Hallintopoliittinen osasto
Lainvalmistelu- ja oikeusyksikkö
Vanhempi hallitussihteeri Kosti Honkanen

Eduskunnan perustuslakivaliokunnalle

Hallituksen esitys sotilastiedustelusta annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi (HE 106/2026 vp.)

1. Johdanto

Hallituksen esityksessä HE 104/2026 vp ehdotetaan muutettavaksi sotilastiedustelusta annettua lakia ja eräitä siihen liittyviä lakeja. Esityksen tavoitteena on saattaa sotilastiedustelua koskeva sääntely vastaamaan turvallisuus- ja kybertoimintaympäristön muutosta, teknologista kehitystä sekä voimassa olevan lainsäädännön soveltamisessa havaittuja muutostarpeita. Ehdotuksilla parannettaisiin sotilastiedusteluviranomaisen mahdollisuuksia hankkia aikaisempaa tarkemmin ja kohdennetummin tietoa sotilastiedustelun kohteista, turvattaisiin viranomaisen toimintakyky kansallisesti ja osana liittokuntaa sekä vahvistettaisiin viranomaisten ja muiden toimijoiden välistä yhteistyötä. Hallituksen esitykseen sisältyy muun muassa tietoliikennetiedustelun teknisten tietojen käsittelyä, hakuehtojen määrittämistä ja tietojen tallentamista koskevia muutoksia, uusia tietojärjestelmätiedustelun toimivaltuuksia, Rajavartiolaitoksen osallistumista sotilastiedusteluun, yleisesti saatavilla olevista lähteistä tapahtuvaa tiedonhankintaa sekä tiedusteluviranomaisten tietojenvaihtoa koskevaa sääntelyä.

Ehdotukset ovat valtiosääntöoikeudellisesti merkityksellisiä erityisesti perustuslain 6 §:ssä turvatun yhdenvertaisuuden, 7 §:ssä turvattujen elämän sekä henkilökohtaisen vapauden ja turvallisuuden, 10 §:ssä turvattujen yksityiselämän, henkilötietojen ja luottamuksellisen viestin salaisuuden, 12 §:ssä turvattujen sananvapauden ja julkisuusperiaatteen, 15 §:ssä turvatun omaisuudensuojan sekä 21 §:ssä turvatun oikeusturvan kannalta. Arvioinnissa on samalla otettava huomioon perustuslain 7 ja 22 §:stä julkiselle vallalle johtuva velvollisuus suojata yksilöitä ja yhteiskuntaa turvallisuusuhkilta. Ehdotuksilla ei muutettaisi sotilastiedustelun aineellisia kohteita, vaan kehitettäisiin toimivaltuuksia ja niiden teknistä toteuttamista laissa jo määriteltyihin, yhteiskunnan kannalta kaikkein vakavimpiin uhkiin kohdistuvan tiedonhankinnan tehostamiseksi. Ehdotusten hyväksyttävyyttä on arvioitava kokonaisuutena ottaen huomioon toimivaltuuksien täsmällinen kohdentaminen, välttämättömyys ja oikeasuhtaisuus, tuomioistuimen ennakkokontrolli, tiedusteluvalvontavaltuutetun riippumaton valvonta sekä tietojen käsittelyä, minimointia ja hävittämistä koskevat oikeusturvatakeet.

2. Vaikutukset perus- ja ihmisoikeuksiin

Hallituksen esityksen ehdotukset ovat merkityksellisiä erityisesti perustuslain 10 §:ssä turvattujen yksityiselämän, henkilötietojen ja luottamuksellisen viestin salaisuuden kannalta. Lisäksi ehdotuksilla on liittymäkohtia yhdenvertaisuuteen, henkilökohtaiseen turvallisuuteen, sananvapauteen ja julkisuusperiaatteeseen, omaisuudensuojaan, elinkeinovapauteen sekä oikeusturvaan. Eräitä ehdotuksia on arvioitava myös Suomen täysivaltaisuuden, julkisen vallan käytön lakisidonnaisuuden, virkavastuun ja julkisen hallintotehtävän antamista koskevien vaatimusten näkökulmasta.

