslakivaliokunnan käsityksen mukaan mahdollistavan hyvin laajan viestintäverkon alueen kattavan tietojen keräämisen ja tallentamisen eikä ehdotetun lain 63 § (voimassa oleva 66 §) sisällä "hetkellisyyttä" koskevaa mainintaa lukuun ottamatta nimenomaisia rajoittavia kriteereitä tietojen keräämiselle ja tallentamiselle. Perustuslakivaliokunta katsoi, että ehdotetussa sääntelyssä voi tältä osin nähdä ns. massavalvonnan piirteitä, kun esityksen perustelujenkin mukaan (HE 203/2017 vp. s. 280) teknisten tietojen käsittely tietoliikenteestä voisi tapahtua hetkellisesti kaikkeen viestintäverkon osassa liikkuvaan tietoliikenteeseen kohdistuen. Perustuslakivaliokunta katsoi, että säännös edellytti yleiseen ja kohdentamattomaan tietoliikenteen seurannan kiellosta säätämistä laissa, jotta säännös oli mahdollinen tavallisen lain säätämisjärjestyksessä.

Perustuslakivaliokunta on katsonut, että miehittämättömän ilma-aluksen kauko-ohjauksessa esimerkiksi matkapuhelimen tai tietokoneen avulla ei ole kysymys sellaisesta perustuslain 10 §:n 2 momentin tarkoittamasta luottamuksellisesta viestinnästä, jolle kyseisen perustuslain säännöksen kautta on ylipäänsä tarkoitettu antaa perustuslain suojaa (PeVL 22/2020 vp). Vaikka esimerkiksi kulkuneuvon ohjaajan ja liikenteenohjauksen välisessä viestinnässä voitiin sinänsä välittää myös luottamuksellisia viestejä henkilöiden välillä, ei kysymys poikkeuksellisen toiminnan tutkinnan luonteesta ja henkilöiden viestien taltiointia koskevasta tietoisuudesta johtuen valiokunnan mukaan kuitenkaan ole perustuslain 10 §:ssä tarkoitetun luottamuksellisen viestin salaisuuden suojan piiriin kuuluvasta toiminnasta (PeVL 62/2010 vp, s. 5). Myös Rajavartiolaitoksen radioteknisen valvonnan arvioitiin kohdistuvan osittain sellaiseen viestiliikenteeseen, joka ei kuulu perustuslain 10 §:n 2 momentin mukaisen luottamuksellisen viestin salaisuuden piiriin (PeVL 15/2024 vp, kappale 9).

Valiokunta on viimeaikaisessa käytännössään pitänyt esimerkiksi Rajavartiolaitoksen radioteknistä valvontaa koskevaa sääntelyä tuolloin ehdotetussa laajuudessa, ottaen erityisesti huomioon valvonnalle laissa ehdotetut rajoitukset, suhteellisen vähäisenä puuttumisena luottamuksellisen viestin salaisuuden suojaan ja arvioinut sääntelyä perusoikeuksien yleisten rajoitusedellytysten kannalta (PeVL 15/2024 vp, kappaleet 12—13). Perustuslakivaliokunta piti ajallisesti rajoittamatonta radioviestinnän välitystietojen käsittelyä, joka kohdistui tietyllä

maantieteellisellä alueella tai sen välittömässä läheisyydessä oleviin erottelemattomiin laitteisiin, perustuslain kannalta ongelmattomana. Tietojen hävittämisestä säädetään erikseen ja henkilötietojen käsittelystä ja poistamisesta henkilötietojen käsittelystä Rajavartiolaitoksessa annetussa laissa. Päätöksen radioteknisestä valvonnasta tekee Rajavartiolaitoksen esikunnan raja- ja meriosaston päällikkö.

Nyt käsiteltävänä oleva säännösehdotus kohdistuu tietoihin, joita ovat erilaiset tietoliikenneverkon tekniset ohjaus- ja muiden laitteistojen tuottamat tekniset tiedot, mutta myös välitystiedot. Ohjaus- ja muiden laitteistojen tietojen osalta säännösehdotuksen voitaneen katsoa olevan ongelmaton perustuslain kannalta.

Välitystietojen osalta, vaikka kyse on henkilötiedosta, niitä ei säännösehdotuksen mukaan saisi käsitellä tavalla, josta voidaan tunnistaa yksittäinen luonnollinen henkilö. Näin ollen pelkän välitystiedon perusteella ei voida tehdä johtopäätöksiä yksittäisen henkilön toiminnasta, ellei tietoa yhdistetä muuhun tietoon ja näin selvitetä välitystietoa käyttänyt henkilö ja hänen yksityiselämäänsä. Tähän säännösehdotus ei anna mahdollisuutta. Lisäksi toimintaa ohjaa esimerkiksi tarkoitussidonnaisuuden periaate.

Säännösehdotuksessa ei voida katsoa olevan kyse yleisestä ja kohdentamattomasta tietoliikenteen tiedustelusta, koska kyse on varsinaisen tietoliikennetiedustelun mahdollisimman tarkan kohdentamisen mahdollistamisesta. Säännösesityksen ei voida katsoa myöskään olevan yleistä tietoliikenteen tiedustelua, koska toimivaltuus kohdistuisi tiettyyn Suomen rajan ylittävään viestintäverkon osaan ja siinä tiettynä ajanhetkenä liikkuvaan tietoliikenteen teknisiin tietoihin. Toimivaltuudella ei myöskään toteuteta tiedustelutehtävää, vaan kyse on tiedustelutehtävän edellyttämästä tiedon hankinnasta tietoliikenteen ja rajat ylittävän tietoliikenneverkon teknisistä ominaisuuksista. Muilta osin kuin tietoliikenteen teknisten tietojen osalta tiedot on poistettava myös hävittämistä koskevan sääntelyn perusteella.

Päätöksen säännösehdotuksen mukaisesta toiminnasta tekisi tuomioistuin ja luvan voimassaolo olisi rajattu 6 kuukauteen. Voimassaoloaika vastaisi sitä, mitä varsinaisen tietoliikennetiedustelun osalta on voimassa olevassa laissa. Teknisten tietojen käsittely kohdistuu tietoliikenteen teknisiin tietoihin eikä niistä voida suoraan tunnistaa yksittäistä henkilöä tai voida merkittävällä tavalla puuttua henkilön yksityiselämän suojaan. Ehdotettu säännös sisältää edelleen kiellon muodostaa teknisten tietojen käsittelyssä analyysiä, josta voidaan tunnistaa yksittäinen henkilö. Kiellon voidaan katsoa korostavan perustuslaissa ja sotilastiedustelusta annetussa laissa säädettyä tarkoitussidonnaisuuden periaatetta.

Säännösehdotus puuttuu perustuslain 10 §:n suojaamaan yksityisyyden suojaan, mutta säännöksen nojalla tietoliikenteen teknisiä tietoja käsitellään teknisestä näkökulmasta. Edellä todetun perusteella säännösehdotus voidaan käsitellä perustuslain 10 §:n 4 momentin nojalla tavallisen lain säätämisjärjestyksessä. Tietoliikenteen teknisten tietojen aiempaa paremmalla analysoinnilla voidaan katsoa olevan perusoikeusmyönteisiä vaikutuksia, sillä sen voidaan arvioida parantavan varsinaisen tietoliikennetiedustelun kohdentamista.

10.2.2.3 Hakuehtojen määrittäminen

Määrittäminen

Esityksen 1. lakiehdotuksen 67 a § puuttuu viestin sisältöön. Pykälän 1 momentin mukaan Puolustusvoimien tiedustelulaitos voisi tietoliikennetiedustelun tarkemmaksi kohdentamiseksi kerätä ja tallentaa tietoliikennettä Suomen rajan ylittävän viestintäverkon osasta ja käsitellä sitä,

jos se on välttämätöntä kohdetta kuvaavien uusien hakuehtojen määrittämiseksi. Kerättävän ja tallennettavan tietoliikenteen määrä ei saa ylittää 5 prosenttia kohteena olevan Suomen rajan ylittävän viestintäverkon osan kapasiteetista. Hakuehdot on määritelty lain 10 §:n 1 kohdan mukaan tiedoksi, jonka perusteella tietoliikennetiedustelulla viestintäverkon osasta mahdollisimman rajatusti ja täsmällisesti valitaan tietoliikennetiedustelun kohteena oleva tietoliikenne ja puuttuminen luottamuksellisen viestin salaisuuden suojaan rajautuu tiedustelun tarkoituksen kannalta välttämättömään. Määritelmä on tehty eduskunnan myötävaikutuksella (PuVM 9/2018 vp. sekä PeVL 36/2018 vp. ja PeVL 76/2018 vp.). Koska hakuehto rajaa tietoliikennetiedustelulla saatavan tiedon vain tiedustelun tarkoituksen kannalta välttämättömään, uusien sotilastiedustelun kohteeseen kohdistuvien hakuehtojen määrittäminen ei ole voimassa olevan sääntelyn mukaisesti useinkaan mahdollista.

Perustuslakivaliokunta on katsonut käytännössään radiolaitteiden teknisen valvonnan osalta, että sääntely, jonka perusteella sähkömagneettisia aaltoja käyttävän laitteen yksilöinti tapahtuu käytännössä automaattisesti teknisin menetelmin, ja sen avulla rajataan tarpeettomia kohteita pois radioteknisen valvonnan piiristä, on ongelmaton perustusoikeuksien kannalta (PeVL 15/2024 vp. kohta 12). Radioteknisessä valvonnassa tuotettu tieto on säännöksen perustelujen mukaan suodatettu sellaiseen muotoon, että loppukäyttäjä ei saisi tietää radiolaitteen yksilöintiin käytettäviä tunnistetietoja.

Uusien hakuehtojen määrittäminen kohdistuisi tietoliikennevirtaan sen konekielisessä muodossa, josta ei ennen tietoliikenteen teknistä käsittelyä pystytä suoraan selvittämään ja lukemaan välitystietoja tai viestin sisältöä; tietoliikennevirrassa on kyse merkkijonosta, binäärimuodosta (numeroiden 1 ja 0 muodostamista sarjoista), josta ei ole suoraan luettavissa tarkempia tietoja. Se, mihin järjestykseen merkit asettuvat, johtuu muun muassa sähköisen viestin lähettäneen tahon organisaation käyttämästä tietojärjestelmästä, käytetyistä muista laitteista ja ohjelmistoista. Merkkijonoihin vaikuttavat lisäksi muun muassa käytetyt protokollat.

Nyt käsiteltävänä olevan säännösehdotuksen mukaan tietoliikennevirtaa käsiteltäisiin automaattisilla ja manuaalisilla teknisillä menetelmillä hakuehdon määrittelemiseksi. Määrittelyssä ei saisi hyödyntää viestin merkityssisällössä olevaa tietoa. Hakuehtojen määrittämisessä ei saisi myöskään yhdistellä tietoja tavalla, josta selviäisi viestin semanttinen sisältö taikka tietoa, josta voidaan tehdä henkilön yksityiselämää koskevia päätelmiä. Tietojen saaminen henkilöstä tai tämän henkilökohtaisesta elämästä ei ole myöskään ehdotetun toimivaltuuden tarkoitus, vaan tarkoituksena on määrittää hakuehtoja, jotta tietoliikennetiedustelu kohdentuisi laissa säädetyn hakuehdon määritelmän mukaisesti välttämättömään.

Jotta tietoliikennetiedustelu olisi mahdollisimman kohdennettua ja sillä saataisiin odotettua välttämättömään rajattua tietoa, tiedusteluviranomaisella on oltava ennakkotieto hakuehdon kohdistumisesta niin, että se puuttuu viestinnän suojaan mahdollisimman rajatusti. Nyt käsiteltävänä olevassa säännösehdotuksessa hakuehtojen määrittäminen perustuisi kohteen tietoliikenteen oletettuun säännönmukaisuuteen tai ominaispiirteeseen.

Esitetty säännös koskisi tietoliikenteen käsittelyä sen teknisessä muodossa ja tietoliikenteen merkkijonojen tutkimista ja tulkintaa. Viranomaisella olisi lähtötieto etsittävän tietoliikenteen oletetusta säännönmukaisuudesta tai teknisestä erityispiirteestä, jonka perusteella tietoliikenteestä määritettäisiin hakuehtoja. Uusien hakuehtojen perusteella varsinaista tietoliikennetiedustelua voidaan kohdentaa tarkasti sotilastiedustelun kohteeseen. Tällä voidaan katsoa olevan perusoikeusmyönteisiä vaikutuksia, koska sotilastiedustelun kannalta tarpeetonta tietoa pystyttäisiin suodattamaan aiempaa paremmin jo heti alkuvaiheessa.

Koska toimivaltuuden kohteena on tietoliikennevirta, voidaan toimivaltuuden käytön kohteena olevia tietoja pitää siinä määrin anonymisoituina, ettei niistä voida suoraan selvittää yksittäisen henkilön yksityiselämää koskevia tietoja tai viestinnän sisältöä tavalla, joka puuttuisi yksityisyyden tai viestin salaisuuden suojaan merkittävällä tavalla. Jotta tiedot voitaisiin selvittää, edellyttäisi tämä lakiehdotuksen mukaan varsinaisen tietoliikennetiedustelun (68 ja 70 §) käyttöä. Muussa tapauksessa toiminnassa rikottaisiin sotilastiedustelusta annetun lain yleisiä periaatteita ja muutenkin viranomainen syyllistyisi rikolliseen toimintaan.

Toimivaltuuden käyttö olisi sidottu välttämättömyyteen. Tässä tapauksessa välttämättömyys tarkoittaisi sitä, että uusia hakuehtoja ei käytännössä pystyttäisi määrittämään toisella tavalla tai määrittäminen vaatisi kohtuuttomasti resursseja.

Kuten aiemminkin on jo todettu, perutuslakivaliokunta on lausuntokäytännössään todennut, että tietoliikennetiedustelu ei voi olla yleistä, kohdentumaton ja kaikenkattavaa tietoliikenteen seurantaa (PeVL 36/2018 vp. ja PeVM 4/2018 vp. s. 8). Tämä rajoitus on huomioitu sotilastiedustelusta annetun lain 65 §:ssä. Toisaalta EIT on uusimmassa ratkaisukäytännössään katsonut, että tietoliikenteen kerääminen, vaikka kohdistuukin laajaan joukkoon ihmisiä, ei itsessään puutu henkilön yksityisyyden suojaan yhtä mittavasti kuin tilanteessa, jossa tiedusteluviranomaisen analyytikko selvittää viestinnän sisältöä ja yhdistelee tietoja kohteena olevan toiminnan tarkemmaksi selvittämiseksi (mm. Centrum för Rättvisa, kohdat 239–245).

Nyt käsiteltävänä olevassa säännösehdotuksessa tarkoitettu hakuehtojen määrittämistä ei voida katsoa täysin kohdentamattomaksi, sillä se perustuu kohteen tietoliikenteen oletettuun säännönmukaisuuteen tai ominaispiirteeseen, jotka on mainittava tuomioistuimen luvassa. Lisäksi oletettu säännönmukaisuus tai ominaispiirre olisi perusteltava, eli miksi ennakkotiedon perusteella uusia hakuehtoja pystyttäisiin määrittämään. Näin ollen päätöksentekoa koskevan sääntelyn mukaisesti sotilastiedusteluviranomaisella olisi oltava suuntaa antava käsitys kohteena olevan toimijan tietoliikenteestä, jotta hakuehtojen määrittämisessä ei jouduta käymään kaikkea mahdollista tietoliikennettä läpi.

Säännösehdotuksen ei voitane myöskään katsoa olevan yleistä. Nyt käsiteltävänä olevaa toimivaltuutta olisi rajattu fyysisesti tiettyyn Suomen rajan ylittävään viestintäverkon osaan, minkä lisäksi käsiteltävän tiedon määrä olisi rajoitettu 5 prosenttiin kyseisen viestintäverkon osan kapasiteetista, eli siitä määrästä, jonka viestintäverkon osa voi teknisesti enimmillään kuljettaa.

Edellä kuvatusti ehdotetulla toimivaltuudella hankittavien tietojen ei voida itsessään katsoa puuttuvan syvällisesti yksityisen viestin suojaan. Syvällinen puuttuminen edellyttäisi sotilastiedusteluviranomaisella olevien muiden tietojen yhdistelemistä kohteena olevan tietoliikenteen kanssa sekä muiden tiedustelumenetelmien käyttöä.

Ehdotettu säännös sisältäisi kiellon, jonka mukaan analyysissä ei saisi syntyä yksittäistä henkilöä kuvaavaa tai viestin sisältöä kuvaavaa tietoa. Tietoliikenteen käsittely tapahtuisi tietoliikenteen teknisessä, konekielisessä muodossa.

Esityksen 1. lakiehdotuksen 67 b §:ssä säädettäisiin 67 a §:n toimivaltuutta koskevasta päätöksenteosta. Vaatimuksessa ja päätöksessä olisi tuotava ilmi tiedustelutehtävä ja sitä koskevat tosiseikat. Lisäksi vaatimuksessa olisi perusteltava välttämättömyys.

Keskeisenä seikkana vaatimuksessa olisi tuotava ilmi kohteen tietoliikenteen oletettu säännönmukaisuus tai ominaispiirre, jonka perusteella hakuehtoja määritetään ja perustelut sille. Kohdan mukaisesti sotilastiedusteluviranomaisella olisi oltava suuntaa antava käsitys

kohteena olevan toimijan tietoliikenteestä, jotta hakuehtojen määrittämisessä ei jouduta käymään kaikkea mahdollista tietoliikennettä läpi. Vaatimuksessa olisi myös perusteltava, miksi tämän ennakkotiedon perusteella uusia hakuehtoja pystyttäisiin määrittelemään. Luvassa olisi myös mainittava tiedustelutehtävä.

Vaikka toimivaltuus itsestään selvästi puuttuu viestinnän sisältöön, ei puuttumisen astetta voida pitää vastaavana kuin mistä on kyse lain 68 ja 70 §:ssä. Ehdotetun säännöksen tavoitteena olevien tarkempien hakuehtojen määrittämisellä voidaan katsoa olevan perusoikeusmyönteisiä vaikutuksia.

Edellä kuvatuin perustein säännösehdotuksen ei voida katsoa puuttuvan yksityisen veistin salaisuuden suojaan tavalla, joka olisi yhtä merkittävää kuin mitä varsinaisessa tietoliikennetiedustelussa (lain 68 ja 70 §). Näin ollen säännös voidaan käsitellä tavallisen lain säätämisjärjestyksessä perustuslain 10 §:n 4 momentin mukaisesti.

Luvan voimassaoloaika

Esityksen 1. lakiehdotuksen 67 b §:n mukaan lupa hakuehtojen määrittämiseen voitaisiin antaa kuudeksi kuukaudeksi kerrallaan. Ajanjakso vastaisi sitä, mitä ehdotetaan teknisten tietojen käsittelyn luvan voimassaolon ajaksi ja toisaalta sitä, mitä on jo voimassa olevassa laissa varsinaisen tietoliikennetiedustelun luvan voimassaolo.

Perustuslakivaliokunta on kiinnittänyt huomiota (PeVL 35/2018 vp. ja PeVL 36/2018 vp.) huomiota lupien voimassaoloaikoihin viittaamalla EIT:n ratkaisukäytännön kehittymiseen. Perustuslakivaliokunta on viitannut tapauksiin Centrum för Rättvisa ja Big Brother Watch. Kummassakin tapauksessa todettiin tiedonhankinta EIS:n mukaan mahdolliseksi, jos toiminta perustui tuomioistuimen lupaan ja tiedonhankinnan kesto oli enintään kuusi kuukautta. EIT painotti useiden itsenäisten tiedustelutoimintaa valvovien elimien olemassaolon merkitystä järjestelmän hyväksyttävyydelle.

Nyt käsiteltävänä olevana olevassa tapauksessa toimintaa valvoo useat itsenäiset elimet. Lisäksi ehdotetun 67 a §:n mukaisen toiminnan yksityisen viestinnän suojaan puuttumisen syvyyden ei voida arvioida olevan yhtä syvälle käyvää kuin lain 68 ja 70 §:ssä tarkoitetun varsinaisen tietoliikennetiedustelun. Luvan voimassaoloaika kuusi kuukautta voidaan katsoa perustuslain kannalta ongelmattomaksi.

10.2.2.4 Teknisten tietojen ja tietoliikenteen säilytysaika

Säilytysaika

Esityksen 1. lakiehdotuksen 66 §:n 2 momentti ja 67 a §:n 4 momentissa säädettäisiin erityisistä tallentamisajoista. Teknisten tietojen osalta tallentamisaika olisi 18 kuukautta ja hakuehtojen määrittämisessä käytettävien tietojen osalta tallennusaika olisi 12 kuukautta.

Perustuslakivaliokunta on ottanut kantaa (PeVL 18/2014 vp.) tietojen säilyttämisaikoihin tilanteessa, jossa teleyritykset velvoitetaan säilyttämään kaikkiin tilaajiinsa liittyviä tietoja laissa tarkemmin säädetyn ajan. Hallituksen esitys, josta lausunto on annettu, koski niin kutsutun Data Retention -direktiivin kumoamista. Perustuslakivaliokunta on katsonut, että 12 kuukauden aika siitä päivästä, jona viestintä tapahtui, on oikeasuhtaisuuden kannalta hyväksyttävää ja vastaavan viranomaisten tarpeita (PeVL 3/2008 vp.). Perustuslakivaliokunta (PeVL 15/2024 vp.) on myös pitänyt Rajavartiolaitoksen radioteknisen valvonnan osalta

hyväksyttävänä sitä, että valvonnassa syntyneet vielä kohdentamattomat tallenteet voidaan säilyttää vuoden ajan tallenteen syntymisestä. Lisäksi radioteknisen valvonnan suuntaamiseksi sekä valvontakohteiden erottelemiseksi ja rajaamiseksi käsiteltävät henkilötiedot poistetaan viimeistään viiden vuoden kuluttua tiedon rekisteriin merkitsemisestä.

Perustuslakivaliokunta on lausuntokäytännössään pitänyt ongelmattomana henkilötietojen säilyttämistä yhden vuoden ajan (PeVL 21/2013 vp. ja PeVL 13/2017) vaikka henkilön ei epäillä liittyvän esimerkiksi kansallista turvallisuutta vakavasti uhkaavaan toimintaan. Valiokunta on kuitenkin kiinnittänyt huomiota siihen, että mitä pidemmäksi tietojen säilytysaika muodostuu, sitä olennaisempaa on huolehtia tietoturvasta, tietojen käytön valvonnasta ja rekisteröidyn oikeusturvasta (mm. PeVL 28/2016 vp.).

Teleyritysten velvollisuutta tunnistamistietojen yleisen ja kohdentamattoman säilyttämisen osalta perustuslakivaliokunta on todennut (PeVL 35/2004 vp.), että tunnistamistietojen säilyttämiseen liittyy valiokunnan mielestä aina riskejä yhtä hyvin luottamuksellisen viestinnän suojan kuin henkilötietojen suojan kannalta. Riskit kasvavat, mitä kauemmin tietoja säilytetään. Esimerkiksi kolmen vuoden säilyttämisaikaa on pidetty yleisen henkilötietolainsäädännön kannalta poikkeuksellisen pitkänä (PeVL 35/2004 vp, s. 4 ja PeVL 26/1998 vp, s. 3).

Nyt käsiteltävänä olevien ehdotusten kannalta merkittävää on se, mitä tietoja tallennettaisiin, kuinka kattavaa tietojen tallentaminen on, kuinka pitkä tallennusaika on ja mihin tallennettuja tietoja voidaan käyttää. Lisäksi merkityksellistä on se, missä muodossa tiedot ovat.

Teknisten tietojen osalta kyse on tietoliikenteen teknisten tietojen käsittelystä. Tekniset tietojen käsittelyssä tietoliikenteen teknisiä tietoja käsitellään tietyn viestintäverkon osan tunnistamiseksi sekä tietoliikenteen reitittymisen ja muutosten seuraamiseksi. Kyse on teknisestä analyysistä eikä tietoihin sisälly viestin sisältöä. Teknisistä tiedoista, vaikka olisivatkin henkilötietoja, ei voida tehdä syvällisiä päätelmiä henkilön yksityiselämästä.

Käsiteltävänä olevassa 1. lakiehdotuksen 66 §:n 3 momentissa säilytysaika olisi 18 kuukautta tietoliikenteen teknisten tietojen keräämisestä. Tallentamisen määrä voisi olla 5 prosenttia kohteena olevan Suomen rajan ylittävän viestintäverkon osan kapasiteetista, eli siitä määrästä, minkä viestintäverkon osa voi enimmillään teknisesti kuljettaa. Tietoliikenteen tekniset tiedot sisältävät myös välitystietoja, mutta niistä sellaisenaan ei voida tunnistaa välitystietoa käyttävää henkilöä tai muuten puuttua hänen oikeuksiinsa merkittävästi. Henkilön tunnistaminen edellyttää muita luvanvaraisia toimenpiteitä. Tallennuksen piiriin ei suodattuisi viestinnän sisältöä. Tallennusajan päätyttyä tallennetut tiedot häviävät automaattisesti.

Ehdotettu 18 kuukauden säilytysaikaa voidaan pitää välttämättömänä, jotta teknisten tietojen käsittelyssä olisi käytössä myös historiatietoa. Historiatieto on olennaista relevantin viestintäverkon osan tunnistamisessa, jotta esimerkiksi voidaan tunnistaa tietyltä alueelta tulevan tietoliikenteen säännönmukaisuuksia. Lisäksi historiatieto on välttämätöntä globaalin tietoliikenneverkossa käytettyjen laitteiden ja topologioiden tunnistamisessa. Nykytahtisessa teknologian kehityksessä 18 kuukautta voidaan pitää ajanjaksona, jonka aikana voidaan havaita merkittävimmät tekniset muutokset tietoliikenneverkossa tapahtuneista muutoksista. Sanotun ajanjakson aikana sotilastiedusteluviranomainen myös pystyy reagoimaan globaalissa viestintäverkossa tapahtuneisiin teknisiin muutoksiin. Tiedoilla olisi myös merkitystä 67 a §:ssä ehdotetun hakuehtojen määrittämisen kannalta sekä varsinaisessa tietoliikennetiedustelussa (68 ja 70 §).

Käsiteltävänä olevan säännösehdotuksen mukaisessa toiminnassa ei saisi hankkia tietoa tiedustelun kohteista, vaan kyse on tietoliikenteen teknisestä seurannasta. Näin ollen 18 kuukauden säilytysaikaa ei voida pitää ongelmallisena perustuslain kannalta.

Käsiteltävänä olevan 1. lakiehdotuksen 67 a §:n 4 momentin mukaan säilytysaika olisi 12 kuukautta. Ajanjakso olisi lyhyempi kuin mitä ehdotetussa 66 §:ssä säädettäisiin. Ehdotetussa säännöksessä tarkoitettu hakuehtojen määrittäminen tapahtuu vaiheessa, jossa tietoliikenteestä ei voida suoraan selvittää viestin semanttista sisältöä. Tietoliikenteen tallennus tapahtuu tietoliikenteen teknisessä (bitit ja tavut) muodossa, joten tallennetun tietoliikenteen semanttisen sisällön selvittäminen ja se, onko tietoliikenteessä sotilastiedustelun kohteeseen liittyvää tietoa, edellyttää muita luvanvaraisia toimenpiteitä sotilastiedusteluviranomaiselta.

Tallennuksen piiriin tulisi tietoliikenteen teknisten tietojen lisäksi myös muu osa viestinnästä; tallennusajan on oltava lyhyempi kuin teknisten tietojen osalta. Tallennus voisi kohdistua viiteen prosenttiin kohteena olevan viestintäverkon osan kapasiteetista, eli siihen määrään tietoliikennettä, mitä viestintäverkon osassa voi kerralla teknisesti enintään kulkea. Kapasiteetti voidaan selvittää muun muassa tietoliikennekaapeleiden ja -kuitujen teknisistä tiedoista. Ehdotetun tallennusajan jälkeen tiedot häviäisivät automaattisesti tietojärjestelmästä.

Tietojen tallentaminen on välttämätöntä esitetyn 67 a §:n hakuehtojen määrittämisen sekä varsinaisen tietoliikennetiedustelun (68 ja 70 §) kannalta, jotta tietoliikennetiedustelu kohdistuisi ainoastaan välttämättömään osaan tietoliikennettä. Tietoliikenteen historiatietoon vertaamisella on merkittävä osa määritettäessä uusia hakuehtoja ja hankittaessa tietoa tiedustelun kohteesta.

Tallennettujen tietojen voidaan katsoa olevan hyödynnettävissä 12 kuukauden ajan, jonka aikana säilytetyistä tiedoista voidaan katsoa olevan hyötyä. Teknologisen kehityksen ollessa intensiteetiltään korkeaa, mainittua ajanjaksoa pidemmälle tallennusajalle ei ole perusteita ja ehdotettua ajanjaksoa vanhempien tietojen voidaan katsoa kadottavan merkityksensä säännösehdotuksen tarkoituksiin.

Yksityisyyden suojan kannalta olennaista on myös se, että sähköiset viestit eivät liiku viestintäverkossa koherenttina kokonaisuutena, vaan tietoliikennepaketteina, jotka jokainen hakeutuvat tehokkainta reittiä pitkin määränpäähänsä.

Perustuslakivaliokunta on katsonut 12 kuukauden tietojen säilyttämisen ajan ongelmattomaksi henkilötietojen osalta, vaikka se kohdistuisi erittelemättä tiettyyn ihmisryhmään (Suomen rajan ylittävät henkilöt). Nyt käsiteltävänä olevassa tilanteessa tallennettavat tiedot olisivat järjestelmässä tietoliikenteen teknisessä muodossa, joka ei ole suoraan yhdistettävissä yksittäiseen luonnolliseen henkilöön eikä viestin sisältö selvitettävissä. Toimivaltuuden nojalla ei voitaisi hankkia tietoa esimerkiksi yksittäisen henkilön toiminnasta.

Perustuslakivaliokunnan käytännön mukaisesti (mm. PeVL 28/2016 vp.) ehdotettujen säännösten mukaisessa toiminnassa huolehdittaisiin tietoturvasta, tietojen käytön valvonnasta ja rekisteröidyn oikeusturvasta. Valvonnasta huolehtivat sisäisen valvonnan lisäksi keskeisesti tiedusteluvalvontavaltuutettu ja tietosuojavaltuutettu sekä oikeusturvasta tuomioistuimen ennakkokontrollin lisäksi tiedusteluvalvontavaltuutettu ja tietosuojavaltuutettu.

Kerättyjä ja tallennettuja tietoja koskisi myös laissa säädetty yleinen tietojen hävittämisvelvollisuus. Näin ollen tietoliikennettä olisi hävitettävä sitä mukaan, kun se todetaan tarpeettomaksi. Joka tapauksessa tietoliikenne häviäisi säädetyn määräajan tultua täyteen.

Vaikka järjestelmään tallentuisi sinänsä kohdentamattomasti välitystietoja ja tietoliikennettä, ei sotilastiedusteluviranomainen voi käyttää tietoja ilman tuomioistuimen antamaa lupaa toimivaltuudelle, jolla tallennettuja tietoja saadaan käyttää. Näin ollen sotilastiedusteluviranomainen ei voi selvittää esimerkiksi tuntemattoman IP-osoitteen käyttäjää sotilastiedustelusta annetun lain 104 §:ää käyttämällä, ellei tieto ole tullut varsinaisessa tietoliikennetiedustelussa (lain 68 tai 70 §) esille.

Edellä todetuin perustein ehdotettuja tallennusaikoja voidaan pitää välttämättöminä, eikä säännösehdotusten voida katsoa olevan ristiriidassa perustuslain 10 §:n luottamuksellisen viestin salaisuuden suojan kanssa.

Tallennettujen tietojen käyttäminen

Esityksen 1. lakiehdotuksen 66 §:ssä, 67 a §:ssä, 68 §:ssä ja 70 §:ssä säädettäisiin ehdotettujen 66 ja 67 §:ssä tarkoitettujen tallennettujen tietojen käyttämisestä. Tietojen käyttäminen olisi porrastettu sen mukaan, kuinka syvällisesti toimivaltuuksilla voidaan puuttua yksityiselämän suojaan. Toisin sanoen teknisten tietojen käsittelyssä (ehdotettu 66 §) voidaan käyttää ainoastaan teknisiä tietoja, hakuehtojen määrittelyssä (ehdotettu 67 a §) voidaan käyttää teknisiä tietoja ja viittä prosenttia kohteena olevan viestintäverkon osan tietoliikennettä ja varsinaisessa tietoliikennetiedustelussa (68 ja 70 §), joka puuttuu kaikista syvällisimmin yksityiselämän suojaan, voisi käyttää tallennettuja teknisiä tietoja ja hakuehtojen määrittämisen perusteella tallennettuja tietoja.

Jotta tallennettuja tietoja voitaisiin käyttää, edellyttää tämä aina tuomioistuimen lupaa varsinaisen toimivaltuuden käyttöä koskevan lupapäätöksen yhteydessä.

Edellä kuvattujen säännösehdotusten nojalla tallennettujen tietojen käytön voidaan osittain katsoa olevan lähellä ylimääräisen tiedon käyttöä. Ylimääräisellä tiedolla tarkoitetaan perinteisesti rikostorjunnassa telekuuntelulla, televalvonnalla, tukiasematietojen hankkimisella ja teknisellä tarkkailulla saatua tietoa, joka ei liity tiettyyn rikokseen tai vaaran torjumiseen taikka joka koskee muuta rikosta kuin sitä, jonka estämistä tai paljastamista varten lupa tai päätös on annettu.

Ylimääräisen tiedon käyttöä koskeva sääntely poliisilaissa on säädetty perustuslakivaliokunnan myötävaikutuksella (PeVL 67/2010 vp, s. 4—5, PeVL 33/2013 vp, s. 5—7). Valiokunta on tarkastellut sääntelyä perustuslain 10 §:ssä turvatun luottamuksellisen viestin salaisuuden kannalta. Valiokunnan mukaan on selvää, että kaikki sinänsä laillisella salaisella pakkokeinolla saatu ylimääräinen tieto ei voi olla rajoituksetta käytettävissä minkä tahansa rikoksen selvittämiseen. Luottamuksellisen viestin salaisuutta turvaavan säännöksen ensisijaisena tarkoituksena on suojata luottamukselliseksi tarkoitetun viestin sisältö ulkopuolisilta. Viestin sisältö ei menetä perustuslain suojaa pelkästään sen perusteella, että esimerkiksi telekuuntelun avulla on saatu tieto siitä. Perustuslain 10 §:n sääntely rajoittaa viestin sisällön käyttöä tämän jälkeenkin. Tämä on olennaista myös sen vuoksi, että salaisen pakkokeinon kohteeksi voi joutua kuuntelun varsinaisen kohteen lisäksi myös ulkopuolinen henkilö. Lisäksi on valiokunnan mukaan huomattava, että ylimääräisen tiedon käytön salliminen muiden vakavuusasteeltaan vähäisempien rikosten kuin kunkin telepakkokeinon perusterikosten selvittämiseen merkitsee eräänlaista välillistä telepakkokeinon käytön rajoittamisen väljennystä (PeVL 33/2013 vp, s. 6/II). (PeVL 99/2022 vp.).

Perustuslakivaliokunnan mukaan estettä ei ole ollut sille, että ylimääräisen tiedon käyttöä koskevan säännöksen piiriin otetaan joitakin sellaisiakin yksittäisiä rikoksia, joiden

enimmäisrangaistus on kaksi vuotta vankeutta mutta jotka kuitenkin vakavuusasteeltaan rinnastuvat muihin ylimääräisen tiedon käyttämisen edellytyksenä oleviin rikoksiin ja jotka täyttävät perustuslain 10 §:ssä luottamuksellisen viestin salaisuuden rajoittamiselle asetetut vaatimukset (PeVL 33/2013 vp, s. 7/I).

Perustuslakivaliokunta on rikostorjunnan osalta edellyttänyt tuomioistuimen antamaa lupaa edellytyksenä telepakkokeinolla saadun ylimääräisen tiedon käyttämiselle (PeVL 66/2010 vp s. 10/II; PeVL 67/2010 vp s. 5/I).

Esityksen 1. lakiehdotuksen 66 §:ssä, 67 a §:ssä, 68 §:ssä ja 70 §:ssä ehdotettu oikeus sotilastiedusteluviranomaiselle tallentaa tietoliikenteen teknisiä tietoja ja Suomen rajan ylittävän viestintäverkon osan tietoliikennettä voidaan pitää peruslähtökohdiltaan vastaavana tilanteena kuin rikostorjunnan ylimääräisen tiedon käyttöä. ”Ylimääräistä tietoa” hankitaan muun toimivaltuuden käytön (66 § ja 67 a §) yhteydessä kuin se, millä toimivaltuudella tietoa käytetään (67 a §, 68 ja 70 §). Ehdotetuilla muutoksilla sotilastiedusteluviranomainen voi tallentaa tietoa, joka ei liity tilanteessa käsillä olevaan tuomioistuimen lupaan.

Lukuun ottamatta teknisten tietojen käsittelyä, luvan perusteena on aina sotilaallinen toiminta tai kansallista turvallisuutta vakavasti uhkaava toiminta. Sotilastiedustelusta annetun lain 4 §:ssä on tyhjentävästi lueteltu toiminta, jonka perusteella tiedustelumenetelmiä voidaan käyttää. Toisin kuin rikostorjunnan osalta, luvan perusteena olevassa toiminnassa ei ole kyse lievemmästä ja vakavammasta toiminnasta, johon voitaisiin kohdistaa eri tiedustelumenetelmiä, vaan kaikki 4 §:ssä mainittu toiminta on yhtä vakavaa suojattavien oikeushyvien näkökulmasta.

Tallennettujen tietojen käyttö edellyttää tuomioistuimen lupaa, jossa muilta kuin teknisten tietojen käsittelyn osalta on mainittava tiedustelumenetelmän käytön kohde. Lisäksi on mainittava kohdentamisessa olennaiset seikat, kuten tietoliikenteen säännönmukaisuus hakuehtojen määrittämisessä tai hakuehdot varsinaisessa tietoliikennetiedustelussa. Teknisten tietojen osalta käsiteltävät tiedot olisi jo muutenkin rajattu teknisiin tietoihin.

Esityksen 1. lakiehdotuksen 67 a §:ssä hakuehtojen määrittämisen edellytyksenä olisi välttämättömyys, joka vastaisi sitä, mitä varsinaisen tietoliikennetiedustelun osalta on jo voimassa olevassa laissa. Tallennettuja tietoja ei myöskään saisi käyttää muiden kuin ehdotettujen 66 §:ssä ja 67 a §:ssä sekä jo säädettyjen 68 ja 70 §:ssä tarkoitettujen tiedustelumenetelmien käytössä.

Teknisten tietojen historiatiedon avulla varsinaisessa tietoliikennetiedustelussa pystyttäisiin todentamaan esimerkiksi se, onko kohde viestinyt jo aiemmin Suomen rajan ylittävän viestintäverkon osan kautta. Tiedot ovat välttämättömiä esimerkiksi kahden viestivän tahon pidempikestoisen kanssakäymisen varmistamiseksi (viestin sisällöllä ei ole merkitystä) tai mahdollisimman tarkkojen hakuehtojen määrittämisen varmistamiseksi.

Kaikki edellä mainittujen toimivaltuuksien käytön edellytyksenä on tuomioistuimen lupa. Tuomioistuin voi myös rajoittaa toimivaltuuksien käytön kohdentumista tallennettuun tietoon kokonaan tai esimerkiksi ajallisesti. Tuomioistuimelle tehtävässä vaatimuksessa olisi myös esitettävä se, että toimivaltuutta tullaan käyttämään myös tallennettuihin tietoihin ja perusteltava se.

Edellä tarkoitettujen säännösten perusteella tallennettuja tietoja ei voida käyttää muiden tiedustelumenetelmien kuin tietoliikennetiedustelun kokonaisuuden yhteydessä.

Säännösehdotuksen voidaan katsoa parantavan tietoliikennetiedustelun kokonaisuuden kohdentumista ja tätä kautta säännösehdotuksella voidaan katsoa olevan perusoikeusmyönteisiä vaikutuksia.

10.2.2.5 Tiedonhankinta sotilastiedustelun kohteen tietoliikenteestä

Viestin sisältöön kohdistuvat hakuehdot

Lakiehdotuksen 70 §:n muutokset puuttuvat viestin sisällön suojaan. Säännösehdotuksesta poistettaisiin ehdoton kielto käyttää viestin sisältöön meneviä kielellisiä hakuehtoja. Viestin sisältöön menevien kielellisten hakuehtojen käyttö olisi mahdollista yhdessä muiden kuin viestin kielellistä sisältö kuvaavien hakuehtojen kanssa. Muut kuin viestin sisältöä koskevat kielelliset hakuehdot voisivat olla myös viestin sisällössä.

Perustuslakivaliokunta ei ole ottanut suoraan kantaa viestin sisältöön menevien hakuehtojen käytön kieltoon, lukuun ottamatta haittaohjelmaa kuvaavaa tietoa. Perustuslain 10 §:ää koskevassa hallituksen esityksessä (HE 198/2017 vp.) on todettu, että vieraan valtion viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa. Perustuslakivaliokunta totesi muutosta koskeneessa mietinnössään (PuVM 4/2018 vp.), että vaikka vieraan valtion sotilas- tai muun viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa, sotilastiedustelutoimivaltuuksia ei voida kohdistaa kaikissa tapauksissa niin täsmällisesti, ettei olisi vaaraa viranomaisten tilapäisestä pääsystä yksittäisten, tiedustelutehtävään liittymättömien henkilöiden viestintää koskeviin tietoihin, mikä tulee perustuslakivaliokunnan mielestä tavallisissa laeissa rajata mahdollisimman vähäiseksi. Näin ollen viestin sisältöön menevän hakuehdon käyttö on voinut olla mahdollista valtiollisen toimijan tietoliikenteeseen kohdistuvassa tiedustelussa.

Uudemmassa käytännössään perustuslakivaliokunta on aiempaa tarkemmin arvioinut haittaohjelman tai käskyn suhdetta perustuslain 10 §:n 2 momenttiin. Perustuslakivaliokunta kiinnitti kyberturvallisuuslakia koskevasta hallituksen esityksestä (HE 57/2024 vp.) antamassaan lausunnossa (PeVL 62/2024 vp, kohta 12) huomiota siihen, että lakiehdotusten mukainen haitallisen tietokoneohjelman tai käskyn sisältämä viesti jää kokonaan perustuslain 10 §:n luottamuksellisen viestin salaisuuden soveltamisalan ulkopuolelle. Kyse ei siten ole vain siitä puheena olevan esityksen säätämisjärjestysperusteluissa osin viitatusta seikasta, että tällainen viesti jäisi luottamuksellisen viestin ydinalueen ulkopuolelle. Tällainen viesti ei nauti perustuslain 10 §:n 2 momentin mukaista suojaa, eikä sitä koskevaa sääntelyä tarvitse arvioida 10 §:n 4 momentin mukaisten erityisten tai perusoikeuksien yleisten rajoitusedellytysten valossa. (PeVL 62/2024 vp., kohta 12). Näin ollen myös voimassa olevan sotilastiedustelusta annetun lain 70 §:n 3 momentti vastaa sitä, mitä perustuslakivaliokunta on myöhemmin käytännössään vahvistanut.

Perustuslakivaliokunta on lausuntokäytännössään (PeVM 4/2018 vp.) korostanut sitä, että perustuslain 10 §:n 4 momentin sääntely ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa. Perustuslain 10 §:ään sisältyvä välttämättömyyskriteeri puolestaan tarkoittaa valiokunnan mukaan, että luottamuksellisen viestin salaisuuteen kohdistunut rajoitus on sallittu vain, jos tiedonhankinta ei ole mahdollista vähemmän puuttuvin keinoin, ja että tiedon hankkimisessa puututaan luottamuksellisen viestin salaisuuteen mahdollisimman kohdennetusti ja rajoitetusti. Valiokunta on muutenkin korostanut perusoikeuksien yleisten rajoitusedellytysten merkitystä uutta rajoitusperustetta tulkittaessa.

Perustuslakivaliokunta on HE 203/2017 koskevissa lausunnoissaan (PeVL 36/2018 vp. s. 24 ja 76/2018 vp. s. 3) edellyttänyt hakuehtojen määritelmästä säätämistä. Lakiin säädettiin

perustuslakivaliokunnan myötävaikutuksella hakuehtojen määritelmä, jonka mukaan sillä tarkoitetaan tietoa, jonka perusteella tietoliikennetiedustelulla viestintäverkon osasta mahdollisimman rajatusti ja täsmällisesti valitaan tietoliikennetiedustelun kohteena oleva tietoliikenne ja puuttuminen luottamuksellisen viestin salaisuuden suojaan rajautuu tiedustelun tarkoituksen kannalta välttämättömään.

Voimassa olevan viestin sisältöön menevän hakuehdon ehdottoman kiellon myötä perustuslakivaliokunnan myötävaikutuksella säädetty hakuehdon määritelmä ei aina rajaa ensi vaiheessa tietoliikennetiedustelulla hankittua tietoa välttämättömään. Voimassa olevan lain 70 §:n mukaan hakuehtojen mukaista tietoliikennettä voidaan käsitellä automaattisesti ja manuaalisesti, missä vaiheessa hankittuun tietoliikenteeseen voidaan kohdistaa myös viestin sisältöä koskevia hakuehtoja. Vaikka yksittäinen viranomainen ei hakuehtojen mukaisen tietoliikenteen teknisen käsittelyn yhteydessä varsinaisesti perehdy tietoliikenteessä olevien viestien sisältöön, voidaan hakuehtojen mukaisen tietoliikenteen käsittelyä ylipäänsä pitää merkittävämpänä puuttumisena viestin salaisuuden suojaa kuin sitä, että tietoliikennettä rajattaisiin hakuehtoja vastaavaan tietoliikenteeseen (myös aiemmin EIT tapaus Centrum för Rättvisa).

Nyt esitetty ehdotus antaisi mahdollisuuden käyttää viestin sisältöön kohdistuvia kielellisiä hakuehtoja yhdessä muiden (jo nykyisin sallittujen) hakuehtojen kanssa. Viestin kielellisellä sisällöllä tarkoitetaan käytännössä viestin semanttista sisältöä, eli viestin merkityksellistä sisältöä. Näin ollen hakuehtona voitaisiin käyttää kielellisiä ilmaisuja yhdessä muiden kuin viestin sisältöä kuvaavien kielellisten hakuehtojen kanssa. Hakuehtojen yhdistelmä rajaa tietoliikennetiedustelujärjestelmään tulevaa tietoliikennettä aiempaa tarkemmin, jolloin viranomaisen manuaalisessa ja automaattisessa käsittelyssä on aiempaa vähemmän tietoliikennettä. Tämän voidaan katsoa toteuttavan voimassa olevaa sääntelyä paremmin perustuslakivaliokunnan esittämää vaatimusta tietoliikennetiedustelun kohdentumisesta ainoastaan välttämättömään.

Esityksessä ehdotetaan myös, että jo voimassa olevan sääntelyn mukainen hakuehto (muu kuin kielellinen hakuehto) voisi olla viestin sisällössä. Tässä yhteydessä tarkoitetun hakuehdon voidaan katsoa kohdentuvan tarkasti. Esimerkiksi tilanteessa, jossa varsinainen viesti välitystietoineen on toisen viestin sisällä (esimerkiksi VPN-tunnelointi), hakuehdot kohdistuvat oikein ja välttämättömään, vaikka hakuehto ei kohdistukaan viestin ulompaan kuoreen. Toisaalta hakuehto voi olla viestin sisällössä tilanteessa, jossa kohteena olevan käyttämä laite tallentaa pilvipalveluun tietoja, kuten yhteystietoja. Tässäkin tapauksessa hakuehdon voidaan katsoa kohdistuvan välttämättömään.

Määritelmällisesti viestin sisältöä kuvaavat hakuehdot voivat olla jo nykyisen hakuehdon määritelmän alassa, tosin hakuehdon ollessa viestin sisällössä, viestintä on hävitettävä viipymättä.

Nyt käsiteltävänä olevaa ehdotusta voidaan pitää suhteellisena, sillä tarpeetonta tietoliikennettä voitaisiin poistaa jo tietoliikenteen hakuehtojen käyttöön perustuvassa tietoliikenteen hankinnan vaiheessa. Tällä hetkellä sotilastiedusteluviranomainen voi hakuehtojen mukaisen tietoliikenteen hankinnan jälkeen käsitellä viestintää automaattisesti ja manuaalisesti, missä vaiheessa viestintään voidaan kohdistaa myös kielellisiä hakuehtoja. Ehdotuksen myötä sotilastiedusteluviranomaisen jatkokäsiteltäväksi tulisi aiempaa vähemmän viestintää ja tiedonhankinta tietoliikenteestä olisi näin ollen kohdennetumpaa ja rajatumpaa.

Ehdotetulla muutoksella voidaan arvioida olevan perusoikeusmyönteisiä vaikutuksia, sillä se rajaisi sotilastiedusteluviranomaisen käsittelyyn tulevan tietoliikenteen määrää ja toteuttaisi

hakuehdon määritelmää aiempaa paremmin. Lisäksi hakuehtojen käytön vaiheessa tapahtuvaa viestintään puuttumista ei voida pitää yhtä merkittävänä puuttumisena yksityisyyden suojaan kuin sitä, että viranomaisen virkamies käsittelee ja perehtyy viestin sisältöön.

Suomessa olevaan henkilöön tai telepäätelaitteeseen kohdistuvat hakuehdot

Esityksen 1. lakiehdotuksen 68 ja 70 §:n mukaan tietoliikenteeseen kohdistuvaa tiedustelu koskevia säännöksiä muutettaisiin niin, että ehdoton kielto käyttää Suomessa olevaan tai oletettavasti olevaan henkilöön tai päätelaitteeseen kohdistuvia hakuehtoja muuttuisi. Muutoksen myötä tällaisia hakuehtoja voitaisiin käyttää tilapäisesti. Käytännössä tilapäisyys merkitsisi sitä ajanjaksoa, jonka aikana Suomessa olevaan kohteeseen pystyttäisiin kohdistamaan tarkempia tiedustelumenetelmiä.

Perustuslakivaliokunta ei ole nimenomaisesti ottanut kantaa Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöivien tietojen käyttämiseen hakuehtona. Perustuslakivaliokunta on lausuntokäytännössään (PeVM 4/2018 vp.) korostanut sitä, että perustuslain 10 §:n 4 momentin sääntely ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa. Perustuslain 10 §:ään sisältyvä välttämättömyyskriteeri puolestaan tarkoittaa valiokunnan mukaan, että luottamuksellisen viestin salaisuuteen kohdistunut rajoitus on sallittu vain, jos tiedonhankinta ei ole mahdollista vähemmän puuttuvin keinoin, ja että tiedon hankkimisessa puututaan luottamuksellisen viestin salaisuuteen mahdollisimman kohdennetusti ja rajoitetusti. Valiokunta on muutenkin korostanut perusoikeuksien yleisten rajoitusedellytysten merkitystä uutta rajoitusperustetta tulkittaessa.

Voimassa oleva sotilastiedustelusta annettu laki ei anna mahdollisuutta käyttää Suomeen saapuneesta kohteesta saatua tietoa, sillä lain 82 §:n 2 momentin mukaan saatu tieto olisi hävitettävä viipymättä ja hakuehdon käyttö lopetettava.

Nyt käsiteltävänä olevassa säännösehdotuksessa ehdotetaan, että tietoliikennetiedustelussa voitaisiin käyttää tilapäisesti Suomessa oleskelevaan tai oletettavasti oleskelevaan henkilöön tai tämän telepäätelaitteeseen kohdistuvaa hakuehtoa. Perustuslakivaliokunnan myötävaikutuksella säädetyllä hakuehdolla tarkoitetaan tietoa, jonka perusteella tietoliikennetiedustelulla viestintäverkon osasta mahdollisimman rajatusti ja täsmällisesti valitaan tietoliikennetiedustelun kohteena oleva tietoliikenne ja puuttuminen luottamuksellisen viestin salaisuuden suojaan rajautuu tiedustelun tarkoituksen kannalta välttämättömään. Hakuehto, joka sinänsä kohdistuu oikeaan kohteeseen, ei valikoi tietoliikennettä sen mukaan, missä pääte laite mahdollisesti sijaitsee.

Suomessa oleskelevaan tai oletettavasti oleskelevaan henkilön tai tämän telepäätelaitteeseen kohdistuvan hakuehdon käyttöä rajattaisiin ajallisesti tilapäisyyteen. Hakuehdon käyttö olisi lopetettava ja siirryttävä käyttämään kohdennetumpaa tiedustelumenetelmää heti, kun se on käytännössä mahdollista. Tätä tosin ilmaisee jo laissa lain 70 §:n 1 momentissa säädetty edellytys, että kyseistä tiedustelumenetelmää voidaan käyttää vain, jos tieto ei ole hankittavissa muulla tiedustelumenetelmällä. Tilapäisyys-kriteeri korostaisi osaltaan suhteellisuusperiaatteen ja tarkoitussidonnaisuuden periaatteen toteutumista lain 68 ja 70 §:n osalta sekä 70 §:n 1 momentissa säädettyä viimesijaisuutta.

On huomattava, että muutosehdotuksen ei voida katsoa mahdollistavan kohdennetumpien tiedustelumenetelmien kiertämistä. Muilta osin tietoliikennetiedustelua koskevat rajoitukset esimerkiksi Suomen sisäistä tietoliikennettä koskien ovat edelleen voimassa. Näin ollen kohteena olisi joka tapauksessa tietoliikenne, joka on tarkoitettu Suomen rajan ylittäväksi.

Suomen rajan ulkopuolelta tuleva sotilaallinen toimija tai kansallista turvallisuutta vakavasti uhkaava toimija on pystyttävä tunnistamaan ja kohteeseen on voitava käyttää mahdollisimman kohdennettuja tiedustelumenetelmiä myös tämän saapuessa Suomen alueelle. Tässä tapauksessa Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöivät tiedot ovat tarkkoja ja kohdistuvat tuomioistuimen luvan mukaisesti tarkasti sotilastiedustelun kohteena olevaan toimijaan.

Perustuslain suojaamia oikeushyviä, kuten kansallinen turvallisuus ja Suomen täysivaltaisuus sekä ihmisten hengen ja terveyden suojaaminen, voidaan pitää niin merkittävinä, että myös Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen käytön kiellon poisto hakuehtona on perusteltua. Etenkin Suomen täysivaltaisuuden suojaamisen osalta merkittävänä voidaan pitää tietoa, että valtiollinen toimija saapuu Suomeen tai kohteena oleva valtiollinen toimija viestii vakituiseen Suomessa olevan tahon kanssa. Näin ollen säännösehdotuksella voidaan katsoa olevan myös perusoikeusmyönteisiä vaikutuksia.

10.2.2.6 Oikeusturva

Perustuslain 21 §:n mukaan jokaisella on oikeus saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivytystä lain mukaan toimivaltaisessa tuomioistuimessa tai muussa viranomaisessa sekä oikeus saada oikeuksiaan ja velvollisuuksiaan koskeva päätös tuomioistuimen tai muun riippumattoman lainkäyttöelimen käsiteltäväksi. Käsittelyn julkisuus sekä oikeus tulla kuulluksi, saada perusteltu päätös ja hakea muutosta samoin kuin muut oikeudenmukaisen oikeudenkäynnin ja hyvän hallinnon takeet turvataan lailla.

Perustuslakivaliokunta toteaa perusoikeusuudistuksesta antamassaan mietinnössä, että perusoikeuksia rajoitettaessa on huolehdittava riittävistä oikeusturvajärjestelyistä. (PeVM 25/1994 vp, s. 5.) Oikeusturvajärjestelyillä viitataan ennen kaikkea muutoksenhakumahdollisuuteen, mutta kysymykseen voivat tulla myös muut menettelylliset oikeusturvatakeet.

Euroopan ihmisoikeussopimuksen oikeutta tehokkaaseen oikeussuojakeinoon koskevan 13 artiklan mukaan jokaisella, jonka sopimuksessa tunnustettuja oikeuksia ja vapauksia on loukattu, on oltava käytettävissään tehokas oikeussuojakeino kansallisen viranomaisen edessä siinäkin tapauksessa, että oikeuksien ja vapauksien loukkauksen ovat tehneet virantoimituksessa olevat henkilöt.

Perutuslakivaliokunta on korostanut sotilastiedustelusta annetun lain käsittelyssä (PeVL 36/2018 vp.) vahvoja oikeusturvatakeita, laaja-alaista ja tehokasta tiedusteluvaltuuksien käytön valvontaa sekä riittäviä soveltamisrajoituksia. Kyse on poikkeuksellisesta rajoitusperusteesta, jossa on irtauduttu rikosperusteisesta toiminnasta ja joka tulee siten sovellettavaksi ti-lanteissa, joissa ei tiedonhankintavaiheessa tai muutoinkaan voida kohdistaa konkreettista ja yksilöityä rikosepäilyä (PeVM 4/2018 vp, s. 8).

Tiedustelun tarkoituksesta johtuen ennakollinen lupamenettely ja tiedustelun toimeenpanon valvonta eivät yleensä voi tulla tiedustelun kohteen tietoon. Menettelyn itsessään tulee siten antaa turva mielivaltaa vastaan. Valiokunnan mielestä EIT:n käytännöstä ilmenee, että oikeudellinen kontrolli tuomioistuimessa turvaa parhaiten kontrollin itsenäisyyden ja puolueettomuuden vaatimukset (PeVL 36/2018 vp.).

Tiedustelumenetelmien osalta oikeusturvavaatimuksen täyttyminen asettaa erityisiä haasteita, koska toimivaltuuksien kohteet eivät voi turvautua tavanomaisiin oikeusturvakeinoihin

varsinaisen tiedustelumenetelmän käyttöä koskevan päätöksen osalta. Tämän takia on oltava muita oikeusturvajärjestelyitä, joilla yksilön oikeusturva taataan riittävällä varmuudella samalla viranomaisten mielivaltaa ja väärinkäytöksiä ehkäisten.

Tiedustelutoiminnassa korostuvat oikeusturvajärjestelyjen ja valvonnan tehokkuus sekä asianmukaisuus. Myös ihmisoikeusvelvoitteet ja Euroopan unionin oikeusjärjestys edellyttävät luottamuksellisen viestin salaisuuden suojaan puuttuvien toimivaltuuksien käytön valvonnalta tehokkuutta ja riippumattomuutta. On tärkeää, että tiedusteluviranomaisella ei ole rajoittamatonta harkintavaltaa tiedonhankinnan kohdentamisessa.

Yksi tapa rajoittaa viranomaisen harkintavaltaa on osoittaa vakavinta puuttumista perusoikeussuojaan tarkoittava tiedustelumenetelmien käytöstä päättäminen riippumattomalle tuomioistuimelle (muun muassa Weber ja Saravia v. Saksa). Tietoliikennetiedustelun osalta tiedusteluviranomaisella ei voi myöskään olla suoraa ja rajoittamatonta pääsyä tietoliikenneverkkoihin (Kennedy v. Yhdistynyt Kuningaskunta).

EIT:n ratkaisukäytännössä korostuu myös se, että ensisijainen vastuu toiminnan lainmukaisuudesta on viranomaisella. Tämä korostaa osaltaan sitä, että perusoikeuksien rajoittamisvaltuuksia annetaan vain henkilöille, joilla on riittävä koulutus ja pätevyys, mikä taas korostuu tilanteissa, joissa viranomaisen päätöksistä ei lähtökohtaisesti tehdä ilmoitusta päätöksen kohteelle (PeVL 17/1998 vp, s. 2–3). Riittävällä koulutuksella ja pätevyydellä varmistetaan myös perus- ja ihmisoikeusnormien tunnistaminen ja kyky perus- ja ihmisoikeusnormien soveltamiseen käsillä olevassa tilanteessa.

Ilmoitusvelvollisuuden toisena puolena on nähty sen preventiivinen vaikutus viranomaistoimintaan. Ilmoitusvelvollisuus toisin sanoen ohjaa viranomaista käyttämään tiedustelumenetelmiä oikeassa laajuudessa ja ehkäisten väärinkäytöksiä, koska tiedonhankinta tulee kohteen tietoisuuteen jossain vaiheessa.

Ilmoittamisella on katsottu lisäksi olevan merkitystä yleisesti tiedonhankintakeinojen käytön luotettavuuden kannalta. Yhteisöllä on yleisesti intressi valvoa, että tiedonhankintakeinoja käytetään hyväksyttävissä rajoissa.

Tiedustelumenetelmien osalta ei voida käyttää muutoksenhakumahdollisuutta tai ilmoitusvelvollisuutta oikeusturvan takeena. Voidaan kuitenkin katsoa, että tätä kompensoidaan muilla valvonta- ja oikeusturvajärjestelyillä. Näitä ovat riippumaton ulkopuolinen valvonta (tiedusteluvalvontavaltuutettu), joka valvoo laajasti toimintaa sekä tiedustelumenetelmien käyttöä etukäteisesti, reaaliaikaisesti ja jälkikäteisesti. Syvästi perusoikeuksiin puuttuvista tiedustelumenetelmistä päätöksen tekee tuomioistuin, jolle toimitettavassa vaatimuksessa esitettävistä seikoista on säädetty tarkoin laissa. Sotilastiedusteluviranomaisen oman, sisäisen laillisuusvalvonnan lisäksi sotilastiedustelua valvoo Puolustusvoimien asessori ja puolustusministeriö. Toimintaa valvoo myös eduskunnan oikeusasiamies.

Edellä todettujen lisäksi puolustusministeriön on toimitettava kertomus kerran vuodessa eduskunnan tiedusteluvalvontavaliokunnalle, eduskunnan oikeusasiamiehelle ja tiedusteluvalvontavaltuutetulle tiedustelumenetelmien käytöstä ja niiden suojaamisesta.

Kansalaisten ja yksittäisten henkilöiden osalta merkittävä on oikeus tehdä tiedusteluvalvontavaltuutetulle tutkimispyyntö (laki tiedustelutoiminnan valvonnasta 12 §) ja kantelu (laki tiedustelutoiminnan valvonnasta 11 §).

Vaikka sinänsä ilmoitusvelvollisuudella taataan yksilön mahdollisuus oikeusturvaan ja luodaan läpinäkyvyyttä, voidaan salaisessa viranomaistoiminnassa katsoa olevan kyse ennen kaikkea toiminnan vastuullisuudesta. Kyse on siitä, voidaanko virkamiehet saattaa oikeudelliseen vastuuseen mahdollisista laiminlyönneistä. Kuten edellä on todettu, sotilastiedustelutoiminnan valvontaan osallistuu useita ulkopuolisia, toiminnasta riippumattomia tahoja, jotka yksin ja yhdessä toteuttavat myös yksilön oikeusturvaa. Lisäksi vaatimuksia ja päätöksiä sotilastiedusteluviranomaisessa tekevät erityisen koulutuksen ja perehtyneisyyden saaneet virkamiehet, tiedustelumenetelmän käytön edellytykset on tarkkaan säädetty sekä tiedustelumenetelmien käyttöä koskevien vaatimusten ja päätösten sisällöstä on tarkkaan säädetty. Yksilö itse voi taas tehdä tutkimispyynnön tai kantelun tiedusteluvalvontavaltuutetulle vaikkei olisi ilmoitusta tiedustelumenetelmän käytöstä saanutkaan.

Koska tiedusteluvalvontavaltuutetulle tehtävien tutkimispyyntöjen ja kanteluiden edellytyksenä ei ole kohteelle tai kohteeksi joutuneelle toimitettu ilmoitus, voidaan tämän osaltaan myös kompensoivan ilmoitusvelvollisuuden preventiivistä vaikutusta. Koska kuka tahansa voi tehdä tutkimispyynnön tai kantelun, voidaan sotilastiedusteluviranomaiseen katsoa kohdistuvan laajaa valvontaa myös kansalaisten osalta. Tämä osaltaan ohjaa sotilastiedusteluviranomaista tarkkaan lainsoveltamiseen, jotta tiedusteluvalvontavaltuutetulle tehty tutkimispyyntö tai kantelu eivät johda jatkotoimenpiteisiin. Tiedusteluvalvontavaltuutettu voi saattaa asian esitukintaviranomaisen selvitettäväksi ja toisaalta myös keskeyttää tai lopettaa tiedustelumenetelmän käytön, jolloin asia on myös saatettava tuomioistuimen ratkaistavaksi. Rikosvastuuseen saattaminen ja vahingonkorvausten maksaminen aiheuttavat koko sotilastiedustelutoiminnalle niin merkittäviä riskejä, kuten maineriski ja luottamuksen rapautuminen sotilastiedusteluviranomaiseen, että tämäkin ohjaa sotilastiedusteluviranomaista toimimaan lakia tarkasti noudattaen ja toiminnan tarkkaan suuntaamiseen ja kohdentamiseen.

Tietoliikennetiedustelussa kokonaisuutena käsitellään henkilötietoja, joten sitä voidaan oikeusturvan osalta arvioida myös tästä näkökulmasta. Henkilötietojen käsittelystä Puolustusvoimissa säädetään siitä annetussa laissa. Sen mukaan henkilö voi henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain 29 §:n mukaisesti pyytää tietosuojavaltuutettua tarkastamaan henkilötietojen ja niiden käsittelyn lainmukaisuus.

Vaikka tiedonhankinnan kohteelle ei annettaisi ilmoituksella tietoa häneen kohdistuneesta tietoliikennetiedustelusta, voidaan järjestelmän kokonaisuudessaan katsoa takaavan yksilön oikeusturvan asettamat vaatimukset ja viranomaisen vastuu toimenpiteistään voidaan toteuttaa. Tiedustelutoiminnassa yksilön oikeusturva toteutuukin useamman tekijän yhteisvaikutuksesta.

Ehdotetun sääntelyn ei siten katsota olevan ongelmallinen perustuslain 21 §:n kannalta.

10.2.3 Sotilastiedusteluviranomaisen ulkopuolisen suorittamat toimenpiteet

10.2.3.1 Viranomaisen ulkopuolinen taho

Toimenpiteiden suorittamisen luonteesta

Hallituksen esityksen 1. lakiehdotuksen 42 §:n 2 momentissa ehdotetaan, että säännöksen tarkoittaman laitteen, menetelmän tai ohjelmiston asentamisen tai poisottamisen voisi suorittaa myös viranomaisen ulkopuolinen taho. Säännöksen tarkoittama toimi olisi rajattu asennukseen ja poisottamiseen. Ehdotetulla sääntelyllä on merkitystä perustuslain 2 §:n 3 momentissa säädetyn oikeusvaltioperiaatteen, 10 §:ssä säädetyn yksityiselämän suojan, 21 §:ssä säädetyn

oikeusturvan, 22 §:ssä säädetyn perusoikeuksien turvaamisen ja 124 §:ssä säädetyn julkisen hallintotehtävän antamista koskevan perustuslain säännöksen kannalta.

Ehdotetussa sääntelyssä olisi kyse viranomaisen toimivallassa olevien toimenpiteiden tapauskohtaisesta suorittamisesta tilanteessa, jossa tiedusteluviranomainen ei itse pääse suorittamaan tiedustelumenetelmän käytön mahdollistavaa toimenpidettä tai toimenpiteen suorittaminen vaatisi kohtuuttomia resursseja suhteessa saataviin hyötyihin. Kyse on osittain ohjatun tietolähdetoiminnan kaltaisesta tilanteesta. Ohjatusta tietolähdetoiminnasta on säädetty perustuslakivaliokunnan myötävaikutuksella (PeVL 66/2010 vp.).

Ehdotettujen toimenpiteiden suorittaminen tapahtuisi viranomaisvalvonnan ja -ohjauksen alaisena tiedustelumenetelmän käytön mahdollistamiseksi, jos varsinaista tiedustelumenetelmää koskevat edellytykset täyttyvät ja tiedustelumenetelmän käytöstä on tehty asianmukainen päätös tai saatu lupa.

Ehdotetun säännöksen arvioinnin kannalta lähimmän verrokin voimassa olevassa lainsäädännössä voidaan katsoa olevan tietolähdetoiminta ja pieneltä osin peitetoiminta, joiden kautta säännösehdotuksen suhdetta perustuslakiin voidaan jossain määrin arvioida. Kummankin osalta on huomattava, että nyt käsiteltävänä oleva säännösehdotus ei kuitenkaan edellytä pääsääntöisesti henkilöltä kohteena olevaan toimintaa soluttautumista.

Tietolähdetoimintaa ei ole arvioitu perustuslakivaliokunnan tähänastisessa lausuntokäytännössä perusoikeuksien kannalta. Tietolähdetoimintaa koskeva säännös on katsottu tarpeelliseksi hallinnon lainalaisuusperiaatteen näkökulmasta (HE 266/2004 vp s. 24). Esityksessä ehdotettiin useita muutoksia poliisilakiin, mutta perustuslakivaliokunta ei ole katsonut nimenomaisesti tietolähdetoiminnan perustuslainmukaisuuden (PeVL 11/2005 vp.) arviointia tarpeelliseksi. Tietolähdetoimintaa koskevia säännöksiä on muutettu poliisi- ja pakkokeinolakien kokonaisuudistuksessa (806/2011 ja 872/2011). Esityksiä koskevissa perutuslakivaliokunnan lausunnoissa (PeVL 66/2010 vp. ja PeVL 67/2010 vp.) perustuslainmukaisuutta ei edelleenkään katsottu tarpeelliseksi arvioida. Vastaavasti tiedustelutoimintaa koskevan lainsäädännön osalta tietolähdetoimintaa koskevien säännösten perustuslainmukaisuutta ei arvioitu (PeVL 35/2018 vp. ja 36/2018 vp.).

Kuten tietolähdetoiminnassa, säännösehdotuksessa esitettyjen toimenpiteiden suorittaminen perustuu lähtökohtaisesti henkilön pääsyyn tiettyyn tilaan, laitteelle tai tietojärjestelmään sekä henkilön olemassa oleviin kontakteihin, ihmissuhteisiin ja tavanomaiseen kanssakäymiseen. Toimenpiteiden suorittamista ei voitaisi arvioida perusoikeussuojan rajoittamisen kannalta samoista lähtökohdista kuin peiteltyä tiedonhankintaa tai peitetoimintaa, koska toimenpiteissä ei ole kyse soluttautumisesta vaan henkilön olemassa olevien pääsyn ja verkostojen hyödyntämisestä. Sotilastiedusteluviranomaisella ei ole lähtökohtaisesti vastaavaa pääsyä näihin tai pääsy vaatisi merkittävien resurssien käyttämistä. Kuten tietolähdetoiminnassa. toimenpiteitä suorittavan henkilön olisi voitava suorittaa toimenpiteitä tavalla, joka vastaisi hänen normaalia toimintaansa tai kanssakäymistä, koska muussa tapauksessa toiminta voisi johtaa viime kädessä henkilön hengen ja terveyden vaarantavaan tilanteeseen.

Tietolähdetoiminnassa ei katsota olevan kyse julkisen vallan puuttumisesta henkilön yksityiselämään, vaan yksilöiden keskinäisistä suhteista ja kanssakäymisestä sekä niiden hyödyntämisestä kohteena olevan uhan seurannassa. Toimenpiteiden suorittamisessa voidaan katsoa olevan vastaavasta tilanteesta kyse siltä osin, kuin toimenpiteen suorittamisessa jouduttaisiin hyödyntämään ihmissuhteita ja kanssakäymistä, joka voi olla edellytyksenä esimerkiksi tiettyyn tilaan pääsylle.

Nyt käsiteltävänä olevan säännösehdotuksen voidaan katsoa sisältävän myös piirteitä peitetoiminnasta. Perustuslakivaliokunta on rikostorjunnan osalta luonnehtinut peitetoimintaa epäsovinnaiseksi toimivaltuudeksi, sillä se antaa viranomaiselle oikeuden toimia vastoin joitain rikosoikeudellisia kieltoja ilman virkavastuuta. Valiokunnan lausunnon mukaan hallinnon lainalaisuuden periaatteen voidaan katsoa merkitsevän muun ohella sitä, että viranomaiselle ei ilman erittäin painavia syitä ja täsmällisesti määriteltyjä edellytyksiä voida antaa toimivaltaa suorittaa toimia, jotka muutoin ovat rikosoikeudellisesti sanktioituja myös viranomaisen tekeminä (PeVL 5/1999 vp, s. 5). Esityksessä ehdotetaan säädettävän viranomaisen ulkopuoliselle oikeus suorittaa toimenpiteitä, jotka voisivat täyttää tilanteen mukaan jonkin rikoksen tunnusmerkistön. Tarkoitetut toimenpiteet ovat kuitenkin sellaisia, joita viranomainen itse voi tehdä syyllistymättä rikokseen.

Koska kyse on tiedustelumenetelmän käyttöön sidotusta liitännäisestä toimenpiteestä, toimenpiteen suorittaminen on sidottu sotilastiedustelusta annetun lain 4 §:n kohteisiin perustuvaan tiedustelutehtävään sekä tiedustelumenetelmän käyttöä koskevaan päätökseen tai lupaan. Näin ollen toimenpiteiden suorittamista koskevassa säännöksessä ei ole tarpeen erikseen sitoa toimenpiteiden suorittamista sotilastiedustelun kohteisiin vastaavasti kuin mitä on säädetty ohjatun tietolähdetoiminnan ja peitetoiminnan osalta.

Toimenpiteen suorittamisessa ei ole kyse yksityiselämän suojan kannalta merkityksellisestä soluttautumisesta.

Edellä todetun myötä ja siksi, että kyse on luonteeltaan epäitsenäisestä toiminnasta, toimenpiteiden suorittamisessa ei voida katsoa olevan kyse toiminnasta, jota olisi perusteltua arvioida eri tavoin kuin tietolähteen käyttöä.

Ehdotetun sääntelyn ei katsota eroavan perusoikeusjärjestelmän näkökohdista arvioiden perustuslakivaliokunnan myötävaikutuksella säädetystä ohjatun tietolähteen käytöstä (PeVL 66/2010 vp ja PeVL 67/2010). Toimenpiteiden suorittamisen perusteella olisi mahdollista kohdentaa tarkemmin tiedustelumenetelmiä ilman, että aiempaa kattavaa tiedonhankintaa joudutaan tekemään. Tällä voidaan katsoa olevan perusoikeusmyönteisiä vaikutuksia, kun muiden perusoikeuksiin merkittävästikin puuttuvien tiedustelumenetelmien käyttöajat ja -tarpeet vähentyisivät.

Suhde julkisen vallan käyttämiseen

Perustuslain 124 §:n mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan antaa vain viranomaiselle.

Julkisella hallintotehtävällä viitataan verraten laajaan hallinnollisten tehtävien kokonaisuuteen, johon kuuluu muun ohella lakien toimeenpanoon sekä yksityisten henkilöiden ja yhteisöjen oikeuksia, velvollisuuksia ja etuja koskevaan päätöksentekoon liittyviä tehtäviä (PeVL 8/2022 vp, s. 3–4).

Perustuslain 124 §:ssä tarkoitetun julkiseen hallintotehtävään liittyen lähtökohtana on, että tällaisten tehtävien antaminen yksityiselle ei saa vaarantaa perusoikeuksia, oikeusturvaa eikä muita hyvän hallinnon vaatimuksia (ks. esim. PeVL 48/2001 vp, s. 3). Perustuslakivaliokunnan tulkintakäytännössä on katsottu, että oikeusturvan ja hyvän hallinnon vaatimusten toteutumisen varmistaminen perustuslain 124 §:ssä tarkoitetussa merkityksessä edellyttää, että asian

käsittelyssä noudatetaan hallinnon yleislakeja ja että asioita käsittelevät toimivat virkavastuulla (PeVL 3/2009 vp, s. 4 ja PeVL 20/2006 vp, s. 2).

Perustuslakivaliokunnan lausuntokäytännössä on arvioitu useissa eri yhteyksissä erinäisiä toimintoja suhteessa niiden luonteeseen julkisena hallintotehtävänä (ks. esim. PeVL 26/2017 vp). Perustuslakivaliokunnan käytännössä julkisen hallintotehtävän hoitamisena on pidetty muun muassa yksityisten palveluntuottajien tarjoamia lakisääteisiä sosiaali- ja terveyspalveluja (PeVL 15/2018 vp), järjestyksen ja turvallisuuden ylläpitämistä (PeVL 20/2002 vp, s. 2), vartioimisliiketoimintaa (PeVL 28/2001 vp, s. 5), viranomaisten yhteishankintayhtiönä toimimista (PeVL 15/2019 vp), meripelastustoimea (PeVL 24/2001 vp), lakisääteistä työeläkevakuutusta (PeVL 45/1996 vp), viranomaisen vastuulla olevaa neuvontaa (PeVL 11/2006 vp) ja jätehuoltotehtäviä (PeVL 58/2010 vp).

Merkittävänä julkisen vallan käyttönä on taas pidetty perustuslakiuudistuksen esitöiden mukaan esimerkiksi itsenäiseen harkintaan perustuvaa oikeutta käyttää voimakeinoja tai puuttua muuten merkittävällä tavalla yksilön perusoikeuksiin (HE 1/1998 vp, s. 179/II, ks. myös PeVL 28/2001 vp, s. 5—6). Valiokunta on käytännössään katsonut, että kotirauhan piiriin kohdistuvat tarkastusvaltuudet merkitsevät oikeutta puuttua merkittävällä tavalla perustuslaissa jokaiselle turvattuun kotirauhan suojaan eikä tällaista valtuutta voida näin ollen antaa yksityiselle tavallisella lailla (ks. PeVL 40/2002 vp, s. 3/II ja PeVL 46/2001 vp, s. 3/II).

Koska ulkopuolisen suorittamissa toimenpiteissä voidaan katsoa olevan kyse tietolähdetoimintaa lähellä olevasta toimenpiteistä, voidaan säännösehdotusta arvioida sen kautta. Tietolähdetoimintaa ei ole arvioitu perustuslain 124 §:n kannalta perustuslakivaliokunnan tähänastisessa lausuntokäytännössä. Esityksessä katsotaan, että toimenpiteiden suorittamisessa ei ole kyse yksityiselle henkilölle annettavasta julkisesta hallintotehtävästä. Vaikka esityksessä ehdotetaan sotilastiedusteluviranomaisen ulkopuoliselle henkilölle suorittaa aiempaa aktiivisempia toimenpiteitä tiedustelumenetelmän käytön mahdollistamiseksi, ei tämän voida eroavan luonteeltaan tietolähdetoiminnasta siten, että toimenpiteiden suorittamista olisi arvioitava perustuslain 124 §:ssä tarkoitetuksi julkiseksi hallintotehtäväksi.

Kuten tietolähdetoiminta, sotilastiedusteluviranomaisen ulkopuolisen henkilön mahdollisuus suorittaa toimenpiteitä tiedustelumenetelmän käytön mahdollistamiseksi voidaan arvioida tärkeäksi. Henkilön pääsyllä tiettyyn tilaan tai järjestelmään voidaan arvioida olevan tiedusteluoperaation suorittamisen ja onnistumisen sekä tätä kautta koko Suomen maanpuolustuksen kautta jopa ratkaisevassa roolissa. Ulkopuolisen suorittamissa toimenpiteissä on lähtökohtaisesti kyse toimenpiteestä, jota viranomaiset eivät pysty suorittamaan muita keinoja käyttämällä tai kyse on tilanteesta, jossa muiden keinojen käyttäminen tiedustelutehtävän tavoitteeseen pääsemiseksi ei olisi mahdollista aika- tai resurssirajoitteiden vuoksi. Kyse on siis yksityisen henkilön tarjoamien ja olemassa olevien mahdollisuuksien hyödyntämisestä.

Vastaavasti kuin tietolähdetoiminnassa, toimenpiteen suorittava henkilö on osallisena sotilastiedustelun kohteena olevassa toiminnassa sekä liikkuu toimintaan liittyvissä tiloissa ja käyttää toimintaan liittyviä tietojärjestelmiä. Tietolähdetoimintaa vastaavasti, toimenpiteen suorittaminen muuttuu kielletyksi, jos toimenpiteen suorittava henkilö joutuisi soluttautumaan tilaan, johon hänellä ei ole entuudestaan pääsyä, tai toimintaan, johon hän ei entuudestaan kuulu (HE 222/2010, s. 348). Näissä tapauksissa voidaan katsoa olevan kyse viranomaisille kuuluvan peitetoimintatoimivaltuuden käyttämisestä. Toisaalta, jos henkilö omaehtoisesti hankkiutuu mukaan tiettyyn toimintaan tai saa pääsyn tiettyyn tilaan, kyse ei olisi peitetoimintatoimivaltuuden käyttämisestä tai kiertämisestä.

Vaikka nyt käsiteltävänä olevassa säännösehdotuksessa voidaan katsoa olevan kyse sotilastiedusteluviranomaisen ulkopuolisen henkilön tietolähdetoimintaa aktiivisemmasta toiminnasta, ehdotetun säännöksen tilanteissa suoritettava toimenpiteet eivät muodostu luonteeltaan sellaisiksi tehtäviksi, joita olisi arvioitava julkisena hallintotehtävänä. Suoritettavat toimenpiteet eivät perustuisi henkilön itsenäiseen harkinta- tai päätöksentekovaltaan. Henkilö ei myöskään tekisi toiminnan osana sellaisia itsenäisiä ratkaisuja, jotka vaikuttaisivat yksityisten oikeuksiin tai velvollisuuksiin.

Toimenpiteiden suorittamisessa olisi aina kyse sotilastiedusteluviranomaisen päätökseen ja harkintaan perustuvasta toiminnasta. Toimenpiteiden suorittaminen tapahtuisi epäitsenäisesti sotilastiedusteluviranomaisen tarkoin asettamissa puitteissa sekä ohjeiden ja valvonnan alaisena. Toimenpiteen suorittamisen perustana olisi aina sotilastiedusteluviranomaisen päätös tiedustelumenetelmän käyttämisestä ja toimenpide suoritettaisiin päätöksen mukaisesti täsmällisesti määritettyjen toimien suorittamiseen suunnitelmallisesti ja tapauskohtaisesti ominaisuuksiltaan sopivaksi arvioidun henkilön toimesta. Yksityinen henkilö ei käyttäisi toimenpiteen suorittamisessa julkista valtaa, vaan kyseessä olisi nimenomaisesti sotilastiedusteluviranomaisen toimivaltuus, jossa tiedustelumenetelmän käyttö olisi mahdollista yksityisen henkilön suorittamien toimenpiteiden takia.

Sotilastiedusteluviranomaisen ulkopuolisen henkilön toimenpiteissä olisi kyse käytännössä sotilastiedusteluviranomaisen toimivaltuuksien käyttöön liittyvästä tukemisesta hyödyntäen henkilön jo olemassa olevaa asemaa tiedustelun kohteena olevassa toiminnassa. Toimenpiteet olisivat hyvin tarkoin rajattuja ja myös tältä osin luonteeltaan epäitsenäisiä, kun kyse olisi esimerkiksi kuuntelulaitteen jättämisestä tiettyyn ennalta määrättyyn paikkaan. Tietolähteelle ei ehdoteta annettavaksi oikeuksia perusoikeuksien ydinalueelle kohdistuvien toimivaltuuksien käyttöön, vaan kyse olisi edellä todetusti yksinomaan viranomaisen toimivaltuudesta. Ehdotettavasta sääntelystä ei katsota toiminnan epäitsenäinen luonne huomioiden seuraavan myöskään tältä osin julkisen hallintotehtävän antamista yksityiselle henkilölle.

On huomattava, että koska sotilastiedusteluviranomaisella ei ole oikeutta tiedustelumenetelmän käyttöön tai toimenpiteiden suorittamiseen pysyväisluonteiseen asumiseen käytettävässä tilassa, ei se olisi mahdollista myöskään tilanteessa, jossa viranomaisen ulkopuolinen taho suorittaisi toimenpiteen.

Ehdotettua sääntelyä voidaan pitää oikeasuhtaisena, sillä osallisuus toimenpiteisiin olisi rajattu pelkästään tilanteisiin, joissa se olisi välttämätöntä toimivaltaisen viranomaisen toimivaltuuden käyttämiseksi. Sääntelyn oikeasuhtaisuuden sekä oikeusturvajärjestelyjen osalta on huomionarvoista, että viranomaisen ulkopuolista henkilöä ei voitaisi käyttää viranomaisille annettujen toimivaltuuksien käyttöä koskevien edellytysten tai rajoitusten kiertämiseen, vaan tilanteen mukaan kyseessä olevalle tiedustelumenetelmälle asetettujen edellytysten tulisi aina täyttyä eikä toimivaltuuskohtaisesta päätöksentekomenettelystä voitaisi poiketa (Allan v. Yhdistynyt kuningaskunta 5.11.2002, Van Vondel v. Alankomaat 25.10.2007, M.M. v. Alankomaat 8.4.2003 ja A. v. Ranska 23.11.1993)

Se, että tietolähde suorittaisi toimenpiteen voisi olla välttämätöntä tilanteissa, joissa vain tietolähteellä olisi pääsy sellaisiin tiloihin tai paikkoihin taikka porukoihin, joihin esitutkintaviranomaisilla ei muutoin olisi käytännön syistä mahdollisuutta päästä, vaikka oikeudellisesti tämä olisikin sallittua. Näistä tietolähteen toimesta tehtävistä toimista säädettäisiin sääntelyn tarkoitukseen nähden ja sääntely-yhteys huomioon ottaen riittävän täsmällisesti ja tarkkarajaisesti ehdotetussa pakkokeinolain 10 luvun 40 a §:n 3 momentissa. Ehdotettu tehostaisi tietolähdetoimintaa ja muiden tutkintakeinojen käyttömahdollisuuksia sekä

siten yleisesti rikosten selvittämistä, mitä voidaan pitää perusoikeusjärjestelmän kannalta hyväksyttävänä perusteena rajoittaa kotirauhan suojaa.

Nyt käsiteltävänä olevan säännösehdotuksen mukaisesti viranomaisen ulkopuolisella ei ole itsenäiseen harkintaan perustuvaa oikeutta käyttää merkittävällä tavalla yksilön perusoikeuksiin puuttuvaa toimivaltaa. Säännöksen mukaisessa tilanteessa on kyse esineen, menetelmän tai ohjelmiston asentamisesta tai poisottamisesta, eli viranomaisen ulkopuolinen taho suorittaa teknisen toimenpiteen, jolla mahdollistetaan viranomaisen julkisen vallan käyttö. Asentaminen tai poisottaminen on suoritettava viranomaisen ohjeistuksen mukaisesti. Ulkopuolisella taholla ei ole myöskään pääsyä eikä tarkempaa tietoa siitä, mitä tietoa esineellä, menetelmällä tai ohjelmistolla hankitaan varsinaisesta kohteesta.

Käsiteltävänä olevan säännösehdotuksen mukaan esineen, menetelmän tai ohjelmiston asentaminen ja poisottaminen tapahtuvat viranomaisen pyynnöstä. Näin ollen pyynnön kohteena oleva henkilö voi myös kieltäytyä toimenpiteen suorittamisesta; toiminta perustuisi henkilön vapaaehtoisuuteen eikä kyse olisi velvollisuudesta.

10.2.3.2 Rajavartiolaitoksen suorittamat toimenpiteet

Verrattuna voimassa olevaan sotilastiedustelusta annettuun lakiin uutena säännöksenä 1. lakiehdotuksen 18 a §:ssä säädettäisiin, että Rajavartiolaitos voi suorittaa tiettyjen tiedustelumenetelmien käyttöön liittyvän yksittäisen toimenpiteen.

Ehdotus on merkityksellinen perustuslain 2 §:n 3 momentin kannalta. Sen mukaan julkisen vallan käyttämisen tulee perustua lakiin. Perustuslakivaliokunta on lausunnossaan PeVL 35/2008 vp arvioinut hallituksen esityksen laiksi poliisin, tullin ja rajavartiolaitoksen yhteistoiminnasta sekä eräiksi siihen liittyviksi laeiksi (HE 26/2008 vp.) sisältynyttä vastaavanlaista säännöstä koskien poliisin, tullin ja rajavartiolaitoksen (PTR-viranomaiset) toimimista toisen PTR-viranomaisen tehtäväalueella. Perustuslakivaliokunnan lausunnon mukaan valiokunta on useasti katsonut, että yksityiseen kohdistuvan julkisen toimivallan siirtäminen sopimuspohjaisesti viranomaiselta toiselle ei ole valtiosääntöoikeudellisesti asianmukaista (ks. esim. PeVL 23/1994 vp, s. 2/I ja PeVL 11/1994 vp, s. 1/II). Valiokunta kuitenkin piti edellä mainittuun lakiehdotukseen sisältyvää järjestelyä PTR-viranomaisten yhteistyöstä eri viranomaisten voimavarojen tarkoituksenmukaisen käytön vaatimana ja myös valtiosääntöoikeudellisesti hyväksyttävänä.

Perustuslakivaliokunta piti aiempaan käytäntöönsä viitaten kuitenkin tarpeellisena, että säännöksiä oli sanonnallisesti täsmennettävä koskemaan vain "yksittäistä" rikostorjuntaan liittyvän toimenpiteen suorittamista. Vastaavasti mainintaa ilman pyyntöä suoritettavasta kiireellisestä toimenpiteestä on valiokunnan mielestä tarpeen kielellisesti tarkentaa osoittamaan, että myös näissä tapauksissa toinen PTR-viranomainen saa käyttää vain niitä toimivaltuuksia, jotka sillä on omalla tehtäväalueellaan.

Perustuslakivaltiokunta ei ole ottanut nimenomaisesti kantaa toisen viranomaisen antamaan apuun tilanteessa, jossa apua pyytävällä viranomaisella ei ole toimivaltuuksia suorittaa kyseistä toimenpidettä (esim. HE 82/2023, PeVL 36/2024 vp.). Joka tapauksessa merkittävänä julkisen vallan käyttönä on pidetty perustuslakiuudistuksen esitöiden mukaan esimerkiksi itsenäiseen harkintaan perustuvaa oikeutta käyttää voimakeinoja tai puuttua muuten merkittävällä tavalla yksilön perusoikeuksiin (HE 1/1998 vp, s. 179/II, ks. myös PeVL 28/2001 vp, s. 5—6).

Ehdotetulla sääntelyllä ei tehtäisi perusoikeuksien kannalta ongelmallista tehtävien siirtämisestä viranomaiselta toiselle, vaan tehtävän suorittamisessa käytettäisiin toista viranomaista, jolla on

jo osaamista säännöksessä tarkoitetun yksittäisten toimenpiteen suorittamisesta. Tiedustelumenetelmät, joita koskevia toimenpiteitä Rajavartiolaitos voisi suorittaa, olisi rajattu tiettyihin yksittäisiin menetelmiin, joita vastaavia toimenpiteitä Rajavartiolaitos voi jo suorittaa rikosten ennalta estämisessä ja paljastamisessa rikostorjunnasta Rajavartiolaitoksessa annetun lain mukaan. Toimenpiteillä ei myöskään saisi selvittää viestin sisältöä. Lisäksi Rajavartiolaitoksen tehtävien suorittamiseen nimettävillä virkamiehillä on oltava riittävä koulutus suoriutua säännöksessä esitetyistä toimenpiteistä.