Postiosoite
Postadress
Postal Address
Puolustusministeriö
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
kirjaamo@defmin.fi
www.defmin.fi

Esityksessä ehdotetut teknisten tietojen käsittely, hakuehtojen määrittäminen, tietojen tallentaminen, sisältöön menevät hakuehdot sekä kotimaan tietojärjestelmätiedustelu laajentavat tai täsmentävät sotilastiedusteluviranomaisen mahdollisuuksia käsitellä sähköistä viestintää ja tietojärjestelmissä olevia tietoja. Ehdotukset merkitsevät siten puuttumista yksityiselämän ja luottamuksellisen viestin salaisuuden suojaan. Toisaalta niiden tarkoituksena on parantaa tiedonhankinnan kohdentamista ja vähentää sivullisten tietojen joutumista tiedusteluprosessin myöhempiin, yksityisyyteen voimakkaammin puuttuviin käsittelyvaiheisiin.

Perustuslain 10 §:n 4 momentin kannalta ehdotusten hyväksyttävyyttä tukee se, että tiedonhankinta kohdistuu edelleen vain sotilaalliseen toimintaan tai kansallista turvallisuutta vakavasti uhkaavaan toimintaan. Esityksellä ei lähtökohtaisesti laajenneta sotilastiedustelun aineellista kohdealaa, vaan kehitetään keinoja hankkia tietoa jo laissa määritellyistä kohteista muuttuneessa teknologisessa toimintaympäristössä. Keskeisiä oikeasuhtaisuuden takeita ovat toimivaltuuksien välttämättömyys, täsmällinen kohdentaminen, vähimmän haitan periaate, tuomioistuimen ennakkokontrolli, tiedusteluvalvontavaltuutetun riippumaton valvonta sekä tarpeettomien ja tiedustelukiellon alaisten tietojen hävittäminen.

Tietojen tallentaminen lisää puuttumista yksityisyyden suojaan, koska se mahdollistaa aineiston myöhemmän käsittelyn ja analysoinnin. Puuttumista rajoittavat kuitenkin tallennettavan tietomäärän lakisääteinen rajaus, määräaikaiset säilytysajat, automaattinen hävittäminen sekä se, että tallennettujen tietojen käyttäminen tiedustelutarkoituksiin edellyttää erillistä, tuomioistuimen luvan perusteella käytettävää tiedustelumenetelmää. Tietojen käsittelystä muodostettavat lokitiedot mahdollistavat käytön yhdistämisen tiettyyn lupaan ja toiminnan jälkikäteisen valvonnan

Sisältöön menevien hakuehtojen salliminen merkitsee laadullisesti merkittävää puuttumista luottamuksellisen viestin salaisuuteen. Ehdotuksen tarkoituksena ei kuitenkaan ole yleinen viestien sisällön seuranta, vaan tiedonhankinnan rajaaminen tilanteissa, joissa tekniset hakuehdot eivät erottele tiedustelun kohteeseen liittyvää tietoliikennettä riittävän tarkasti. Kun sisällöllistä hakuehtoa käytetään yhdessä muiden kohdentavien hakuehtojen kanssa, se voi vähentää jatkokäsittelyyn valikoituvan sivullisen viestinnän määrää. Hakuehtoa ei saa käyttää yleiseen aihepiiri-, mielipide- tai henkilöryhmäperusteiseen seurantaan, vaan sillä on oltava yksilöity yhteys tuomioistuimen luvassa tarkoitettuun toimintaan.