Ehdotetussa sääntelyssä olisi kyse viranomaisen toimivallassa olevien toimenpiteiden tapauskohtaisesta suorittamisesta tilanteissa, joissa sotilastiedusteluviranomainen ei itse pääse suorittamaan tiedustelumenetelmän käyttöön liittyviä toimenpiteitä tai toimenpiteiden suorittaminen vaatisi kohtuuttomia resursseja. Lisäksi suoritettavat toimenpiteet ovat luonteeltaan epäitsenäisiä. Ehdotuksen tapauksissa toisella viranomaisella ei ole lainmukaista mahdollisuutta perehtyä kerättyyn aineistoon, vaan se on luovutettava käsiteltäväksi apua pyytäneelle viranomaiselle käsittelemättömänä.

Nyt käsiteltävänä olevan esityksen 1. lakiehdotuksen 18 a §:n 2 momentin mukaan Rajavartiolaitos voisi suorittaa rajavartiolain 28 §:ssä tarkoitettuja toimenpiteitä sotilastiedusteluviranomaisen pyynnöstä. Tilanteessa on kyse toisen viranomaien toimivallassa olevien toimenpiteiden suorittamisesta muusta syystä kuin niiden alkuperäiseen käyttötarkoitukseen; sotilastiedusteluviranomaisella ei ole oikeutta määrätä rajatarkastuksen suorittamisesta. Säännösehdotuksessa esitetään, että laajennetusta käyttöperusteesta säädettäisiin nimenomaisesti.

Toisaalta voidaan todeta, että rajavartiolain 28 §:n nojalla Rajavartiolaitos voi suorittaa rajatarkastuksia ilman rikosepäilyä. Rajavalvonnalla voidaan katsoa tarkoitettavan kansainvälisillä rajoilla tapahtuvaa toimintaa, jonka tavoitteena on ylläpitää rauhallisia oloja, turvata alueellinen koskemattomuus ja estää laittomat rajanylitykset. Näin ollen ehdotuksen ei voida katsoa laajentavan merkittävästi Rajavartiolaitoksen toimivaltuuksien käyttöä. Lisäksi esityksen 11. lakiehdotuksen 3 §:n muutoksessa ehdotetaan, että Rajavartiolaitoksen tehtäväksi säädettäisiin sotilastiedusteluun osallistuminen.

Hallituksen esityksen 1. lakiehdotuksen 18 a § on viranomaisten voimavarojen tarkoituksenmukaisen käytön vaatima ja siten linjassa perustuslakivaliokunnan kannanoton kanssa. Säännöstä voidaan pitää valtiosääntöoikeudellisesti hyväksyttävänä. Säännöstä voidaan pitää tarkkana sen osalta, milloin toinen viranomainen voi suorittaa toimenpiteitä. Lisäksi, koska vastuu on sotilastiedusteluviranomaisella, toimenpiteisiin kohdistuu vahvaa valvontaa.

10.2.4 Tekninen laitetarkkailu

Tekniseen laitetarkkailuun liittyen esityksessä ehdotetaan, että teknisen laitetarkkailun lupaa ei enää jatkossa haettaisi ja määrättäisi tiettyjä yksilöityjä laitteita tai ohjelmistoja koskien, vaan arvioitavana olisi, voidaanko teknistä laitetarkkailua kohdistaa mihin tahansa tietyn sotilastiedustelun kohteeseen liittyvän henkilön käytössä olevaan laitteeseen tai ohjelmistoon. Epäillyn käyttämien laitteiden ja ohjelmistojen selvittäminen jäisi sotilastiedusteluviranomaisen virkamiehen virkavastuulla selvitettäväksi asiaksi. Tämän olisi tehtävä toimenpiteen kohteena olevista laitteista ja ohjelmistoista erillinen päätös, jossa olisi nimenomaisesti perusteltava syyt toimenpiteen kohteena olevien laitteiden ja ohjelmistojen valitsemiselle.

Lakiehdotuksessa olisi kyse uudentyyppisestä sääntelyratkaisusta, eikä vastaavaa ole poliisilaissa tai pakkokeinolaissa.

Käsiteltävänä olevan arvioinnin kannalta olennainen on teknisestä laitetarkkailusta seuraava perusoikeusrajoitus, joka kohdistuu yksityisyyden ja jossain määrin luottamuksellisen viestin suojaan. Ratkaisevaa merkitystä tämän kannalta ei ole kohteena olevan henkilön käyttämien laitteiden tai ohjelmistojen taikka näihin kohdistuvien lupien lukumäärällä. Olennaista tämän sijaan on, voidaanko sotilastiedustelun kohteeseen liittyvän henkilön yksityisyyden tai luottamuksellisen viestinnän suojaa rajoittaa hänen käyttämäänsä laitteeseen tai ohjelmistoon kohdistettavalla teknisellä laitetarkkailulla. Ehdotettu muistuttaa perustuslakivaliokunnan myötävaikutuksella (PeVL 35/2018 vp ja PeVL 36/2018 vp) poliisilain 5 a luvussa ja sotilastiedustelusta annetun lain 4 luvussa säädettyä telekuuntelua. Ehdotetun sääntelyn mukaan teknisen laitetarkkailun kohdentamisesta olisi lisäksi tehtävä edellä kuvattu perusteltu päätös.

Henkilöperusteisen teknisen laitetarkkailun lupa olisi voimassa kolme kuukautta, jonka jälkeen asia olisi saatettava uudelleen lupaharkintaan. Uudessa harkinnassa olisi esitettävä myös henkilön käyttämät uudet laitteet ja ohjelmistot.

Perustuslakivaliokunta on ottanut kantaa telekuuntelun kohdistumisesta henkilöön pakkokeinolain muutosta koskien (HE 2172022 vp. PeVL 98/2022 vp.). Perustuslakivaliokunta on jo ennen perusoikeusuudistuksen voimaantuloa pitänyt oleellisena oikeusturvakysymyksenä, että telekuunteluvaltuuden edellytyksenä on aina riippumattoman tuomioistuimen yksittäistapauksessa konkreettisen rikosepäilyn johdosta antama lupa (PeVL 8/1994 vp, s. 2/II). Myöhemmässä käytännössä valiokunta on muun muassa torjunut ehdotuksen telekuuntelun mahdollistamisesta lyhytaikaisesti ilman tuomioistuimen lupaa (PeVL 66/2010 vp, s. 10—11). Valiokunta on lisäksi pitänyt aiheellisena sen harkitsemista, että muitakin salaisia pakkokeinoja koskevaa ratkaisutoimivaltaa osoitettaisiin tuomioistuinten toimivaltaan (PeVL 66/2010 vp, s. 9/II). Perustuslakivaliokunta on todennut käsityksenään, että pakkokeinolain muutos oli omiaan heikentämään telepakkokeinojen käyttöä koskevaa oikeussuojaa.

Esityksen 1. lakiehdotuksen 33 §:ään esitetään lisättäväksi säännös päätöksenteosta tilanteessa, jossa tekninen laitetarkkailu kohdistuu henkilöön ja tiedustelumenetelmän käytön piiriin lisättäisiin uusi laite tai ohjelmisto. Vastaava muutos tehtäisiin telekuuntelun (36 §) osalta uuden teleosoitteen tai telepäätelaitteen osalta.

Samalla edellä tarkoitettuhiin tiedustelumenetelmien käyttöön liittyen sotilastiedustelusta annettuun lakiin lisättäisiin uusi 82 a §, joka koskisi telekuuntelun ja tiettyjen muiden tiedustelumenetelmien käytön keskeyttämistä, jos käy ilmi, että telekuuntelu kohdistuu muuhun kuin luvan kohteena olevalta lähtöisin olevaan tai hänelle tarkoitettuun viestiin. Vastaavasti teknisen laitetarkkailun osalta tiedustelumenetelmän käyttö olisi keskeytettävä, jos käy ilmi, että tiedustelumenetelmän käyttö kohdistuu muuhun kuin kohteena olevan käyttämään laitteeseen tai ohjelmistoon.

Nyt käsiteltävänä olevan säännösehdotuksen kannalta on keskeistä, että sotilastiedusteluviranomaisen toimintaa valvoo ulkopuolinen valvoja (tiedusteluvalvontavaltuutettu) etukäteisesti, reaaliaikaisesti ja jälkikäteisesti. Valvonnan reaaliaikaisuuden takaa osaltaan sotilastiedusteluviranomaisen velvollisuus tehdä ilmoitus valtuutetulle tiedustelumenetelmän käyttöä koskevasta päätöksestä. Nyt käsiteltävänä olevan ehdotuksen mukaan sotilastiedusteluviranomaisessa tehtäisiin päätös aina uuden laitteen tai ohjelmiston lisäämisestä luvan piiriin. Näin ollen myös uudet laitteet ja ohjelmistot ovat ulkopuolisen laillisuusvalvonnan piirissä, kunne mahdollinen jatkolupa tekniselle laitetarkkailulle haetaan tuomioistuimesta.

Tiedusteluvalvontavaltuutetulla on oikeus keskeyttää tai lopettaa tiedustelumenetelmän käyttö, jos hän katsoo valvottavan menetelleen lainvastaisesti tiedustelutoiminnassa. Tuomioistuimen

harkinnassa olevasta tiedustelumenetelmästä valtuutettu voi antaa väliaikaisen määräyksen ja asia on saatettava tuomioistuimen käsiteltäväksi. Näin ollen, vaikka sotilastiedusteluviranomainen itse tekee päätöksen henkilön käyttämän laitteen tai ohjelmiston lisäämisestä teknisen laitetarkkailun luvan piiriin, tiedusteluvalvontavaltuutettu valvoo tätä ja voi tarvittaessa puuttua asiaan.

Sanotuista syistä ehdotusta ei ole pidettävä perusoikeuksien suojan kannalta ongelmallisena.

10.2.5 Ulkopuolisen laitteen tai tietojärjestelmän käyttäminen

Esityksen 1. lakiehdotuksen 42 §:n 3 momentilla on merkitystä perustuslain 15 §:n kannalta. Perustuslain 15 §:n 1 momentin mukaan jokaisen omaisuus on turvattu.

Perustuslakivaliokunta on vakiintuneessa lausuntokäytännössään todennut, että esimerkiksi Puolustusvoimien oikeudella käyttää tilapäisesti kiinteistöjä on katsottu olevan perustuslain 15 §:ssä turvatun omaisuuden suojan kannalta sotilaalliseen maanpuolustukseen liittyvä painava yhteiskunnallinen tarve. Sotilaallisen harjoitustoiminnan ja puolustusvalmiuden kohottamisen tarpeet ovat perusoikeusjärjestelmän kannalta hyväksyttäviä perusteita rajoittaa omaisuuden suojaa. Kiinteistön tilapäisen käytön edellytetään olevan välttämätöntä säännöksessä mainittujen toimintojen kannalta (esimerkiksi PeVL 51/2006 vp. s. 5).

Perustuslakivaliokunta ei ole ottanut kantaa täysin vastaavaan tilanteeseen, mistä nyt käsiteltävänä olevassa säännösehdotuksessa olisi kyse.

Nyt käsiteltävänä olevan säännösehdotuksen mukaan sotilastiedusteluviranomainen voisi käyttää ulkopuolisen laitetta tai tietojärjestelmää, jos se on välttämätöntä menetelmän tai ohjelmiston asentamiseksi ja poisottamiseksi tai menetelmällä tai ohjelmistolla hankittavien tietojen vastaanottamiseksi. Säännöksen mukaisesti tässä tarkoituksessa käytettävä ulkopuoliselle tai tämän laitteistolle tai tietojärjestelmälle ei saa aiheutua tarpeetonta vahinkoa. Käyttö olisi myös rajattava ajallisesti välttämättömään, eikä yksittäistä laitteistoa tai tietojärjestelmää lähtökohtaisesti voitaisi käyttää kuin välttämättömän ajan esimerkiksi yksittäisen tietoteknisen käskyn saattamiseksi tiedonhankinnan kohteeseen. Vastaavasti tietoja kotiutettaessa olisi arvioitava tiedon kotiuttamista useiden eri laitteistojen ja tietojärjestelmien kautta.

Itsestään selvää on se, että sotilastiedusteluviranomainen ei voisi hankkia tietoa välittäjänä olevan laitteen tai tietojärjestelmän sisältämistä tai sen kautta kulkevista muista tiedoista.

Säännösehdotus on välttämätön, jotta sotilastiedustelun kohteena olevasta toiminnasta saataisiin tietoa. Kaikissa tilanteissa sotilastiedusteluviranomaisella ei ole mahdollisuutta päästä vaivihkaisesti suorittamaan säännösehdotuksessa tarkoitettuja toimenpiteitä. Toimenpiteen suorittamisen edellytyksenä olisi välttämättömyys, eli toimenpidettä ei käytännössä muilla keinoin voitaisi suorittaa.

Omaisuudensuojan tilapäinen rajoitus on välttämätön hyväksyttävän tavoitteen, eli viimekädessä Suomen suvereniteetin turvaamiseksi ja kansallisen turvallisuuden suojaamiseksi. Puuttuminen perusoikeuksiin voidaan arvioida vähäiseksi.

10.2.6 Aineen, omaisuuden tai esineen haltuunotto ja näytteen ottaminen

Esityksen 1. lakiehdotuksen 56 a §:ssä esitettävä aineen, omaisuuden tai esineen tilapäinen haltuunotto koskisi tilanteita, joissa lain esitetyssä 55 a §:n näytteenoton tai säädetyn 56 §:n

jäljentämisen toimivaltuuden käyttö sitä välttämättä edellyttää, sotilastiedusteluviranomaisella on oikeus ottaa aine, omaisuus tai esine tilapäisestit haltuun. Aine, omaisuus tai esine on palautettava viivytyksettä haltuunoton tarkoituksen toteuduttua. Ehdotettu 56 a § vastaisi toimintana sitä, mitä pakkokeinolain 7 luvun 8 §:n 1 momentissa säädetään, mutta keskeisenä erona on se, että toimivaltuutta ei ole tarkoitettu käytettäväksi pidempikestoisessa haltuunotossa. Lisäksi tiedustelutoiminnan luonne huomioon ottaen, aine, esine tai omaisuus olisi pyrittävä palauttamaan haltuunottohetken sijaintiin mahdollisimman muuttumattomana, jotta tiedustelutoiminta ei paljastuisi.

Säännösehdotus koskisi perustuslain 15 §:n 1 momenttia, joka suojaa omistajalle kuuluvaa oikeutta hallita, käyttää ja hyödyntää omaisuuttaan, kuten tavaroitaan ja asiakirjojaan, haluamallaan tavalla sekä valtaa määrätä niistä.

Esityksen 1. lakiehdotuksen 56 a §:n nojalla tehtävä haltuunotto tarkoittaisi esineen, aineen tai omaisuuden omistajan käyttöoikeuden ja määräämisvallan tilapäistä rajoitusta. Ehdotettua 56 a §:n sääntelyä voitaisiin kuitenkin pitää perusoikeusjärjestelmän kokonaisuuden kannalta hyväksyttävänä ja painavan yhteiskunnallisen tarpeen vaatimana, sillä toimivaltuutta käyttämällä sotilastiedusteluviranomainen voisi varmistaa laissa säädettyjen tehtäviensä asianmukaisen hoitamisen, esimerkiksi tarkastamalla kohteena olevan toimijan tiloissa olevan aineen koostumuksen. Toimenpiteen kohteena olisi aine, esine tai omaisuus, joka on tai jota voidaan käyttää yhdessä tai erikseen ihmisten vahingoittamiseen taikka aineen, esineen tai omaisuuden hallussapito on jo muualla lainsäädännössä lähtökohtaisesti kielletty. Tallaisia lakeja voisivat olla esimerkiksi ampuma-aselaki (1/1998) ja kemikaalilaki (599/2013). Myös järjestyslaki (612/2003) kieltää tiettyjen aineiden ja esineiden hallussapidon yleisellä paikalla kokonaan (9 §). Nyt käsiteltävänä olevan ehdotuksen tilanteessa ei kuitenkaan olisi kyse vähäisistä tilanteista.

Omaisuuden suojaan puuttumista rajoittaa se, että sotilastiedustelutoiminta tapahtuu lähtökohtaisesti sen kohteelta salassa ja toimenpiteiden paljastuminen pyritään estämään viimeiseen asti. Lisäksi puuttumisen laajuutta rajoittaa sotilastiedustelusta annetussa laissa säädetyt periaatteet, etenkin vähimmän haitan periaate, josta säädetään lain 7 §:ssä. Sen mukaan sotilastiedustelun toimivaltuuden käytöllä ei kenenkään oikeuksiin saa puuttua enempää eikä kenellekään saa aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi. Edellä tarkoitetun perusteella näytteenotto rajoittuu tosiasiallisesti ja oikeudellisesti vähäiseen määrään kohteena olevasta omaisuudesta, käytännössä niin vähäiseen, ettei sitä silmämääräisellä havainnoinnilla voida havaita.

Toimivaltuuden käytöstä ilmoittamisessa sovellettaisiin ilmoittamisvelvollisuutta koskevia säännöksiä. Kuten muiden tiedustelumenetelmien osalta. henkilö, jonka aine, esine tai omaisuus olisi joutunut toimivaltuuden käytön kohteeksi, voisi tehdä tutkimispyynnön tai kantelun tiedusteluvalvontavaltuutetulle huolimatta siitä, onko hän saanut ilmoituksen tai onko hänellä perusteltu epäilys tiedustelumenetelmän käytön kohteeksi joutumisesta. Puuttuminen perusoikeuksiin voidaan arvioida vähäiseksi.

Omaisuudensuojan tilapäinen rajoitus on välttämätön hyväksyttävän tavoitteen, eli viimekädessä Suomen suvereniteetin turvaamiseksi ja kansallisen turvallisuuden suojaamiseksi.

10.2.7 Asevelvolliset ja muut harjoitukseen osallistuvat

Säännösehdotuksia, jotka koskevat (kansainvälistä yhteistyötä (1. lakiehdotuksen 20 §).) asevelvollisuuslain mukaisessa palveluksessa olevan tai vapaaehtoiseen harjoitukseen osallistuvan osallistumista sotilastiedusteluun (1. lakiehdotuksen 91 §) (sekä laitteen,

menetelmän tai ohjelmiston asentaminen ja poisottaminen (1. lakiehdotuksen 42 §),) on arvioitava hallintotehtävän antamista muulle kuin viranomaiselle koskevan perustuslain sääntelyn kannalta.

Perustuslain 124 §:n mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle (HE 1/1998 vp, s. 179).

Varusmiesten ja muiden palveluksessa tai harjoituksessa olevien asevelvollisten käyttämiselle erilaiseen perustuslain 127 §:ssä säädettyyn maanpuolustusvelvollisuuteen perustuvaan palvelukseen ei ole asetettu lähtökohtaisia oikeudellisia rajoitteita.

Reservin kertausharjoituksilla pidetään yllä varusmiespalveluksen aikana saatuja sotilaallisia tietoja ja taitoja sekä koulutetaan vaativampiin tehtäviin.

Sotilastiedusteluviranomaista avustaessaan harjoitukseen osallistuvalla olisi 91 §:n nojalla oikeus käyttää toimivaltuuksia ainoastaan tiedustelumenetelmän käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa. Harjoitukseen osallistuva ei päätä tiedustelumenetelmän käytöstä tai tiedustelumenetelmän käytön kohdentamisesta. Heidän käytössään olevista tiedustelumenetelmistä säädettäisiin nimenomaisesti.

Harjoitukseen osallistuvalla olisi oltava tiedolliset ja taidolliset valmiudet tehtävien hoitamiseen. Vastaavan kaltaista sääntelyä reserviläisten toimivaltuuksista on sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain 10 luvussa, joka koskee normaaliolojen vakavia häiriötilanteita ja poikkeusoloja. Kyseessä ei voida katsoa olevan itsenäisestä harkintavallasta eikä merkittävästä julkisen vallan käytöstä.

10.2.8 Valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuva tiedustelu

Esityksen 1. lakiehdotuksen 61 a §:ssä esitetään säädettäväksi valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvasta tiedustelusta. Tiedustelumenetelmän käytön kohteena voisivat olla tietojärjestelmään kuuluvat ohjelmistot ja laitteistot.

Perustuslain 10 §:n muuttamista koskevassa hallituksen esityksessä (HE 198/2017 vp.) on todettu, että vieraan valtion viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa. Perustuslakivaliokunta totesi muutosta koskeneessa mietinnössään (PuVM 4/2018 vp.), että vaikka vieraan valtion sotilas- tai muun viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa, sotilastiedustelutoimivaltuuksia ei voida kohdistaa kaikissa tapauksissa niin täsmällisesti, ettei olisi vaaraa viranomaisten tilapäisestä pääsystä yksittäisten, tiedustelutehtävään liittymättömien henkilöiden viestintää koskeviin tietoihin, mikä tulee perustuslakivaliokunnan mielestä tavallisissa laeissa rajata mahdollisimman vähäiseksi.

Perustuslakivaliokunta esitti keskeisiä perusteita, jotka on otettava huomioon arvioitaessa luottamuksellisen viestin salaisuuden rajoittamisen perusteena olevia perustuslain 10 §:n 4 momentissa tarkoitettua sotilaallista toimintaa ja muuta kansallista turvallisuutta vakavasti uhkaavaa toimintaa. Valiokunta korosti vahvoja oikeusturvatakeita, laaja-alaista ja tehokasta tiedusteluvaltuuksien käytön valvontaa sekä riittäviä soveltamisrajoituksia. Kyse on poikkeuksellisesta rajoitusperusteesta, jossa on irtauduttu rikosperusteisesta toiminnasta ja joka tulee siten sovellettavaksi tilanteissa, joissa ei tiedonhankintavaiheessa tai muutoinkaan voida

kohdistaa konkreettista ja yksilöityä rikosepäilyä (PeVM 4/2018 vp, s. 8). Tiedustelutoiminnan rikostorjunnasta ja rikostutkinnasta eroava luonnekin huomioon ottaen tiedustelulainsäädännössä omaksuttua sääntelymallia ei perustuslakivaliokunnan mielestä voitu käyttää perusteluna rikostorjuntaan ehdotetulle tiedustelulainsäädäntöä vastaavalle sääntelylle (PeVL 99/2022 vp.).

Sotilastiedustelusta annetun lain eduskuntakäsittelyssä valiokunta on korostanut toimivaltuuksien osalta, että säännöksen soveltamisala rajautuu hallituksen esityksen perusteluissa (HE 203/2017 vp.) kuvatuilla tavoin tiedon hankkimiseen vain Suomeen kohdistuvasta sotilaallisesta toiminnasta taikka Suomen turvallisuusympäristön kannalta merkityksellisestä sotilaallisesta toiminnasta. Valiokunta on painottanut tarvetta tulkita rajoitusperustetta suppeasti (PeVM 4/2018 vp, s. 7). Valiokunta on korostanut myös perusoikeuksien yleisten rajoitusedellytysten merkitystä perustuslain 10 §:n rajoitusperustetta tulkittaessa (PeVM 4/2018 vp, s. 8—9).

Tiedustelumenetelmänä 1. lakiehdotuksen 61 a §:ssä ehdotetussa säännöksessä olisi kyse telekuuntelun, televalvonnan, teknisen laitetarkkailun ja teknisen kuuntelun toimenpiteitä yhdistelevästä toimivaltuudesta. Kaikkia edellä tarkoitettuja yksittäisiä tiedustelumenetelmiä on arvioitu perusteellisesti perustuslakivaliokunnan lausuntokäytännössä.

Nyt käsiteltävänä olevaa ehdotusta voidaan osittain arvioida jo nykyisin sallittua henkilöön kohdistuvaa telekuuntelua ja -valvontaa sekä tässä esityksessä ehdotettavaa henkilöön kohdistuvaa teknistä laitetarkkailua vasten. Kohteena olisi kuitenkin valtiollinen toimija, jonka käyttämien laitteiden, ohjelmistojen ja tietoliikenneyhteyksien muodostamassa kokonaisuudessa hankittaisiin tietoa.

Käsiteltävänä olevan arvioinnin kannalta olennainen on uuden toimivaltuuden aiheuttama perusoikeuspuuttuminen, joka kohdistuu luottamuksellisen viestinnän suojaan. Kuten todettu, valtiollisen toimijan viestintä ei nauti vastaavaa perusoikeussuojaa kuin mitä on yksityisillä henkilöillä. Näin ollen arvioinnin kannalta keskeistä on se, miten paljon uuden toimivaltuuden käytön piiriin tulisi muuta kuin kohteena olevan valtiollisen toimijan viestintää. Ratkaisevaa merkitystä ei ole valtiollisen toimijan käyttämien laitteiden, ohjelmistojen, telepäätelaitteiden ja -osoitteiden taikka näihin kohdistuvien toimivaltuuslupien lukumäärällä. Olennaista on, voidaanko kohteessa mahdollisesti käsiteltävänä olevien yksityisten henkilöiden luottamuksellisen viestinnän suojaa rajoittaa.

Perustuslakivaliokunta on jo ennen perusoikeusuudistuksen voimaantuloa pitänyt oleellisena oikeusturvakysymyksenä, että esimerkiksi telekuunteluvaltuuden edellytyksenä on aina riippumattoman tuomioistuimen yksittäistapauksessa konkreettisen rikosepäilyn johdosta antama lupa (PeVL 8/1994 vp, s. 2/II).

Tässä hallituksen esityksessä ehdotetun uuden toimivaltuuden käytön edellytykset vastasivat sitä, mitä muidenkin perusoikeussuojaan merkittävästi puuttuvien toimivaltuuksien kohdalla on säädetty. Lisäksi toimivaltuuden käytön kohteena on laissa erikseen säädetyt kohteet sekä niiden osalta valtiollinen toimija, joka on laissa määritelty.

Päätöksentekotaso tai käytön edellytykset eivät poikkeaisi siitä, mitä on säädetty henkilöön kohdistuvasta telekuuntelusta ja -televalvonnasta tai tässä esityksessä ehdotettavasta teknisestä laitetarkkailusta. Kysymys on päätöksentekotason muuttamisesta asiassa, jossa tiedustelumenetelmien käyttöön erityisesti perehtyneellä sotilaslakimiehellä tai muulla virkamiehellä on nykyisinkin vahva asema. Ehdotetun uuden toimivaltuuden osalta on syytä korostaa, että ehdotetun sääntelyn mukaan tiedustelumenetelmien käyttöön erityisesti

perehtyneen sotilaslakimiehen tai muun virkamiehen on tehtävä tuomioistuimen luvassa määritetyssä tietojärjestelmäkokonaisuudessa toimenpiteen kohteena olevista laitteista, ohjelmistoista, telepäätelaitteista ja teleosoitteista päätös, jossa on nimenomaisesti perusteltava syyt niiden valitsemiselle, eli se, miksi kohde on osana päätöksessä tarkoitettua tietojärjestelmää. Perusteluvelvollisuus on jo nykyisin muiden tiedustelumenetelmien osalta korkea, ja päätös on vahvan laillisuusvalvonnan kohteena.

Valtiollisen toimijan tietyssä tietojärjestelmäkokonaisuudessa käyttämien laitteiden, ohjelmistojen, telepäätelaitteiden ja teleosoitteiden yksilöintitietojen selvittäminen jäisi tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen virkavastuulla selvitettäväksi asiaksi.

Säännöksen tarkoittamassa toiminnassa voi tiedonhankinnan piiriin kuitenkin tulla myös sivullisen viestintää. Esityksen 1. lakiehdotuksen 85 §:ssä säädettäisiin, että valtiollisen toimijan tietojärjestelmätiedustelu Suomessa olisi keskeytettävä ja sillä hankitut tiedot hävitettävä välittömästi, jos sillä saataisiin muita kuin valtiollisen toimijan tietojärjestelmässä käsiteltäviä tietoja.

Päätöksen tiedustelumenetelmän käytöstä tekisi tuomioistuin. Esityksen 1. lakiehdotuksen 61 b §:ssä olisi tarkkaan säädetty edellytyksistä sekä lupavaatimuksessa ja -päätöksessä mainittavista seikoista. Koska kyseessä voidaan katsoa olevan jo nykyisin laissa säädettyjä toimenpiteitä yhdistelevästä toimivaltuudesta, jonka kohteena olevan valtiollisen toimijan tietojärjestelmän kokonaisuus voi muuttua tiedustelumenetelmän käytön aikana saatujen tietojen perusteella luvan voimassaolon aikana, päätöksen tiedustelumenetelmän käytön kohteena olevasta tietojärjestelmään liittyvästä laitteesta, ohjelmistosta, telepäälaitteesta tai teleosoitteesta tekisi ehdotetun 61 b §:n mukaan tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies. Päätöksessä tarkoitettu tietojärjestelmä tai sen osa olisi otettava osaksi tiedustelumenetelmän käyttöä koskevaa mahdollista uutta lupavaatimusta.

Toimivaltuuden käyttöön kohdistuu vahva ulkoinen tiedusteluvalvontavaltuutetun valvonta. Kuten aiemmin todettu, sotilastiedusteluviranomaisella on ilmoitusvelvollisuus tekemistään päätöksistä tiedusteluvalvontavaltuutetulle. Näin ollen tuomioistuimen myöntämän luvan alassa oleviin uusia laitteita, ohjelmistoja, telepäätelaitteita ja teleosoitteita koskevista päätöksistä tehtäisiin ilmoitus tiedusteluvalvontavaltuutetulle vastaavasti kuin esimerkiksi henkilöön kohdistuvan telekuuntelun osalta on asian laita. Tiedusteluvalvontavaltuutettu valvoo sitä, että uudet laitteet, ohjelmistot sekä telepäätelaitteet- ja osoitteet ovat tuomioistuimen myöntämässä luvassa tarkoitetun tietojärjestelmän kokonaisuudessa.

Säännösehdotuksen voidaan katsoa olevan ongelmaton perustuslain kannalta. Ehdotus parantaa sotilastiedusteluviranomaisen mahdollisuuksia hankkia tietoa valtiollisesta toimijasta, mitä kautta viime kädessä pystytään suojaamaan henkilöiden henkeä ja terveyttä sekä parantamaan yhteiskunnan turvallisuutta. Lisäksi sääntelyllä voidaan katsoa olevan perusoikeusmyönteisiä vaikutuksia.

10.2.9 Ulkomaisen virkamiehen osallistuminen sotilastiedusteluun

Ehdotettu sääntely 1. lakiehdotuksen 20 §:ssä ulkomaisen virkamiehen osallistumisesta Suomen alueella tiedustelumenetelmän käyttöön on merkityksellistä perustuslain 1 §:ssä tarkoitetun Suomen täysivaltaisuuden kannalta.

Perustuslain 1 §:n 1 momentin mukaan Suomi on täysivaltainen tasavalta. Perustuslain 1 §:n 3 momentin mukaan Suomi osallistuu kansainväliseen yhteistyöhön rauhan ja ihmisoikeuksien

turvaamiseksi sekä yhteiskunnan kehittämiseksi. Suomi on Euroopan unionin jäsen ja kuuluu Pohjois-Atlantin puolustusliittoon.

Perustuslain esitöissä on todettu, että ”valtion täysivaltaisuus kattaa sekä sisäisen että ulkoisen suvereenisuuden. Sisäisellä suvereenisuudella tarkoitetaan sitä, että valtion sisällä valtiovalta on korkein oikeudellinen muiden yläpuolella oleva valta. Sisäisen suvereenisuuden keskeisenä sisältönä on kyky säätää kaikkien valtion alueella julkista valtaa käyttävien viranomaisten ja muiden toimielinten toimivallasta. Siihen kuuluu myös valta päättää oikeusjärjestyksen sisällöstä, määrätä valtioelinten toiminnasta ja oikeus käyttää eri tavoin julkista valtaa valtion alueella oleviin ihmisiin ja esineisiin nähden. Ulkoisella suvereenisuudella tarkoitetaan valtion vapautta päättää itsenäisesti suhteistaan toisiin valtioihin ja kansainvälisiin järjestöihin.” (HE 1/1998 vp, s. 71). Suomi on myös solminut kahden välisiä puolustusyhteistyösopimuksia, joista keskeisenä Yhdysvaltain kanssa solmittu puolustusyhteistyösopimus.

Täysivaltaisuutta koskevan arvioinnin kannalta merkityksellistä on ennen kaikkea sillä, että vieraan valtion ja sen virkamiehen toiminta perustuu Suomen viranomaisten päätökseen (ks. myös PeVL 66/2016 vp, s. 3 ja PeVL 65/2016 vp, s. 3). Tiedustelumenetelmiä käytetään 1. lakiehdotuksen 20 §:n säännöksen mukaan sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa. Lisäksi ulkomainen toimivaltainen virkamies on velvollinen noudattamaan sotilastiedusteluviranomaisen hänelle antamia määräyksiä, rajoituksia ja ohjeita.

Perustuslain esitöiden ja perustuslakivaliokunnan käytännön perusteella merkittävän julkisen vallan käyttämisenä on pidettävä esimerkiksi itsenäiseen harkintaan perustuvaa oikeutta käyttää voimakeinoja tai puuttua muuten merkittävällä tavalla yksilön perusoikeuksiin. Sotilastiedustelua koskevan lain 20 §:ssä ehdotetaan säädettäväksi ulkomaisen toimivaltaisen virkamiehen osallistumisesta tiedustelumenetelmien käyttöön ilman, että menetelmiä on tarkemmin rajattu. Kansainvälisen avun antamista ja pyytämistä koskevasta päätöksenteosta säädettäisiin erikseen siitä annetussa laissa (418/2017).

Vieraan valtion virkamiehen Suomessa toimimisen edellytyksenä olisi pääesikunnan tiedustelupäällikön nimenomainen päätös. Virkamiehen toiminta Suomessa olisi tilapäisluonteista sekä aina suomalaisen virkamiehen ohjaamaa ja valvomaa. Osallistuminen tiedustelumenetelmien käyttöön pysyisi näin ollen aina suomalaisen virkamiehen ohjauksessa ja valvonnassa. Selvää on lisäksi, että vieraan valtion virkamies olisi Suomessa toimiessaan rikos- ja vahingonkorvausoikeudellisen vastuun piirissä. Sotilastiedusteluviranomainen olisi myös vastuussa tarvittavista luvista.

Näistä menettelytakeista ja vastuujärjestelyistä johtuen ehdotetun pykälän ei arvioida olevan ongelmallisessa suhteessa perustuslain 124 §:ssä säädettyyn vaatimukseen siitä, että merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan antaa vain viranomaiselle.

Osallistuminen kattaisi myös sen, että ulkomainen virkamies voisi osallistua hankittujen tietojen analysointiin. Voimassa olevan lain mukaan 111 §:n mukaan muun muassa pääesikunnan tiedustelupäällikkö voi antaa määräyksen, jonka perusteella asiantuntija voi tutkita tallenteita. Nyt käsiteltävänä olevan muutoksen myötä ulkomainen virkamies voisi osallistua tallenteiden tutkimiseen ilman nimenomaista päätöstä. Päätös tehtäisiin siis siinä vaiheessa, kun tehdään päätös ulkomaisen virkamiehen Suomeen saapumisesta ja hänelle annetaan määräykset, rajoitukset ja ohjeet.

Ehdotetun sääntelyn ei siten katsota olevan ongelmallinen perustuslain 1 §:n kannalta.

10.2.10 Tietolähteen turvaaminen

Esityksen 1. lakiehdotuksen 78 a §:ssä ehdotettu sääntely tietolähteen turvaamisesta on merkityksellinen perustuslain 8 §:ssä säädetyn rikosoikeudellisen laillisuusperiaatteen kannalta. Sen mukaan ketään ei saa pitää syyllisenä rikokseen eikä tuomita rangaistukseen sellaisen teon perusteella, jota ei tekohetkellä ole laissa säädetty rangaistavaksi. Rikoksesta ei saa tuomita ankarampaa rangaistusta kuin tekohetkellä on laissa säädetty. Rikosoikeudellinen laillisuusperiaate on saanut konkreettisemman sisällön muun muassa perustuslakivaliokunnan lausuntokäytännössä. Rikosoikeudellinen laillisuusperiaate sisältää vaatimuksen sääntelyn täsmällisyydestä. Sen mukaan kunkin rikoksen tunnusmerkistö on ilmaistava laissa riittävällä täsmällisyydellä siten, että säännöksen sanamuodon perusteella on ennakoitavissa, onko jokin toiminta tai laiminlyönti rangaistavaa (PeVL 10/2000 vp, s. 2/I, PeVL 41/2001 vp, s. 2/II, 48/2002 vp, s. 2). Euroopan ihmisoikeustuomioistuimen ja EU-tuomioistuimen käytännössä laillisuusperiaatteelle on annettu käytännössä vastaava ydinsisältö, jossa on korostettu rikossääntelyn ennustettavuutta eli sitä, että säännöksen sanamuodon perusteella voidaan ennakoida, mikä on rangaistavaa (ks. PeVL 12/2021 vp, s. 14, PeVL 20/2018 vp, s. 2, PeVL 10/2016 vp ja PeVL 56/2014 vp, s. 2/II sekä niissä viitatut lausunnot).

Perustuslakivaliokunta on vakiintuneessa lausuntokäytännössä pitänyt rangaistussäännösten sisältämiä avoimia tekotapoja lähtökohtaisesti ongelmallisena rikosoikeudellisen laillisuusperiaatteen kannalta (esim. PeVL 20/2022 vp, s. 4, PeVL 12/2021 vp, 58 kappale, PeVL 20/2018 vp, s. 2 ja PeVL 6/2014 vp, s. 3/I). Esimerkiksi perustuslakivaliokunta on erävalvontalakia koskevassa muutosehdotuksessa kiinnittänyt huomiota ehdotettuun erävalvontalain 19 a §:n 1 kohtaan, jonka mukaan rangaistavaa olisi erätarkastajan tehtävän noudattamiseksi toimivaltansa rajoissa antaman käskyn tai kiellon noudattamatta jättäminen (niskoittelu erätarkastajaa vastaan). Kohta liittyi erätarkastajan käskyvaltaa koskevaan erävalvontalakiehdotuksen 4 a §:än, jonka nojalla erätarkastajalla olisi erävalvontalaissa tai muussa laissa säädettyä toimivaltuutta käyttäessään oikeus yksittäistapauksessa antaa jokaista velvoittavia, erävalvontatehtävän toteuttamiseksi tarpeellisia käskyjä ja kieltoja, jonka perustusvaliokunta on todennut jäävän varsin yleisluonteiseksi. Perustuslakivaliokunta on katsonut ehdotuksen 19 a §:n 1 kohdassa tarkoitetun rangaistavan käyttäytymisen ala jää hyvin epäselväksi (PeVL 21/2024 vp, s. 3–4).

Perustuslakivaliokunta on ottanut kantaa tulkinnanvaraisina tai arvostuksenvaraisina pidettyjen käsitteiden käyttöön rangaistussäännöksissä. Esimerkiksi lahjuksen ottamista kansanedustajana koskevan esityksen yhteydessä perustuslakivaliokunta on todennut, että erilaisia näkemyksiä voidaan esittää esimerkiksi siitä, milloin kansanedustaja on toiminut ehdotetussa säännöksessä tarkoitetulla tavalla lahjuksena pidettävän "edun vuoksi" ja että tulkinnoille jää sijaa myös sen suhteen, milloin kansanedustajan on katsottava toimivan "edustajantoimessaan jonkin... asian ratkaisemiseksi" (PeVL 29/2001 vp, s. 4). Myös esimerkiksi käsitettä ”tavanomainen vieraanvaraisuus” on pidetty arvostuksenvaraisena (PeVL 68/2010 vp, s. 5).

Liittyen viranomaisen harkintavaltaan perustuslakivaliokunta on todennut, että esimerkiksi valeostoa on valiokunnan käytännössä luonnehdittu epäsovinnaiseksi toimivaltuudeksi, joka merkitsee poliisin oikeutta toimia vastoin joitain rikosoikeudellisia kieltoja ilman virkavastuuta. Valiokunta on painottanut, että tällainen virkatoiminta on valtiosääntöoikeudellisesti jo sinänsä merkittävää hallinnon lainalaisuuden periaatteen kannalta. Valeoston osalta merkityksellistä oli, että periaatteen voidaan katsoa merkitsevän muun ohella sitä, että viranomaiselle ei ilman erittäin painavia syitä ja täsmällisesti määriteltyjä edellytyksiä voida antaa uudenlaista toimivaltaa suorittaa toimia, jotka muutoin ovat rikosoikeudellisesti sanktioituja myös viranomaisen tekeminä (PeVL 5/1999 vp, s. 5/I). Perustuslakivaliokunta on todennut näin myös

tuoreemmassa vuoden 2019 sotilastiedustelusta annettua lakia koskevassa uudistuksessa (PeVL 36/2018, s. 15).

Nyt käsiteltävänä olevassa säännösehdotuksessa rikosvastuun rajaus on rajattu tarkasti tilanteisiin, joissa tietolähteeseen kohdistuu hengen tai terveyden vaara. Lisäksi kyseessä on tietolähde, joka edellyttää sotilastiedustelusta annetun lain mukaisesti henkilöä koskevien määriteltyjen edellytysten täyttymistä, henkilön rekisteröimistä ja tietolähteen käyttöä koskevan päätöksen tekemistä. Henkilöpiiri, jota säännösehdotus koskisi olisi rajattu.

Myös toimenpiteet, joista pääesikunnan tiedustelupäällikkö voisi päättää, on rajattu siihen, että tietolähde järjestetään Suomeen.

Säännösehdotuksen tavoitteita voidaan pitää perusteltuina ja katsoa, että muutoksilla suojattaisiin tärkeää oikeushyvää eli toisen henkeä ja terveyttä.

10.2.11 Muita arvioitavia seikkoja

Haittaohjelmaa koskeva tieto

Perustuslakivaliokunta on arvioinut haittaohjelman tai käskyn suhdetta perustuslain 10 §:n 2 momenttiin viimeaikaisessa lausuntokäytännössään. Perustuslakivaliokunta kiinnitti kyberturvallisuuslakia koskevasta hallituksen esityksestä (HE 57/2024 vp.) antamassaan lausunnossa (PeVL 62/2024 vp, kohta 12) huomiota siihen, että lakiehdotusten mukainen haitallisen tietokoneohjelman tai käskyn sisältämä viesti jää kokonaan perustuslain 10 §:n luottamuksellisen viestin salaisuuden soveltamisalan ulkopuolelle. Kyse ei siten ole vain siitä säätämisjärjestysperusteluissa osin viitatusta seikasta, että tällainen viesti jäisi luottamuksellisen viestin ydinalueen ulkopuolelle. Tällainen viesti ei nauti perustuslain 10 §:n 2 momentin mukaista suojaa, eikä sitä koskevaa sääntelyä tarvitse arvioida 10 §:n 4 momentin mukaisten erityisten tai perusoikeuksien yleisten rajoitusedellytysten valossa. (PeVL 62/2024 vp., kohta 12)

Nyt käsiteltävänä olevan hallituksen esityksen 1. lakiehdotuksen 18 §:n 2 momentin käsittelyn osalta kyse ei ole perustuslain 10 §:ssä tarkoitetusta viestinnästä, jolloin tietojen luovutuksen osalta arvio ei perustu perusoikeuksiin puuttumiseen. Näin ollen säännösehdotusta ei tarvitse arvioida perustuslain 10 §:n kannalta.

Velvoitteidenhoitoselvitys

Esityksen 6. lakiehdotuksessa HTSY-lain 6 §:n 1 momenttiin ehdotetaan uutta 41 kohtaa, jonka nojalla Harmaan talouden selvitysyksikkö voisi laatia velvoitteidenhoitoselvityksen sotilastiedusteluviranomaiselle sen tehtävien hoitamiseksi. Ehdotetussa säännöksessä yksilöitäisiin siten tarkkarajaisesti viranomainen, jonka toimintaa tukemaan selvitys voitaisiin tähän tarkoitukseen laatia. Voimassa olevan HTSY-lain mukaan velvoitteidenhoitoselvitys voidaan laatia suojelupoliisille kansallisen turvallisuuden suojaamiseksi sitä vakavasti uhkaavalta toiminnalta. HTSY-lain mukaan velvoitteidenhoitoselvitysten tietolähteinä voidaan käyttää ainoastaan sellaisia tietoja, jotka velvoitteidenhoitoselvitystä pyytävä viranomainen on oikeutettu saamaan selvityspyynnössä kuvattua käyttötarkoitusta varten. Sotilastiedusteluviranomainen voi osana Puolustusvoimia saada tietoja Puolustusvoimista annetun lain 17 §:n mukaisesti ja henkilötietoja henkilötietojen käsittelystä Puolustusvoimissa annetun lain mukaisesti.

Sotilastiedusteluviranomaisen tiedonsaannin parantaminen sotilaallisista uhkista ja kansallista turvallisuuden suojaamistarkoitukseen katsotaan välttämättömäksi, jotta Harmaan talouden selvitysyksikkö voisi laatia velvoitteidenhoitoselvityksen sotilastiedusteluviranomaiselle. Ehdotettu muutos koskisi sotilastiedustelusta annetun lain 3 §:ssä säädettyä sotilastiedustelun tarkoitusta.

Perustuslakivaliokunta on arvioinut salassapitosäännökset syrjäyttävää tietojensaantioikeutta kiinnittäen huomiota siihen, että oikeudessa on viime kädessä kysymys siitä, että tietoihin oikeutettu viranomainen omine tarpeineen syrjäyttää ne perusteet ja intressit, joita tiedot omaavaan viranomaiseen kohdistuvan salassapidon avulla suojataan. Mitä yleisluonteisempi tietojensaantiin oikeuttava sääntely on, sitä suurempi on vaara, että tällaiset intressit voivat syrjäytyä hyvin automaattisesti. Mitä täydellisemmin tietojensaantioikeus kytketään säännöksissä asiallisiin edellytyksiin, sitä todennäköisemmin yksittäistä tietojensaantipyyntöä joudutaan käytännössä perustelemaan.

Merkitystä on annettu lisäksi sille, että myös tietojen luovuttajan on tällöin mahdollista arvioida pyyntöä luovuttamisen laillisten edellytysten kannalta (PeVL 48/2018 vp). Tietojen luovuttaja voi lisäksi kieltäytymällä tosiasiallisesti tietojen antamisesta saada aikaan tilanteen, jossa tietojen luovuttamisvelvollisuus eli säännösten tulkinta saattaa tulla ulkopuolisen viranomaisen tutkittavaksi. Tämä mahdollisuus on tärkeä tiedonsaannin ja salassapitointressin yhteensovittamiseksi (katso PeVL 17/2016 vp ja siinä viitatut lausunnot).

Ehdotuksien hyväksyttävyyttä tukee se, että tiedonhankinnan kohteena on toiminta, joka on sotilaallista tai vakavasti uhkaa kansallista turvallisuutta ja tiedonsaanti on kytketty sotilastiedustelun tarkoitukseen sekä tiedustelulaeissa määriteltyihin sotilastiedustelun kohteisiin. Hyväksyttävyyttä korostaa myös se, että tiedonsaanti ja tiedonluovutusperusteet on sidottu välttämättömyys- tai tarpeellisuuskriteeriin.

Tietolähdetoiminta

Esityksen 1. lakiehdotuksen 11 §:ssä ehdotetaan säädettäväksi puolustushaaroille mahdollisuutta käyttää sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa myös niin kutsuttua perusmuotoista tietolähdetoimintaa.

Perustuslain 2 §:n 3 momentin mukaan julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Perusoikeuksien rajoittamisen sallittavuutta tulee arvioida paitsi yksittäisiin perusoikeussäännöksiin mahdollisesti sisältyvien lakivarausten kannalta myös perusoikeuksien yleisten rajoitusedellytysten kannalta (PeVM 25/1994 vp).

Perustuslain 10 §:n nojalla on jokaisen yksityiselämä, kunnia ja kotirauha turvattu. Yksityiselämän suojan lähtökohtana on, että yksilöllä on oikeus elää omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä (PeVL 53/2005 vp, PeVL 13/2005 vp, PeVL 11/2005 vp). Yksityiselämän piiriin kuuluu muun muassa yksilön oikeus vapaasti solmia ja ylläpitää suhteita muihin ihmisiin ja ympäristöön. Yksityiselämän suojan takaamiseksi valtiolta edellytetään, että se itse pidättäytyy loukkaamasta yksilön yksityiselämää. Käsite "yksityiselämä" voidaan ymmärtää henkilön yksityistä piiriä koskevaksi yleiskäsitteeksi. Yksityiselämää suojataan perinteisesti rikosoikeuden keinoin (HE 309/1998 vp). Tietolähdetoiminta on merkityksellistä perustuslain 10 §:ssä turvatun yksityiselämän suojan kannalta.

Tietolähteen itsensä kannalta merkityksellistä on perustuslain 7 §:ssä turvattu oikeus elämään sekä henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen. Poliisilain muutos 525/2005 on säädetty perustuslakivaliokunnan myötävaikutuksella (PeVL 11/ 2005 vp), mutta perustuslakivaliokunta ei lausunnossaan käsitellyt tietolähdetoimintaa. Uusi poliisilaki on myös säädetty perustuslakivaliokunnan myötävaikutuksella (PeVL 67/2010 vp). Perustuslakivaliokunta ei tässäkään lausunnossa käsitellyt tietolähdetoimintaa tai tietolähteen ohjattua käyttöä.

Tietolähdetoiminta olisi käytännössä rajattu puolustushaarojen omissa tehtävissään saamiin tietoihin. Kyse ei olisi tietolähteen ohjatusta käytöstä, vaan siitä, että henkilöt itse oma-aloitteisesti kertovat tietojaan puolustushaarojen virkamiehelle. Tiedoista ei myöskään makseta palkkiota, mikä vähentää riskiä tietolähteen epäsuoraan ohjaamiseen palkitsemalla halutun tiedon antaminen.

Maanpuolustusta ja kansallista turvallisuutta voidaan pitää perusoikeusjärjestelmän kannalta hyväksyttävänä perusteena puuttua perusoikeutena turvattuun yksityiselämän suojaan. Suhteellisuusvaatimuksen näkökulmasta tietolähdetoiminnan taustalla on erityisen painava yhteiskunnallinen intressi, joka liittyy myös tavoitteeseen turvata toisten ihmisten perusoikeuksia. Yksityiselämän suojan rajoitus olisi melko vähäinen verrattuna rajoituksen perusteena olevan yhteiskunnallisen intressin tärkeyteen. Lisäksi puolustushaarojen tiedustelulla ei ole itsenäistä toimivaltaa tietolähdetoimintaan, vaan se tapahtuu sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa. Painavan yhteiskunnallisen tarpeen lisäksi perusoikeuden rajoituksen tulee olla välttämätön hyväksyttävän tarkoituksen saavuttamiseksi.

10.2.12 Henkilötietojen suoja

10.2.12.1 Yleistä

Perustuslain 10 §:ssä säädetään yksityiselämän suojasta. Pykälän ensimmäisen momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Momentin toisen lauseen lakivarauksen mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslakivaliokunnan vakiintuneen käytännön mukaan lainsäätäjän liikkumavaraa on rajoittanut lisäksi se, että henkilötietojen suoja osittain sisältyy samassa momentissa turvatun yksityiselämän suojan piiriin. Lainsäätäjän tulee turvata tämä oikeus tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kannalta kokonaisuudessaan (ks. esim. PeVL 48/2018 vp, s. 3 ja PeVL 13/2016 vp, s. 3–4).

Perustuslakivaliokunta on arvioinut erityisesti arkaluonteisten tietojen käsittelyn sallimisen koskevan yksityiselämään kuuluvan henkilötietojen suojan ydintä, minkä vuoksi esimerkiksi tällaisia tietoja sisältävien rekisterien perustamista on arvioitava perusoikeuksien rajoitusedellytysten, erityisesti rajoitusten hyväksyttävyyden ja oikeasuhtaisuuden, kannalta (ks. esim. PeVL 48/2018 vp, s. 3 ja siinä viitatut lausunnot). Myös EU:n yleisen tietosuoja-asetuksen mukaan erityisiä henkilötietoja, jotka ovat erityisen arkaluonteisia perusoikeuksien ja -vapauksien kannalta, on suojeltava erityisen tarkasti, koska niiden käsittelyn asiayhteys voisi aiheuttaa huomattavia riskejä perusoikeuksille ja -vapauksille. Valiokunta on kiinnittänyt erityistä huomiota siihen, että arkaluonteisten tietojen käsittely on syytä rajata täsmällisillä ja tarkkarajaisilla säännöksillä vain välttämättömään (ks. esim. PeVL 3/2021 vp, s. 3 ja PeVL 14/2018, s. 5).

Perustuslakivaliokunta on myös painottanut, että yksityiselämän ja henkilötietojen suoja tulee suhteuttaa toisiin perus- ja ihmisoikeuksiin sekä muihin painaviin yhteiskunnallisiin

intresseihin, kuten yleiseen turvallisuuteen liittyviin intresseihin, jotka voivat ääritapauksessa palautua henkilökohtaisen turvallisuuden perusoikeuteen (PeVL 5/1999 vp, s. 2). Valiokunta on katsonut, että yksityiselämän ja henkilötietojen suojalla ei ole etusijaa muihin perusoikeuksiin nähden. Arvioinnissa on kyse kahden tai useamman perusoikeussäännöksen yhteensovittamisesta ja punninnasta (ks. esim. PeVL 26/2018, s. 4, PeVL 14/2018 vp, s. 8, PeVL 54/2014 vp, s. 2 ja PeVL 10/2014 vp, s. 4).

Perustuslakivaliokunta on EU:n tietosuoja-asetuksen soveltamisalalla tarkistanut kantaansa henkilötietojen suojasta lailla säätämisen vaatimuksen osalta. Valiokunnan mielestä tietosuoja-asetuksen yksityiskohtainen sääntely, jota tulkitaan ja sovelletaan EU:n perusoikeuskirjassa turvattujen oikeuksien mukaisesti, muodostaa yleensä riittävän säännöspohjan myös perustuslain 10 §:ssä turvatun yksityiselämän ja henkilötietojen suojan kannalta. Valiokunnan käsityksen mukaan tietosuoja-asetuksen sääntely vastaa asianmukaisesti tulkittuna ja sovellettuna myös Euroopan ihmisoikeussopimuksen mukaan määräytyvää henkilötietojen suojan tasoa. Näin ollen erityislainsäädäntöön ei ole tietosuoja-asetuksen soveltamisalalla enää valtiosääntöisistä syistä välttämätöntä sisällyttää kattavaa ja yksityiskohtaista sääntelyä henkilötietojen käsittelystä (PeVL 14/2018 vp, s. 4). Valiokunta on kuitenkin pitänyt selvänä, että erityislainsäädännön tarpeellisuutta on arvioitava myös tietosuoja-asetuksen edellyttämän riskiperustaisen lähestymistavan mukaisesti kiinnittämällä huomiota tietojen käsittelyn aiheuttamiin uhkiin ja riskeihin. Mitä korkeampi riski käsittelystä aiheutuu luonnollisen henkilön oikeuksille ja vapauksille, sitä perustellumpaa on yksityiskohtaisempi sääntely. Tällä seikalla on erityistä merkitystä arkaluonteisten tietojen käsittelyn kohdalla (ks. esim. PeVL 51/2018 vp, s. 3 ja PeVL 14/2018 vp, s. 4–6). Perustuslakivaliokunta on kiinnittänyt myös erityistä huomiota sääntelytarpeeseen silloin, kun henkilötietoja käsittelee viranomainen (PeVL 14/2018 vp, s. 4–5).

Perustuslakivaliokunta on katsonut, että toisin kuin suoraan sovellettava tietosuoja-asetus, rikosasioiden tietosuojadirektiivi ei sisällä sellaista yksityiskohtaista sääntelyä, joka muodostaisi riittävän säännöspohjan perustuslain 10 §:ssä turvatun yksityiselämän ja henkilötietojen suojan kannalta. Perustuslakivaliokunnan mielestä henkilötietojen käsittelyä koskevaa sääntelyä on tällaisissa perusoikeusherkissä sääntelykonteksteissa edelleen arvioitava valiokunnan aiemman sääntelyn lakitasoisuutta, täsmällisyyttä ja kattavuutta korostaneen käytännön pohjalta. Henkilötietojen suojaan liittyvät sääntelyn kattavuuden, täsmällisyyden ja tarkkarajaisuuden vaatimukset voidaan kuitenkin joiltain osin täyttää myös tietosuoja-asetuksen soveltamisalan ulkopuolella kansalliseen oikeuteen sisältyvällä yleislailla (ks. PeVL 51/2018 vp, s. 3, PeVL 26/2018 vp, s. 3–4, PeVL 14/2018 vp, s. 7).

Perustuslakivaliokunta on tiedonsaantioikeuksia ja tietojen luovuttamista koskevassa lausuntokäytännössään kiinnittänyt huomiota siihen, mihin ja ketä koskeviin tietoihin tiedonsaantioikeus ulottuu ja miten tiedonsaantioikeus sidotaan tietojen välttämättömyyteen. Viranomaisen tietojensaantioikeus ja tietojenluovuttamismahdollisuus ovat voineet liittyä jonkin tarkoituksen kannalta tarpeellisiin tietoihin, jos tietosisällöt on pyritty luettelemaan laissa tyhjentävästi. Jos taas tietosisältöjä ei ole samalla tavoin luetteloitu, sääntelyyn on valiokunnan mukaan pitänyt sisällyttää vaatimus tietojen välttämättömyydestä jonkin tarkoituksen kannalta. Valiokunta ei toisaalta ole pitänyt hyvin väljiä ja yksilöimättömiä tietojensaantioikeuksia perustuslain kannalta mahdollisina edes silloin, kun ne on sidottu välttämättömyyskriteeriin. Valiokunta on antanut merkitystä luovutettavien tietojen luonteelle arkaluonteisina tietoina arvioidessaan tietojen saamista ja luovuttamista koskevaa sääntelyn kattavuutta, täsmällisyyttä ja sisältöä (ks. esim. PeVL 48/2018 vp, s. 4–5, PeVL 38/2016 vp, s. 3 ja PeVL 17/2016 vp, s. 2–3).

Perustuslakivaliokunta on pitänyt tärkeänä, että siltä osin kuin Euroopan unionin lainsäädäntö edellyttää kansallista sääntelyä tai mahdollistaa sen, tätä kansallista liikkumavaraa käytettäessä otetaan huomioon perus- ja ihmisoikeuksista seuraavat vaatimukset. Valiokunta on tämän johdosta painottanut, että hallituksen esityksessä on erityisesti perusoikeuksien kannalta merkityksellisen sääntelyn osalta syytä tehdä selkoa kansallisen liikkumavaran alasta (ks. esim. PeVL 1/2018 vp, s. 3, PeVL 26/2017 vp, s. 42, PeVL 2/2017 vp, s. 2, PeVL 44/2016 vp, s. 4).

Henkilötietojen käsittelyyn sotilastiedusteluviranomaisessa sovelletaan käsittelytarkoituksen mukaan joko henkilötietojen käsittelystä Puolustusvoimissa annettua laki (332/2019) tai henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettua lakia (1054/2018, jäljempänä rikosasioiden tietosuojalaki). Näiden lakien muodostaman kokonaisuuden soveltamisalalla ei sovelleta lainkaan EU:n tietosuoja-asetusta eikä yleistä tietosuojalakia.

Erityissääntelyä täydentää yleinen tietosuoja-asetus (EU 2016/679). Yleisen tietosuoja-asetuksen ja rikosasioiden tietosuojalain mukaan henkilötietoja ovat kaikki sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti. Välillinen tunnistaminen voi tapahtua esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Henkilötietojen käsittely sotilastiedustelussa kuuluu yleisen tietosuoja-asetuksen soveltamisalaan ja perustuu asetuksen 6 artiklan 1 kohdan e alakohtaan, jonka mukaan henkilötietojen käsittely on sallittua yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi.

Nyt käsiteltävänä olevassa esityksessä ehdotetaan uuden tyyppistä sääntelyä (etenkin 1. lakiehdotuksen 66 § ja 67 a §), jossa käsitellään henkilötietoja, mutta niistä ei hankita tietoja henkilöiden tunnistamiseksi tai tietoa heidän yksityiselämästään. Säännöksissä on kyse ennen kaikkea tietoliikennetiedustelun tekniseen kohdistamiseen ja tarkempien hakuehtojen määrittämiseen liittyvästä tietoliikenteen teknisestä käsitellystä. Ehdotusten nojalla voidaan tallentaa tietoja, joita voidaan käyttää myös muissa ehdotettujen toimivaltuuksien käyttämisessä sekä varsinaisessa tietoliikennetiedustelussa.

10.2.12.2 Tietoliikenteen teknisten tietojen käsittely ja hakuehtojen määrittäminen

Voimassa olevan Puolustusvoimien henkilötietolain lähtökohtana on, että tietoliikenteen tekniset tiedot ovat, pois lukien tietoliikenneverkon laitteiden ohjausliikenne ja muu ainoastaan laitteiden välinen tietoliikenne, tunnistettavaan henkilöön suoraan tai välillisesti liittyviä tietoja eli henkilötietoja. Vastaavasti voidaan todeta ehdotettavan tietoliikennetiedustelun hakuehtojen määrittämisen osalta.

Vaikka ehdotettujen tietoliikenteen teknisten tietojen käsittely ja hakuehtojen määrittäminen kohdistuu pääsääntöisesti tietoihin, joista voidaan välillisesti tunnistaa henkilö eivätkä ehdotukset anna mahdollisuutta hankkia tietoja sotilastiedustelun kohteesta, toimivaltuuksilla hankittujen tallennettujen tietojen käyttö varsinaisessa tietoliikennetiedustelussa antaa mahdollisuuden yhdistää myös muuta sotilastiedusteluviranomaisen tietoliikennetiedustelussa käytettävää tai käytössä olevaa tietoa. Vaikka teknisten tietojen käsittely ja hakuehtojen määrittäminen sisältää myös muita tietoja kuin henkilötietoja, koko tietoaineiston käsittelyyn olisi tarkoituksenmukaista soveltaa henkilötietojen käsittelyä koskevia edellytyksiä.

Esityksessä tarkoitetun teknisten tietojen käsittelyn ja hakuehtojen määrittämisen tallenteisiin voi sisältyä yleisen tietosuoja-asetuksen 9 artiklassa tarkoitettuihin erityisiin henkilötietoryhmiin kuuluvia tietoja tai muutoin valtiosääntöisesti arkaluonteisiksi katsottavia tietoja. Varsinaisessa tietoliikennetiedustelussa käsittelyn yhteydessä voi olla kyse edellä

mainittujen tietojen käsittelystä. Yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan g alakohdan mukaan erityisiin henkilötietoryhmiin kuuluvien tietojen käsittely on sallitussa, kun käsittely on tarpeen tärkeää yleistä etua koskevasta syystä unionin oikeuden tai jäsenvaltion lainsäädännön nojalla, edellyttäen että se on oikeasuhteinen tavoitteeseen nähden, siinä noudatetaan keskeisiltä osin oikeutta henkilötietojen suojaan ja siinä säädetään asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn perusoikeuksien ja etujen suojaamiseksi. Edellä kuvatulla tavalla käsittely katsotaan tältäkin osin oikeasuhtaiseksi. Tältä osin käsittelyä rajoittaa henkilötietojen käsittelystä Puolustusvoimissa annetun lain 3 §:ssä säädetyt periaatteet ja 4 §:n 2 momentissa viitattu rikosasioiden henkilötietolain 11 §, jossa erityisiin henkilötietoryhmiin kuuluvien tietojen tallettaminen ja muu käsittely on sallittua vain, jos käsittely on rekisterin käyttötarkoituksen kannalta välttämätöntä.

10.2.12.3 Henkilötietojen vertailu

Esityksen 13. lakiehdotuksen 37 a §:ssä ehdotetaan, että sotilastiedusteluviranomainen saisi tietojärjestelmänsä ylläpitämiseksi verrata henkilörekisterin, josta sotilastiedusteluviranomainen voi saada tietoja muun lain nojalla, tietoja talletettujen henkilötietojensa sisältöön. Tarpeettomat tiedot on hävitettävä viipymättä sen jälkeen kuin vertailu on suoritettu. Tarpeettomia henkilötietoja ei saa tallettaa.

Säännöksessä tarkoitettuja tietoja sotilastiedusteluviranomainen voi jo nykyisellään saada laissa säädetyn oikeutensa perusteella. Näin ollen henkilötietojen käsittelyä on arvioitu kulloisenkin lain käsittelyn yhteydessä. Säännöksen mahdollistavan vertailun voidaan katsoa parantavan sotilastiedusteluviranomaisen henkilörekistereiden tietojen ajantasaisuutta ja näin sillä voidaan katsoa olevan perusoikeusmyönteisiä vaikutuksia.

Esitettyä säännöstä ei voi pitää yksityisyyden suojan kannalta erityisen merkittävänä, sillä vertailun mahdollistaminen ei laajentaisi tietosisältöä, johon sotilastiedusteluviranomaisella on jo tällä hetkellä oikeus. Säännös selventäisi ja tekisi lainsäädäntöä tarkkarajaisemmaksi siltä osin kuin sotilastiedusteluviranomaisella on oikeus saada tarpeellisia henkilötietoja tehtäviensä suorittamiseksi ja rekisterinsä ylläpitämiseksi teknisen käyttöyhteyden avulla tai tietojoukkona. Säännöksellä ei siten muutettaisi nykyistä oikeustilaa, mutta huomioitaisiin teknisen kehityksen vaatimukset tietosuojalle ja rekisterin oikeellisuudelle.

10.2.12.4 Yhteenveto

Käytännön toiminnan tasolla tietosuojavaatimukset on sotilastiedusteluviranomaisessa huomioitu jo aiemmin voimassa olevan teknisten tietojen käsittelyn ja varsinaisen tietoliikennetiedustelun osalta, koska kyseessä on olemassa oleva toimivaltuus. Sääntelyn asiasisällöllisillä muutoksilla ei arvioida olevan vaikutusta valittuihin tietosuojaratkaisuihin. Hakuehtojen määrittämisen osalta kyse olisi uudesta tavasta käsitellä henkilötietoja. Tältä osin käytännön toteutuksessa olisi huomioitava alusta alkaen sisäänrakennettu ja oletusarvoinen tietosuoja sekä tietosuojaperiaatteet. Tietosuojaperiaatteet on säädetty henkilötietojen käsittelystä Puolustusvoimissa annetun lain 3 §:ssä, josta on luettavissa lainmukaisuuden varmistaminen, käyttötarkoitussidonnaisuus, käsiteltävien tietojen minimointi, käsiteltävien tietojen täsmällisyydestä varmistuminen, käsiteltävien tietojen säilytyksen rajoittaminen ja käsiteltävien henkilötietojen suojaaminen sekä syrjintäkielto. Tietosuojaperiaatteiden voidaan katsoa täydentävän sotilastiedustelusta annetun lain 5–9 §:ssä säädettyjä periaatteita. Rekisterinpitäjän toimivan sotilastiedusteluviranomaisen olisi toteutettava kaikki tarvittavat tekniset ja organisatoriset toimenpiteet tietosuojaperiaatteiden toteuttamiseksi ja rekisteröityjen oikeuksien suojelemiseksi. Sotilastiedusteluviranomaisen on myös varmistuttava siitä, että hankittavat laitteet, ohjelmistot ja muut oheistuotteet täyttävät niille asetetut vaatimukset.

Yleisen tietosuoja-asetuksen 35 artiklassa säädetään velvollisuudesta toteuttaa tietosuojaa koskeva vaikutustenarviointi, jos tietyntyyppinen käsittely etenkin uutta teknologiaa käytettäessä todennäköisesti aiheuttaa käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin. Ehdotettuun radiotekniseen valvontaan saattaa sisältyä tällaisia riskejä. Näin ollen rekisterinpitäjänä toimivan Rajavartiolaitoksen esikunnan tulee ennen ehdotettavan uuden toimivaltuuden käyttöönottoa toteuttaa tarkempi arviointi suunniteltujen käsittelytoimien vaikutuksista henkilötietojen suojalle yleisen tietosuoja-asetuksen vaatimusten mukaisesti. Rekisterinpitäjän tulee myös kiinnittää erityistä huomiota rekisteröityjen informointiin, koska ehdotetun sääntelyn mukaan radioteknisestä valvonnasta ei muutoin erikseen ilmoitettaisi.

Sotilastiedustelusta annetussa laissa ja henkilötietojen käsittelystä Puolustusvoimissa annetussa laissa säädetään kattavasti ja yksityiskohtaisesti käsiteltävistä henkilöryhmistä, käsiteltävien tietojen sisällöstä ja sallituista käyttötarkoituksista, henkilötietojen luovuttamisesta ja poistamisesta sekä rekisteröidyn oikeuksien toteuttamisesta ja poikkeuksista rekisteröidyn oikeuksiin. Esityksessä ei ehdoteta erityissääntelyä sellaisista asiakokonaisuuksista, joista säädetään kattavasti ja täsmällisesti tietosuojan yleislainsäädännössä. Yleinen tietosuoja-asetus, tietosuojalaki ja rikosasioiden tietosuojalaki sisältävät yksityiskohtaiset säännökset muun muassa rekisterinpitäjän vastuusta ja rekisteröidyn oikeuksista, tietoturvallisuudesta ja henkilötietojen käsittelyn valvonnasta sekä lainvastaisen henkilötietojen käsittelyn seuraamuksista.

10.3 Laki Puolustusvoimista

10.3.1 Tiedonhankinta yleisesti saatavilla olevista lähteistä

Esityksen 2. lakiehdotuksessa ehdotetaan lisättäväksi puolustusvoimista annettuun lakiin uudet 8 b ja 8 c §:t. Säännökset koskisivat tiedonhankintaa yleisesti saatavilla olevista lähteistä, eli tietovarannoista, jotka ovat kaikkien saatavilla yleisesti tai maksua vastaan.

Julkisen vallan käytön tulee perustua lakiin. Kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Tästä oikeusvaltioperiaatteesta ja siihen olennaisesti liittyvästä hallinnon lainalaisuuden periaatteesta säädetään perustuslain 2 §:n 3 momentissa.

Oikeusvaltioperiaatteen noudattaminen edellyttää, että julkisen vallan käyttäjällä on aina viime kädessä eduskunnan säätämään lakiin palautettavissa oleva toimivaltaperuste. Viranomaisella ei siten voi olla sellaista julkisen vallan käyttämistä tarkoittavaa toimivaltaa, jolla ei ole nimenomaista tukea laissa.

Yleisesti saatavilla olevien lähteiden tiedonhankinnassa ei aina ole kyse henkilötietojen käsittelystä. Tyypillisesti esimerkiksi tietoteknisin keinoin yleisesti saatavilla olevista lähteistä kerättyyn tietoon kuitenkin sisältyy henkilötietoja, jotka liittyvät yleisen tietosuoja-asetuksen 4 artiklassa ja rikosasioiden tietosuojalain 3 §:ssä tarkoitetulla tavalla tunnistettuun tai tunnistettavissa olevaan henkilöön. Ehdotus on siten merkityksellinen erityisesti perustuslain 10 §:ssä turvatun yksityiselämän ja henkilötietojen suojan kannalta.

Euroopan unionin perusoikeuskirjan 8 artiklassa edellytetään, että henkilötietojen käsittelyn on tapahduttava tiettyä tarkoitusta varten. Tietosuoja-asetuksen käyttötarkoitussidonnaisuutta koskevan 5 artiklan 1 kohdan b alakohdan mukaan henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten. Tietojen minimointia koskevan 5 artiklan 1 kohdan c alakohdan mukaan henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään.

Käyttötarkoitussidonnaisuuden ja tietojen minimoinnin periaatteista säädetään vastaavasti myös rikosasioiden tietosuojadirektiivin 4 artiklassa sekä kansallisesti rikosasioiden tietosuojalain 5 ja 6 §:ssä. Myös perustuslakivaliokunta on arvioidessaan henkilötietojen käsittelyä koskevaa lainsäädäntöä pitänyt henkilötietojen suojan kannalta tärkeinä sääntelykohteina muun ohella rekisteröinnin tavoitetta, tietosisältöjä ja sallittuja käyttötarkoituksia (ks. esim. PeVL 51/2018 vp, s. 8 ja PeVL 14/2018 vp, s. 2). Valiokunta on edellyttänyt erityisesti arkaluonteisten tietojen käsittelyn rajoittamista täsmällisillä ja tarkkarajaisilla laintasoisilla säännöksillä vain välttämättömään (ks. esim. PeVL 51/2018 vp, s. 10).

Perustuslakivaliokunta on voimassa olevaa poliisin henkilötietolakia koskevassa lausunnossaan arvioinut ehdotusta, joka koski muun muassa julkisista lähteistä rikosanalyysin yhteydessä kerättyjen tietojen käsittelemistä tilanteissa, joissa tiedot eivät liity suoraan käsillä olevaan poliisin yksittäiseen tehtävään. Ehdotettu säännös olisi mahdollistanut tietojen tallettamisen poliisin rekisteriin kuuden kuukauden ajaksi niiden merkityksellisyyden arvioimiseksi. Perustuslakivaliokunnan käsityksen mukaan ehdotetun sääntelyn perusteella olisi muodostunut laaja, tietosisällöiltään ja käsittelyn tarkoitukseltaan oikeudellisesti kontrolloimaton rekisteri, joka voisi sisältää laajasti myös arkaluonteisia tietoja. Säännösehdotukset olisivat mahdollistaneet poliisin tehtävien kannalta merkityksettömien tietojen keräämisen ja tallettamisen rekisteriin jopa kuuden kuukauden ajaksi. (PeVL 51/2018 vp, s. 9–10.)

Perustuslakivaliokunta piti säännösten poistamista ehdotetussa muodossa edellytyksenä lakiehdotuksen käsittelemiselle tavallisen lain säätämisjärjestyksessä. Valiokunta huomautti kuitenkin, että henkilötietojen käsittelyn perusteiden arvioinnista voidaan perustuslain estämättä säätää esimerkiksi perustuslakivaliokunnan myötävaikutuksella (PeVL 60/2010 vp, s. 4/ II—5/I) säädetyn poliisilain 5 luvun 55 §:n kaltaisella tiedon hävittämistä koskevalla sääntelyllä (ks. myös pakkokeinolain 57 § ja PeVL 66/2010 vp, s. 10 sekä PeVL 32/2013 vp, s. 6—7). (PeVL 51/2018 vp, s. 9–10.). Henkilötietojen käsittelystä Puolustusvoimissa annetun lain 5 luvussa on yksityiskohtaisesti säädetty tietojen hävittämisestä.

Esityksessä ehdotetussa tiedonhankinnassa yleisesti saatavilla olevista lähteistä sovellettaisiin henkilötietojen käsittelystä Puolustusvoimissa annettua laki, kun kerättyyn tietoon sisältyy henkilötietoja. Henkilötiedot olisi siten hävitettävä sen mukaan, mitä käyttötarkoitukseen sidotusta rekisteristä säädetään. Tämän lisäksi lain 45 §:ssä säädetään, että tilapäisestä henkilörekisteristä henkilötieto on hävitettävä välittömästi sen jälkeen, kun se ei enää ole käyttötarkoituksensa kannalta tarpeellinen. Tilapäisen henkilörekisterin tarpeellisuutta on arvioitava vähintään kolmen vuoden välein.

Sovellettavaksi tulisi myös muu Puolustusvoimien henkilötietolain sääntely, kuten erityisiin henkilötietoryhmiin kuuluvien henkilötietojen käsittelylle säädetty välttämättömyysvaatimus. Henkilötietojen lisäksi myös muu yleisesti saatavilla olevista lähteistä hankittu tieto olisi ehdotetun puolustusvoimista annetun lain 8 c §:n mukaan hävitettävä viipymättä sen jälkeen, kun on käynyt ilmi, ettei tietoa tarvita Puolustusvoimien tehtävien suorittamiseksi.

Vaikka esityksen 2. lakiehdotuksen 8 b §:ssä ei voida katsoa olevan kyse julkisen vallan käyttämisestä, voidaan toiminta katsoa kuitenkin sen verran keskeiseksi nyky-yhteiskunnassa, että siitä on tarpeen säätää lailla. Etenkin säännöksen 3 momentissa säädettäväksi esitetty peitteen käyttö on toimintaa, jota viranomaisen ei katsota voivan toteuttaa ilman nimenomaista lainsäännöstä.

10.3.2 Virkanimitykset

Esityksen 2. lakiehdotuksessa ehdotetaan lisättäväksi puolustusvoimista annetun lain 36 a §:ään uusi 3 momentti.

Perustuslain 2 §:n mukaan julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Julkisen vallan käytön tulee olla palautettavissa eduskunnan säätämässä laissa olevaan toimivaltaperusteeseen (HE 1/1998 vp). Perustuslain 80 §:n 1 momentin perusteella yksilön oikeuksien ja velvollisuuksien perusteista on säädettävä lailla.

Ehdotettu sääntely on merkityksellistä yhdenvertaisuutta koskevan perustuslain 6 §:n, oikeutta elämään ja henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen koskevan perustuslain 7 §:n, oikeutta työhön ja julkisen vallan velvollisuutta huolehtia työvoiman suojelusta koskevan 18 §:n, julkisuutta koskevan perustuslain 12 §:n sekä oikeusturvaa koskevan perustuslain 21 §:n kannalta. Perustuslain 22 §:n mukaan julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen. Lisäksi sääntelyä voidaan tarkastella Euroopan ihmisoikeussopimuksen oikeutta elämään koskevan 2 artiklan 1 kohdan sekä oikeudenmukaista oikeudenkäyntiä koskevan 6 artiklan 1 kohdan kannalta. Edelleen perustuslakivaliokunta on valtioneuvoston ihmisoikeusselontekoa 2014 koskevassa lausunnossaan korostanut hallituksen esitysten valmistelun kehittämistä niin, että säätämisjärjestysperusteluissa tarkasteltaisiin ehdotuksia myös perustuslain 22 §:n mukaisen perus- ja ihmisoikeuksien turvaamisvelvoitteen eikä ainoastaan perus- ja ihmisoikeusristiriitojen kannalta (PeVL 52/2014 vp, s. 3). Euroopan ihmisoikeussopimuksen 17 artikla koskee oikeuksien väärinkäytön kieltoa.

Perusoikeuksia ei ole asetettu keskinäiseen tärkeysjärjestykseen. Esitykseen liittyvät eri perus- ja ihmisoikeudet, joiden keskinäistä suhdetta ja yhteensovittamista on punnittava. Edelleen ihmis- ja perusoikeuksia on tarkasteltava suhteessa painaviin yhteiskunnallisiin intresseihin kuten kansallinen turvallisuus tai yleinen turvallisuus. Yleisen turvallisuuden intressit voivat ääritapauksessa palautua henkilökohtaisen turvallisuuden perusoikeuteen (ks. PeVL 5/1999 vp, s. 2). Huomioon on otettava myös perusoikeuksien yleiset rajoitusedellytykset (PeVM 25/1994 vp, s. 5), jotka muun ohessa edellyttävät, että rajoitukset ovat tarkkarajaisia ja riittävän täsmällisesti määriteltyjä ja niiden olennainen sisältö ilmenee laista. Rajoitusperusteiden tulee olla hyväksyttäviä ja rajoittamisen tulee olla painavan yhteiskunnallisen tarpeen vaatimaa. Tavallisella lailla ei voi säätää perusoikeuden ytimeen ulottuvaa rajoitusta. Edelleen rajoitusten on oltava suhteellisuusvaatimuksen mukaisia ja välttämättömiä hyväksyttävän tarkoituksen saavuttamiseksi. Perusoikeuksia rajoitettaessa on huolehdittava riittävistä oikeusturvajärjestelyistä.

Perustuslain 6 § sisältää yleisen yhdenvertaisuuslausekkeen ja syrjintäkiellon. Yhdenvertaisuusnäkökohdilla on merkitystä niin, että lailla ei voida asettaa mielivaltaisesti ihmisiä toisiaan edullisempaan tai epäedullisempaan asemaan. Yhdenvertaisuussäännös ei kuitenkaan edellytä kaikkien ihmisten kaikissa suhteissa samanlaista kohtelua, elleivät asiaan vaikuttavat olosuhteet ole samanlaisia (HE 309/1993 vp. s. 42–43). Perustuslain 6 §:n 2 momentissa tarkoitetulle erilaisen kohtelun mahdollistavalle hyväksyttävälle perusteelle asetettavat vaatimukset on perustuslakivaliokunnan käytännössä edellytetty olevan asiallisessa ja kiinteässä yhteydessä lain tarkoitukseen (esim. PeVL 44/2010 vp.). Nyt esitetyn sääntelyn ei voida katsoa muodostuvan ongelmalliseksi yhdenvertaisuusperiaatteen näkökulmasta. Tiettyjen Puolustusvoimien tehtävien täyttäminen avoimeksi julistamatta ei itsessään aseta ihmisiä eriarvoiseen asemaan. Erilaiselle virantäyttömenettelylle on hyväksyttävät ja painavat

yhteiskunnalliset syyt. Yhdenvertaisuusnäkökulma on kuitenkin tärkeä huomioida osana Puolustusvoimien henkilöstöpolitiikkaa.

Perustuslakivaliokunta on lausunut perustuslain 7 §:än liittyen poikkeuksellisesta henkilökohtaisen turvallisuuden uhasta liittyen Puolustusvoimien kansainvälisiin tehtäviin (PeVL 65/2016 vp). Perustuslakivaliokunnan mukaan kansainvälisiin tehtäviin voi lakiehdotuksen mukaan sisältyä sotilaallista voimankäyttöä ja siten poikkeuksellista henkilökohtaisen turvallisuuden uhkaa, mikä on merkityksellistä myös perustuslain 7 §:n näkökulmasta. Perustuslakivaliokunta on vuonna 2020 liittyen valmiuslain nojalla annettaviin asetuksiin esittänyt näkökulmia yhteydestä perustuslain 7 §:n 1 momentin julkisen vallan velvollisuuteen turvata jokaisen oikeus elämään (PeVM 2/2020 vp). Perustuslakivaliokunnan mietinnössä PeVM 5/2020 vp, käsiteltäessä valmiuslain nojalla annettua valtioneuvoston asetusta väliaikaisista poikkeuksista sovellettaessa eräitä vuosilomalain, työaikalain ja työsopimuslain säännöksiä, on kiinnitetty huomiota myös perustuslain 18 §:n 1 momentissa julkiselle vallalle asetettuun velvollisuuteen huolehtia työvoiman suojelusta.

Uudemmassa käytännössään perustuslakivaliokunta on muun muassa suojelupoliisin nimitysmenettelyn julkisuutta koskevasta lakiehdotuksesta todennut, että julkisuuden rajoittamisen tavoitteet kiinnittyvät perustuslain 7 §:n lisäksi myös perustuslain 18 §:ssä julkiselle vallalle asetettuun velvollisuuteen suojella työvoimaa. Valiokunta piti sääntelyn hyväksyttävyyden kannalta tärkeänä, että poikkeaminen hakumenettelyn julkisuudesta edellyttää yksittäistapauksellista arviointia.

Virkoihin nimittämisen muutoksenhaun osalta ehdotusta on arvioitava perustuslain 21 §:n oikeusturvasäännöksen kannalta ja Euroopan ihmisoikeussopimuksen 6 artiklan 1 kohdan kannalta (oikeus oikeudenmukaiseen oikeudenkäyntiin). Perustuslain 21 §:n 1 momentin mukaan jokaisella on oikeus saada oikeuksiaan ja velvollisuuksiaan koskeva päätös tuomioistuimen tai muun riippumattoman lainkäyttöelimen käsiteltäväksi. Lisäksi oikeus hakea muutosta samoin kuin muut oikeudenmukaisen oikeudenkäynnin ja hyvän hallinnon takeet ovat perustuslain 21 §:n 2 momentin mukaan turvattava. Säännöksellä ei kuitenkaan ole tarkoitettu estää säätämästä tähän oikeuteen vähäisiä poikkeuksia, kunhan ne eivät muodostu pääsäännöksi eivätkä vaaranna yksilön oikeutta oikeudenmukaiseen oikeudenkäyntiin (HE 309/1993 vp, s. 74).

Päätettäessä virkaan nimittämisestä on viranomaisen noudatettava asianomaista virkaa koskevien kelpoisuusvaatimusten ja muiden mahdollisten erityisten vaatimusten lisäksi perustuslain 125 §:n 2 momentissa säädettyjä yleisiä virkanimitysperusteita. Tästä huolimatta kenelläkään ei ole kuitenkaan subjektiiviseksi luonnehdittavaa oikeutta tulla nimitetyksi valtion virkaan. Valtion virkamieslain muutos tuli voimaan vuoden 2019 alussa ja lain 59 §:ssä säädetään muutoksenhausta virkanimityksiin. Valtion virkamieslain muutosta koskeneessa hallituksen esityksessä on (HE 77/2017 vp) on asiaa arvioitu perustuslakivaliokunnan lausuntojen nojalla (PeVL 63/2010 vp, PeVL 16/2000 vp, PeVL 10/2009 vp, PeVL 46/2002 vp, PeVL 18/2011 vp, PeVL 51/2010 vp). Edellä mainitusta hallituksen esityksestä annetusta perustuslakivaliokunnan lausunnosta PeVL 42/2017 vp tulee esille, että kysymystä valtion virkanimityksiin liittyvästä valituskiellosta on käsitelty useita kertoja perustuslakivaliokunnassa ja valiokunnan aiempi kannanotto on ollut perusteena edellä mainitulle virkamieslain muuttamiselle. Perustuslakivaliokunnan lausunnon mukaan perustuslain 21 §:n säännökset eivät estä säätämästä lailla vähäisiä poikkeuksia niissä turvattuihin oikeuksiin, kunhan tällaiset poikkeukset eivät muuta kulloinkin kyseessä olevan oikeusturvatakeen asemaa pääsääntönä eivätkä yksittäistapauksessa vaaranna yksilön oikeusturvaa (ks. esim. PeVL 68/2014 vp, s. 3/I). Edelleen perustuslakivaliokunta toteaa, että mikä tahansa yksilön kannalta myönteinen viranomaistoimi ei kuitenkaan ole yksilön oikeutta koskeva päätös perustuslain mielessä.

Perustuslakivaliokunta on katsonut, että valiokunnan käytännössä virkaan nimittämistä ei ole pidetty subjektiivisena oikeutena, johon liittyisi perustuslain 21 §:ssä ja Euroopan ihmisoikeussopimuksen 6 artiklan 1 kappaleessa tarkoitettu oikeus saada asiansa tuomioistuimen käsiteltäväksi. Virkanimityspäätöksiin sisältyy kuitenkin harkintaa, jota ohjataan ja rajoitetaan lainsäädännöllä. Harkinnan lähtökohtana on perustuslain 125 §:n 2 momentti, jossa säädetään yleisistä nimitysperusteista julkisiin virkoihin.

Euroopan ihmisoikeussopimuksen 6 artiklan perusteella virkaan nimittäminen ei ole henkilön oikeuksia tai velvollisuuksia koskeva päätös. Sopimuskohdan ei sinänsä voida katsoa estävän muutoksenhakuoikeuden poistamista. Euroopan ihmisoikeussopimuksen 6 artiklan 1 kohdan soveltuvuutta virkamiesoikeudellisiin asioihin on arvioitu Euroopan ihmisoikeustuomioistuimen ratkaisuissa. Keskeinen kysymys on tällöin ollut se, onko virkamiestä koskeva asia sellainen, jossa päätetään hänen oikeuksistaan ja velvollisuuksistaan ja jossa pääsy tuomioistuimeen tulisi näin ollen turvata.

Perustuslakivaliokunta totesi hallituksen vuoden 2015 vuosikertomusta koskevassa lausunnossaan (PeVL 25/2016 vp—K10/2016 vp), että sen saaman selvityksen mukaan muun muassa tasavallan presidentin sekä valtioneuvoston yleisistunnon tekemiin nimityksiin sekä esimerkiksi puolustus- ja ulkoasiainhallinnon alojen lukuisiin nimitysratkaisuihin liittyi sellaisia erityispiirteitä, jotka saattavat antaa aiheen erillisjärjestelyihin. Perustuslakivaliokunnan lausunnossa todetaan, että sen saaman selvityksen mukaan perustavanlaatuinen kysymys on se, voiko valitusoikeus olla ehdoton ja koskea kaikkia virkasuhteita.

Esityksessä ei ehdoteta poistettavaksi muutoksenhakuoikeutta, kun virka tai virkasuhde täytetään julkisesti. Julkinen hakumenettely olisi myös edelleen virantäyttömenettelyssä pääsääntönä.

Perustuslain 12 §:n 2 momentin mukaan viranomaisen hallussa olevat asiakirjat ja tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta. Esityksessä ehdotetaan mahdollistettavaksi julkisessa hakumenettelyssä henkilön tunnistetiedon eli nimen luovutukseen julkisuutta koskeva rajoitus viran tai virkasuhteen täytöstä ilmoitettaessa, mikä liittyy muiden perusteiden ohella erittäin tärkeään yleiseen etuun, kuten kansallisen turvallisuuden suojaamiseen, sekä erittäin tärkeään yksityiseen etuun, äärimmillään hengen ja terveyden suojaamiseen. Säännösehdotusta ei ole muotoiltu salassapitosäännökseksi. Perustuslain 12 §:n 2 momentissa mahdollistetaan myös muun tyyppisiä julkisuuden rajoituksia (PeVL 8/2021 vp s. 8). Nimen ja muun tiedon salassapitoa olisi arvioitava julkisuuslain 24 §:n perusteella tietoa pyydettäessä (yleisöjulkisuus) ja asianosaisjulkisuuden osalta julkisuuslain 11 §:n 1 momentin ja 2 momentin 1 kohdan perusteella. Ehdotetussa sääntelyssä suojattava intressi määrittyy julkisuuslain salassa pitoa koskevien säännösten mukaisesti ja ehdotus antaa menettelykehikon rajoitetumpaan avoimuuteen.