Tietoliikennetiedustelun ilmoitusvelvollisuudesta luopuminen on merkityksellinen perustuslain 21 §:ssä turvatun oikeusturvan kannalta, koska henkilö ei ilman ilmoitusta välttämättä tiedä joutuneensa tiedustelun kohteeksi. Ilmoittaminen voisi tietoliikennetiedustelun erityisluonteen vuoksi kuitenkin edellyttää tiedustelutehtävän kannalta tarpeettomia henkilöllisyyden selvittämistoimia sekä paljastaa tiedustelun kohdentamista, menetelmiä tai pitkäkestoisia tietotarpeita. Oikeusturvan painopiste siirtyisi tällöin henkilökohtaisesta jälkikäteisilmoituksesta tiedusteluvalvontavaltuutetun oma-aloitteiseen ja koko tiedusteluketjun kattavaan valvontaan. Henkilöllä säilyisi lisäksi mahdollisuus tehdä valtuutetulle tutkimispyyntö.

Sotilastiedusteluviranomaisen ulkopuolisten henkilöiden, Rajavartiolaitoksen ja ulkomaisen virkamiehen osallistumista koskevissa ehdotuksissa keskeistä on, että tiedustelumenetelmän käytön edellytysten arviointi, kohdentaminen ja päätöksenteko säilyvät suomalaisella sotilastiedusteluviranomaisella. Avustavalle toimijalle ei annettaisi itsenäistä harkintavaltaa perusoikeuksiin puuttumisesta. Viranomainen vastaisi toiminnan

lainmukaisuudesta, ja toiminta tapahtuisi sen ohjauksessa ja valvonnassa. Näin rajattuna ehdotukset eivät merkitse merkittävän julkisen vallan tai sotilastiedustelutehtävän siirtämistä viranomaisorganisaation ulkopuolelle.

Yleisesti saatavilla olevista lähteistä tapahtuva tiedonhankinta ja peitteen käyttäminen ovat merkityksellisiä erityisesti henkilötietojen suojan ja sananvapauden kannalta. Ehdotuksella ei kuitenkaan anneta oikeutta päästä ei-julkisiin tietoihin tai kiertää tietojärjestelmien käyttörajoituksia. Peite suojaa Puolustusvoimiin olevan yhteyden, tiedonhankinnan tarkoituksen ja henkilöstön turvallisuuden, mutta ei muodosta itsenäistä tiedonhankintatoimivaltuutta. Tehtäväsidonnaisuus, tietojen minimointi, käyttötarkoitussidonnaisuus ja henkilötietojen käsittelyä koskeva sääntely rajoittavat tietojen keräämistä ja myöhempää käyttöä.

Esityksellä voidaan arvioida olevan myönteisiä perus- ja ihmisoikeusvaikutuksia. Ehdotukset parantavat viranomaisten kykyä tunnistaa ja torjua sotilaallisia ja kansallista turvallisuutta vakavasti uhkaavia toimia sekä suojata ihmisten henkeä, henkilökohtaista turvallisuutta, omaisuutta ja yhteiskunnan välttämättömien palvelujen jatkuvuutta. Arvioinnissa on siten otettava huomioon perustuslain 7 ja 22 §:stä julkiselle vallalle johtuva velvollisuus turvata perus- ja ihmisoikeuksien toteutuminen myös vakavissa turvallisuusuhkissa.

3. Tietoliikennetiedustelu

Teknisten tietojen käsittely

Ehdotus puuttuisi perustuslain 10 §:ssä säädettyyn yksityisyyden suojaan. Voimassa olevat säännökset on säädetty perustuslakivaliokunnan myötävaikutuksella. Perustuslakivaliokunta on katsonut, että voimassa olevan lain mukainen teknisten tietojen käsittely on lähimpänä tietoliikenteen yleistä valvontaa (PeVL 36/2017 vp.).

Voimassa olevan lain esitöiden mukaan hetkellisyydellä on tarkoitettu lyhyttä ajallista hetkeä tai joka kymmenennentuhannen IP-paketin ottamista tietoliikennevirrasta. Käytännössä sääntely on osoittautunut haastavaksi sen tarkoitukseen nähden.