Virkojen ja virkasuhteiden täyttö ilman avointa hakumenettelyä poikkeaa hallinnon lähtökohtaisesta avoimuudesta ja julkisuusperiaatteesta. Rajoituksesta ehdotetaan säädettäväksi lailla perusoikeuksien yleisten rajoitusedellytysten mukaisesti. Poikkeamiselle on kuitenkin hyväksyttävä ja painava yhteiskunnallinen intressi ja se on rajoitettu välttämättömään. Poikkeus on siten oikeassa suhteessa rajoitukseen ja sen tavoitteeseen nähden. Puolustusvoimien viroista, joiden tehtävät edellyttävät viran täyttöä ilman hakumenettelyä, ei ole mahdollista laatia tyhjentävää listaa, ja Puolustusvoimien olisi osoitettava, että viran täyttäminen kussakin yksittäistapauksessa on välttämätöntä kyseessä olevan tehtävän näkökulmasta ilman julkista hakua. Täsmällinen ja tarkka rajaus toteutuu Puolustusvoimien nimitystoimivallan kautta ottaen

huomioon säädetyt perusteet välttämättömyyden arvioinnille. Yleisestä julkisesta hakumenettelystä poikkeaminen olisi kansallisen turvallisuuden ja valtion edun mukainen objektiivinen peruste ottaen huomioon myös, että henkilöllä ei ole subjektiivista oikeutta tulla nimitetyksi. Kyse on tehtävien perusteella rajatusta henkilöpiiristä ja ehdotettu sääntely muodostaisi rajoitetun ja hyväksyttävän poikkeuksen. Tietyt päällikkötason tai tehtäviltään vastaavat virat tulisi aina täyttää julkisen hakumenettelyn kautta.

Euroopan ihmisoikeussopimuksen 2 artiklan mukaan jokaisen oikeus elämään on suojattava laissa. Perusoikeutena oikeus elämään on keskeisin ja siihen kohdistuva uhka vakavin yksittäisen virkamiehen kannalta. Lakiehdotus liittyy painavaan yhteiskunnalliseen intressiin, maanpuolustukseen ja kansalliseen turvallisuuteen. Suomen maanpuolustukseen ja kansallista turvallisuuteen kohdistuvia uhkia vastaan ja niitä ehkäisevästi Puolustusvoimien on välttämätöntä kyetä toimimaan keinoin, joihin liittyviä tehtäviä suorittavien henkeä ja terveyttä suojataan alusta lukien. Rikostorjunnassa ja sotilastiedustelussa henkilöpiiri on myös laajempi kattaen myös ulkopuolisten, kuten tietolähteiden, suojaamisen. Edellä mainitut uhkat kohdistuvat yleisemminkin yhteiskuntaan ja sen jäseniin eikä ensisijaisesti yksilöön, jolloin kyse on laajemmin yhteiskunnan jäsenten perus- ja ihmisoikeuksien suojaamisesta, joista merkityksellisimmillään on kysymys oikeudesta elämään. Esityksessä ehdotetut keinot perustuvat lakiin ja niiden voidaan katsoa olevan oikeasuhtaisia hyväksyttävän tavoitteen kannalta.

10.4 Perusoikeusrajoitusten täsmällisyys, tarkkarajaisuus ja oikeasuhtaisuus

Välttämättömyys

Luottamuksellisen viestin salaisuuden suojan rajoittamisen edellyttää perustuslain 10 §:n 4 momentin mukaan välttämättömyyttä. Tämä edellytys seuraa myös perusoikeuksien yleisistä rajoitusedellytyksistä.

Arvioitaessa lakiehdotusten säännösten välttämättömyyttä on otettava huomioon, että luottamuksellisen viestin salaisuuden suojaan puuttuvalla tiedustelumenetelmällä saataisiin hankkia tietoa vain sellaisesta sotilastiedustelun kohteena olevasta toiminnasta (laki sotilastiedustelusta 4 §), joka on luonteeltaan sotilaallista tai vakavasti uhkaa kansallista turvallisuutta. Sotilastiedustelun kohteet on määritelty laissa tyhjentävästi, joka vastaisi EIT:n ratkaisukäytännön vaatimuksia. Esimerkiksi pelkkä laissa oleva maininta siitä, että salaisia valtuuksia saadaan käyttää kansallisen turvallisuuden suojaamiseksi, ei ole riittävä ennakoitavuusvaatimuksen täyttämiseksi (Zakharov v. Venäjä). Toisaalta kansallisen lain ei voida edellyttää täsmällisesti ja tyhjentävästi luetteloivan kaikkia niitä tilanteita, joissa viranomaiset saavat käyttää salaisia valtuuksia. Lain säännöksen, jonka mukaan salaisten valtuuksien käyttöperusteena on terrorismin uhka, on esimerkiksi katsottava täyttävän ihmisoikeussopimuksen asettaman ennakoitavuusvaatimuksen (Szabo & Vissy v. Unkari).

Sotilastiedustelun kohteita koskevassa sotilastiedustelusta annetun lain 4 §:ssä yksilöidään ja konkretisoidaan perustuslain 10 §:n 4 momenttiin sisältyvää sääntelyä, jonka mukaan sotilaallisen toiminnan lisäksi kansallista turvallisuutta vakavasti uhkaavalla toiminnalla tarkoitetaan kansanvaltaista valtio- ja yhteiskuntajärjestystä, yhteiskunnan perustoimintoja, suuren ihmismäärän henkeä tai terveyttä taikka kansainvälistä rauhaa ja turvallisuutta uhkaavaa toimintaa. Koska ensiksi mainitun säännöksen jokainen kohta olisi johdettavissa yhdestä tai useammasta sotilaallisen toiminnan tai kansallisen turvallisuuskäsitteen kattamasta suojeluintressistä, pykälä on täyttänyt tältä osin korostuneet vaatimukset välttämättömyydestä ja ennakoitavuudesta.

Käsiteltävänä olevassa esityksessä esitetään uusia toimivaltuuksia, jotka kohdistuisivat edellä mainittuihin sotilastiedustelun kohteisiin. Koska kohteena oleva ennen kaikkea valtiollinen toiminta on vahvasti resursoitua ja toimijoiden toimintatavat kehittyvät kiihtyvää tahtia, on sotilastiedusteluviranomaisen pystyttävä hankkimaan tarvittavaa tietoa myös varsinaisen viestin sisällön ulkopuolelta toimivaltuuksien asianmukaiseksi kohdentamiseksi.

Ehdotetulla sääntelyllä suojataan ennen kaikkea toisia perusoikeuksia, ja sääntelylle on painava yhteiskunnallinen intressi.

Täsmällisyys ja tarkkarajaisuus

Perustuslakivaliokunta on viranomaisten toimivaltuuksia koskevaa sääntelyä arvioidessaan pitänyt arvion lähtökohtana sitä, että viranomaisen toimivaltuuksien sääntely on merkityksellistä perustuslain 2 §:n 3 momentissa vahvistetun oikeusvaltioperiaatteen kannalta (ks. PeVL 51/2006 vp, s. 2). Julkisen vallan käytön tulee momentin mukaan perustua lakiin, ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Lähtökohtana on, että julkisen vallan käytön tulee olla aina palautettavissa eduskunnan säätämässä laissa olevaan toimivaltaperusteeseen (HE 1/1998 vp, s. 74/II). Lailla säätämiseen taas kohdistuu yleinen vaatimus lain täsmällisyydestä ja tarkkuudesta. Toimivaltasääntely on valiokunnan käsityksen mukaan yleensä merkityksellistä myös perustuslaissa turvattujen perusoikeuksien näkökulmasta (ks. PeVL 67/2016 vp, PeVL 10/2016 vp).

Tiedustelumenetelmien käytön yleiset edellytykset on koottu sotilastiedustelua annetun lain 12 §:ään (Amann v. Sveitsi, Kopp v. Saksa, Kruslin v. Ranska, Huvig v. Ranska). Kaikkia tiedustelumenetelmiä koskevana yleisenä edellytyksenä on, että tiedustelumenetelmän käyttö on välttämätöntä ja että sillä voidaan perustellusti olettaa saatavan tärkeää tietoa tiedustelutehtävän kannalta. Jos tiedustelumenetelmä kohdistetaan valtiolliseen toimijaan, tiedustelumenetelmän käytön yleisenä edellytyksenä on, että tietojen saaminen on tarpeen tiedustelutehtävän kannalta. Kyse on niin sanotusta perustellusta tuloksellisuusodotuksesta.

Koska hakuehtojen määrittäminen ja muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu voi sisältää merkittävää puuttumista yksityisen suojattuihin oikeushyviin, edellytyksenä on näiden menetelmien käytön osalta välttämättömyys. Lisäksi muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvassa tiedustelussa erityisenä edellytyksenä on, että tietoja ei saada hankittua muulla tiedustelumenetelmällä.

Lisäksi tiedustelumenetelmien käytölle säädettäisiin erityisiä edellytyksiä, joista ehdotetaan säädettäväksi kunkin tiedustelumenetelmän kohdalla (Amann v. Sveitsi, Kopp v. Saksa, Kruslin v. Ranska, Huvig v. Ranska). Toimivaltuuksia koskevasta sääntelystä käy ilmi, mitä valtuuksia käytettäessä saa tehdä ja miten tällöin on meneteltävä, vaatimuksen ja päätöksen tietosisältö, mikä taho tiedustelusta päättää, tiedustelua koskevan luvan, päätöksen tai määräyksen voimassaolo, mahdolliset kuuntelu-, katselu-, jäljentämis- ja tiedustelukiellot samoin kuin tiedustelun käytöstä ilmoittaminen tai ilmoittamatta jättäminen. Säännökset oikeusturvaan liittyen ovat selkeitä.

Hyväksyttävyys ja suhteellisuus

Sotilastiedustelussa on lain mukaan kunnioitettava perus- ja ihmisoikeuksia sekä noudatettava suhteellisuusperiaatetta, vähimmän haitan periaatetta, tarkoitussidonnaisuuden periaatetta ja syrjintäkieltoa. Periaatteet ohjaavat kaikkea tiedustelutoimintaa.

Sotilastiedusteluviranomaisen on tiedustelutoimivaltuuksia käyttäessään valittava perusteltavissa olevista tiedustelumenetelmistä se, joka parhaiten edistää näiden perus- ja ihmisoikeuksien toteutumista.

Suhteellisuusperiaate edellyttää arvioimaan, onko tiedustelumenetelmän käyttö puolustettavaa suhteessa tiedustelua koskevan toimeksiannon tärkeyteen, kiireellisyyteen, tavoiteltavaan päämäärään ja muihin tilanteen kokonaisarviointiin vaikuttaviin seikkoihin. EIT ja EUT ovat ratkaisukäytännössään korostaneet suhteellisuusperiaatteen noudattamisen tärkeyttä erityisesti tietoliikennetiedustelun yhteydessä (esimerkiksi Zakharov v. Venäjä, Weber ja Saravia v. Saksa, Digital Rights Ireland). Tietoliikennetiedustelulta ja hakuehtojen määrittämiseltä edellytetään siksi viimesijaisuutta eli sitä, että tietojen hankkiminen muulla menetelmällä olisi mahdotonta tai kohtuuttoman vaikeaa, ja hakuehtojen määrittämiseltä välttämättömyyttä. Lisäksi muun kuin valtiollisen toimijan tietoliikenteen tiedustelu edellyttää, että tietoja ei ole hankittavissa muulla tavalla.

Vähimmän haitan periaatteesta johtuu, että sotilastiedusteluviranomaisen toimenpiteillä ei kenenkään oikeuksiin saa puuttua enempää eikä kenellekään saisi aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tiedustelutehtävän suorittamiseksi.

Sotilastiedusteluviranomainen saa tarkoitussidonnaisuuden periaatteen mukaisesti käyttää tiedustelutoimivaltuuksiaan vain säädettyyn tarkoitukseen.

Sotilastiedustelun toimenpiteiden kohdentaminen on toteutettava syrjimättömästi. Tästä on sotilastiedustelusta annetussa lakiin otettu nimenomainen säännös. Sotilastiedustelun toimenpiteen kohdentaminen ei saa ilman hyväksyttävää perustetta perustua henkilöiden ikään, sukupuoleen, alkuperään, kansalaisuuteen, asuinpaikkaan, kieleen, uskontoon, vakaumukseen, mielipiteeseen, poliittiseen toimintaan, ammattiyhdistystoimintaan, perhesuhteisiin, terveydentilaan, vammaisuuteen, seksuaaliseen suuntautumiseen tai muuhun henkilöön liittyvään syyhyn. Sääntely vahvistaa perustuslain 6 §:n 2 momentin yhdenvertaisuusperiaatetta tiedustelutoiminnassa.

Oikeusturvajärjestelyt

Tiedustelutoiminnassa korostuvat oikeusturvajärjestelyjen ja valvonnan tehokkuus sekä asianmukaisuus. Myös ihmisoikeusvelvoitteet ja Euroopan unionin oikeusjärjestys edellyttävät luottamuksellisen viestin salaisuuden suojaan puuttuvien toimivaltuuksien käytön valvonnalta tehokkuutta ja riippumattomuutta.

Tiedusteluviranomaisella ei voi olla rajoittamatonta harkintavaltaa tiedonhankinnan kohdentamisessa. Yksi tapa rajoittaa viranomaisen harkintavaltaa on osoittaa vakavinta puuttumista perusoikeussuojaan aiheuttavien tiedustelumenetelmien käytöstä päättäminen tuomioistuimelle (muun muassa Weber ja Saravia v. Saksa). Tiedusteluviranomaisella ei myöskään voi olla suoraa ja rajoittamatonta pääsyä tietoliikenneverkkoihin (Kennedy v. Yhdistynyt Kuningaskunta). Tätä ehkäistään tiedustelumenetelmän käytön edellytysten ja periaatteiden lisäksi sillä, että esimerkiksi telekuuntelun ja tietoliikennetiedustelun kytkennän täytäntöönpanosta huolehtii viranomaisen ulkopuolinen taho.

EIT:n mukaan lupaharkinnan alan on käytävä ilmi laista. Laissa ehdotetaan säädettäväksi lupaa koskevan hakemuksen ja päätöksen sisällöstä. Lupaharkinnan, joka perustuu hakuehtojen tai kansallista turvallisuutta vaarantavan toiminnan tai henkilöiden mahdollisen täsmällisen kuvauksen hyväksymiseen, voidaan katsoa täyttävän EIT:n vaatimukset. Luvan kestosta säädetään myös tarkkarajaisesti..

10.5 Säännösehdotukset Euroopan ihmisoikeustuomioistuimen ratkaisukäytännön kannalta

10.5.1 Tietoliikennetiedustelu

EIT on lukuisissa ratkaisuissaan todennut, että tietoliikennetiedustelu on mahdollista EIS:n 8 artiklan nojalla ja se kuuluu kansalliseen harkintavaltaan. EIT on myös todennut, että kansallisen turvallisuuden alalla kansallinen harkintavalta kansallisen turvallisuuden laajuudesta ja käytettävistä keinoista kuuluu jäsenvaltiolle.

Uusimmassa tietoliikennetiedustelu koskevassa ratkaisukäytännössään EIT on toistanut pitkäaikaista linjaansa tietoliikennetiedustelusta, mutta myös kehittänyt ratkaisukäytäntöään sallittavalle tietoliikennetiedustelulle asettamistaan edellytyksistä. Kuten aiemmin EIT:n ratkaisukäytäntöä koskevassa jaksossa 5.2.1 on tuotu ilmi, sallittavuuden edellytyksiä on nykyisin kahdeksan aiemman kuuden sijaan.

Huomattava on myös se, että EIT:n käsittelyssä olleissa ratkaisuissa tietoliikennetiedustelua ei ole jaettu eri toimivaltuuksiin, kuten Suomessa. Näin ollen saman toimivaltuuden nojalla on voitu suorittaa muun muassa tietoliikenteen teknisen kehittymisen seurantaa, määrittää uusia hakuehtoja sekä hankkia tietoja varsinaisesta uhasta. Kuvaavaa on se, että tapauksessa Centrum för Rättvisa EIT toteaa, että signaalitiedustelun tekninen kehittäminen on itsestään selvää (kohta 207). Vastaavasti hakuehtojen määrittämisestä on ruotsalaisessa signaalitiedustelua koskevassa lainsäädännössä todettu ainoastaan lain perusteluissa.

EIT ei torju ehdottomasti ns. massavalvonnan (bulk interception regime) käyttöä. EIT katsoo, että sillä torjuttavien uhkien vakavuus, uhkien takana olevien henkilöiden kyky toimia paljastumatta tietoverkoissa ja sähköisen viestinnän reitityksen ennakoimattomuus perustelevat kansallista turvallisuutta vaarantavien uhkien tunnistamiseen tähtäävän massavalvonnan käyttöönoton kuulumista kansallisen harkintamarginaalin alaan. EIT on pitänyt yleisemminkin harkintamarginaalia laajana kansallisen turvallisuuden turvaamisen keinovalikoiman valinnassa (mm. Weber ja Saravia kohta 106, Big Brother Watch kohta 274 ja Centrum för Rättvisa kohta 252). EIT painottaa kuitenkin, että sekä kohdistettujen että massavalvontajärjestelmien sääntelyn tulee vallan väärinkäytön estämiseksi täyttää ainakin edellä luetteloidut vähimmäisvaatimukset.

Nyt käsiteltävänä olevan esityksen 1. lakiehdotuksen 66 §, 67 §, 67 a §, 67 b §, 68 § ja 69 §:ää on arvioitava EIT:n uudemmassa ratkaisukäytännössä toteamien kahdeksan edellytyksen kautta. Laissa on säädettävä: 1) perusteista, joiden perusteella tiedon hankinta voidaan sallia, 2) olosuhteista, joissa tiedonhankinta voi kohdistua henkilön viestintään, 3) luvan myöntämismenettelystä, 4) tiedon valinnassa, tutkimisessa ja käytössä noudatettavista menettelyistä, 5) varotoimista, joita on noudatettava luovutettaessa materiaalia eri osapuolille, 6) toimenpiteen kestosta, tiedon säilyttämisen rajoituksista ja olosuhteista, joissa tieto on poistettava ja tuhottava, 7) menettelyistä ja yksityiskohtaisista säännöistä, joilla riippumaton viranomainen valvoo edellä mainittujen takeiden noudattamista, ja valvojan valtuudesta puuttua lainvastaiseen toimintaan sekä 8) riippumattomasta jälkikäteisestä valvonnasta ja seuraamuksista.

Esityksen 1. lakiehdotuksen edellä viitatut säännökset ovat huomattavasti yksityiskohtaisempia kuin mitä EIT on ratkaisukäytännössään edellyttänyt. Kuten esimerkiksi tapauksessa Centrum för Rättvisa EIT tuo ilmi, myös massamainen tiedustelutoiminta voi olla kansallisen harkintamarginaalin sisällä, kunhan edellytykset täyttyvät. Nyt käsiteltävänä olevassa esityksessä toimivaltuuksista olisi säädetty yksityiskohtaisesti käyttötarkoitusperusteisesti. Lisäksi jokaisen toimivaltuuden käyttöä on rajattu tiettyyn Suomen rajan ylittävän

viestintäverkon osan lisäksi kohdentuvaksi tietoihin, joita kyseistä toimivaltuutta käyttämällä on tarkoitus hankkia, viime kädessä varsinaisessa tietoliikennetiedustelussa hakuehtoperusteisesti. Säännökset sisältävät myös määrällisiä rajoitteita siltä osin, kun kyse ei ole niin kutsutusta varsinaisesta tietoliikennetiedustelusta.

Yleisesti voidaan todeta, että sotilastiedustelusta annetun lain 4 §:ssä säädetään niistä kohteista, joiden perusteella tietoliikennetiedustelua voidaan käyttää ja tietoliikennetiedustelun menetelmien osalta menetelmiä koskevissa säännöksissä on kuvattu se, mihin menetelmä voi kohdistua. Erikseen tietoliikennetiedustelun kokonaisuudessa on menetelmällisesti säädetty niistä perusteista, joiden on täytyttävä, ennen kuin menetelmää voidaan käyttää tiedonhankintaan. Laissa on myös säädetty olosuhteista, joissa tiedonhankinta voi kohdistua henkilön viestintään.

Luvan kaikkiin tietoliikennetiedustelun kokonaisuudessa oleviin toimivaltuuksiin myöntää riippumaton tuomioistuin. Tuomioistuimen luvassa määritetään myös toimenpiteen kesto, joka on korkeintaan kuusi kuukautta.

Tiedon hävittämisestä säädetään yksityiskohtaisesti lain 82 §:ssä, 84 §:ssä ja tarkemmin varsinaisen tietoliikennetiedustelun osalta lain 86 §:ssä.

Toiminnan ensisijainen laillisuusvalvonta tapahtuu EIT:n vakiintuneen oikeuskäytännön mukaisesti viranomaisessa itsessään, eli sotilastiedusteluviranomaisessa. Tämän lisäksi toimintaa valvoo Puolustusvoimien asessori sekä puolustusministeriö.

Ulkopuolisesta valvonnasta säädetään tiedustelutoiminnan valvonnasta annetussa laissa. Lain mukaisesti tiedusteluvalvontavaltuutettu valvoo sotilastiedustelua etukäteisesti, reaaliaikaisesti ja jälkikäteisesti. Lisäksi tiedusteluvalvontavaltuutettu voi keskeyttää tiedustelumenetelmän käytön, jos katsoo valvottavan menetelleen lainvastaisesti. Tiedusteluvalvontavaltuutettu voi myös määrätä tiedot välittömästi hävitettäväksi ja ilmoittaa havaitsemansa lainvastaisen menettelyn esitutkintaan.

Lisäksi valvontaa suorittaa eduskunnan oikeusasiamies ja parlamentaarista valvontaa eduskunnan tiedusteluvalvontavaliokunta.

10.5.2 Teknisten tietojen käsittely ja hakuehtojen määrittäminen

EIT katsoi tapauksessa Centrum för Rättvisa, että Ruotsin laissa säädetty mahdollisuus kerätä tietoliikennettä signaalitiedustelun kehittämiseksi on kansallisen harkintamarginaalin rajoissa (päätöksen kohdat 291–293). EIT:n ratkaisukäytännössä tietoliikennetiedustelun kaltaista järjestelmää ei ole jaoteltu erilaisiin käyttötarkoituksiin, vaan järjestelmät kattavat kokonaisuudessaan sen, mitä nyt esitetyssä 1. lakiehdotuksessa olisi säädetty 66 §:ssä, 67 a §:ssä, 68 §:ssä ja 70 §:ssä. Lisäksi tapauksissa ei ole otettu kantaa siihen, pitäisikö toiminnan olla hetkellistä tai muuta vastaavaa.

Nyt käsiteltävän olevan esityksen 1. lakiehdotuksen 66 §:ää ehdotetaan muutettavaksi niin, että siitä poistetaan hetkellisyys. Lisäksi teknisten tietojen käsittelyn toimivaltuutta voitaisiin käyttää voimassa olevassa laissa määritellyn viestintäverkon osan tunnistamisen lisäksi tietoliikenteen reitittymisen ja muutosten tunnistamiseen. Toimivaltuuden käyttö kohdistuu ainoastaan tietoliikenteen teknisiin tietoihin.

Esityksen 1. lakiehdotuksen 66 §:ssä olisi säädetty niistä perusteista, jolloin tiedonhankinta voidaan sallia. Perusteita olisivat 1) tilastollinen analyysi tietoliikennetiedustelun

kohdentamiseksi viestintäverkon osaan ja 2) tietoliikenteen reitittymisen ja muutosten seuraaminen. Säännösehdotus ei kohdistuisi henkilön viestintään, koska säännös koskisi ainoastaan tietoliikenteen teknisiä tietoja.

Luvan myöntämismenettelystä säädettäisiin 1. lakiehdotuksen 67 §:ssä. Tiedon valinnassa, tutkimisessa ja käytössä noudatettavista menettelyistä säädettäisiin 1. lakiehdotuksen 66 §:ssä, jonka mukaisesti toimivaltuus koskisi tietoliikenteen teknisiä tietoja ja niitä voitaisiin käyttää säännöksessä mainittuihin tarkoituksiin. Luvan kesto olisi 67 §:ssä ehdotetun mukaisesti korkeintaan 6 kuukautta.

Tietoliikenteen teknisiä tietoja voitaisiin käyttää myös 18 kuukauden ajan niiden hankkimisesta teknisten tietojen käsittelyssä ja 12 kuukauden ajan hakuehtojen määrittämiseen (1. lakiehdotus 67 a §) sekä varisnaisessa tietoliikennetiedustelussa (1. lakiehdotuksen 68 ja 70 §). Muilta osin tiedot olisi hävitettävä laissa säädettyjen menettelyjen mukaisesti.

EIT ei ole ottanut suoranaisesti kantaa tietoliikennetiedustelussa hakuehtojen määrittämiseen. Centrum för Rättvisa -tapauksessa EIT toteaa, että Ruotsin laissa säädetty mahdollisuus kerätä tietoliikennettä signaalitiedustelun kehittämiseksi on kansallisen harkintamarginaalin rajoissa (päätöksen kohdat 291–293). EIT ei nähnyt estettä, että tietoliikennettä saatiin kerätä myös kehittämistarkoituksiin.

EIT ratkaisukäytännöstä ei ole havaittavissa tapauksia, joissa tietoliikennetiedustelun kaltaista järjestelmää olisi jaoteltu vastaavalla, yhtä yksityiskohtaisella tavalla kuin nykytilassa on Suomessa ja nyt esitettävien ehdotusten myötä. Näin ollen suomalaista järjestelmää voidaan pitää tarkkuudeltaan ja tarkkarajaisuudeltaan poikkeuksellisena. Lisäksi EIS:n kannalta merkittävää on myös se, että jokaisesta tietoliikennetiedustelun kokonaisuudessa olevasta toimivaltuudesta päätöksen tekee tuomioistuin.

Näin ollen voidaan katsoa, että 1. lakiehdotuksen 66 § ja 67 a § ovat EIS:n kannalta ongelmattomia.

10.5.3 Viestinnän sisältöön menevät hakuehdot

Esityksen 1. lakiehdotuksen 68 ja 70 §:ään esitettyjen muutosten myötä säännöksistä poistettaisiin kielto käyttää Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.

EIT on ratkaisukäytännössään korostanut sitä, että tiedonhankinnan on kohdistuttava valtion rajan ylittävään tietoliikenteeseen (esim. Centrum för Rättvisa kohta 236 ja siinä viitatut tapaukset Weber ja Saravia sekä Liberty ja muut). Tätä voidaan toteuttaa muun muassa kohdistamalla tiedonhankinta tiettyihin valtion rajan ylittäviin pisteisiin ja suodattamalla joukosta valtion sisäinen tietoliikenne. Kotimaisen tietoliikenteen poistaminen on voitu toteuttaa myös jälkikäteisesti tämän tultua ilmi, vaikkei sitä voidakaan pitää optimaalisena.

EIT ei ole ottanut kantaa siihen, voiko toinen viestinnän osapuoli olla tiedustelumenetelmää käyttävän viranomaisen kotimaassa. EIT käsittelemissä tapauksissa on korostunut se, että kyse on oltava rajat ylittävästä uhkasta ja että valtion sisäiseen tietoliikenteeseen ei ole syytä kohdistaa näin pitkälle menevää tiedonhankintaa.

Kuten on jo tuotu esiin, EIT on pitänyt tietoliikennetiedustelunkaltaisia järjestelmiä arvioidessaan keskeisenä edellytyksenä sitä, että se perustuu hakuehtojen käyttöön. EIT on myös hyväksynyt sen, että tietoliikennettä käytetään järjestelmän kehittämiseen ja

suuntaamiseen. EIT ei siis tee eroa sen suhteen, kohdistuvatko hakuehdot viestinnän välitystietoihin vai viestin semanttiseen sisältöön; huomiota ei ole kiinnitetty siihen, mihin tietoihin ja mihin osaan tietoliikennevirtaa hakuehto kohdistuu.

Yleisesti EIT:n ratkaisukäytännössä on korostunut se, että ulkopuolisen tuomioistuimen tai sitä vastaavan on hyväksyttävä käytettävät hakuehdot ennen kuin tiedustelumenetelmän käyttö aloitetaan.

Esityksen 1. lakiehdotuksen 68 ja 70 §:n ei voida katsoa olevan ristiriidassa EIS:n kanssa.

10.5.4 Muuhun kuin valtiolliseen toimijaan kohdistuvasta tietoliikennetiedustelusta ilmoittamisesta luopuminen

EIT on lukuisissa ratkaisuissaan, viimeisimpänä Centrum för Rättvisa ja Big Brother Watch, ottanut kantaa, että EIS:n 8 artiklan ja 13 artiklan kannalta keskeistä on se, onko tiedustelumenetelmien kohteeksi joutuneella mahdollisuus saada tieto kohteeksi joutumisesta. Se, miten kohteeksi joutunut tai sellaista epäilevä saa riittävän tiedon asiasta, voidaan toteuttaa joko ilmoittamalla tai ulkopuolisen riippumattoman toimielimen toimesta. Centrum för Rättvisa ja Big Brother Watch -tapauksissa EIT toteaa, että henkilö voi saada parempaa suojaa viranomaisten toimintaa vastaan toimielimeltä, jolle kuka tahansa itsensä tiedustelumenetelmän käytön kohteeksi epäilevä voi saattaa asiansa tutkittavaksi. Tällöin korostuu toimielimen itsenäisyys tiedusteluviranomaisen toiminnasta sekä riittävät toimivaltuudet tosiasiallisesti puuttua viranomaisen toimintaan.

Järjestelmissä, joissa oikeussuoja perustuu ilmoittamiseen, voi käytännössä käydä niin, että erilaisten poikkeusjärjestelyiden takia kohteeksi joutunut henkilö ei voi kuitenkaan käytännössä koskaan saada tietoa tiedustelumenetelmän kohteeksi joutumisesta.

Nyt käsiteltävänä olevassa hallituksen esityksessä ehdotetaan, että tietoliikennetiedustelusta ei ilmoitettaisi sen kohteeksi joutuneelle. Nykytilassa valtiolliselle toimijalle ei ilmoiteta missään tilanteessa. EIS:n kannalta ratkaisu noudattelisi yleiseurooppalaista linjaa; käytännössä missään maassa tietoliikennetiedustelusta ei ilmoiteta, tosin Ruotsissa on käynnissä lainmuutosprosessi tämän osalta.

EIS:n järjestelmässä ilmoittamisvelvollisuus voidaan korvata muilla järjestelyillä, jotka takaavat vastaavat lopputuloksen kohteeksi joutuneelle tai joka epäilee joutuneensa tiedustelumenetelmän käytön kohteeksi. EIT:n käytännössä todetusti tätä kautta kohteeksi joutunut saa usein asiansa käsiteltyä paremmin kuin ilmoituksen perusteella. Suomalaisessa tiedustelulainsäädännön kokonaisuudessa järjestely tarkoittaisi tiedusteluvalvontavaltuutettua. Lisäksi kokonaisuudessa on huomioitava, että syvimmin perusoikeuksiin puuttuvista tiedustelumenetelmien käytöstä päätöksen tekee rippumaton tuomioistuin.

Tapauksessa Centrum för Rättvisa on otettu kantaa siihen, voidaanko ruotsalaisen signaalitiedustelun valvovaa viranomaista pitää tehokkaana oikeusturvakeinona. Tapauksessa todetaan, että valvovan viranomaisen on oltava tiedustelutoiminnasta riippumaton, valvojan on pystyttävä antamaan oikeudellisesti sitovia päätöksiä tiedusteluviranomaiseen nähden ja valvottava toimintaa etukäteisesti, reaaliaikaisesti ja jälkikäteisesti.

Suomessa vastaava rooli on tiedusteluvalvontavaltuutetulla. Valtuutetun laillisuusvalvonta tarkoittaa tiedustelutoiminnan laillisuusvalvontaa kokonaisvaltaisesti etukäteisesti (osallistumisoikeus mm. tuomioistuin käsittelyyn), reaaliaikaisesti ja jälkikäteisesti. Valtuutettu voi määrätä tiedustelumenetelmän käytön keskeytettäväksi tai lopetettavaksi, ja

tiedusteluviranomaista koskevan lainsäädännön mukaisesti tiedustelumenetelmän käytöllä saadut tallenteet ja muistiinpanot on hävitettävä. Tiedustelumenetelmän käytön keskeyttämistä tai lopettamista koskeva päätös on saatettava tuomioistuimen käsiteltäväksi. Tiedusteluvalvontavaltuutetun päätökset ovat oikeudellisesti sitovia.

Tiedusteluvalvontavaltuutettu voi antaa myös huomautuksen ja muun muassa saattaa valvottavan tietoon käsityksen lainmukaisesta menettelystä. Näiltä osin voidaan todeta, että sotilastiedusteluviranomainen on noudattanut ja saattanut osaksi toimintaansa valtuutetun antamat oikeudellisesti sitomattomat huomiot.

Valtuutetulle myös kuka tahansa voi tehdä tutkimispyynnön tai valituksen.

Valtuutettu on tehnyt pelkästään vuonna 2024 tiedusteluviranomaisiin 153 (vrt Centrum för Rättvisa kohta 351) valvontakäyntiä ja tämän lisäksi sellaisia valvontakäyntejä, jotka koskivat tiedustelumenetelmien käytöstä laadittuja pöytäkirjoja, sekä perehtymiskäyntejä, jotka koskivat yleisemmin Suojelupoliisin ja sotilastiedusteluviranomaisten toimintaa (tiedusteluvalvontavaltuutetun kertomus vuodelta 2024).

Näin ollen voidaan katsoa, että tiedusteluvalvontavaltuutettu täyttää EIS:n vaatimukset tehokkaasta oikeusturvan takeesta myös tilanteessa, jossa kohteeksi joutuneelle ei tehtäisi ilmoitusta.

10.6 Säännösehdotukset Euroopan unionin tuomioistuimen ratkaisukäytännön kannalta

Kuten aiemmin on todettu jaksossa 5.2.2, Euroopan unionilla ja sen tuomioistuimella ei ole sinänsä toimivaltaa ratkaista jäsenvaltioiden maanpuolustuksen ja kansallisen turvallisuuteen liittyviä kysymyksiä. Toimivaltaa voi kuitenkin olla välillisesti, kuten tilanteessa, jossa palveluntarjoajat velvoitetaan tallentamaan ja siirtämään asiakkaistaan yksityisyyden suojan alaan kuuluvia tietoja maanpuolustuksen tai kansallisen turvallisuuden suojaamisen tarpeisiin.

Euroopan unionin tuomioistuin on muun muassa ratkaisussaan La Quadrature du Net ym. v. Premier ministre ym. (yhdistetyt asiat C-511/18, C-512/18 ja C-520/18) katsonut (kohta 103), että kun jäsenvaltiot panevat suoraan täytäntöön sähköisen viestinnän luottamuksellisuudesta poikkeavia toimenpiteitä asettamalla tällaisen viestinnän palveluntarjoajille käsittelyä koskevia velvollisuuksia, asianomaisten henkilöiden tietosuojaan ei sovelleta sähköisen viestinnän tietosuojadirektiiviä. Ehdotetussa sääntelyssä ei asetettaisi viestinnän palveluntarjoajille velvollisuuksia, joten sääntelyä ei ole tarpeen arvioida tarkemmin mainitun direktiivin näkökulmasta.

Kuitenkin voidaan todeta, että nyt käsiteltävät säännösehdotukset ovat yhteensopivia Euroopan unionin perusoikeuskirjan ja siihen liittyvän Euroopan unionin tuomioistuimen oikeuskäytännön kanssa, erityisesti viestintäsalaisuusdirektiivin (2002/58/EY) ja siihen liittyvän La Quadrature du Net -ratkaisun valossa.

Unionin tuomioistuimen aiheeseen liittyvät ratkaisut (mm. Digital Rights Ireland (C-293/12 ja C-594/12), Schrems (C-362/14) ja Tele2 Sverige ja Watson (C-698/15 ja C-203/15)) koskevat teleyritysten yleistä ja erittelemätöntä tunnistamistietojen keräämistä ja säilyttämistä viranomaistarkoituksiin. Nyt käsiteltävänä olevassa esityksessä kyse on viranomaisen itsensä keräämistä ja säilyttämistä tiedoista, joiden hankkimista ja tallentamista rajataan fyysisesti, teknisesti, määrällisesti ja ajallisesti. Perusperiaatteiden lisäksi näin ollen Euroopan unionin tuomioistuimen ratkaisuilla ei ole vaikutusta nyt esitettyjen lakiehdotusten kannalta.

10.7 Yhteenveto

Ehdotettu sääntely sisältää täsmälliset säännökset. Perusoikeuksien rajoituksen olennainen sisältö ilmenee suoraan laista. Uudet toimivaltuudet edellyttävät tuomioistuimen päätöstä. Sääntely täyttää siten lailla säätämisen ja tarkkarajaisuuden vaatimukset. Suhteellisuusvaatimuksen kannalta olennaista on, että ehdotetun toimivaltuussääntelyn kohteena on sotilastiedustelusta annetun lain 4 §:ssä mainittu toiminta. Lisäksi sotilastiedusteluviranomaisen toimivallasta on jo aiemmin säädetty tarkkarajaisesti. Sääntelyn oikeasuhtaisuutta on arvioitava voimassa olevaa lainsäädäntöä vasten, etenkin sotilastiedustelusta annettua laki, henkilötietojen käsittelystä Puolustusvoimissa annettua lakia ja tiedustelutoiminnan valvonnasta annettua lakia vasten.

Tässä esityksessä ehdotettavan lainsäädännön arvioidaan täyttävän EIT:n ratkaisukäytännön ja perustuslakivaliokunnan tulkintakäytännön asettamat vaatimukset perus- ja ihmisoikeuksien huomioon ottamisesta.

Esitykseen sisältyvät lakiehdotukset voidaan hallituksen käsityksen mukaan käsitellä tavallisen lain säätämisjärjestyksessä.

Esitykseen liittyvät lakiehdotukset sisältävät uudentyyppistä sääntelyä. Perustuslain kannalta keskeisiksi voidaan katsoa esityksen 1. lakiehdotuksen 33, 42, 61 a, 61 b, 62, 63, 66, 67 a, 67 b, 78 a ja 89 a §:t. Lisäksi keskeisenä voidaan pitää 1. lakiehdotuksen 18 a §:n kokonaisuutta (mukaan lukien 7. ja 8. lakiehdotus).

Tämän ja muiden valtiosääntöoikeudellisten näkökohtien vuoksi hallitus pitää tarkoituksenmukaisena, että eduskunta pyytää esityksestä perustuslakivaliokunnan lausunnon.

Ponsi

Edellä esitetyn perusteella annetaan eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

1.

Laki

sotilastiedustelusta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan sotilastiedustelusta annetun lain (590/2019) 43 §:n 3 momentti, 74 § ja 78 §:n 5 momentti,

muutetaan 11 §:n 2 momentti, 15 §:n 1 momentti, 18 §, 20 §:n 3 momentti, 33 §:n 2 ja 3 momentti, 36 §:n 1 momentti, 42 ja 44 §, 45 §:n 1 ja 4 momentti, 51 §:n 3 momentti, 53 §:n 1 momentti, 55 §:n 3 momentti, 62 §:n 2 ja 3 momentti, 64 ja 66–68 §, 69 §:n otsikko ja 2 momentti, 70 §, 71 §:n 2 momentti, 77 §:n 1 momentti, 82 §:n 1 ja 2 momentti, 85, 86, 89, 91, 93 ja 94 §, 9 luvun otsikko, 96 §, 97 §:n 2 momentti, 99 ja 101 §, 104 §:n 2 momentti sekä 111 §:n 1 momentti, sellaisena kuin niistä on 20 §:n 3 momentti laissa 333/2025, sekä

lisätään lakiin uusi 18 a §, 33 §:ään uusi 4 momentti, 36 §:ään uusi 4 momentti, lakiin uusi 46 a ja 46 b §, 51 §:ään uusi 4 momentti, jolloin nykyinen 4 ja 5 momentti siirtyvät 5 ja 6 momentiksi, lakiin uusi 55 a, 56 a, 61 a ja 61 b §, 62 §:ään uusi 4 momentti, 63 §:ään uusi 3 momentti, jolloin nykyinen 3 momentti siirtyy 4 momentiksi, lakiin uusi 67 a, 67 b, 78 a, 89 a ja 89 b § sekä 104 §:ään uusi 3 momentti seuraavasti:

11 §

Sotilastiedusteluviranomaiset

.— —

Maa-, Meri- ja Ilmavoimat voivat käyttää tiedustelutehtävän suorittamiseksi tietolähdetoimintaa sekä radiosignaalitiedustelua. Maa-, Meri- ja Ilmavoimat ovat sotilastiedustelutoiminnassa sotilastiedusteluviranomaisen alaisia.

— —

15 §

Tiedustelutoiminnan yhteensovittaminen

Sotilas- ja siviilitiedustelutoimintaa sovitetaan yhteen tasavallan presidentin kanslian, valtioneuvoston kanslian, ulkoministeriön, puolustusministeriön ja sisäministeriön kesken sekä tarvittaessa muiden ministeriöiden ja viranomaisten kesken.

— —

18 §

Yhteistyö muiden viranomaisten sekä yritysten ja muiden yhteisöjen kanssa

Sotilastiedusteluviranomaisen on tarpeen mukaan toimittava yhteistyössä muiden viranomaisten kanssa sotilastiedustelun tarkoituksenmukaiseksi hoitamiseksi. Sotilastiedusteluviranomainen voi tehtävänsä toteuttamiseksi luovuttaa muille viranomaisille salassapitosäännösten estämättä muita kuin henkilötietoja, jos tietojen luovuttaminen on tarpeen maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi.

Sotilastiedusteluviranomainen voi salassapitosäännösten estämättä tehtävänsä toteuttamiseksi luovuttaa yrityksille ja muille yhteisöille haittaohjelmaan liittyvän tunnistamistiedon tai luovuttaa muun tiedon kuin henkilötiedon, jos tietojen luovuttaminen on tarpeen maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi.

Tietojen luovuttamisesta rikostorjuntaan säädetään 6 luvussa.

Sotilastiedusteluviranomaisen ja muiden viranomaisten välisen yhteistyön järjestämisestä sekä yhteistyöhön osallistuvista tahoista ja niiden tehtävistä voidaan antaa tarkempia säännöksiä valtioneuvoston asetuksella.

18 a §

Yhteistoiminta Rajavartiolaitoksen kanssa

Sen lisäksi, mitä 18 §:ssä säädetään, Rajavartiolaitos voi sotilastiedusteluviranomaisen päätöksellä ja tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen pyynnöstä suorittaa 22, 26, 28, 30, 32, 41, 42, 54 ja 56 §:ssä säädetyn tiedustelumenetelmän käyttöön liittyvän yksittäisen toimenpiteen, jos se on välttämätöntä tiedustelutehtävän suorittamiseksi. Rajavartiolaitoksessa pyynnön kohteena olevan toimenpiteen suorittamisesta päättää pidättämiseen oikeutettu virkamies. Rajavartiolaitoksen on sotilastiedusteluviranomaisen pyynnöstä ilman aiheetonta viivytystä keskeytettävä tässä momentissa tarkoitettu toimenpide.

Jos sotilastiedusteluviranomaisella ei ole toimivaltuutta tiedustelutehtävän hoitamiseksi tarpeellisen toimenpiteen suorittamiseen, Rajavartiolaitos voi tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen pyynnöstä suorittaa Rajavartiolaitokselle säädetyn tehtävän yhteydessä rajavartiolain (578/2005) 28 §:ssä tarkoitettuja toimenpiteitä, jotka ovat välttämättömiä sotilastiedustelutehtävän kannalta. Toimenpiteen kohteena oleva henkilö on velvollinen olemaan läsnä toimenpiteitä suoritettaessa enintään 12 tuntia kerrallaan. Rajavartiolaitoksessa toimenpiteen suorittamisesta päättää rajanylityspaikan esimies tai vähintään luutnantin arvoinen rajavartiomies.

Rajavartiolaitoksella on rajanylityspaikan esimiehenä toimivan rajavartiomiehen tai vähintään luutnantin arvoisen rajavartiomiehen päätöksellä oikeus käyttää vääriä, harhauttavia tai peiteltyjä tietoja silloin kun se on välttämätöntä tässä pykälässä tarkoitetun toimenpiteen paljastumisen estämiseksi.

Rajavartiolaitoksen on luovutettava tässä pykälässä tarkoitetulla toimenpiteellä saadut tallenteet ja asiakirjat käsittelemättöminä sotilastiedusteluviranomaiselle sekä hävitettävä toimenpiteen suorittamisessa syntyneet tallenteet ja asiakirjat, jollei tietojen käsittely ole tarpeen Rajavartiolaitokselle säädettyjen muiden tehtävien suorittamiseksi. Tallenteiden ja asiakirjojen tarkastamisesta sekä muista tiedonkäsittelyyn liittyvistä tehtävistä vastaa sotilastiedusteluviranomainen.

20 §

Kansainvälinen yhteistyö

— —

Ulkomaisella toimivaltaisella virkamiehellä on pääesikunnan tiedustelupäällikön päätöksellä oikeus Suomen alueella sotilastiedusteluviranomaisen tehtävien hoitamiseksi toimia

yhteistoiminnassa sotilastiedusteluviranomaisen virkamiehen kanssa ja tämän ohjauksessa ja valvonnassa oikeus osallistua Suomen alueella tiedustelumenetelmän käyttöön. Ulkomainen virkamies on velvollinen noudattamaan sotilastiedusteluviranomaisen hänelle antamia määräyksiä, rajoituksia ja ohjeita.

— —

33 §

Teknisestä laitetarkkailusta päättäminen

— —

Lupa voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan. Silloin, kun toimenpiteen kohteena on henkilö, lupa voidaan antaa enintään kolmeksi kuukaudeksi kerrallaan.

Teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) toimenpiteen perusteena oleva tiedustelutehtävä;

2) toimenpiteen kohteena oleva tekninen laite tai ohjelmisto taikka teknistä laitetta tai ohjelmistoa käyttävä henkilö;

3) tosiseikat, joihin teknisen laitetarkkailun edellytykset ja kohdistaminen perustuvat;

4) luvan voimassaoloaika kellonajan tarkkuudella;

5) teknistä laitetarkkailua johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;

6) mahdolliset teknisen laitetarkkailun rajoitukset ja ehdot.

Tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää toimenpiteen kohteena olevista teknisistä laitteista tai ohjelmistoista, jos toimenpiteen kohteena on henkilö. Päätöksessä on mainittava perustelut toimenpiteen kohteena olevien laitteiden tai ohjelmistojen valitsemiselle.

36 §

Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättäminen

Tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta. Jos telekuuntelua tai tietojen hankkimisesta telekuuntelun sijasta koskeva asia ei siedä viivytystä, tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää televalvonnasta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta.

— —

Tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää toimenpiteen kohteena olevista teleosoitteista tai telepäätelaitteista, jos toimenpiteen kohteena on henkilö. Päätöksessä on mainittava perustelut toimenpiteen kohteena olevien teleosoitteiden tai telepäätelaitteiden valitsemiselle.

42 §

Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen

Sotilastiedusteluviranomaisen palveluksessa olevalla virkamiehellä on oikeus sijoittaa telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tekniseen kuunteluun, tekniseen katseluun, tekniseen seurantaan tai tekniseen laitetarkkailuun,

valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedusteluun tai ulkomaan tietojärjestelmätiedusteluun käytettävä laite, menetelmä tai ohjelmisto esineeseen, aineeseen, omaisuuteen, tilaan tai muuhun paikkaan taikka tietojärjestelmään, jos mainitun tiedustelumenetelmän käyttö sitä edellyttää. Sotilastiedusteluviranomaisen 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. Laitteen, menetelmän tai ohjelmiston asentaminen tai sen poisottaminen ei saa tapahtua pysyväisluonteiseen asumiseen käytettävässä tilassa.

Sotilastiedusteluviranomaisen pyynnöstä viranomaisen ulkopuolisella henkilöllä on oikeus tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa toteuttaa tiedustelumenetelmän käytön edellyttämä 1 momentissa tarkoitettu yksittäinen asennus- tai poistamistoimenpide, jos se on välttämätöntä tiedustelumenetelmän käyttämiseksi.

Sotilastiedusteluviranomaisella on oikeus menetelmän tai ohjelmiston asentamiseksi tai poisottamiseksi ja tiedonsiirtämiseksi tietoteknisin menetelmin tilapäisesti käyttää yksityisen tai yhteisön laitetta tai tietojärjestelmän osaa, jos se on välttämätöntä tiedustelumenetelmän käyttämiseksi. Sotilastiedusteluviranomainen ei saa aiheuttaa vähäistä suurempaa haittaa tai vahinkoa käytettävälle laitteelle tai tietojärjestelmälle. Sotilastiedusteluviranomainen on velvollinen korvaamaan aiheuttamansa vähäistä suuremman haitan tai vahingon.

44 §

Peitetoimintaa koskeva suunnitelma

Peitetoiminnan toteuttamisesta on laadittava kirjallinen suunnitelma, jonka tulee sisältää peitetoimintaa koskevan päätöksenteon ja peitetoiminnan toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava.

45 §

Peitetoiminnasta päättäminen

Pääesikunnan tiedustelupäällikkö päättää peitetoiminnasta.

— —

Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava.

46 a §

Yksinomaan tietoverkossa toteutettava peitetoiminta

Yksinomaan tietoverkossa toteutettavalla peitetoiminnalla tarkoitetaan 4 §:ssä tarkoitettuun toimintaan kohdistuvaa tietoverkossa tapahtuvaa suunnitelmallista tiedonhankintaa käyttämällä soluttautumista, jossa tiedonhankinnan edellyttämän luottamuksen hankkimiseksi tai tiedonhankinnan paljastumisen estämiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka valmistetaan tai käytetään vääriä asiakirjoja.

Sotilastiedustelunviranomaisella on oikeus kohdistaa henkilöön tai henkilöryhmään peitetoimintaa tietoverkossa, jos sillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta on laadittava kirjallinen suunnitelma, jonka tulee sisältää päätöksenteon ja peitetoiminnan toteuttamisen kannalta

oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava.

46 b §

Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättäminen

Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättää tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

Yksinomaan tietoverkossa toteutettavaa peitetoimintaa koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Yksinomaan tietoverkossa toteutettavaa peitetoimintaa koskeva päätös on tehtävä kirjallisesti.

Päätöksessä on mainittava:

1) toimenpiteen perusteena oleva tiedustelutehtävä;

2) tiedonhankinnan kohteena oleva henkilö tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmä riittävästi yksilöitynä;

3) tosiseikat, joihin yksinomaan tietoverkossa toteutettava peitetoiminta perustuu;

4) päätöksen voimassaoloaika kellonajan tarkkuudella;

5) yksinomaan tietoverkossa toteutettavaa peitetoimintaa johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;

6) mahdolliset yksinomaan tietoverkossa toteutettavaa peitetoimintaa koskevat rajoitukset ja ehdot.

Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava.

51 §

Tietolähdetoiminta

— —

Tietolähteen ohjatussa käytössä tietoja ei saa pyytää hankittavaksi sellaisella tavalla, joka edellyttäisi viranomaiselle kuuluvien toimivaltuuksien käyttöä.

Ennen tietolähteen ohjattua käyttöä tietolähteelle on tehtävä selkoa hänen oikeuksistaan ja velvollisuuksistaan sekä erityisesti hänelle lain mukaan sallitusta ja kielletystä toiminnasta. Tietolähteen ohjatussa käytössä tietoja ei saa pyytää hankittavaksi sellaisella tavalla, joka vaarantaisi tietolähteen tai muun henkilön hengen tai terveyden. Tietolähteen turvallisuudesta on tarpeen mukaan huolehdittava tiedonhankinnan aikana ja sen jälkeen.

— —

53 §

Tietolähteen ohjatusta käytöstä päättäminen

Pääesikunnan tiedustelupäällikkö taikka tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää tietolähteen ohjatusta käytöstä.

— —

55 §

Paikkatiedustelusta päättäminen

— —

Pääesikunnan tiedustelupäällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää kulkuneuvoon kohdistuvasta paikkatiedustelusta sekä muusta kuin 1 momentissa tarkoitetusta paikkatiedustelusta.

— —

55 a §

Näytteenotto paikkatiedustelussa

Sotilastiedusteluviranomaisella on oikeus paikkatiedustelussa ottaa aineesta, omaisuudesta tai esineestä näyte, jos se on tarpeen tiedustelutehtävän suorittamiseksi.

56 a §

Aineen, omaisuuden tai esineen tilapäinen haltuunotto

Jos 55 a §:ssä tarkoitettu näytteenotto tai 56 §:ssä tarkoitettu jäljentäminen sitä välttämättä edellyttää, sotilastiedusteluviranomaisella on oikeus ottaa aine, omaisuus tai esine tilapäisesti haltuun. Aine, omaisuus tai esine on palautettava viivytyksettä haltuunoton tarkoituksen toteuduttua.

61 a §

Valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuva tiedustelu

Valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvalla tiedustelulla tarkoitetaan Suomen alueella tapahtuvaa tiedonhankintaa valtiollisen toimijan Suomessa hallinnoiman tai käyttämän tietojärjestelmän siitä osasta, joka toteuttaa tai edesauttaa tiedustelutehtävän kohteena olevaa toimintaa tai joka tallentaa tai välittää tiedustelutehtävän kohteena olevaan toimintaan liittyviä tietoja.

Valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvaa tiedustelua saa käyttää vain siinä laajuudessa kuin on välttämätöntä tiedon hankkimiseksi tiedustelutehtävän kohteena olevasta toiminnasta.

61 b §

Valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvasta tiedustelusta päättäminen

Tuomioistuin päättää valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvasta tiedustelusta tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta.

Lupa valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvaan tiedusteluun voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvaa tiedustelua koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) tiedustelutehtävä;

2) toimenpiteen kohteena oleva valtiollinen toimija ja sen käyttämä tietojärjestelmä;

3) tosiseikat, joihin valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvan tiedustelun edellytykset ja kohdistaminen perustuvat;

4) valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvaa tiedustelua koskevan luvan voimassaoloaika kellonajan tarkkuudella;

5) valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvan tiedustelun suorittamista johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;

6) mahdolliset valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvan tiedustelun rajoitukset ja ehdot.

Tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää toimenpiteen kohteena olevista teleosoitteista tai telepäätelaitteista taikka laitteista tai ohjelmistoista tiedustelumenetelmää koskevan luvan voimassaolon aikana. Päätöksessä on mainittava perustelut toimenpiteen kohteena olevien teleosoitteiden tai telepäätelaitteiden taikka laitteiden tai ohjelmistojen valitsemiselle.

62 §

Ulkomaan tietojärjestelmätiedustelu

— —

Sotilastiedusteluviranomainen saa kohdistaa tietojärjestelmään ulkomaan tietojärjestelmätiedustelua, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

Ulkomaan tietojärjestelmätiedustelun toteuttamisesta on laadittava kirjallinen suunnitelma, jonka tulee sisältää ulkomaan tietojärjestelmätiedustelua ja siihen liittyviä toimenpiteitä koskevan päätöksenteon ja toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava.

Sotilastiedusteluviranomaisella on osana ulkomaan tietojärjestelmätiedustelua oikeus tehdä tarvittavia kansainvälisen oikeuden mukaisia tietoteknisiä toimenpiteitä Suomen alueen ulkopuolella olevassa tietojärjestelmässä, jos sillä tai sen kautta voidaan aiheuttaa Suomen maanpuolustukselle tai kansalliselle turvallisuudelle vakavaa uhkaa. Toimenpiteiden on oltava välttämättömiä, suhteellisia ja väliaikaisia.

63 §

Ulkomaan tietojärjestelmätiedustelusta päättäminen

— —

Pääesikunnan tiedustelupäällikkö päättää 62 §:n 4 momentissa säädetyistä toimenpiteistä. Ennen Pääesikunnan tiedustelupäällikön päätöstä asia on käsiteltävä valmistelevasti 15 §:n 1 momentissa tarkoitettujen viranomaisten kesken sekä tarvittaessa linjattava ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteisessä kokouksessa.

— —

64 §

Ulkomailla tapahtuva sotilastiedustelu

Tämän lain 12 §:n 3 momentin, 51 §:n 3 momentin, 60 §:n 3 momentin ja 85 §:n 2 momentin säännöksiä voidaan yksittäistapauksessa jättää soveltamatta ulkomailla tapahtuvassa sotilastiedustelussa ja tiedustelumenetelmien käytössä, jos se on välttämätöntä. Lain 79, 80 ja 89 §:ää ei sovelleta ulkomailla tapahtuvassa sotilastiedustelussa ja tiedustelumenetelmien käytössä.

Ulkomailla tapahtuvasta sotilastiedustelusta ja sallituista tiedustelumenetelmistä päättää pääesikunnan tiedustelupäällikkö. Päätöksessä tarkoitetun yksittäisen tiedustelumenetelmän

käytöstä päättää tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

Sotilastiedusteluviranomaisen virkamiehen osallistuminen tässä pykälässä tarkoitettuun ulkomailla tapahtuvaan sotilastiedusteluun edellyttää asianomaisen virkamiehen suostumusta.

Tiedustelumenetelmän käyttöä koskevan päätöksen, esityksen ja suunnitelman sisällön osalta noudatetaan, mitä esityksestä, suunnitelmasta, vaatimuksesta tai päätöksestä tässä laissa säädetään.

66 §

Teknisten tietojen käsittely viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi

Puolustusvoimien tiedustelulaitos voi viestintäverkon tietoliikenteestä kerätä ja tallentaa tietoliikenteen teknisiä tietoja ja automaattisen tietojenkäsittelyn avulla käsitellä niitä:

1) tilastollista analyysia varten tietoliikennetiedustelun kohdentamiseksi viestintäverkon osaan;

2) tietoliikenteen reitittymisen ja muutosten seuraamiseksi.

Edellä 1 momentissa tarkoitetussa toiminnassa ei saa muodostaa tietoa, josta voidaan tunnistaa yksittäinen luonnollinen henkilö.

Tässä pykälässä tarkoitettuja teknisiä tietoja voidaan tallentaa enintään 18 kuukauden ajaksi. Tallennettavien teknisten tietojen määrä ei saa ylittää 5 prosenttia kohteena olevan Suomen rajan ylittävän viestintäverkon osan kapasiteetista. Tallennettuja tietoja voidaan käyttää 1 momentissa sekä jäljempänä tässä laissa säädettyihin tarkoituksiin.

Puolustusvoimien tiedustelulaitoksen on hävitettävä kerätyt ja tallennetut tietoliikenteen tekniset tiedot viimeistään 3 momentissa säädetyn tallennusajan päätyttyä.

67 §

Teknisten tietojen käsittelystä päättäminen viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi

Tuomioistuin päättää teknisten tietojen käsittelystä viestintäverkon osan tunnistamiseksi tai tietoliikenteen reitittymisen ja muutosten tunnistamiseksi tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta.

Lupa voidaan antaa ja päätös tehdä luvan antopäivästä tai päätöksen tekopäivästä alkaen enintään kuudeksi kuukaudeksi kerrallaan ja lupa tai päätös voi koskea myös 66 §:n 3 momentissa tarkoitettuja tallennettuja tietoja.

Vaatimuksessa ja päätöksessä on mainittava:

1) maantieteellinen alue tai verkkoalue, jolta tulevaan tai jolle menevään tietoliikenteeseen teknisten tietojen käsittely kohdistetaan, taikka kohde, jonka tietoliikenteen reitittymistä tai muutosta seurataan;

2) viestintäverkon osat, joista tietoa haetaan;

3) käsittelyä johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies; ja

4) suunnitelma käsittelyn toteuttamisesta.

67 a §

Tietoliikennetiedustelu hakuehtojen määrittämiseksi

Puolustusvoimien tiedustelulaitos voi kerätä ja tallentaa Suomen rajan ylittävän viestintäverkon osan tietoliikennettä tietoliikennetiedustelun tarkemmaksi kohdentamiseksi ja hakuehtojen määrittämiseksi sotilastiedustelun kohteen tietoliikenteen oletetun säännönmukaisuuden tai ominaispiirteen perusteella.

Hakuehtojen määrittämisessä tietoliikenteen käsittelyn on tapahduttava tietoliikenteen konekielisessä muodossa. Hakuehtojen määrittämisessä ei saa hyödyntää viestin merkityssisällössä olevia tietoja. Hakuehtojen määrittämisen tuloksena ei saa syntyä viestin sisältöä kuvaavaa tietoa taikka tietoa, josta voidaan tehdä henkilön yksityiselämää koskevia päätelmiä.

Kerättävän ja tallennettavan tietoliikenteen määrä ei saa ylittää 5 prosenttia kohteena olevan Suomen rajan ylittävän viestintäverkon osan kapasiteetista. Kerätty ja tallennettu tietoliikenne voidaan säilyttää enintään 12 kuukautta. Tallennettuja tietoja voidaan käyttää 1 momentissa ja jäljempänä tässä laissa säädettyihin tarkoituksiin.

Hakuehtojen määrittämisessä voidaan käyttää 66 §:n 3 momentin perusteella tallennettuja teknisiä tietoja.

Puolustusvoimien tiedustelulaitoksen on hävitettävä kerätyt ja tallennetut tietoliikenteen tekniset tiedot viimeistään 3 momentissa tarkoitetun tallennusajan päätyttyä.

67 b §

Hakuehtojen määrittämisestä päättäminen

Tuomioistuin päättää hakuehtojen määrittämisestä tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta.

Lupa voidaan antaa ja päätös tehdä luvan antopäivästä tai päätöksen tekopäivästä alkaen enintään kuudeksi kuukaudeksi kerrallaan ja lupa tai päätös voi koskea myös 66 §:n 3 momentissa ja 67 a §:n 3 momentissa tarkoitettuja tallennettuja tietoja.

Vaatimuksessa ja päätöksessä on mainittava:

1) tiedustelutehtävä, jota varten hakuehtoja määritetään ja sitä koskevat tosiseikat;

2) tosiseikat, joihin hakuehtojen määrittämisen välttämättömyys perustuu;

3) kohteen tietoliikenteen oletettu säännönmukaisuus tai ominaispiirre, jonka perusteella hakuehtoja määritetään, ja perustelut oletukselle;

4) viestintäverkon osat, joista tietoa haetaan;

5) suunnitelma hakuehtojen määrittämisestä;

6) luvan voimassaoloaika kellonajan tarkkuudella;

7) hakuehtojen määrittämistä johtava ja valvova Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;

8) mahdolliset hakuehtojen määrittämistä koskevat rajoitukset ja ehdot.

68 §

Valtiolliseen toimijaan kohdistuva tietoliikennetiedustelu

Puolustusvoimien tiedustelulaitos voi Suomen rajan ylittävästä viestintäverkon tietoliikenteestä automaattisen tietojenkäsittelyn avulla hankkia tietoa tiedustelutehtävän kannalta olennaisesta valtiollisesta toimijasta ja sen tietoliikenteestä sekä käsitellä tällaisen toimijan viestintää. Tietojen hankkiminen tietoliikenteestä perustuu valtiollista toimijaa kuvaavien hakuehtojen käyttöön.

Puolustusvoimien tiedustelulaitos voi käsitellä tietoliikenteestä hankittua tietoa automaattisesti ja manuaalisesti.

Hakuehtona voidaan tilapäisesti käyttää Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.

Tässä pykälässä tarkoitettu tiedonhankinta voi kohdistua myös 66 §:n 3 momentin ja 67 a §:n 3 momentin nojalla tallennettuihin tietoihin.

69 §

Valtiolliseen toimijaan kohdistuvasta tietoliikennetiedustelusta päättäminen

— —

Lupa voidaan antaa ja päätös tehdä luvan antopäivästä tai päätöksen tekopäivästä alkaen enintään kuudeksi kuukaudeksi kerrallaan ja lupa tai päätös voi koskea myös 66 §:n 3 momentissa ja 67 a §:n 3 momentissa tarkoitettuja tallennettuja tietoja.

— —

70 §

Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu

Puolustusvoimien tiedustelulaitos voi Suomen rajan ylittävästä viestintäverkon tietoliikenteestä automaattisen tietojenkäsittelyn avulla hankkia tietoa tiedustelutehtävän kannalta olennaisen muun kuin valtiollisen toimijan tietoliikenteestä, jos tiedot eivät ole hankittavissa muulla tiedustelumenetelmällä. Tietojen hankkiminen tietoliikenteestä perustuu hakuehtojen käyttöön.

Hakuehtona voidaan tilapäisesti käyttää Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.

Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvan tiedustelun kohdentamisessa voidaan käyttää viestin sisältöön kohdistuvia hakuehtoja. Kielellisiä ilmaisuja voidaan käyttää hakuehtona ainoastaan yhdessä teknisten tietojen kanssa.

Puolustusvoimien tiedustelulaitos voi käsitellä tietoliikenteestä hankittua tietoa automaattisesti ja manuaalisesti.

Tässä pykälässä tarkoitettu tiedonhankinta voi kohdistua myös 66 §:n 3 momentin ja 67 a §:n 3 momentin nojalla tallennettuihin tietoihin.

71 §

Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta päättäminen

— —

Lupa voidaan antaa ja päätös tehdä luvan antopäivästä tai päätöksen tekopäivästä alkaen enintään kuudeksi kuukaudeksi kerrallaan ja lupa tai päätös voi koskea myös 66 §:n 3 momentissa ja 67 a §:n 3 momentissa tarkoitettuja tallennettuja tietoja.

— —

77 §

Tiedustelumenetelmää käyttävän virkamiehen turvaaminen

Tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää, että peiteltyä tiedonhankintaa, peitetoimintaa tai valeostoa toteuttava sekä tietolähdetoimintaa valmisteleva tai toteuttava virkamies taikka tällaisessa toiminnassa käytettävä tila varustetaan kuuntelun ja katselun mahdollistavalla teknisellä laitteella, jos varustaminen on perusteltua virkamiehen turvallisuuden varmistamiseksi.

— —

78 a §

Tietolähteen hengen ja terveyden turvaaminen

Pääesikunnan tiedustelupäällikön päätöksellä sotilastiedusteluviranomainen voi antaa tietolähteelle yksittäistapauksessa käytettäväksi vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka tietolähteen käytettäväksi valmistettavia vääriä asiakirjoja, jos se on välttämätöntä tietolähteen hengen ja terveyden suojaamiseksi. Rekisterimerkintä on oikaistava sen jälkeen, kun tässä momentissa tarkoitettuja edellytyksiä ei enää ole.

Pääesikunnan tiedustelupäällikön päätöksellä sotilastiedusteluviranomainen voi järjestää tietolähteen Suomeen, jos se on välttämätöntä tietolähteen hengen ja terveyden suojaamiseksi ja menettelyä voidaan kokonaisuutena arvioiden pitää puolustettavana.

Tietolähteellä on oikeus saapua maahan 2 momentissa tarkoitetussa tilanteessa sekä käyttää maahantulon yhteydessä 1 momentissa tarkoitettuja vääriä tietoja, merkintöjä ja asiakirjoja.

82 §

Tiedustelukiellot

Telekuuntelua, telekuuntelun sijasta toimitettavaa tietojen hankkimista, teknistä kuuntelua, teknistä katselua, teknistä laitetarkkailua, radiosignaalitiedustelua, valtiolliseen toimijaan Suomessa kohdistuvaa tietojärjestelmätiedustelua tai tietoliikennetiedustelua ei saa kohdistaa sellaiseen viestintään tai tietoon, josta osapuoli ei saa todistaa tai josta hänellä on oikeus olla todistamatta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n tai 22 §:n 2 momentin nojalla.

Jos telekuuntelun, telekuuntelun sijasta tapahtuvan tietojen hankkimisen, teknisen kuuntelun, teknisen katselun, teknisen laitetarkkailun, radiosignaalitiedustelun, valtiolliseen toimijaan Suomessa kohdistuvan tietojärjestelmätiedustelun tai tietoliikennetiedustelun aikana tai muulloin ilmenee, että kyseessä on viesti, jonka kuuntelu ja katselu on kielletty, toimenpide on keskeytettävä ja sillä saadut tallenteet ja sillä saatuja tietoja koskevat muistiinpanot on hävitettävä välittömästi.

— —

85 §

Tiedustelumenetelmän käytön keskeyttäminen

Jos käy ilmi, että telekuuntelu tai televalvonta kohdistuu muuhun kuin luvan kohteena olevalta henkilöltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin taikka että teknisen kuuntelun kohteena oleva henkilö ei oleskele kuunneltavassa tilassa tai muussa paikassa, tiedustelumenetelmän käyttö on tältä osin keskeytettävä niin pian kuin mahdollista sekä tällaiset kuuntelulla saadut tallenteet ja televalvonnalla saadut tiedot sekä tällaisilla tiedustelumenetelmillä saatuja tietoja koskevat muistiinpanot on hävitettävä heti.

Velvollisuus keskeyttämiseen sekä tallenteiden ja muistiinpanojen hävittämiseen koskee radiosignaalitiedustelua, jos käy ilmi, että radiosignaalitiedustelu kohdistuu muun kuin valtiollisen toimijan viestin sisältöön.

Velvollisuus keskeyttämiseen sekä tallenteiden ja muistiinpanojen hävittämiseen koskee myös teknistä laitetarkkailua, jos käy ilmi, että tarkkailu kohdistuu sellaiseen luottamukselliseen viestiin, jota koskevasta telekuuntelusta, televalvonnasta ja muusta teknisestä tarkkailusta kuin

laitetarkkailusta säädetään 4 luvussa, taikka että toimenpiteen kohteena oleva henkilö ei käytä tarkkailun kohteena olevaa laitetta tai ohjelmistoa.

Jos käy ilmi, että valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuva tiedustelu kohdistuu sellaiseen tietojenkäsittelylaitteeseen, tiedonsiirtolaitteeseen tai tietoja käsittelevään ohjelmistoon, joka ei kuulu luvan kohteena olevaan tietojärjestelmään, on valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuva tiedustelu tältä osin keskeytettävä niin pian kuin mahdollista ja sillä saadut tallenteet ja tiedot sekä saatuja tietoja koskevat muistiinpanot on hävitettävä heti.

Jos paikkatiedustelun aikana ilmenee, että tiedustelu on kohdistunut tietoon, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20 tai 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, on tiedustelu siltä osin heti keskeytettävä ja tietoa koskevat muistiinpanot ja jäljennökset heti hävitettävä. Muu kuin tässä momentissa tarkoitettu tieto voidaan kuitenkin säilyttää ja tallettaa, jos tieto on tarpeen 79 tai 80 §:ssä tarkoitetuissa tapauksissa.

86 §

Tietoliikennetiedustelulla hankittujen tietojen hävittäminen

Sen lisäksi, mitä 82 §:n 2 momentissa säädetään, tietoliikennetiedustelulla saatu tieto on hävitettävä viipymättä sen jälkeen, jos on käynyt ilmi, että:

1) viestinnän molemmat osapuolet olivat Suomessa silloin, kun viestintä tapahtui;

2) lähettäjällä tai vastaanottajalla taikka tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta kyseisestä tiedosta 82 §:n 1 momentissa mainittujen säännösten nojalla;

3) tietoa ei tarvita maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi.

Hävittämisestä vastaa sotilastiedusteluviranomainen. Jos Puolustusvoimien tiedustelulaitos on toimittanut tiedot suojelupoliisille tietoliikennetiedustelun teknisessä toteuttamisessa suojelupoliisin puolesta, hävittämisestä vastaa suojelupoliisi.

89 §

Ilmoitusvelvollisuus

Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta ja teknisen tarkkailun käytöstä sekä viestiin kohdistuvasta jäljentämisestä ja viestiin kohdistuvasta lähetyksen jäljentämisestä on viipymättä ilmoitettava tiedonhankinnan kohteena olleelle henkilölle sen jälkeen, kun tiedustelumenetelmän käytön tarkoitus on saavutettu.

Suunnitelmallisesta tarkkailusta, peitellystä tiedonhankinnasta, peitetoiminnasta, valeostosta, tietolähteen ohjatusta käytöstä, paikkatiedustelusta, muuhun kuin viestiin kohdistuvasta jäljentämisestä ja muuhun kuin viestiin kohdistuvasta lähetyksen jäljentämisestä ei ole velvollisuutta ilmoittaa tiedonhankinnan kohteelle, jos asiassa ei ole aloitettu esitutkintaa 79 tai 80 §:ssä tarkoitetun ilmoituksen perusteella. Jos esitutkinta aloitetaan, noudatetaan, mitä pakkokeinolain (806/2011) 10 luvun 60 §:n 2–7 momentissa säädetään.

Silloin, kun käsitellään pakkokeinolain 10 luvun 60 §:n 3 momentissa tarkoitettua tiedustelumenetelmän käyttöä koskevan ilmoituksen lykkäämistä tai ilmoituksen tekemättä jättämistä, vaatimuksen tekee tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

Tiedustelumenetelmän käytöstä ei ole velvollisuutta ilmoittaa tiedustelumenetelmän käytön kohteelle, jos kohteena on ollut valtiollinen toimija.

89 a §

Muun kuin valtiollisen toimijan tietoliikennetiedustelusta ilmoittaminen

Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta ei ilmoiteta tiedustelumenetelmän käytön kohteeksi joutuneelle.

Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta on ilmoitettava osapuolelle, jolla on velvollisuus tai oikeus olla todistamatta tiedosta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n taikka 22 §:n 2 momentin nojalla, jos tieto, josta on oikeus tai velvollisuus olla todistamatta, on selvitetty tietoliikennetiedustelussa. Velvollisuutta ilmoittaa ei kuitenkaan ole, jos tietoliikennetiedustelulla saatu tieto on hävitetty 85 tai 86 §:n perusteella.

89 b §

Ilmoituksen tekeminen, lykkääminen ja tekemättä jättäminen

Ilmoitus 89 §:ssä tai 89 a §:n 2 momentissa tarkoitetulle henkilölle on tehtävä viipymättä kirjallisesti sen jälkeen, kun edellä tarkoitetun tiedustelumenetelmän käytön tarkoitus on saavutettu. Tiedustelumenetelmän käytöstä on kuitenkin ilmoitettava mainituissa lainkohdissa tarkoitetulle henkilölle viimeistään vuoden kuluttua tiedustelumenetelmän käytön lopettamisesta.

Jos tiedonhankinnan kohteena olevan henkilöllisyys tai Suomessa oleva asuinpaikka ei ole tiedossa tässä pykälässä tarkoitetun määräajan tai lykkäyksen päättyessä, tiedustelumenetelmän käytöstä on ilmoitettava kirjallisesti hänelle ilman aiheetonta viivytystä henkilöllisyyden ja Suomessa olevan asuinpaikan selvittyä.

Tiedonhankinnan kohteelle ilmoittamisesta on samalla annettava kirjallisesti tieto luvan myöntäneelle tuomioistuimelle.

Tuomioistuin voi pääesikunnan tiedustelupäällikön tai tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta päättää, että 89 §:n 1 momentissa ja 89 a §:n 2 momentissa tarkoitettua ilmoitusta tiedonhankinnan kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedustelumenetelmän käytön turvaamiseksi, maanpuolustuksen kannalta tai kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi.

Ilmoitus saadaan tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi taikka hengen tai terveyden suojaamiseksi.

Ilmoitusta koskevan asian käsittelyssä tuomioistuimessa noudatetaan, mitä 116 §:ssä säädetään.

91 §

Muussa kuin virkasuhteessa olevan toimivaltuudet

Asevelvollisuuslain (1438/2007) mukaisessa palveluksessa tai vapaaehtoisesta maanpuolustuksesta annetun lain (556/2007) 18 ja 19 §:ssä tarkoitetussa vapaaehtoisessa harjoituksessa oleva riittävän koulutuksen saanut henkilö saa tiedustelutehtävän suorittamiseksi tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa käyttää 4 luvussa tarkoitettuja tiedustelumenetelmiä lukuun ottamatta ohjattua tietolähdetoimintaa, peitetoimintaa ja valeostoa.

Edellä 1 momentissa tarkoitetussa palveluksessa tai harjoituksessa oleva sotilastiedusteluviranomaisen palveluksesta eronnut tiedustelumenetelmien käyttöön erityisesti perehtynyt henkilö saa käyttää tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa 4 luvussa tarkoitettuja tiedustelumenetelmiä.

93 §

Muussa kuin virkasuhteessa olevan virkavastuu

Henkilöön sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä hänen suorittaessaan tässä laissa tarkoitettuja tehtäviä.

94 §

Muussa kuin virkasuhteessa olevan vahingonkorvausvastuu

Tämän lain mukaista tehtävää suorittavan henkilön aiheuttamasta vahingosta vastaa valtio sen mukaan kuin vahingonkorvauslaissa (412/1974) säädetään.

Vapaaehtoisesta maanpuolustuksesta annetun lain 18 ja 19 §:ssä tarkoitettuun vapaaehtoiseen harjoitukseen osallistuvan korvausvastuuseen hänen suorittaessaan tämän lain mukaista tehtävää sovelletaan vahingonkorvauslain 4 luvun säännöksiä asevelvollisen korvausvastuusta.

9 luku

Ilmaisukielto, viestinnän välittäjää, datakeskuspalvelun tarjoajaa ja tiedonsiirtäjää koskevat velvollisuudet ja oikeudet sekä tietojen käyttö ja saanti

96 §

Viestinnän välittäjän ja datakeskuspalvelun tarjoajan avustamisvelvollisuus

Viestinnän välittäjän ja kyberturvallisuuslain (124/2025) 2 §:n 2 kohdassa tarkoitetun datakeskuspalvelun tarjoajan on ilman aiheetonta viivytystä tehtävä viestintäverkkoon tai datakeskuspalveluun telekuuntelun, televalvonnan ja valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvan tiedustelun edellyttämät kytkennät sekä annettava sotilastiedusteluviranomaisen käyttöön telekuuntelun toimeenpanoa varten tarpeelliset tiedot, välineet ja henkilöstö. Sama koskee myös niitä tilanteita, joissa sotilastiedusteluviranomainen toteuttaa telekuuntelua, televalvontaa taikka viestintäverkkoon tai datakeskuspalveluun kohdistuvaa valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvaa tiedustelua teknisellä laitteella. Viestinnän välittäjän ja datakeskuspalvelun tarjoajan on lisäksi annettava tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen käyttöön hallussaan olevat teknisen seurannan toimeenpanoa varten tarpeelliset tiedot.

Sotilastiedusteluviranomaisella sekä toimenpiteen suorittajalla ja avustavalla henkilöstöllä on oikeus telekuuntelua ja viestintäverkkoon kohdistuvaa valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvaa tiedustelua varten tarpeellisen yhteyden kytkemiseksi päästä myös muihin kuin viestinnän välittäjän tai datakeskuspalvelun tarjoajan hallinnassa oleviin tiloihin, ei kuitenkaan vakituiseen asumiseen käytettyihin tiloihin. Toimenpiteestä päättää tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies.

97 §

Tiedonsiirtäjän velvollisuus myötävaikuttaa tietoliikennetiedustelun edellyttämän liityntäpisteen rakentamiseen ja ylläpitämiseen

— —

Jos 1 momentissa tarkoitettua liityntäpistettä ei voida toteuttaa tiedonsiirtäjän myötävaikutuksella tai jos se on välttämätöntä tiedustelun suojaamiseksi, Puolustusvoimien tiedustelulaitoksella on oikeus toteuttaa liityntäpiste tiedonsiirtäjän hallinnoimaan viestintäverkon osaan. Jollei tiedustelun suojaaminen muuta edellytä, tiedonsiirtäjän tulee mahdollisuuksien mukaan olla paikalla tietoliikennetiedustelun edellyttämää liityntäpistettä toteutettaessa.

99 §

Korvaus viestinnän välittäjälle ja datakeskuspalvelun tarjoajalle

Viestinnän välittäjällä ja datakeskuspalvelun tarjoajalla on oikeus saada valtion varoista korvaus 96 §:ssä tarkoitetusta sotilastiedusteluviranomaisen avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista siten kuin sähköisen viestinnän palveluista annetun lain 299 §:ssä säädetään. Korvauksen maksamisesta päättää toimenpiteen suorittanut sotilastiedusteluviranomainen.

101 §

Muutoksenhaku korvauspäätökseen

Viestinnän välittäjälle, datakeskuspalvelun tarjoajalle tai tiedonsiirtäjälle annettuun korvauspäätökseen saa vaatia oikaisua. Oikaisuvaatimuksesta säädetään hallintolaissa (434/2003).

Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

Hallinto-oikeuden on varattava Liikenne- ja viestintävirastolle tilaisuus tulla kuulluksi.

104 §

Tietojen saanti yksityiseltä yhteisöltä

— —

Jos tiedot ovat tarpeen tiedustelutehtävän suorittamiseksi, sotilastiedusteluviranomaisella on yksittäistapauksessa oikeus pyynnöstä saada viestinnän välittäjältä tai datakeskuspalvelun tarjoajalta yhteystiedot sellaisesta teleosoitteesta, jota ei mainita julkisessa luettelossa, tai teleosoitteen tai telepäätelaitteen yksilöivät tai palvelun käyttäjän tai tilaajan tunnistamiseksi tarpeelliset tiedot. Sotilastiedusteluviranomaisella on vastaava oikeus saada postitoimintaa harjoittavalta yhteisöltä jakeluosoitetietoja.

Sotilastiedusteluviranomaisella on oikeus saada tässä pykälässä tarkoitetut tiedot viipymättä ja maksutta, jollei laissa toisin säädetä.

111 §

Tallenteiden tutkiminen

Tiedustelumenetelmien käytössä kertyneitä tallenteita saa tutkia vain tuomioistuin ja pääesikunnan tiedustelupäällikkö, sotilastiedusteluviranomaisen tehtävään määrätty virkamies taikka tiedusteluvalvontavaltuutettu tai hänen määräämänsä virkamies. Tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen määräyksestä tai tuomioistuimen osoituksen mukaan tallennetta saa tutkia myös muu kuin edellä tarkoitettu

sotilastiedusteluviranomaisen virkamies, asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankintaa toteutettaessa.

— —

Tämä laki tulee voimaan päivänä kuuta 20 .

2.

Laki

puolustusvoimista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään puolustusvoimista annettuun lakiin (551/2007) uusi 8 b ja 8 c §, 36 a §:ään, sellaisena kuin se on laissa 890/2018, uusi 3 momentti seuraavasti:

8 b §

Tiedonhankinta yleisesti saatavilla olevista lähteistä

Puolustusvoimat voi hankkia ja käsitellä tehtäviensä suorittamiseksi tietoa yleisesti saatavilla olevista lähteistä.

Puolustusvoimilla on oikeus käyttää teknisiä laitteita, menetelmiä tai ohjelmistoja tiedon hakemiseen ja tallentamiseen 1 momentissa tarkoitetusta lähteestä.

Puolustusvoimat saa käyttää 1 momentissa tarkoitetun tiedonhankinnan suojaamisessa tehtävän salaamiseksi vääriä, harhauttavia tai peiteltyjä tietoja.

Pääesikunta tekee päätöksen niistä Puolustusvoimien hallintoyksiköistä, joilla on oikeus käyttää 3 momentissa tarkoitettua tiedonhankinnan suojaamista.

Edellä 4 momentissa tarkoitetun hallintoyksikön päällikkö päättää 3 momentissa tarkoitetusta tiedonhankinnan suojaamisesta.

8 c §

Yleisesti saatavilla olevista lähteistä hankitun tiedon hävittäminen

Edellä 8 b §:ssä tarkoitetussa tiedonhankinnassa saatu tieto on hävitettävä viipymättä sen jälkeen, kun on käynyt ilmi, ettei tietoa tarvita Puolustusvoimien tehtävien suorittamiseksi.

Henkilötietojen käsittelystä säädetään henkilötietojen käsittelystä Puolustusvoimissa annetussa laissa (332/2019).

36 a §

Viran haettavaksi julistaminen

— —

Täytettäessä hakumenettelyssä muuta kuin 1 tai 2 momentissa tarkoitettua virkaa tai virkasuhdetta Puolustusvoimat voi jättää ilmoittamatta virkaa tai virkasuhdetta hakeneiden nimet sekä nimitetyn nimen muille hakijoille, jos haettavan tehtävän luonne sitä välttämättä edellyttää. Viran tai virkasuhteen täyttämisestä on kuitenkin ilmoitettava hakijoille ja nimityspäätöksessä on mainittava täytettävänä ollut virka tai virkasuhde, päätöksen tehnyt viranomainen sekä nimityspäivä.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

3.

Laki

rikoslain 17 luvun 7 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan rikoslain (39/1889) 17 luvun 7 §:n 2 momentti, sellaisena kuin se on laissa 650/2004, seuraavasti:

7 §

Valtionrajarikos

— —

Valtionrajarikoksesta ei tuomita ulkomaalaista, joka 1 momentissa tarkoitetun teon johdosta käännytetään tai karkotetaan maasta, eikä ulkomaalaista, joka pakolaisuuden perusteella hakee turvapaikkaa tai oleskelulupaa Suomessa. Valtionrajarikoksesta ei tuomita myöskään ulkomaalaista, joka on tehnyt 1 momentissa tarkoitetun teon sen vuoksi, että hän on ollut 25 luvun 3 tai 3 a §:ssä tarkoitetun ihmiskaupan kohteena tai joka on tehnyt 1 momentissa tarkoitetun teon sotilastiedustelusta annetun lain 78 a §:n 3 momentin perusteella.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

4.

Laki

Finanssivalvonnasta annetun lain 71 d §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan Finanssivalvonnasta annetun lain (878/2008) 71 d §, sellaisena kuin se on laissa 276/2025, seuraavasti:

71 d §

Oikeus luovuttaa tietoja suojelupoliisille ja sotilastiedusteluviranomaiselle

Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa säädetään, Finanssivalvonnalla on oikeus luovuttaa salassapitosäännösten estämättä pyynnöstä tietoja suojelupoliisille, jos tiedot ovat välttämättömiä suojelupoliisin toimialaan kuuluvien rikosten ennalta estämiseksi ja kansallisen turvallisuuden suojaamiseksi sitä vakavasti uhkaavalta toiminnalta sekä sotilastiedusteluviranomaiselle, jos tiedot ovat välttämättömiä sotilastiedusteluviranomaisen tiedustelutehtävän kannalta.

Finanssivalvonnalla on oikeus luovuttaa salassapitosäännösten estämättä oma-aloitteisesti suojelupoliisille tai sotilastiedusteluviranomaiselle Finanssivalvonnan hallussa olevia tietoja liittyen rahanpesuun tai terrorismin rahoittamiseen, pakotesääntelyn kiertämiseen tai muihin epätavallisiin liiketoimiin liittyvistä järjestelyistä, joilla varoja siirretään kolmansiin maihin ja toimilla epäillään vaarannettavan kansallista turvallisuutta, jos tiedot ovat tarpeellisia suojelupoliisin toimialaan kuuluvien rikosten ennalta estämiseksi ja kansallisen turvallisuuden suojaamiseksi sitä vakavasti uhkaavalta toiminnalta taikka jos tiedot ovat tarpeellisia sotilastiedusteluviranomaisen toimialaan kuuluvan tiedustelutehtävän kannalta.

Edellä 1 ja 2 momentissa tarkoitettujen tietojen luovuttamiseen sovelletaan, mitä 71 §:n 5 momentissa säädetään.

Tämä laki tulee voimaan päivänä kuuta 20 .

5.

Laki

Harmaan talouden selvitysyksiköstä annetun lain 6 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan Harmaan talouden selvitysyksiköstä annetun lain (1207/2010) 6 §:n 1 momentin 40 kohta sellaisena kuin se on laissa 24/2026, sekä

lisätään 6 §:n 1 momenttiin, sellaisena kuin se on laeissa 308/2016, 858/2016, 1159/2016, 1413/2016, 1419/2016, 324/2017, 454/2017, 1112/2017, 404/2018, 414/2018, 722/2019, 1399/2019, 624/2020, 488/2021, 690/2021, 1134/2021, 495/2022, 713/2022, 1119/2022, 1327/2022, 1340/2022, 1355/2022, 743/2023, 190/2024, 940/2024, 260/2025, 277/2025 ja 24/2026, uusi 41 kohta seuraavasti:

6 §

Velvoitteidenhoitoselvityksen käyttötarkoitus

Velvoitteidenhoitoselvitys laaditaan tukemaan:

— —

40) rahapelilain (10/2026) 10 §:ssä säädetyn luotettavuuden ja sopivuuden selvittämistä;

41) sotilastiedustelusta annetussa laissa (590/2019) tarkoitettua sotilastiedustelua.

— —

Tämä laki tulee voimaan päivänä kuuta 20 .

6.

Laki

tuloverolain 92 b §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan tuloverolain (1535/1992) 92 b §:n 3 kohta, sellaisena kuin se on laissa 404/2025, seuraavasti:

92 b §

Todistelupalkkiot, vihjepalkkiot ja tietolähdetoiminnasta maksettavat palkkiot

Veronalaista tuloa eivät ole:

— —

3) viranomaisen maksama palkkio sotilastiedustelusta annetussa laissa (590/2019) ja poliisilaissa (872/2011) tarkoitetulle tietolähteelle tiedustelutehtävien hoitamiseksi merkityksellisten tietojen hankkimisesta tai tiedusteluviranomaisen avustamisesta sekä rikostorjunnasta Rajavartiolaitoksessa annetussa laissa (108/2018) tarkoitetulle tietolähteelle rajaturvallisuuden ylläpitämiseen liittyvien tehtävien hoitamiseksi merkityksellisten tietojen hankkimisesta.

Tämä laki tulee voimaan päivänä kuuta 20 .

7.

Laki

rajavartiolain muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan rajavartiolain (578/2005) 3 §:n 3 momentti, sellaisena kuin se on laissa 749/2014, ja
lisätään lakiin uusi 25 a § seuraavasti:

3 §

Rajavartiolaitoksen tehtävät

— —

Rajavartiolaitos suorittaa poliisi- ja tullitehtäviä ja etsintä-, pelastus- ja ensihoitotehtäviä sekä osallistuu sotilaalliseen maanpuolustukseen ja sotilastiedusteluun. Rajavartiolaitoksen tehtävistä meripelastustoimen alalla säädetään meripelastuslaissa.

25 a §

Rajavartiolaitoksen osallistuminen sotilastiedusteluun

Rajavartiolaitos osallistuu sotilastiedusteluviranomaisen pyynnöstä sotilastiedusteluun hankkimalla tietoja ja tekemällä toimenpiteitä sotilastiedusteluviranomaisten tiedustelutehtävien tukemiseksi.

Rajavartiolaitoksen toimivaltuuksista sotilastiedusteluun osallistumisessa säädetään sotilastiedustelusta annetussa laissa (590/2019).

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

8.

Laki

henkilötietojen käsittelystä Rajavartiolaitoksessa annetun lain 32 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään henkilötietojen käsittelystä Rajavartiolaitoksessa annetun lain (639/2019) 32 §:ään, sellaisena kuin se on laissa 430/2024, uusi 2 momentti seuraavasti:

32 §

Henkilötietojen luovuttaminen toiselle rikosasioiden tietosuojalaissa tarkoitetulle toimivaltaiselle viranomaiselle

— —

Rajavartiolaitos saa luovuttaa salassapitosäännösten estämättä 15 b §:ssä tarkoitettuja tietoja Puolustusvoimille sotilastiedustelusta annetussa laissa (590/2019) säädettyjä tehtäviä varten.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

9.