Esityksen 1. lakiehdotuksen 66 §:n mukaan teknisten tietojen käsittelyn toimivaltuudesta poistettaisiin vaatimus teknisten tietojen käsittelyn hetkellisyydestä. Näin ollen teknisten tietojen käsittelyllä voitaisiin käsitellä tietoliikennettä koko luvan voimassaolonajan, eli sotilastiedusteluviranomainen pystyisi vakituisesti seuraamaan, miltä alueelta tietoliikennettä tulee Suomen rajan yli. Tämä on välttämätöntä oikeiden viestintäverkon osien tunnistamiseksi.

Lisäksi säännösehdotuksen mukaan teknisten tietojen käsittelyä voitaisiin käyttää myös tietoliikenteen reitittymisen ja muutosten seuraamiseksi. Globaalissa tietoliikenneverkossa tapahtuu alituiseen muutoksia tietoliikenteen reitittymisessä ja käytettävässä teknologiassa. Reitittymisessä tapahtuvien muutosten seuraaminen on välttämätöntä tietoliikenteen liikkumisen säännönmukaisuuksien tunnistamiseksi ja sen tunnistamiseksi teknisellä tasolla, kohdistuuko tietoliikennetiedustelun toimivaltuudet oikeaan viestintäverkon osaan.

Tietoliikenteen muutoksilla tarkoitettaisiin myös globaalin viestintäverkon teknologiassa tapahtuvia muutoksia. Tämä on välttämätöntä, jotta tietoliikennetiedustelujärjestelmäl-

lä pystytään tehokkaasti tuottamaan haluttua tietoa ja että resurssit on kohdennettu käytettävän teknologian kannalta oikein.

Teknisten tietojen käsittelyä koskevan toimivaltuuden tarkoituksena ei ole hankkia tietoa viestinnän sisällöstä tai yksittäisten henkilöiden toiminnasta, vaan tunnistaa tietoliikennetiedustelun teknisen toteuttamisen kannalta merkityksellinen viestintäverkon osa sekä tietoliikenteen reitittyminen ja siinä tapahtuvat muutokset. Toimivaltuus on tarpeen, koska tietoliikenteen reitittyminen, tekniset rakenteet ja käytetyt palvelut muuttuvat nopeasti. Ilman ajantasaista teknistä tietoa tietoliikennetiedustelua ei voida kohdistaa riittävän luotettavasti siihen viestintäverkon osaan, jossa tiedustelutehtävän kannalta merkityksellisen tietoliikenteen voidaan perustellusti olettaa kulkevan. Hallituksen esityksessä teknisten tietojen käsittely kytketään nimenomaan viestintäverkon osan sekä tietoliikenteen reitittymisen ja siinä tapahtuvien muutosten tunnistamiseen ja varsinaisen tietoliikennetiedustelun tarkempaan kohdentamiseen.

Teknisten tietojen käsittely toimii siten tietoliikennetiedustelua edeltävänä kohdentamis- ja minimointimekanismina. Sen avulla voidaan välttää tiedustelun kohdistaminen sellaisiin viestintäverkon osiin, joissa tiedustelun kohteeseen liittyvää tietoliikennettä ei kulje, sekä vähentää sivullisten tietoliikenteen joutumista varsinaisen tietoliikennetiedustelun piiriin. Toimivaltuus ei laajenna tiedustelun aineellisia kohteita, vaan parantaa edellytyksiä rajata myöhempi tiedonhankinta vain laissa tarkoitetun tiedustelutehtävän kannalta välttämättömään tietoliikenteeseen.

Vaikka teknisten tietojen käsittely ei kohdistu viestin semanttiseen sisältöön, sääntelyn kohteena olevat tiedot voivat kuulua perustuslain 10 §:ssä turvatun yksityiselämän ja luottamuksellisen viestin salaisuuden piiriin. Ehdotuksen perusoikeusvaikutuksia rajoittavat kuitenkin käsiteltävien tietojen tekninen luonne, käsittelyn täsmällisesti rajattu tarkoitus, käsittelyn automatisointi sekä se, ettei toimivaltuutta saa käyttää viestinnän sisällön selvittämiseen tai kohteiden toiminnan yleiseen kartoittamiseen. Käsittelyä rajoittavat lisäksi välttämättömyys, suhteellisuus, vähimmän haitan periaate, tarkoitussidonnaisuus, tietojen minimointi, säilytysajan rajallisuus sekä tarpeettomien tietojen hävittämisvelvollisuus.