Laki

henkilötietojen käsittelystä Puolustusvoimissa annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään henkilötietojen käsittelystä Puolustusvoimissa annettuun lakiin (332/2019) uusi 37 a § seuraavasti:

37 a §

Sotilastiedusteluviranomaisen oikeus ylläpitää henkilörekisteriään

Jos rekisterinpitäjälle on muualla laissa säädetty oikeus salassapitosäännösten estämättä luovuttaa henkilörekisteristään teknisen käyttöyhteyden avulla tai tietojoukkona henkilötietoja Puolustusvoimille, sotilastiedusteluviranomainen saa tietojärjestelmänsä ylläpitämiseksi verrata kyseisen henkilörekisterin tietoja talletettujen henkilötietojensa sisältöön. Tarpeettomat tiedot on hävitettävä viipymättä sen jälkeen kuin vertailu on suoritettu. Tarpeettomia henkilötietoja ei saa tallettaa.

Jos tietojen käsittelyn alkuperäiseksi tai muuksi kuin alkuperäiseksi käyttötarkoitukseksi on säädetty maanpuolustus tai kansallinen turvallisuus, sotilastiedusteluviranomaisella on lisäksi salassapitosäännösten estämättä oikeus verrata tietojärjestelmässään toisesta tietojärjestelmästä kerättyä tietojoukkoa, jos menettely on välttämätön tietojen käsittelyn mahdollistamiseksi korkean tietoturvatason tietojärjestelmässä. Tietojoukko on hävitettävä viipymättä sen jälkeen, kun tarve vertailulle on päättynyt. Vertaamista varten kerättävät tiedot on pidettävä erillään muista sotilastiedusteluviranomaisen käsittelemistä tiedoista.

Tämä laki tulee voimaan päivänä kuuta 20 .

Helsingissä 4.6.2026

Pääministeri

Petteri Orpo

Puolustusministeri Antti Häkkänen

Liite
Rinnakkaistekstit

1.

Laki

sotilastiedustelusta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan sotilastiedustelusta annetun lain (590/2019) 43 §:n 3 momentti, 74 § ja 78 §:n 5 momentti,

muutetaan 11 §:n 2 momentti, 15 §:n 1 momentti, 18 §, 20 §:n 3 momentti, 33 §:n 2 ja 3 momentti, 36 §:n 1 momentti, 42 ja 44 §, 45 §:n 1 ja 4 momentti, 51 §:n 3 momentti, 53 §:n 1 momentti, 55 §:n 3 momentti, 62 §:n 2 ja 3 momentti, 64 ja 66–68 §, 69 §:n otsikko ja 2 momentti, 70 §, 71 §:n 2 momentti, 77 §:n 1 momentti, 82 §:n 1 ja 2 momentti, 85, 86, 89, 91, 93 ja 94 §, 9 luvun otsikko, 96 §, 97 §:n 2 momentti, 99 ja 101 §, 104 §:n 2 momentti sekä 111 §:n 1 momentti, sellaisena kuin niistä on 20 §:n 3 momentti laissa 333/2025, sekä

lisätään lakiin uusi 18 a §, 33 §:ään uusi 4 momentti, 36 §:ään uusi 4 momentti, lakiin uusi 46 a ja 46 b §, 51 §:ään uusi 4 momentti, jolloin nykyinen 4 ja 5 momentti siirtyvät 5 ja 6 momentiksi, lakiin uusi 55 a, 56 a, 61 a ja 61 b §, 62 §:ään uusi 4 momentti, 63 §:ään uusi 3 momentti, jolloin nykyinen 3 momentti siirtyy 4 momentiksi, lakiin uusi 67 a, 67 b, 78 a, 89 a ja 89 b § sekä 104 §:ään uusi 3 momentti seuraavasti:

Voimassa oleva laki	*Ehdotus*
11 §	11 §
Sotilastiedusteluviranomaiset	*Sotilastiedusteluviranomaiset*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Sotilastiedustelutoiminnasta Maa-, Meri- ja Ilmavoimissa säädetään 60 §:ssä. Maa-, Meri- ja Ilmavoimat ovat sotilastiedustelutoiminnassa sotilastiedusteluviranomaisen alaisia.	Maa-, Meri- ja Ilmavoimat voivat käyttää tiedustelutehtävän suorittamiseksi tietolähdetoimintaa sekä radiosignaalitiedustelua. Maa-, Meri- ja Ilmavoimat ovat sotilastiedustelutoiminnassa sotilastiedusteluviranomaisen alaisia.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
18 §	18 §
Yhteistyö muiden viranomaisten sekä yritysten ja muiden yhteisöjen kanssa	*Yhteistyö muiden viranomaisten sekä yritysten ja muiden yhteisöjen kanssa*
Sotilastiedusteluviranomaisen on tarpeen mukaan toimittava yhteistyössä muiden viranomaisten kanssa sotilastiedustelun tarkoituksenmukaiseksi hoitamiseksi. Sotilastiedusteluviranomainen voi tehtävänsä	Sotilastiedusteluviranomaisen on tarpeen mukaan toimittava yhteistyössä muiden viranomaisten kanssa sotilastiedustelun tarkoituksenmukaiseksi hoitamiseksi. Sotilastiedusteluviranomainen voi tehtävänsä

Voimassa oleva laki	*Ehdotus*
toteuttamiseksi luovuttaa muille viranomaisille salassapitosäännösten estämättä muita *tietoja* kuin henkilötietoja, jos tietojen luovuttaminen on tarpeen maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi. *Henkilötietojen luovuttamisesta säädetään henkilötietojen käsittelystä Puolustusvoimissa annetussa laissa.*	toteuttamiseksi luovuttaa muille viranomaisille salassapitosäännösten estämättä muita kuin henkilötietoja, jos tietojen luovuttaminen on tarpeen maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi.
Sotilastiedusteluviranomainen voi salassapitosäännösten estämättä tehtävänsä toteuttamiseksi luovuttaa yrityksille ja muille yhteisöille *tiedustelun menetelmien ja järjestelmien kehittämiseksi* haittaohjelmaan liittyvän tunnistamistiedon tai luovuttaa muun kuin henkilötiedon, jos tietojen luovuttaminen on *välttämätöntä Puolustusvoimien toiminnan* tai kansallisen turvallisuuden suojaamiseksi.	Sotilastiedusteluviranomainen voi salassapitosäännösten estämättä tehtävänsä toteuttamiseksi luovuttaa yrityksille ja muille yhteisöille haittaohjelmaan liittyvän tunnistamistiedon tai luovuttaa muun tiedon kuin henkilötiedon, jos tietojen luovuttaminen on *tarpeen maanpuolustuksen kannalta* tai kansallisen turvallisuuden suojaamiseksi.
Tietojen luovuttamisesta rikostorjuntaan säädetään *79 ja 80 §:ssä.*	Tietojen luovuttamisesta rikostorjuntaan säädetään *6 luvussa.*
Sotilastiedusteluviranomaisen ja muiden viranomaisten välisen yhteistyön järjestämisestä sekä yhteistyöhön osallistuvista tahoista ja niiden tehtävistä voidaan antaa tarkempia säännöksiä valtioneuvoston asetuksella.	Sotilastiedusteluviranomaisen ja muiden viranomaisten välisen yhteistyön järjestämisestä sekä yhteistyöhön osallistuvista tahoista ja niiden tehtävistä voidaan antaa tarkempia säännöksiä valtioneuvoston asetuksella.
(uusi)	18 a §
	Yhteistoiminta Rajavartiolaitoksen kanssa
	Sen lisäksi, mitä 18 §:ssä säädetään, Rajavartiolaitos voi sotilastiedusteluviranomaisen päätöksellä ja tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen pyynnöstä suorittaa 22, 26, 28, 30, 32, 41, 42, 54 ja 56 §:ssä säädetyn tiedustelumenetelmän käyttöön liittyvän yksittäisen toimenpiteen, jos se on välttämätöntä tiedustelutehtävän suorittamiseksi. Rajavartiolaitoksessa pyynnön kohteena olevan toimenpiteen suorittamisesta päättää pidättämiseen oikeutettu virkamies. Rajavartiolaitoksen on sotilastiedusteluviranomaisen pyynnöstä ilman aiheetonta viivytystä keskeytettävä tässä momentissa tarkoitettu toimenpide.

Voimassa oleva laki	*Ehdotus*
	Jos sotilastiedusteluviranomaisella ei ole toimivaltuutta tiedustelutehtävän hoitamiseksi tarpeellisen toimenpiteen suorittamiseen, Rajavartiolaitos voi tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen pyynnöstä suorittaa Rajavartiolaitokselle säädetyn tehtävän yhteydessä rajavartiolain (578/2005) 28 §:ssä tarkoitettuja toimenpiteitä, jotka ovat välttämättömiä sotilastiedustelutehtävän kannalta. Toimenpiteen kohteena oleva henkilö on velvollinen olemaan läsnä toimenpiteitä suoritettaessa enintään 12 tuntia kerrallaan. Rajavartiolaitoksessa toimenpiteen suorittamisesta päättää rajanylityspaikan esimies tai vähintään luutnantin arvoinen rajavartiomies. Rajavartiolaitoksella on rajanylityspaikan esimiehenä toimivan rajavartiomiehen tai vähintään luutnantin arvoisen rajavartiomiehen päätöksellä oikeus käyttää vääriä, harhauttavia tai peiteltyjä tietoja silloin kun se on välttämätöntä tässä pykälässä tarkoitetun toimenpiteen paljastumisen estämiseksi. Rajavartiolaitoksen on luovutettava tässä pykälässä tarkoitetulla toimenpiteellä saadut tallenteet ja asiakirjat käsittelemättöminä sotilastiedusteluviranomaiselle sekä hävitettävä toimenpiteen suorittamisessa syntyneet tallenteet ja asiakirjat, jollei tietojen käsittely ole tarpeen Rajavartiolaitokselle säädettyjen muiden tehtävien suorittamiseksi. Tallenteiden ja asiakirjojen tarkastamisesta sekä muista tiedonkäsittelyyn liittyvistä tehtävistä vastaa sotilastiedusteluviranomainen.
20 §	20 §
Kansainvälinen yhteistyö	*Kansainvälinen yhteistyö*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Ulkomaisella toimivaltaisella virkamiehellä on pääesikunnan tiedustelupäällikön päätöksellä oikeus Suomen alueella sotilastiedusteluviranomaisen tehtävien hoitamiseksi toimia yhteistoiminnassa	Ulkomaisella toimivaltaisella virkamiehellä on pääesikunnan tiedustelupäällikön päätöksellä oikeus Suomen alueella sotilastiedusteluviranomaisen tehtävien hoitamiseksi toimia yhteistoiminnassa

Voimassa oleva laki	*Ehdotus*
sotilastiedusteluviranomaisen virkamiehen kanssa ja tämän ohjauksessa ja valvonnassa *käyttää 22, 24, 43, 47, 51, 60 ja 66 §:ssä tarkoitettuja tiedustelumenetelmiä*. Ulkomainen virkamies on velvollinen noudattamaan sotilastiedusteluviranomaisen hänelle antamia määräyksiä, rajoituksia ja ohjeita.	sotilastiedusteluviranomaisen virkamiehen kanssa ja tämän ohjauksessa ja valvonnassa *oikeus osallistua Suomen alueella tiedustelumenetelmän käyttöön*. Ulkomainen virkamies on velvollinen noudattamaan sotilastiedusteluviranomaisen hänelle antamia määräyksiä, rajoituksia ja ohjeita.
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
33 §	33 §
Teknisestä laitetarkkailusta päättäminen	*Teknisestä laitetarkkailusta päättäminen*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
Lupa voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan. Teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava: 1) toimenpiteen perusteena oleva tiedustelutehtävä; 2) toimenpiteen kohteena oleva tekninen laite tai ohjelmisto; 3) tosiseikat, joihin teknisen laitetarkkailun edellytykset ja kohdistaminen perustuvat; 4) luvan voimassaoloaika kellonajan tarkkuudella; 5) teknistä laitetarkkailua johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies; 6) mahdolliset teknisen laitetarkkailun rajoitukset ja ehdot.	Lupa voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan. Teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava: 1) toimenpiteen perusteena oleva tiedustelutehtävä; 2) toimenpiteen kohteena oleva tekninen laite tai ohjelmisto *taikka teknistä laitetta tai ohjelmistoa käyttävä henkilö*; 3) tosiseikat, joihin teknisen laitetarkkailun edellytykset ja kohdistaminen perustuvat; 4) luvan voimassaoloaika kellonajan tarkkuudella; 5) teknistä laitetarkkailua johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies; 6) mahdolliset teknisen laitetarkkailun rajoitukset ja ehdot. Tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää toimenpiteen kohteena olevista teknisistä laitteista tai ohjelmistoista, jos toimenpiteen kohteena on henkilö. Päätöksessä on mainittava perustelut toimenpiteen kohteena olevien laitteiden tai ohjelmistojen valitsemiselle.
(uusi)	
36 §	36 §
Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättäminen	*Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättäminen*

Voimassa oleva laki	*Ehdotus*
Tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta.	Tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta. *Jos telekuuntelua tai tietojen hankkimisesta telekuuntelun sijasta koskeva asia ei siedä viivytystä, tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää televalvonnasta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta.*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
(uusi)	Tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää toimenpiteen kohteena olevista teleosoitteista tai telepäätelaitteista, jos toimenpiteen kohteena on henkilö. Päätöksessä on mainittava perustelut toimenpiteen kohteena olevien teleosoitteiden tai telepäätelaitteiden valitsemiselle.
42 §	42 §
Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen	*Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen*
Sotilastiedusteluviranomaisen palveluksessa olevalla virkamiehellä on oikeus sijoittaa telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tekniseen kuunteluun, tekniseen katseluun, tekniseen seurantaan tai tekniseen laitetarkkailuun käytettävä laite, menetelmä tai ohjelmisto *toimenpiteen kohteena olevaan* esineeseen, aineeseen, omaisuuteen, tilaan tai muuhun paikkaan taikka tietojärjestelmään, jos mainitun tiedustelumenetelmän käyttö sitä edellyttää. Sotilastiedusteluviranomaisen virkamiehellä on tällöin oikeus laitteen, menetelmän tai ohjelmiston asentamiseksi, käyttöön ottamiseksi ja poistamiseksi salaa mennä edellä mainittuihin kohteisiin tai	Sotilastiedusteluviranomaisen palveluksessa olevalla virkamiehellä on oikeus sijoittaa telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tekniseen kuunteluun, tekniseen katseluun, tekniseen seurantaan tai tekniseen laitetarkkailuun, *valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedusteluun tai ulkomaan tietojärjestelmätiedusteluun* käytettävä laite, menetelmä tai ohjelmisto esineeseen, aineeseen, omaisuuteen, tilaan tai muuhun paikkaan taikka tietojärjestelmään, jos mainitun tiedustelumenetelmän käyttö sitä edellyttää. Sotilastiedusteluviranomaisen virkamiehellä on tällöin oikeus laitteen, menetelmän tai ohjelmiston asentamiseksi,

Voimassa oleva laki	*Ehdotus*
tietojärjestelmään sekä kiertää, purkaa tai muulla vastaavalla tavalla tilapäisesti ohittaa kohteen tai tietojärjestelmän suojaus tai haitata sitä. Laitteen, menetelmän tai ohjelmiston asentaminen tai sen poisottaminen ei saa tapahtua pysyväisluonteiseen asumiseen käytettävässä tilassa.	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. Laitteen, menetelmän tai ohjelmiston asentaminen tai sen poisottaminen ei saa tapahtua pysyväisluonteiseen asumiseen käytettävässä tilassa.
(uusi)	*Sotilastiedusteluviranomaisen pyynnöstä viranomaisen ulkopuolisella henkilöllä on oikeus tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa toteuttaa tiedustelumenetelmän käytön edellyttämä asennus- tai poistamistoimenpide.*
(uusi)	*Sotilastiedusteluviranomaisella on oikeus menetelmän tai ohjelmiston asentamiseksi tai poisottamiseksi ja tiedonsiirtämiseksi tilapäisesti käyttää yksityisen tai yhteisön laitetta tai tietojärjestelmää, jos se on välttämätöntä tiedustelumenetelmän käyttämiseksi. Sotilastiedusteluviranomainen ei saa aiheuttaa vähäistä suurempaa haittaa tai vahinkoa käytettävälle laitteelle tai tietojärjestelmälle.*
43 §	43 §
Peitetoiminta	*Peitetoiminta*
Peitetoiminnalla tarkoitetaan tiettyyn henkilöön tai hänen toimintaansa taikka, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmään tai sen toimintaan kohdistuvaa suunnitelmallista tiedonhankintaa käyttämällä soluttautumista, jossa tiedonhankinnan edellyttämän luottamuksen hankkimiseksi tai tiedonhankinnan paljastumisen estämiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka valmistetaan tai käytetään vääriä asiakirjoja.	*Peitetoiminnalla* tarkoitetaan tiettyyn henkilöön tai hänen toimintaansa taikka, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmään tai sen toimintaan kohdistuvaa suunnitelmallista tiedonhankintaa käyttämällä soluttautumista, jossa tiedonhankinnan edellyttämän luottamuksen hankkimiseksi tai tiedonhankinnan paljastumisen estämiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka valmistetaan tai käytetään vääriä asiakirjoja.
Sotilastiedusteluviranomainen saa kohdistaa henkilöön tai henkilöryhmään peitetoimintaa, jos tiedustelutehtävän kohteena oleva toiminta on suunnitelmallista, järjestäytynyttä tai ammattimaista taikka	Sotilastiedusteluviranomainen saa kohdistaa henkilöön tai henkilöryhmään peitetoimintaa, jos tiedustelutehtävän kohteena oleva toiminta on suunnitelmallista, järjestäytynyttä tai ammattimaista taikka

Voimassa oleva laki	*Ehdotus*
toiminnan ennakoidaan olevan jatkuvaa tai toistuvaa.	toiminnan ennakoidaan olevan jatkuvaa tai toistuvaa.
Sotilastiedustelun viranomaisilla on oikeus kohdistaa henkilöön tai henkilöryhmään peitetoimintaa tietoverkossa, jos sillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.	*(kumotaan)*
44 §	44 §
*Peitetoimintaa koskeva **esitys ja** suunnitelma*	***Peitetoimintaa koskeva suunnitelma***
Peitetoimintaa koskevassa esityksessä on mainittava: *1) toimenpiteen esittäjä;* *2) tiedonhankinnan kohteena oleva henkilö tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmä riittävästi yksilöitynä;* *3) toimenpiteen perusteena oleva tiedustelutehtävä;* *4) peitetoiminnan tavoite;* *5) peitetoiminnan tarpeellisuus;* *6) muut peitetoiminnan edellytysten arviointia varten tarvittavat tiedot.*	*(kumotaan)*
Peitetoiminnan toteuttamisesta on laadittava kirjallinen suunnitelma, jonka tulee sisältää peitetoimintaa koskevan päätöksenteon ja peitetoiminnan toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava.	Peitetoiminnan toteuttamisesta on laadittava kirjallinen suunnitelma, jonka tulee sisältää peitetoimintaa koskevan päätöksenteon ja peitetoiminnan toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava.
45 §	45 §
Peitetoiminnasta päättäminen	*Peitetoiminnasta päättäminen*
Pääesikunnan tiedustelupäällikkö päättää peitetoiminnasta. *Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättää tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.*	Pääesikunnan tiedustelupäällikkö päättää peitetoiminnasta.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava. *Peitetoiminnan lopettamisesta on tehtävä kirjallinen päätös.*	Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava.

Voimassa oleva laki	*Ehdotus*
(uusi)	46 a § *Yksinomaan tietoverkossa toteutettava peitetoiminta* Yksinomaan tietoverkossa toteutettavalla peitetoiminnalla tarkoitetaan 4 §:ssä tarkoitettuun toimintaan kohdistuvaa tietoverkossa tapahtuvaa suunnitelmallista tiedonhankintaa käyttämällä soluttautumista, jossa tiedonhankinnan edellyttämän luottamuksen hankkimiseksi tai tiedonhankinnan paljastumisen estämiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka valmistetaan tai käytetään vääriä asiakirjoja. Sotilastiedustelunviranomaisella on oikeus kohdistaa henkilöön tai henkilöryhmään peitetoimintaa tietoverkossa, jos sillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta on laadittava kirjallinen suunnitelma, jonka tulee sisältää päätöksenteon ja peitetoiminnan toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava.
(uusi)	46 b § *Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättäminen* Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättää tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies. Yksinomaan tietoverkossa toteutettavaa peitetoimintaa koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan. Yksinomaan tietoverkossa toteutettavaa peitetoimintaa koskeva päätös on tehtävä kirjallisesti. Päätöksessä on mainittava:

Voimassa oleva laki	*Ehdotus*
	1) toimenpiteen esittäjä; 2) peitetoiminnan toteuttamisesta vastaava tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies; 3) tunnistetiedot peitetoiminnan suorittavista virkamiehistä; 4) toimenpiteen perusteena oleva tiedustelutehtävä; 5) tosiseikat, joihin peitetoiminnan edellytykset ja kohdistaminen perustuvat; 6) peitetoiminnan tavoite ja toteuttamissuunnitelma; 7) päätöksen voimassaoloaika; 8) peitetoiminnan mahdolliset rajoitukset ja ehdot. Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava.
51 §	51 §
Tietolähdetoiminta	*Tietolähdetoiminta*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Tietolähteen ohjatussa käytössä tietoja ei saa pyytää hankittavaksi sellaisella tavalla, joka edellyttäisi viranomaiselle kuuluvien toimivaltuuksien käyttöä *tai joka vaarantaisi tietolähteen tai muun henkilön hengen tai terveyden.* Ennen tietolähteen ohjattua käyttöä tietolähteelle on tehtävä selkoa hänen oikeuksistaan ja velvollisuuksistaan sekä erityisesti hänelle lain mukaan sallitusta ja kielletystä toiminnasta. Tietolähteen turvallisuudesta on tarpeen mukaan huolehdittava tiedonhankinnan aikana ja sen jälkeen.	Tietolähteen ohjatussa käytössä tietoja ei saa pyytää hankittavaksi sellaisella tavalla, joka edellyttäisi viranomaiselle kuuluvien toimivaltuuksien käyttöä. Ennen tietolähteen ohjattua käyttöä tietolähteelle on tehtävä selkoa hänen oikeuksistaan ja velvollisuuksistaan sekä erityisesti hänelle lain mukaan sallitusta ja kielletystä toiminnasta. *Tietolähteen ohjatussa käytössä tietoja ei saa pyytää hankittavaksi sellaisella tavalla, joka vaarantaisi tietolähteen tai muun henkilön hengen tai terveyden.* Tietolähteen turvallisuudesta on tarpeen mukaan huolehdittava tiedonhankinnan aikana ja sen jälkeen.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
53 §	53 §
Tietolähteen ohjatusta käytöstä päättäminen	*Tietolähteen ohjatusta käytöstä päättäminen*
Pääesikunnan tiedustelupäällikkö päättää tietolähteen ohjatusta käytöstä.	Pääesikunnan tiedustelupäällikkö *taikka tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.* päättää tietolähteen ohjatusta käytöstä.
— — — — — — — — — — — — — — —	

Voimassa oleva laki	*Ehdotus*
	— — — — — — — — — — — — — — —
55 §	55 §
Paikkatiedustelusta päättäminen	*Paikkatiedustelusta päättäminen*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Pääesikunnan tiedustelupäällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää muusta kuin 1 momentissa tarkoitetusta paikkatiedustelusta.	Pääesikunnan tiedustelupäällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää *kulkuneuvoon kohdistuvasta paikkatiedustelusta sekä* muusta kuin 1 momentissa tarkoitetusta paikkatiedustelusta.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
(uusi)	55 a §
	Näytteenotto paikkatiedustelussa
	Sotilastiedusteluviranomaisella on oikeus paikkatiedustelussa ottaa aineesta, omaisuudesta tai esineestä näyte, jos se on tarpeen tiedustelutehtävän suorittamiseksi.
(uusi)	56 a §
	Aineen, omaisuuden tai esineen tilapäinen haltuunotto
	Jos 55 a §:ssä tarkoitettu näytteenotto tai 56 §:ssä tarkoitettu jäljentäminen sitä välttämättä edellyttää, sotilastiedusteluviranomaisella on oikeus ottaa aine, omaisuus tai esine tilapäisesti haltuun. Aine, omaisuus tai esine on palautettava viivytyksettä haltuunoton tarkoituksen toteuduttua.
(uusi)	61 a §
	Valtiolliseen toimijan tietojärjestelmään kotimaassa kohdistuva tiedustelu
	Valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvalla tiedustelulla tarkoitetaan tiedonhankintaa valtiollisen toimijan Suomessa käyttämien tietojärjestelmien siitä osasta, joka toteuttaa

Voimassa oleva laki	*Ehdotus*
	tai edesauttaa tiedustelutehtävän kohteena olevaa toimintaa tai joka tallentaa tai välittää tiedustelutehtävän kohteena olevaan toimintaan liittyviä tietoja. Valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvaa tiedustelua saa käyttää vain siinä laajuudessa kuin on välttämätöntä tiedon hankkimiseksi tiedustelutehtävän kohteena olevasta toiminnasta.
(uusi)	61 b §
	Valtiolliseen toimijaan kohdistuvasta tietojärjestelmätiedustelusta Suomessa päättäminen
	Tuomioistuin päättää valtiolliseen toimijan tietojärjestelmään kotimaassa kohdistuvasta tiedustelusta tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta. *Lupa valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvaan tiedusteluun voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.* *Valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvaan tiedustelua koskevassa vaatimuksessa ja päätöksessä on mainittava:* *1) tiedustelutehtävä;* *2) toimenpiteen kohteena oleva valtiollinen toimija ja sen käyttämä tietojärjestelmä;* *3) tosiseikat, joihin valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvan tiedustelun edellytykset ja kohdistaminen perustuvat;* *4) valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvaa tiedustelua koskevan luvan voimassaoloaika kellonajan tarkkuudella;* *5) valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvan tiedustelun suorittamista johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;* *6) mahdolliset valtiollisen toimijan tietojärjestelmään kohdistuvan tiedustelun rajoitukset ja ehdot.*

Voimassa oleva laki	*Ehdotus*
	Tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää toimenpiteen kohteena olevista teleosoitteista tai telepäätelaitteista taikka laitteista tai ohjelmistoista tiedustelumenetelmää koskevan luvan voimassaolon aikana. Päätöksessä on mainittava perustelut toimenpiteen kohteena olevien teleosoitteiden tai telepäätelaitteiden taikka laitteiden tai ohjelmistojen valitsemiselle.
62 §	62 §
Ulkomaan tietojärjestelmätiedustelu	*Ulkomaan tietojärjestelmätiedustelu*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Puolustusvoimien tiedustelulaitos saa kohdistaa tietojärjestelmään ulkomaan tietojärjestelmätiedustelua, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.	*Sotilastiedusteluviranomainen* saa kohdistaa tietojärjestelmään ulkomaan tietojärjestelmätiedustelua, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.
Ulkomaan tietojärjestelmätiedustelun toteuttamisesta on laadittava kirjallinen suunnitelma, jonka tulee sisältää ulkomaan tietojärjestelmätiedustelua koskevan päätöksenteon ja toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava.	Ulkomaan tietojärjestelmätiedustelun toteuttamisesta on laadittava kirjallinen suunnitelma, jonka tulee sisältää ulkomaan tietojärjestelmätiedustelu*a ja siihen liittyviä toimenpiteitä* koskevan päätöksenteon ja toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava.
(uusi)	*Sotilastiedusteluviranomaisella on osana ulkomaan tietojärjestelmätiedustelua oikeus tehdä tarvittavia kansainvälisen oikeuden mukaisia tietoteknisiä toimenpiteitä Suomen alueen ulkopuolella olevassa tietojärjestelmässä, jos sillä tai sen kautta voidaan aiheuttaa Suomen maanpuolustukselle tai kansalliselle turvallisuudelle vakavaa uhkaa. Toimenpiteiden on oltava välttämättömiä, suhteellisia ja väliaikaisia.*
63 §	63 §
Ulkomaan tietojärjestelmätiedustelusta päättäminen	*Ulkomaan tietojärjestelmätiedustelusta päättäminen*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
(uusi)	

Voimassa oleva laki	*Ehdotus*
	Pääesikunnan tiedustelupäällikkö päättää 62 §:n 4 momentissa säädetyistä toimenpiteistä. Ennen Pääesikunnan tiedustelupäällikön päätöstä asia on käsiteltävä valmistelevasti 15 §:n 1 momentissa tarkoitettujen viranomaisten kesken sekä tarvittaessa linjattava ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteisessä kokouksessa.
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
64 §	64 §
Ulkomailla tapahtuva sotilastiedustelu	*Ulkomailla tapahtuva sotilastiedustelu*
Tämän lain 12 §:n 3 momentin, 60 §:n 3 momentin ja 85 §:n 2 momentin säännöksiä voidaan yksittäistapauksessa jättää soveltamatta ulkomailla tapahtuvassa sotilastiedustelussa ja tiedustelumenetelmien käytössä, jos se on välttämätöntä. Lain 79, 80 ja 89 §:ää ei sovelleta ulkomailla tapahtuvassa sotilastiedustelussa ja tiedustelumenetelmien käytössä.	Tämän lain 12 §:n 3 momentin, *51 §:n 3 momentin*, 60 §:n 3 momentin ja 85 §:n 2 momentin säännöksiä voidaan yksittäistapauksessa jättää soveltamatta ulkomailla tapahtuvassa sotilastiedustelussa ja tiedustelumenetelmien käytössä, jos se on välttämätöntä. Lain 79, 80 ja 89 §:ää ei sovelleta ulkomailla tapahtuvassa sotilastiedustelussa ja tiedustelumenetelmien käytössä.
Muualla kuin Suomessa toteutettavasta sotilastiedustelusta ja tiedustelumenetelmien käytöstä päättää pääesikunnan tiedustelupäällikkö.	*Ulkomailla tapahtuvasta* sotilastiedustelusta päättää pääesikunnan tiedustelupäällikkö. *Tiedustelutoimintaan liittyvästä yksittäisen tiedustelumenetelmän käytöstä päättää tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.*
Sotilastiedusteluviranomaisen virkamiehen osallistuminen tässä pykälässä tarkoitettuun ulkomailla tapahtuvaan sotilastiedusteluun edellyttää asianomaisen virkamiehen suostumusta.	*Sotilastiedusteluviranomaisen virkamiehen osallistuminen tässä pykälässä tarkoitettuun ulkomailla tapahtuvaan sotilastiedusteluun edellyttää asianomaisen virkamiehen suostumusta.*
Tiedustelumenetelmän käyttöä koskevan päätöksen, esityksen ja suunnitelman sisällön osalta noudatetaan, mitä esityksestä, suunnitelmasta, vaatimuksesta tai päätöksestä tässä laissa säädetään.	Tiedustelumenetelmän käyttöä koskevan päätöksen, esityksen ja suunnitelman sisällön osalta noudatetaan, mitä esityksestä, suunnitelmasta, vaatimuksesta tai päätöksestä tässä laissa säädetään.
66 §	66 §
Teknisten tietojen käsittely	

Voimassa oleva laki	*Ehdotus*
Tietoliikennetiedustelun kohdentamiseksi Puolustusvoimien tiedustelulaitos voi viestintäverkon tietoliikenteestä *hetkellisesti* kerätä ja tallentaa tietoliikenteen teknisiä tietoja ja automaattisen tietojenkäsittelyn avulla käsitellä niitä tilastollista analyysiä varten.	*Teknisten tietojen käsittely* ***viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi***
	Puolustusvoimien tiedustelulaitos voi viestintäverkon tietoliikenteestä kerätä ja tallentaa tietoliikenteen teknisiä tietoja ja automaattisen tietojenkäsittelyn avulla käsitellä niitä:
	1) tilastollista analyysia varten tietoliikennetiedustelun kohdentamiseksi viestintäverkon osaan;
	2) tietoliikenteen reitittymisen ja muutosten seuraamiseksi.
Tilastollisen analyysin tulokseen ei saa sisältyä tietoa, josta voidaan tunnistaa yksittäinen luonnollinen henkilö.	Edellä 1 momentissa tarkoitetussa toiminnassa ei saa muodostaa tietoa, josta voidaan tunnistaa yksittäinen luonnollinen henkilö.
(uusi)	*Tässä pykälässä tarkoitettuja teknisiä tietoja voidaan tallentaa enintään 18 kuukauden ajaksi. Tallennettavien teknisten tietojen määrä ei saa ylittää 5 prosenttia kohteena olevan Suomen rajan ylittävän viestintäverkon osan kapasiteetista. Tallennettuja tietoja voidaan käyttää 1 momentissa sekä jäljempänä tässä laissa säädettyihin tarkoituksiin.*
Puolustusvoimien tiedustelulaitoksen on hävitettävä kerätyt ja tallennetut tietoliikenteen tekniset tiedot *välittömästi sen jälkeen, kun tilastollisen analyysin tulos on valmistunut.*	Puolustusvoimien tiedustelulaitoksen on hävitettävä kerätyt ja tallennetut tietoliikenteen tekniset tiedot viimeistään 3 momentissa säädetyn tallennusajan päätyttyä.
67 §	67 §
Teknisten tietojen käsittelystä päättäminen	*Teknisten tietojen käsittelystä päättäminen* ***viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi***
Tuomioistuin päättää teknisten tietojen käsittelystä tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen *Puolustusvoimien tiedustelulaitoksen* sotilaslakimiehen tai muun virkamiehen vaatimuksesta.	Tuomioistuin päättää teknisten tietojen käsittelystä viestintäverkon osan tunnistamiseksi tai tietoliikenteen reitittymisen ja muutosten tunnistamiseksi tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta.
Lupa voidaan antaa enintään *kolmeksi* kuukaudeksi kerrallaan.	Lupa voidaan antaa ja päätös tehdä luvan antopäivästä tai päätöksen tekopäivästä

Voimassa oleva laki	*Ehdotus*
	alkaen enintään kuudeksi kuukaudeksi kerrallaan ja lupa tai päätös voi koskea myös 66 §:n 3 momentissa tarkoitettuja tallennettuja tietoja.
Teknisten tietojen käsittelyä koskevassa vaatimuksessa ja päätöksessä on mainittava:	Vaatimuksessa ja päätöksessä on mainittava:
1) maantieteellinen alue tai verkkoalue, jolta tulevaan tai jolle menevään tietoliikenteeseen teknisten tietojen käsittely kohdistetaan;	1) maantieteellinen alue tai verkkoalue, jolta tulevaan tai jolle menevään tietoliikenteeseen teknisten tietojen käsittely kohdistetaan, taikka kohde, jonka tietoliikenteen reitittymistä tai muutosta seurataan;
2) viestintäverkon osat, joista tietoa haetaan;	2) viestintäverkon osat, joista tietoa haetaan;
3) *teknisten tietojen* käsittelyä johtava ja valvova *Puolustusvoimien tiedustelulaitoksen* tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;	3) käsittelyä johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies; ja
4) suunnitelma *teknisten tietojen* käsittelyn toteuttamisesta.	4) suunnitelma käsittelyn toteuttamisesta.
(uusi)	67 a §
	Tietoliikennetiedustelu hakuehtojen määrittämiseksi
	Puolustusvoimien tiedustelulaitos voi kerätä ja tallentaa Suomen rajan ylittävän viestintäverkon osan tietoliikennettä tietoliikennetiedustelun tarkemmaksi kohdentamiseksi ja hakuehtojen määrittämiseksi sotilastiedustelun kohteen tietoliikenteen oletetun säännönmukaisuuden tai ominaispiirteen perusteella.
	Hakuehtojen määrittämisessä tietoliikenteen käsittelyn on tapahduttava tietoliikenteen konekielisessä muodossa. Hakuehtojen määrittämisessä ei saa hyödyntää viestin merkityssisällössä olevia tietoja. Hakuehtojen määrittämisen tuloksena ei saa syntyä viestin sisältöä kuvaavaa tietoa taikka tietoa, josta voidaan tehdä henkilön yksityiselämää koskevia päätelmiä.
	Kerättävän ja tallennettavan tietoliikenteen määrä ei saa ylittää 5 prosenttia kohteena olevan Suomen rajan ylittävän viestintäverkon osan kapasiteetista. Kerätty ja tallennettu tietoliikenne voidaan säilyttää enintään 12 kuukautta. Tallennettuja tietoja voidaan käyttää 1 momentissa ja jäljempänä tässä laissa säädettyihin tarkoituksiin.

Voimassa oleva laki	*Ehdotus*
	Hakuehtojen määrittämisessä voidaan käyttää 66 §:n 3 momentin perusteella tallennettuja teknisiä tietoja. *Puolustusvoimien tiedustelulaitoksen on hävitettävä kerätyt ja tallennetut tietoliikenteen tekniset tiedot viimeistään 3 momentissa tarkoitetun tallennusajan päätyttyä.*
(uusi)	67 b §
	Hakuehtojen määrittämisestä päättäminen
	Tuomioistuin päättää hakuehtojen määrittämisestä tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta. *Lupa voidaan antaa ja päätös tehdä luvan antopäivästä tai päätöksen tekopäivästä alkaen enintään kuudeksi kuukaudeksi kerrallaan ja lupa tai päätös voi koskea myös 66 §:n 3 momentissa ja 67 a §:n 3 momentissa tarkoitettuja tallennettuja tietoja.* *Vaatimuksessa ja päätöksessä on mainittava:* *1) tiedustelutehtävä, jota varten hakuehtoja määritetään ja sitä koskevat tosiseikat;* *2) tosiseikat, joihin hakuehtojen määrittämisen välttämättömyys perustuu;* *3) kohteen tietoliikenteen oletettu säännönmukaisuus tai ominaispiirre, jonka perusteella hakuehtoja määritetään, ja perustelut oletukselle;* *4) viestintäverkon osat, joista tietoa haetaan;* *5) suunnitelma hakuehtojen määrittämisestä;* *6) luvan voimassaoloaika kellonajan tarkkuudella;* *7) hakuehtojen määrittämistä johtava ja valvova Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;* *8) mahdolliset hakuehtojen määrittämistä koskevat rajoitukset ja ehdot.*
68 §	68 §

Voimassa oleva laki	*Ehdotus*
Valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu	***Valtiolliseen toimijaan kohdistuva tietoliikennetiedustelu***
Puolustusvoimien tiedustelulaitos voi Suomen rajan ylittävästä viestintäverkon tietoliikenteestä automaattisen tietojenkäsittelyn avulla hankkia tietoa tiedustelutehtävän kannalta olennaisen valtiollisen toimijan tietoliikenteestä sekä käsitellä valtiollisen toimijan viestintää. Tietojen hankkiminen tietoliikenteestä perustuu hakuehtojen käyttöön.	Puolustusvoimien tiedustelulaitos voi Suomen rajan ylittävästä viestintäverkon tietoliikenteestä automaattisen tietojenkäsittelyn avulla hankkia tietoa tiedustelutehtävän kannalta olennaisesta valtiollisesta toimijasta *ja sen tietoliikenteestä* sekä käsitellä tällaisen toimijan viestintää. Tietojen hankkiminen tietoliikenteestä perustuu *valtiollista toimijaa kuvaavien* hakuehtojen käyttöön.
Puolustusvoimien tiedustelulaitos voi käsitellä tietoliikenteestä hankittua tietoa automaattisesti ja manuaalisesti.	Puolustusvoimien tiedustelulaitos voi käsitellä tietoliikenteestä hankittua tietoa automaattisesti ja manuaalisesti.
Hakuehtona ei saa käyttää Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.	*Hakuehtona voidaan tilapäisesti käyttää Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.*
	Tässä pykälässä tarkoitettu tiedonhankinta voi kohdistua myös 66 §:n 3 momentin ja 67 a §:n 3 momentin nojalla tallennettuihin tietoihin.
(uusi)	
69 §	69 §
Valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta päättäminen	*Valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta päättäminen*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Lupa voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.	Lupa voidaan antaa *ja päätös tehdä luvan antopäivästä tai päätöksen tekopäivästä alkaen* enintään kuudeksi kuukaudeksi kerrallaan *ja lupa tai päätös voi koskea myös 66 §:n 3 momentissa ja 67 a §:n 3 momentissa tarkoitettuja tallennettuja tietoja.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
70 §	70 §
Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu	*Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu*
Puolustusvoimien tiedustelulaitos voi Suomen rajan ylittävästä viestintäverkon	Puolustusvoimien tiedustelulaitos voi Suomen rajan ylittävästä viestintäverkon

Voimassa oleva laki	*Ehdotus*
tietoliikenteestä automaattisen tietojenkäsittelyn avulla hankkia tietoa tiedustelutehtävän kannalta olennaisen muun kuin valtiollisen toimijan tietoliikenteestä, jos tiedot eivät ole hankittavissa muulla tiedustelumenetelmällä. Tietojen hankkiminen tietoliikenteestä perustuu hakuehtojen käyttöön.	tietoliikenteestä automaattisen tietojenkäsittelyn avulla hankkia tietoa tiedustelutehtävän kannalta olennaisen muun kuin valtiollisen toimijan tietoliikenteestä, jos tiedot eivät ole hankittavissa muulla tiedustelumenetelmällä. Tietojen hankkiminen tietoliikenteestä perustuu hakuehtojen käyttöön.
Hakuehtona ei saa käyttää Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.	Hakuehtona *voidaan tilapäisesti* käyttää Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.
Muun kuin valtiollisen toimijan *tietoliikenteen tiedustelun kohdentaminen ei saa tapahtua viestin sisällön perusteella, jollei kohdentamisessa käytetä haittaohjelman sisältöä kuvaavaa tietoa.*	Muun kuin valtiollisen toimijan *tietoliikenteeseen kohdistuvan tiedustelun kohdentamisessa voidaan käyttää viestin sisältöön kohdistuvia hakuehtoja. Kielellisiä ilmaisuja voidaan käyttää hakuehtona ainoastaan yhdessä teknisten tietojen kanssa.*
Puolustusvoimien tiedustelulaitos voi käsitellä tietoliikenteestä hankittua tietoa automaattisesti ja manuaalisesti.	Puolustusvoimien tiedustelulaitos voi käsitellä tietoliikenteestä hankittua tietoa automaattisesti ja manuaalisesti.
(uusi)	*Tässä pykälässä tarkoitettu tiedonhankinta voi kohdistua myös 66 §:n 3 momentin ja 67 a §:n 3 momentin nojalla tallennettuihin tietoihin.*
71 §	71 §
Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta päättäminen	*Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta päättäminen*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Lupa voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.	Lupa voidaan antaa *ja päätös tehdä luvan antopäivästä tai päätöksen tekopäivästä alkaen* enintään kuudeksi kuukaudeksi kerrallaan *ja lupa tai päätös voi koskea myös 66 §:n 3 momentissa ja 67 a §:n 3 momentissa tarkoitettuja tallennettuja tietoja.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
74 §	*(kumotaan)*
Haitallista tietokoneohjelmaa koskevien tietojen luovuttaminen yrityksille ja yhteisöille	

Voimassa oleva laki

Sotilastiedusteluviranomainen saa salassapitosäännösten estämättä luovuttaa tietoliikennetiedustelun avulla hankittuja tietoja haitallisesta tietokoneohjelmasta ja sen toiminnasta yritykselle, yhteisölle tai viranomaiselle, jos tietojen luovuttaminen on tarpeen sotilaallisen maanpuolustuksen kannalta, kansallisen turvallisuuden suojaamiseksi tai yrityksen tai yhteisön etujen turvaamiseksi.

77 §

Tiedustelumenetelmää käyttävän virkamiehen turvaaminen

Tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää, että peiteltyä tiedonhankintaa, peitetoimintaa tai valeostoa toteuttava sekä tietolähdetoimintaa valmisteleva tai toteuttava virkamies varustetaan kuuntelun ja katselun mahdollistavalla teknisellä laitteella, jos varustaminen on perusteltua hänen turvallisuutensa varmistamiseksi.

— — — — — — — — — — — — — —

78 §

Tietolähteen turvaaminen

— — — — — — — — — — — — — —

Pääesikunnan tiedustelupäällikkö saa päättää, että tietolähteelle annetaan yksittäistapauksessa käytettäväksi vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka tietolähteen käytettäväksi valmistettavia vääriä asiakirjoja, jos se on välttämätöntä tietolähteen hengen ja terveyden suojaamiseksi. Rekisterimerkintä on oikaistava sen jälkeen, kun tässä momentissa tarkoitettuja edellytyksiä ei enää ole.

(uusi)

Ehdotus

77 §

Tiedustelumenetelmää käyttävän virkamiehen turvaaminen

Tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää, että peiteltyä tiedonhankintaa, peitetoimintaa tai valeostoa toteuttava sekä tietolähdetoimintaa valmisteleva tai toteuttava virkamies taikka tällaisessa toiminnassa käytettävä tila varustetaan kuuntelun ja katselun mahdollistavalla teknisellä laitteella, jos varustaminen on perusteltua virkamiehen turvallisuuden varmistamiseksi.

— — — — — — — — — — — — — —

78 §

Tietolähteen turvaaminen

— — — — — — — — — — — — — —

78 a §

Voimassa oleva laki

Ehdotus

Tietolähteen hengen ja terveyden turvaaminen

Pääesikunnan tiedustelupäällikön päätöksellä sotilastiedusteluviranomainen voi antaa tietolähteelle yksittäistapauksessa käytettäväksi vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka tietolähteen käytettäväksi valmistettavia vääriä asiakirjoja, jos se on välttämätöntä tietolähteen hengen ja terveyden suojaamiseksi. Rekisterimerkintä on oikaistava sen jälkeen, kun tässä momentissa tarkoitettuja edellytyksiä ei enää ole.

Pääesikunnan tiedustelupäällikön päätöksellä sotilastiedusteluviranomainen voi järjestää tietolähteen Suomeen, jos se on välttämätöntä tietolähteen hengen ja terveyden suojaamiseksi ja menettelyä voidaan kokonaisuutena arvioiden pitää puolustettavana.

Tietolähteellä on oikeus saapua maahan 2 momentissa tarkoitetussa tilanteessa sekä käyttää maahantulon yhteydessä 1 momentissa tarkoitettuja vääriä tietoja, merkintöjä ja asiakirjoja.

82 §

Tiedustelukiellot

Telekuuntelua, telekuuntelun sijasta toimitettavaa tietojen hankkimista, teknistä kuuntelua, teknistä katselua, radiosignaalitiedustelua tai tietoliikennetiedustelua ei saa kohdistaa sellaiseen viestintään tai tietoon, josta osapuoli ei saa todistaa tai josta hänellä on oikeus olla todistamatta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n tai 22 §:n 2 momentin nojalla.

Jos telekuuntelun, telekuuntelun sijasta tapahtuvan tietojen hankkimisen, teknisen kuuntelun, teknisen katselun, radiosignaalitiedustelun tai tietoliikennetiedustelun aikana tai muulloin ilmenee, että kyseessä on viesti, jonka kuuntelu ja katselu on kielletty, toimenpide on keskeytettävä ja sillä saadut tallenteet ja sillä

82 §

Tiedustelukiellot

Telekuuntelua, telekuuntelun sijasta toimitettavaa tietojen hankkimista, teknistä kuuntelua, teknistä katselua, teknistä laitetarkkailua, radiosignaalitiedustelua, valtiolliseen toimijaan Suomessa kohdistuvaa tietojärjestelmätiedustelua tai tietoliikennetiedustelua ei saa kohdistaa sellaiseen viestintään tai tietoon, josta osapuoli ei saa todistaa tai josta hänellä on oikeus olla todistamatta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n tai 22 §:n 2 momentin nojalla.

Jos telekuuntelun, telekuuntelun sijasta tapahtuvan tietojen hankkimisen, teknisen kuuntelun, teknisen katselun, *teknisen laitetarkkailun,* radiosignaalitiedustelun, *valtiollisen toimijan tietojärjestelmään*

Voimassa oleva laki	*Ehdotus*
saatuja tietoja koskevat muistiinpanot on hävitettävä välittömästi.	*kotimaassa kohdistuva tiedustelun* tai tietoliikennetiedustelun aikana tai muulloin ilmenee, että kyseessä on viesti, jonka kuuntelu ja katselu on kielletty, toimenpide on keskeytettävä ja sillä saadut tallenteet ja sillä saatuja tietoja koskevat muistiinpanot on hävitettävä välittömästi.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
85 §	85 §
Telekuuntelun, teknisen kuuntelun, radiosignaalitiedustelun, teknisen laitetarkkailun ja paikkatiedustelun keskeyttäminen	***Tiedustelumenetelmän käytön*** *keskeyttäminen*
Jos käy ilmi, että telekuuntelu kohdistuu muuhun kuin luvan kohteena olevalta henkilöltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin taikka että teknisen kuuntelun kohteena oleva henkilö ei oleskele kuunneltavassa tilassa tai muussa paikassa, tiedustelumenetelmän käyttö on siltä osin keskeytettävä niin pian kuin mahdollista sekä kuuntelulla saadut tallenteet ja sillä saatuja tietoja koskevat muistiinpanot heti hävitettävä.	Jos käy ilmi, että telekuuntelu *tai televalvonta* kohdistuu muuhun kuin luvan kohteena olevalta henkilöltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin taikka että teknisen kuuntelun kohteena oleva henkilö ei oleskele kuunneltavassa tilassa tai muussa paikassa, tiedustelumenetelmän käyttö on *tältä* osin keskeytettävä niin pian kuin mahdollista sekä *tällaiset* kuuntelulla saadut tallenteet *ja televalvonnalla saadut tiedot sekä tällaisilla tiedustelumenetelmillä saatuja tietoja koskevat muistiinpanot on hävitettävä heti.*
Velvollisuus keskeyttämiseen sekä tallenteiden ja muistiinpanojen hävittämiseen koskee radiosignaalitiedustelua, jos käy ilmi, että radiosignaalitiedustelu kohdistuu muun kuin valtiollisen toimijan viestin sisältöön.	Velvollisuus keskeyttämiseen sekä tallenteiden ja muistiinpanojen hävittämiseen koskee radiosignaalitiedustelua, jos käy ilmi, että radiosignaalitiedustelu kohdistuu muun kuin valtiollisen toimijan viestin sisältöön.
Velvollisuus keskeyttämiseen sekä tallenteiden ja muistiinpanojen hävittämiseen koskee teknistä laitetarkkailua, jos käy ilmi, että *32 §:n 4 momentissa tarkoitettu henkilö ei käytä tarkkailun kohteena olevaa laitetta.*	Velvollisuus keskeyttämiseen sekä tallenteiden ja muistiinpanojen hävittämiseen koskee *myös* teknistä laitetarkkailua, jos käy ilmi, että *tarkkailu kohdistuu sellaiseen luottamukselliseen viestiin, jota koskevasta telekuuntelusta, televalvonnasta ja muusta teknisestä tarkkailusta kuin laitetarkkailusta säädetään 4 luvussa, taikka että toimenpiteen kohteena oleva henkilö ei käytä tarkkailun kohteena olevaa laitetta tai ohjelmistoa.*
(uusi)	*Jos käy ilmi, että valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvatiedustelu kohdistuu sellaiseen tietojenkäsittelylaitteeseen, tiedonsiirtolaitteeseen tai tietoja käsittelevään ohjelmistoon, joka ei kuulu*

Voimassa oleva laki

Jos paikkatiedustelun aikana ilmenee, että tiedustelu on kohdistunut tietoon, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20 tai 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, on tiedustelu siltä osin heti keskeytettävä ja tietoa koskevat muistiinpanot ja jäljennökset heti hävitettävä.

Muu kuin 4 momentissa tarkoitettu tieto voidaan kuitenkin säilyttää ja tallettaa, jos tieto on tarpeen 79 tai 80 §:ssä tarkoitetuissa tapauksissa.

86 §

Tietoliikennetiedustelulla hankittujen tietojen hävittäminen

Sen lisäksi, mitä 82 §:n 2 momentissa säädetään, tietoliikennetiedustelulla saatu tieto on hävitettävä viipymättä sen jälkeen, jos on käynyt ilmi, että:

1) viestinnän molemmat osapuolet olivat Suomessa silloin, kun viestintä tapahtui; tai

2) lähettäjällä tai vastaanottajalla taikka tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta kyseisestä tiedosta 82 §:n 1 momentissa mainittujen säännösten nojalla.

Hävittämisestä vastaa sotilastiedusteluviranomainen. Jos Puolustusvoimien tiedustelulaitos on toimittanut tiedot suojelupoliisille tietoliikennetiedustelun teknisessä toteuttamisessa suojelupoliisin puolesta, hävittämisestä vastaa suojelupoliisi.

Ehdotus

luvan kohteena olevaan tietojärjestelmään, on valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuva tiedustelu tältä osin keskeytettävä niin pian kuin mahdollista ja sillä saadut tallenteet ja tiedot sekä saatuja tietoja koskevat muistiinpanot on hävitettävä heti.

Jos paikkatiedustelun aikana ilmenee, että tiedustelu on kohdistunut tietoon, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20 tai 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, on tiedustelu siltä osin heti keskeytettävä ja tietoa koskevat muistiinpanot ja jäljennökset heti hävitettävä. *Muu kuin tässä momentissa tarkoitettu tieto voidaan kuitenkin säilyttää ja tallettaa, jos tieto on tarpeen 79 tai 80 §:ssä tarkoitetuissa tapauksissa.*

86 §

Tietoliikennetiedustelulla hankittujen tietojen hävittäminen

Sen lisäksi, mitä 82 §:n 2 momentissa säädetään, tietoliikennetiedustelulla saatu tieto on hävitettävä viipymättä sen jälkeen, jos on käynyt ilmi, että:

1) viestinnän molemmat osapuolet olivat Suomessa silloin, kun viestintä tapahtui;

2) lähettäjällä tai vastaanottajalla taikka tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta kyseisestä tiedosta 82 §:n 1 momentissa mainittujen säännösten nojalla;

3) tietoa ei tarvita maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi.

Hävittämisestä vastaa sotilastiedusteluviranomainen. Jos Puolustusvoimien tiedustelulaitos on toimittanut tiedot suojelupoliisille tietoliikennetiedustelun teknisessä toteuttamisessa suojelupoliisin puolesta, hävittämisestä vastaa suojelupoliisi.

Voimassa oleva laki

89 §

Tiedustelumenetelmän käytöstä ilmoittaminen

Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta ja teknisen tarkkailun käytöstä sekä viestiin kohdistuvasta jäljentämisestä ja viestiin kohdistuvasta lähetyksen jäljentämisestä on viipymättä ilmoitettava tiedonhankinnan kohteena olleelle henkilölle kirjallisesti sen jälkeen, kun tiedustelumenetelmän käytön tarkoitus on saavutettu.

Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta on ilmoitettava tiedonhankinnan kohteena olleelle henkilölle kirjallisesti sen jälkeen, kun tiedustelumenetelmän käytön tarkoitus on saavutettu, ja jos käsittelyssä on manuaalisesti selvitetty tietoliikennetiedustelun suorittamisen hetkellä Suomessa olevan henkilön luottamuksellisen viestin tunnistamistiedot tai sisältö. Velvollisuutta ilmoittaa ei kuitenkaan ole, jos tietoliikennetiedustelulla saatu tieto on hävitetty 86 §:n perusteella.

Tiedustelumenetelmän käytöstä on kuitenkin ilmoitettava tiedonhankinnan kohteelle viimeistään vuoden kuluttua sen käytön lopettamisesta.

Jos tiedonhankinnan kohteena olevan henkilöllisyys ei ole tiedossa 1–3 momentissa tarkoitetun määräajan tai lykkäyksen päättyessä, tiedustelumenetelmän käytöstä on ilmoitettava kirjallisesti hänelle ilman aiheetonta viivytystä henkilöllisyyden selvittyä.

Kohteelle ilmoittamisesta on samalla annettava kirjallisesti tieto luvan myöntäneelle tuomioistuimelle.

Tuomioistuin voi pääesikunnan tiedustelupäällikön tai tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta päättää, että 1 ja 2 momentissa tarkoitettua ilmoitusta tiedonhankinnan kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on

Ehdotus

89 §

Ilmoitusvelvollisuus

Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta ja teknisen tarkkailun käytöstä sekä viestiin kohdistuvasta jäljentämisestä ja viestiin kohdistuvasta lähetyksen jäljentämisestä on viipymättä ilmoitettava tiedonhankinnan kohteena olleelle henkilölle sen jälkeen, kun tiedustelumenetelmän käytön tarkoitus on saavutettu.

(kumotaan)

Voimassa oleva laki

perusteltua käynnissä olevan tiedustelumenetelmän käytön turvaamiseksi, maanpuolustuksen kannalta tai kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saadaan tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi taikka hengen tai terveyden suojaamiseksi.

Suunnitelmallisesta tarkkailusta, peitellystä tiedonhankinnasta, peitetoiminnasta, valeostosta, tietolähteen ohjatusta käytöstä, paikkatiedustelusta, muuhun kuin viestiin kohdistuvasta jäljentämisestä ja muuhun kuin viestiin kohdistuvasta lähetyksen jäljentämisestä ei ole velvollisuutta ilmoittaa tiedonhankinnan kohteelle, jos asiassa ei ole aloitettu esitutkintaa 79 tai 80 §:ssä tarkoitetun ilmoituksen perusteella. Jos esitutkinta aloitetaan, noudatetaan, mitä pakkokeinolain (806/2011) 10 luvun 60 §:n 2–7 momentissa säädetään.

(uusi)

Tiedustelumenetelmän käytöstä ei ole velvollisuutta ilmoittaa tiedustelumenetelmän käytön kohteelle, jos kohteena on ollut valtiollinen toimija.

Ilmoitusta koskevan asian käsittelyssä tuomioistuimessa noudatetaan, mitä 116 §:ssä säädetään.

(uusi)

Ehdotus

Suunnitelmallisesta tarkkailusta, peitellystä tiedonhankinnasta, peitetoiminnasta, valeostosta, tietolähteen ohjatusta käytöstä, paikkatiedustelusta, muuhun kuin viestiin kohdistuvasta jäljentämisestä ja muuhun kuin viestiin kohdistuvasta lähetyksen jäljentämisestä ei ole velvollisuutta ilmoittaa tiedonhankinnan kohteelle, jos asiassa ei ole aloitettu esitutkintaa 79 tai 80 §:ssä tarkoitetun ilmoituksen perusteella. Jos esitutkinta aloitetaan, noudatetaan, mitä pakkokeinolain (806/2011) 10 luvun 60 §:n 2–7 momentissa säädetään.

Silloin, kun käsitellään pakkokeinolain 10 luvun 60 §:n 3 momentissa tarkoitettua tiedustelumenetelmän käyttöä koskevan ilmoituksen lykkäämistä tai ilmoituksen tekemättä jättämistä, vaatimuksen tekee tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

Tiedustelumenetelmän käytöstä ei ole velvollisuutta ilmoittaa tiedustelumenetelmän käytön kohteelle, jos kohteena on ollut valtiollinen toimija.

89 a §

Muun kuin valtiollisen toimijan tietoliikennetiedustelusta ilmoittaminen

Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta ei ilmoiteta tiedustelumenetelmän käytön kohteeksi joutuneelle.

Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta

Voimassa oleva laki	*Ehdotus*
	on ilmoitettava osapuolelle, jolla on velvollisuus tai oikeus olla todistamatta tiedosta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n taikka 22 §:n 2 momentin nojalla, jos tieto, josta on oikeus tai velvollisuus olla todistamatta, on selvitetty tietoliikennetiedustelussa. Velvollisuutta ilmoittaa ei kuitenkaan ole, jos tietoliikennetiedustelulla saatu tieto on hävitetty 85 tai 86 §:n perusteella.
(uusi)	89 b §
	Ilmoituksen tekeminen, lykkääminen ja tekemättä jättäminen
	Ilmoitus 89 §:ssä tai 89 a §:n 2 momentissa tarkoitetulle henkilölle on tehtävä viipymättä kirjallisesti sen jälkeen, kun edellä tarkoitetun tiedustelumenetelmän käytön tarkoitus on saavutettu. Tiedustelumenetelmän käytöstä on kuitenkin ilmoitettava mainituissa lainkohdissa tarkoitetulle henkilölle viimeistään vuoden kuluttua tiedustelumenetelmän käytön lopettamisesta. *Jos tiedonhankinnan kohteena olevan henkilöllisyys tai Suomessa oleva asuinpaikka ei ole tiedossa tässä pykälässä tarkoitetun määräajan tai lykkäyksen päättyessä, tiedustelumenetelmän käytöstä on ilmoitettava kirjallisesti hänelle ilman aiheetonta viivytystä henkilöllisyyden ja Suomessa olevan asuinpaikan selvittyä.* *Tiedonhankinnan kohteelle ilmoittamisesta on samalla annettava kirjallisesti tieto luvan myöntäneelle tuomioistuimelle.* *Tuomioistuin voi pääesikunnan tiedustelupäällikön tai tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta päättää, että 89 §:n 1 momentissa ja 89 a §:n 2 momentissa tarkoitettua ilmoitusta tiedonhankinnan kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedustelumenetelmän käytön turvaamiseksi, maanpuolustuksen kannalta tai kansallisen turvallisuuden*

Voimassa oleva laki	*Ehdotus*
	varmistamiseksi taikka hengen tai terveyden suojaamiseksi. *Ilmoitus saadaan tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi taikka hengen tai terveyden suojaamiseksi.* *Ilmoitusta koskevan asian käsittelyssä tuomioistuimessa noudatetaan, mitä 116 §:ssä säädetään.*
91 §	91 §
Asevelvollisuuslain mukaisessa palveluksessa olevan reserviläisen toimivaltuudet	***Muussa kuin virkasuhteessa olevan toimivaltuudet***
Asevelvollisuuslain (1438/2007) mukaisessa kertausharjoituksessa oleva riittävän koulutuksen saanut reserviläinen saa avustaa sotilastiedusteluviranomaista radiosignaalitiedustelussa, ulkomaan tietojärjestelmätiedustelussa, teknisten tietojen käsittelyssä ja tietoliikennetiedustelun kohdentamisessa.	Asevelvollisuuslain (1438/2007) mukaisessa palveluksessa *tai vapaaehtoisesta maanpuolustuksesta annetun lain (556/2007) 18 ja 19 §:ssä tarkoitetussa vapaaehtoisessa harjoituksessa* oleva riittävän koulutuksen saanut *henkilö* saa *tiedustelutehtävän suorittamiseksi tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa käyttää 4 luvussa tarkoitettuja tiedustelumenetelmiä lukuun ottamatta ohjattua tietolähdetoimintaa, peitetoimintaa ja valeostoa.*
	(kumotaan)
Asevelvollisuuslain 32 §:n 3 momentissa tarkoitettuun kertausharjoitukseen määrätty, mainitun lain 82 §:ssä tarkoitetussa ylimääräisessä palveluksessa oleva tai 86 §:n mukaisen liikekannallepanon aikaiseen palvelukseen määrätty riittävän koulutuksen saanut reserviläinen voi käyttää 1 momentissa säädetyn lisäksi suunnitelmallista tarkkailua, teknistä kuuntelua, teknistä katselua, teknistä seurantaa ja teknistä laitetarkkailua sekä ulkomaan tietojärjestelmätiedustelua tiedustelutehtävän suorittamiseksi. Tässä momentissa tarkoitetussa tiedustelussa ei saa hankkia tietoa viestin sisällöstä.	
	(kumotaan)
Puolustusvoimista annetun lain (551/2007) 47 §:n perusteella sotilastiedusteluviranomaisen palveluksesta eronnut *asevelvollisuuslain mukaisessa kertausharjoituksessa oleva reserviläinen* saa	
	(kumotaan)

Voimassa oleva laki	*Ehdotus*
käyttää 4 luvussa tarkoitettuja tiedustelumenetelmiä.	
Reserviläinen saa käyttää tässä pykälässä tarkoitettuja toimivaltuuksia ainoastaan tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa.	
(uusi)	*Edellä 1 momentissa tarkoitetussa palveluksessa tai harjoituksessa oleva sotilastiedusteluviranomaisen palveluksesta eronnut tiedustelumenetelmien käyttöön erityisesti perehtynyt henkilö saa käyttää tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa 4 luvussa tarkoitettuja tiedustelumenetelmiä.*
93 §	93 §
Asevelvollisuuslain mukaisessa palveluksessa olevan virkavastuu	***Muussa kuin virkasuhteessa olevan virkavastuu***
Asevelvollisuuslain mukaisessa palveluksessa olevaan, joka käyttää 90 tai 91 §:ssä tarkoitettua tiedustelumenetelmää, sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä.	*Henkilöön sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä hänen suorittaessaan tässä laissa tarkoitettuja tehtäviä.*
94 §	94 §
Asevelvollisuuslain mukaisessa palveluksessa olevan vahingonkorvausvastuu	***Muussa kuin virkasuhteessa olevan vahingonkorvausvastuu***
Asevelvollisuuslain mukaisessa palveluksessa olevan reserviläisen tämän lain mukaista tehtävää suorittaessaan aiheuttamasta vahingosta vastaa valtio sen mukaan kuin vahingonkorvauslaissa (412/1974) säädetään.	Tämän lain mukaista tehtävää *suorittavan henkilön* aiheuttamasta vahingosta vastaa valtio sen mukaan kuin vahingonkorvauslaissa (412/1974) säädetään.
Asevelvollisuuslain mukaisessa palveluksessa olevan reserviläisen korvausvastuusta säädetään vahingonkorvauslain 4 luvun 2 §:ssä.	*Vapaaehtoisesta maanpuolustuksesta annetun lain 18 ja 19 §:ssä tarkoitettuun vapaaehtoiseen harjoitukseen osallistuvan korvausvastuuseen hänen suorittaessaan tämän lain mukaista tehtävää sovelletaan vahingonkorvauslain 4 luvun säännöksiä asevelvollisen korvausvastuusta.*
9 luku	9 luku
	Ilmaisukielto, *viestinnän välittäjää, datakeskuspalvelun tarjoajaa* ja

Voimassa oleva laki	*Ehdotus*
Ilmaisukielto, teleyrityksiä ja tiedonsiirtäjää koskevat velvollisuudet ja oikeudet sekä tietojen käyttö ja saanti	**tiedonsiirtäjää koskevat velvollisuudet ja oikeudet sekä tietojen käyttö ja saanti**
96 §	96 §
Teleyrityksen *avustamisvelvollisuus*	***Viestinnän välittäjän ja datakeskuspalvelun tarjoajan*** *avustamisvelvollisuus*
Teleyrityksen on ilman aiheetonta viivytystä tehtävä televerkkoon telekuuntelun ja televalvonnan edellyttämät kytkennät sekä annettava sotilastiedusteluviranomaisen käyttöön telekuuntelun toimeenpanoa varten tarpeelliset tiedot, välineet ja henkilöstö. Sama koskee myös niitä tilanteita, joissa telekuuntelu tai televalvonta toteutetaan sotilastiedusteluviranomaisen toimesta teknisellä laitteella.	*Viestinnän välittäjän ja kyberturvallisuuslain (124/2025) 2 §:n 2 kohdassa tarkoitetun datakeskuspalvelun tarjoajan* on ilman aiheetonta viivytystä tehtävä *viestintäverkkoon tai datakeskuspalveluun telekuuntelun, televalvonnan ja valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvan tiedustelun edellyttämät kytkennät sekä annettava sotilastiedusteluviranomaisen käyttöön* telekuuntelun toimeenpanoa varten tarpeelliset tiedot, välineet ja henkilöstö. Sama koskee myös niitä tilanteita, joissa *sotilastiedusteluviranomainen toteuttaa telekuuntelua, televalvontaa taikka viestintäverkkoon tai datakeskuspalveluun kohdistuvaa valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvaa tiedustelua* teknisellä laitteella. *Viestinnän välittäjän ja datakeskuspalvelun tarjoajan on lisäksi annettava tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen käyttöön hallussaan olevat teknisen seurannan toimeenpanoa varten tarpeelliset tiedot.*
(uusi)	*Sotilastiedusteluviranomaisella sekä toimenpiteen suorittajalla ja avustavalla henkilöstöllä on oikeus telekuuntelua ja viestintäverkkoon kohdistuvaa valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvaa tiedustelua varten tarpeellisen yhteyden kytkemiseksi päästä myös muihin kuin viestinnän välittäjän tai datakeskuspalvelun tarjoajan hallinnassa oleviin tiloihin, ei kuitenkaan vakituiseen asumiseen käytettyihin tiloihin. Toimenpiteestä päättää tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies.*

Voimassa oleva laki	*Ehdotus*
97 §	97 §
Tiedonsiirtäjän velvollisuus myötävaikuttaa tietoliikennetiedustelun edellyttämän liityntäpisteen rakentamiseen ja ylläpitämiseen	*Tiedonsiirtäjän velvollisuus myötävaikuttaa tietoliikennetiedustelun edellyttämän liityntäpisteen rakentamiseen ja ylläpitämiseen*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Jos 1 momentissa tarkoitettua liityntäpistettä ei voida toteuttaa tiedonsiirtäjän myötävaikutuksella, Puolustusvoimien tiedustelulaitoksella on oikeus toteuttaa liityntäpiste tiedonsiirtäjän hallinnoimaan viestintäverkon osaan. Tiedonsiirtäjän tulee mahdollisuuksien mukaan olla paikalla tietoliikennetiedustelun edellyttämää liityntäpistettä toteutettaessa.	Jos 1 momentissa tarkoitettua liityntäpistettä ei voida toteuttaa tiedonsiirtäjän myötävaikutuksella *tai jos se on välttämätöntä tiedustelun suojaamiseksi*, Puolustusvoimien tiedustelulaitoksella on oikeus toteuttaa liityntäpiste tiedonsiirtäjän hallinnoimaan viestintäverkon osaan. *Jollei tiedustelun suojaaminen muuta edellytä,* tiedonsiirtäjän tulee mahdollisuuksien mukaan olla paikalla tietoliikennetiedustelun edellyttämää liityntäpistettä toteutettaessa.
99 §	99 §
Korvaus ***teleyritykselle***	*Korvaus* ***viestinnän välittäjälle ja datakeskuspalvelun tarjoajalle***
Teleyrityksellä on oikeus saada valtion varoista korvaus 96 §:ssä tarkoitetusta sotilastiedusteluviranomaisen avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista siten kuin sähköisen viestinnän palveluista annetun lain 299 §:ssä säädetään. Korvauksen maksamisesta päättää toimenpiteen suorittanut sotilastiedusteluviranomainen.	*Viestinnän välittäjällä ja datakeskuspalvelun tarjoajalla* on oikeus saada valtion varoista korvaus 96 §:ssä tarkoitetusta sotilastiedusteluviranomaisen avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista siten kuin sähköisen viestinnän palveluista annetun lain 299 §:ssä säädetään. Korvauksen maksamisesta päättää toimenpiteen suorittanut sotilastiedusteluviranomainen.
101 §	101 §
Muutoksenhaku korvauspäätökseen	*Muutoksenhaku korvauspäätökseen*
Teleyritykselle tai tiedonsiirtäjälle annettuun korvauspäätökseen saa vaatia oikaisua *siten kuin hallintolaissa (434/2003) säädetään.*	*Viestinnän välittäjälle, datakeskuspalvelun tarjoajalle tai tiedonsiirtäjälle* annettuun korvauspäätökseen saa vaatia oikaisua*. Oikaisuvaatimuksesta säädetään hallintolaissa (434/2003).*
Oikaisuvaatimukseen annettuun päätökseen saa hakea muutosta valittamalla hallinto-oikeuteen siten kuin	*Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).*

Voimassa oleva laki	*Ehdotus*
hallintolainkäyttölaissa (586/1996) säädetään .	*(kumotaan)*
Hallinto-oikeuden päätökseen saa hakea muutosta valittamalla vain, jos korkein hallinto-oikeus myöntää valitusluvan. Hallinto-oikeuden on varattava Liikenne- ja viestintävirastolle tilaisuus tulla kuulluksi.	Hallinto-oikeuden on varattava Liikenne- ja viestintävirastolle tilaisuus tulla kuulluksi.
104 §	104 §
Tietojen saanti yksityiseltä yhteisöltä	*Tietojen saanti yksityiseltä yhteisöltä*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Sotilastiedusteluviranomaisilla on yksittäistapauksessa oikeus pyynnöstä saada *teleyritykseltä ja yhteisötilaajalta* yhteystiedot sellaisesta teleosoitteesta, jota ei mainita julkisessa luettelossa, taikka teleosoitteen tai telepäätelaitteen yksilöivät tiedot, jos tiedot ovat tarpeen tiedustelutehtävän suorittamiseksi. Sotilastiedusteluviranomaisella on vastaava oikeus saada postitoimintaa harjoittavalta yhteisöltä jakeluosoitetietoja.	*Jos tiedot ovat tarpeen tiedustelutehtävän suorittamiseksi,* sotilastiedusteluviranomaisella on yksittäistapauksessa oikeus pyynnöstä saada *viestinnän välittäjältä tai datakeskuspalvelun tarjoajalta* yhteystiedot sellaisesta teleosoitteesta, jota ei mainita julkisessa luettelossa, tai teleosoitteen tai telepäätelaitteen yksilöivät *tai palvelun käyttäjän tai tilaajan tunnistamiseksi tarpeelliset* tiedot. Sotilastiedusteluviranomaisella on vastaava oikeus saada postitoimintaa harjoittavalta yhteisöltä jakeluosoitetietoja.
(uusi)	*Sotilastiedusteluviranomaisella on oikeus saada tässä pykälässä tarkoitetut tiedot viipymättä ja maksutta, jollei laissa toisin säädetä.*
111 §	111 §
Tallenteiden tutkiminen	*Tallenteiden tutkiminen*
Tiedustelumenetelmien käytössä kertyneitä tallenteita saa tutkia vain tuomioistuin ja pääesikunnan tiedustelupäällikkö, sotilastiedusteluviranomaisen tehtävään määrätty *tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu* virkamies taikka tiedusteluvalvontavaltuutettu tai hänen määräämänsä virkamies. *Pääesikunnan tiedustelupäällikön* määräyksestä tai tuomioistuimen osoituksen mukaan tallennetta saa tutkia myös muu kuin edellä tarkoitettu sotilastiedusteluviranomaisen	Tiedustelumenetelmien käytössä kertyneitä tallenteita saa tutkia vain tuomioistuin ja pääesikunnan tiedustelupäällikkö, sotilastiedusteluviranomaisen tehtävään määrätty virkamies taikka tiedusteluvalvontavaltuutettu tai hänen määräämänsä virkamies. Tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen määräyksestä tai tuomioistuimen osoituksen mukaan tallennetta saa tutkia myös muu kuin edellä tarkoitettu sotilastiedusteluviranomaisen virkamies,

Voimassa oleva laki	*Ehdotus*
virkamies, asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankintaa toteutettaessa.	asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankintaa toteutettaessa.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
	Tämä laki tulee voimaan päivänä kuuta 20 .

2.

Laki

puolustusvoimista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään puolustusvoimista annettuun lakiin (551/2007) uusi 8 b ja 8 c §, 36 a §:ään, sellaisena kuin se on laissa 890/2018, uusi 3 momentti seuraavasti:

Voimassa oleva laki	*Ehdotus*
(uusi)	8 b §
	Tiedonhankinta yleisesti saatavilla olevista lähteistä
	Puolustusvoimat voi hankkia ja käsitellä tehtäviensä suorittamiseksi tietoa yleisesti saatavilla olevista lähteistä.
	Puolustusvoimilla on oikeus käyttää teknisiä laitteita, menetelmiä tai ohjelmistoja tiedon hakemiseen ja tallentamiseen 1 momentissa tarkoitetusta lähteestä.
	Puolustusvoimat saa käyttää 1 momentissa tarkoitetun tiedonhaun suojaamisessa tehtävän salaamiseksi vääriä, harhauttavia tai peiteltyjä tietoja.
	Pääesikunta tekee päätöksen niistä Puolustusvoimien hallintoyksiköistä, joilla on oikeus käyttää 3 momentissa tarkoitettua tiedonhankinnan suojaamista.
	Edellä 4 momentissa tarkoitetun hallintoyksikön päällikkö päättää 3 momentissa tarkoitetusta tiedonhankinnan suojaamisesta.

Voimassa oleva laki	*Ehdotus*
(uusi)	8 c § *Yleisesti saatavilla olevista lähteistä hankitun tiedon hävittäminen* *Edellä 8 b §:ssä tarkoitetussa tiedonhankinnassa saatu tieto on hävitettävä viipymättä sen jälkeen, kun on käynyt ilmi, ettei tietoa tarvita Puolustusvoimien tehtävien suorittamiseksi.* *Henkilötietojen käsittelystä säädetään henkilötietojen käsittelystä Puolustusvoimissa annetussa laissa (332/2019).*
36 a § *Viran haettavaksi julistaminen*	36 a § *Viran haettavaksi julistaminen*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
(uusi)	*Täytettäessä muuta kuin 2 momentissa tarkoitettu virkaa tai virkasuhdetta hakumenettelyssä Puolustusvoimat voi jättää ilmoittamatta virkaa tai virkasuhdetta hakeneiden nimet sekä nimitetyn nimen muille hakijoille, jos haettavan tehtävän luonne sitä välttämättä edellyttää. Viran tai virkasuhteen täyttämisestä on kuitenkin ilmoitettava hakijoille ja nimityspäätöksessä on mainittava täytettävänä ollut virka tai virkasuhde, päätöksen tehnyt viranomainen sekä nimityspäivä.* Tämä laki tulee voimaan päivänä kuuta 20 .

3.

Laki

rikoslain 17 luvun 7 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan rikoslain (39/1889) 17 luvun 7 §:n 2 momentti, sellaisena kuin se osaksi on laissa 650/2004, seuraavasti:

Voimassa oleva laki	*Ehdotus*
7 §	7 §
Valtionrajarikos	*Valtionrajarikos*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Valtionrajarikoksesta ei tuomita ulkomaalaista, joka 1 momentissa tarkoitetun teon johdosta käännytetään tai karkotetaan maasta, eikä ulkomaalaista, joka pakolaisuuden perusteella hakee turvapaikkaa tai oleskelulupaa Suomessa. Valtionrajarikoksesta ei tuomita myöskään ulkomaalaista, joka on tehnyt 1 momentissa tarkoitetun teon sen vuoksi, että hän on ollut 25 luvun 3 tai 3 a §:ssä tarkoitetun ihmiskaupan kohteena.	Valtionrajarikoksesta ei tuomita ulkomaalaista, joka 1 momentissa tarkoitetun teon johdosta käännytetään tai karkotetaan maasta, eikä ulkomaalaista, joka pakolaisuuden perusteella hakee turvapaikkaa tai oleskelulupaa Suomessa. Valtionrajarikoksesta ei tuomita myöskään ulkomaalaista, joka on tehnyt 1 momentissa tarkoitetun teon sen vuoksi, että hän on ollut 25 luvun 3 tai 3 a §:ssä tarkoitetun ihmiskaupan *kohteena tai joka on tehnyt 1 momentissa tarkoitetun teon sotilastiedustelusta annetun lain 78 a §:n 2 momentin perusteella*.
	Tämä laki tulee voimaan päivänä kuuta 20 .

4.

Laki

Finanssivalvonnasta annetun lain 71 d §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan Finanssivalvonnasta annetun lain (878/2008) 71 d §, sellaisena kuin se on laissa 276/2025, seuraavasti:

Voimassa oleva laki	*Ehdotus*
71 d §	71 d §
Oikeus luovuttaa tietoja suojelupoliisille ja sotilastiedusteluviranomaiselle	*Oikeus luovuttaa tietoja suojelupoliisille ja sotilastiedusteluviranomaiselle*
Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa säädetään, Finanssivalvonnalla on oikeus luovuttaa salassapitosäännösten estämättä pyynnöstä tietoja suojelupoliisille, jos tiedot ovat välttämättömiä suojelupoliisin toimialaan	Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa säädetään, Finanssivalvonnalla on oikeus luovuttaa salassapitosäännösten estämättä pyynnöstä tietoja suojelupoliisille, jos tiedot ovat välttämättömiä suojelupoliisin toimialaan

Voimassa oleva laki	*Ehdotus*
kuuluvien rikosten ennalta estämiseksi ja kansallisen turvallisuuden suojaamiseksi sitä vakavasti uhkaavalta toiminnalta.	kuuluvien rikosten ennalta estämiseksi ja kansallisen turvallisuuden suojaamiseksi sitä vakavasti uhkaavalta toiminnalta *sekä sotilastiedusteluviranomaiselle, jos tiedot ovat välttämättömiä sotilastiedusteluviranomaisen tiedustelutehtävän kannalta.*
Finanssivalvonnalla on oikeus luovuttaa salassapitosäännösten estämättä omaaloitteisesti suojelupoliisille Finanssivalvonnan hallussa olevia tietoja liittyen rahanpesuun tai terrorismin rahoittamiseen, pakotesääntelyn kiertämiseen tai muihin epätavallisiin liiketoimiin liittyvistä järjestelyistä, joilla varoja siirretään kolmansiin maihin ja toimilla epäillään vaarannettavan kansallista turvallisuutta, jos tiedot ovat tarpeellisia suojelupoliisin toimialaan kuuluvien rikosten ennalta estämiseksi ja kansallisen turvallisuuden suojaamiseksi sitä vakavasti uhkaavalta toiminnalta.	Finanssivalvonnalla on oikeus luovuttaa salassapitosäännösten estämättä omaaloitteisesti suojelupoliisille *tai sotilastiedusteluviranomaiselle* Finanssivalvonnan hallussa olevia tietoja liittyen rahanpesuun tai terrorismin rahoittamiseen, pakotesääntelyn kiertämiseen tai muihin epätavallisiin liiketoimiin liittyvistä järjestelyistä, joilla varoja siirretään kolmansiin maihin ja toimilla epäillään vaarannettavan kansallista turvallisuutta, jos tiedot ovat tarpeellisia suojelupoliisin toimialaan kuuluvien rikosten ennalta estämiseksi ja kansallisen turvallisuuden suojaamiseksi sitä vakavasti uhkaavalta toiminnalta *taikka jos tiedot ovat tarpeellisia sotilastiedusteluviranomaisen toimialaan kuuluvan tiedustelutehtävän kannalta*.
Edellä 1 ja 2 momentissa tarkoitettujen tietojen luovuttamiseen sovelletaan, mitä 71 §:n 5 momentissa säädetään.	Edellä 1 ja 2 momentissa tarkoitettujen tietojen luovuttamiseen sovelletaan, mitä 71 §:n 5 momentissa säädetään.
	Tämä laki tulee voimaan päivänä kuuta 20 .

5.

Laki

Harmaan talouden selvitysyksiköstä annetun lain 6 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan Harmaan talouden selvitysyksiköstä annetun lain (1207/2010) 6 §:n 1 momentin 40 kohta sellaisena kuin se on laissa 24/2026, sekä

lisätään lakiin Harmaan talouden selvitysyksiköstä (1207/2010) 6 §:n 1 momenttiin, sellaisena kuin se on laeissa 308/2016, 858/2016, 1159/2016, 1413/2016, 1419/2016, 324/2017, 454/2017, 1112/2017, 404/2018, 414/2018, 722/2019, 1399/2019, 624/2020, 488/2021,

690/2021, 1134/2021, 495/2022, 713/2022, 1119/2022, 1327/2022, 1340/2022, 1355/2022, 743/2023, 190/2024, 940/2024, 260/2025, 277/2025 ja 24/2026, uusi 41 kohta seuraavasti:

Voimassa oleva laki	*Ehdotus*
6 §	6 §
Velvoitteidenhoitoselvityksen käyttötarkoitus	*Velvoitteidenhoitoselvityksen käyttötarkoitus*
Velvoitteidenhoitoselvitys laaditaan tukemaan:	Velvoitteidenhoitoselvitys laaditaan tukemaan:
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
40) rahapelilain (10/2026) 10 §:ssä säädetyn luotettavuuden ja sopivuuden selvittämistä.	40) rahapelilain (10/2026) 10 §:ssä säädetyn luotettavuuden ja sopivuuden selvittämistä*;* *41) sotilastiedustelusta annetussa laissa (590/2019) tarkoitettua sotilastiedustelua.*
	Tämä laki tulee voimaan päivänä kuuta 20 .

6.

Laki

tuloverolain 92 b §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan tuloverolain (1535/1992) 92 b §:n 3 kohta, sellaisena kuin se on laissa 404/2025, seuraavasti:

Voimassa oleva laki	*Ehdotus*
92 b §	92 b §
Todistelupalkkiot, vihjepalkkiot ja tietolähdetoiminnasta maksettavat palkkiot	*Todistelupalkkiot, vihjepalkkiot ja tietolähdetoiminnasta maksettavat palkkiot*
Veronalaista tuloa eivät ole:	Veronalaista tuloa eivät ole:
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
3) viranomaisen maksama palkkio sotilastiedustelusta annetussa laissa (590/2019) ja poliisilaissa (872/2011) tarkoitetulle tietolähteelle tiedustelutehtävien hoitamiseksi merkityksellisten tietojen hankkimisesta sekä	3) viranomaisen maksama palkkio sotilastiedustelusta annetussa laissa (590/2019) ja poliisilaissa (872/2011) tarkoitetulle tietolähteelle tiedustelutehtävien hoitamiseksi merkityksellisten tietojen hankkimisesta *tai*

Voimassa oleva laki	*Ehdotus*
rikostorjunnasta Rajavartiolaitoksessa annetussa laissa (108/2018) tarkoitetulle tietolähteelle rajaturvallisuuden ylläpitämiseen liittyvien tehtävien hoitamiseksi merkityksellisten tietojen hankkimisesta	*tiedusteluviranomaisen avustamisesta* sekä rikostorjunnasta Rajavartiolaitoksessa annetussa laissa (108/2018) tarkoitetulle tietolähteelle rajaturvallisuuden ylläpitämiseen liittyvien tehtävien hoitamiseksi merkityksellisten tietojen hankkimisesta. Tämä laki tulee voimaan päivänä kuuta 20 .

7.

Laki

rajavartiolain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan rajavartiolain (578/2005) 3 §:n 3 momentti, sellaisena kuin se on laissa 749/2014, ja

lisätään lakiin uusi 25 a § seuraavasti:

Voimassa oleva laki	*Ehdotus*
3 §	3 §
Rajavartiolaitoksen tehtävät	*Rajavartiolaitoksen tehtävät*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Rajavartiolaitos suorittaa poliisi- ja tullitehtäviä, etsintä-, pelastus- ja ensihoitotehtäviä sekä osallistuu sotilaalliseen maanpuolustukseen. Rajavartiolaitoksen tehtävistä meripelastustoimen alalla säädetään meripelastuslaissa.	Rajavartiolaitos suorittaa poliisi- ja tullitehtäviä *ja* etsintä-, pelastus- ja ensihoitotehtäviä sekä osallistuu sotilaalliseen maanpuolustukseen *ja sotilastiedusteluun*. Rajavartiolaitoksen tehtävistä meripelastustoimen alalla säädetään meripelastuslaissa.
(uusi)	25 a § *Rajavartiolaitoksen osallistuminen sotilastiedusteluun* *Rajavartiolaitos osallistuu sotilastiedusteluviranomaisen pyynnöstä*

Voimassa oleva laki	*Ehdotus*
	sotilastiedusteluun hankkimalla tietoja ja tekemällä toimenpiteitä sotilastiedusteluviranomaisten tiedustelutehtävien tukemiseksi. *Rajavartiolaitoksen toimivaltuuksista sotilastiedusteluun osallistumisessa säädetään sotilastiedustelusta annetussa laissa (590/2019).* Tämä laki tulee voimaan päivänä kuuta 20 .

8.

Laki

henkilötietojen käsittelystä Rajavartiolaitoksessa annetun lain 32 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään henkilötietojen käsittelystä Rajavartiolaitoksessa annetun lain (639/2019) 32 §:ään, sellaisena kuin se on laissa 430/2024, uusi 2 momentti seuraavasti:

Voimassa oleva laki	*Ehdotus*
32 §	32 §
Henkilötietojen luovuttaminen toiselle rikosasioiden tietosuojalaissa tarkoitetulle toimivaltaiselle viranomaiselle	*Henkilötietojen luovuttaminen toiselle rikosasioiden tietosuojalaissa tarkoitetulle toimivaltaiselle viranomaiselle*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
(uusi)	*Rajavartiolaitos saa luovuttaa salassapitosäännösten estämättä 15 b §:ssä tarkoitettuja tietoja Puolustusvoimille sotilastiedustelusta annetussa laissa (590/2019) säädettyjä tehtäviä varten.* Tämä laki tulee voimaan päivänä kuuta 20 .

9.

Laki

henkilötietojen käsittelystä Puolustusvoimissa annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään henkilötietojen käsittelystä Puolustusvoimissa annettuun lakiin (332/2019) uusi 37 a § seuraavasti:

Voimassa oleva laki	*Ehdotus*
(uusi)	37 a § *Sotilastiedusteluviranomaisen oikeus ylläpitää henkilörekisteriään* *Jos rekisterinpitäjälle on muualla laissa säädetty oikeus salassapitosäännösten estämättä luovuttaa henkilörekisteristään teknisen käyttöyhteyden avulla tai tietojoukkona henkilötietoja Puolustusvoimille, sotilastiedusteluviranomainen saa tietojärjestelmänsä ylläpitämiseksi verrata kyseisen henkilörekisterin tietoja talletettujen henkilötietojensa sisältöön. Tarpeettomat tiedot on hävitettävä viipymättä sen jälkeen kuin vertailu on suoritettu. Tarpeettomia henkilötietoja ei saa tallettaa.* *Jos tietojen käsittelyn alkuperäiseksi tai muuksi kuin alkuperäiseksi käyttötarkoitukseksi on säädetty maanpuolustus tai kansallinen turvallisuus, sotilastiedusteluviranomaisella on lisäksi salassapitosäännösten estämättä oikeus verrata tietojärjestelmässään toisesta tietojärjestelmästä kerättyä tietojoukkoa, jos menettely on välttämätön tietojen käsittelyn mahdollistamiseksi korkean tietoturvatason tietojärjestelmässä. Tietojoukko on hävitettävä viipymättä sen jälkeen, kun tarve vertailulle on päättynyt. Vertaamista varten kerättävät tiedot on pidettävä erillään muista sotilastiedusteluviranomaisen käsittelemistä tiedoista.* Tämä laki tulee voimaan päivänä kuuta 20 .