Ilman mahdollisuutta selvittää tietoliikenteen muuttuvia reittejä varsinaista tiedustelua jouduttaisiin kohdistamaan laajempiin viestintäverkon osiin tai vanhentuneiden teknisten tietojen perusteella. Tämä voisi lisätä sivullisten tietoliikenteeseen kohdistuvaa puuttumista. Teknisten tietojen rajattu käsittely aikaisemmassa vaiheessa merkitsee siten vähäisempää puuttumista yksityisyyteen kuin heikommin kohdennettu varsinainen tietoliikennetiedustelu.

Näin rajattuna teknisten tietojen käsittely ei muodosta itsenäistä toimivaltuutta tietojen hankkimiseksi henkilöistä tai viestinnän sisällöstä, vaan teknisen välineen, jolla varmistetaan varsinaisen tietoliikennetiedustelun täsmällinen ja oikeasuhtainen kohdentaminen. Toimivallan voidaan tämän vuoksi katsoa olevan perustuslain 10 §:ssä tarkoitetun tiedonhankinnan välttämätön ja yksityisyyden suojaa osaltaan vahvistava toiminto.

Hakuehtojen määrittäminen

Esityksen 1. lakiehdotuksen 67 a §:ssä säädettäisiin sotilastiedusteluviranomaiselle uusi hakuehtojen määrittämistä koskeva toimivaltuus. Ehdotuksen mukaan sotilastiedusteluviranomainen voisi käsitellä tietoliikennevirtaa sen konekielisessä muodossa määrittääkseen uusia sotilastiedustelun kohdetta kuvaavia hakuehtoja.

Etenkin sotilastiedusteluviranomaisen kohteiden kiihtynyt teknologinen kehittäminen ja lisääntyneet resurssit ovat johtaneet kiihtyvään tietojärjestelmien ja uusien tietoliikenteen salaustekniikoiden kehittämiseen. Nykyisen lainmukaisilla tietoliikennetiedustelulla ja siinä käytettävillä hakuehdoilla ei pystytä hankkimaan tehokkaasti tietoa muuttuneiden tietojärjestelmien tuottamasta tiedosta.

Tietojärjestelmän ja sen käyttäjän tuottamaan tietoliikenteeseen vaikuttavat keskeisesti protokolla, joiden avulla toisistaan eroavat laitteet pystyvät käsittelemään tietoa tarkoitetulla tavalla. Käytettävät protokollat myös vaikuttavat siihen, miltä tietoliikennevirta näyttää. Tietoliikennevirtaan vaikuttavat

Säännösehdotuksen tarkoittamassa tilanteessa sotilastiedusteluviranomaisella olisi oletus tietoliikenteen säännönmukaisuudesta tai ominaispiirteestä, eli siitä, miltä tietojärjestelmän tuottama tietoliikennevirta näyttää. Esimerkiksi nykyisin hakuehdot voivat kohdistua tietojärjestelmään, jonka tuottama tietoliikennevirta näyttää muun muassa käytettyjen ohjelmistojen, laitteiden ja protokollien myötä tietyltä. Käytetyt hakuehdot eivät kuitenkaan kohdistu tietojärjestelmän rinnakkaisjärjestelmään, koska siihen kohdistuvia hakuehtoja ei ole eikä niitä voida tunnistaa nykyisin kohteena olevan tietojärjestelmän tuottamasta tietoliikenteestä. Toisaalta on tiedossa, että rinnakkaistietojärjestelmä käyttää pitkälti samoja teknologisia ratkaisuja, mutta rikkaistietojärjestelmään kohdistuvia tarkkoja hakuehtoja ei pystytä muodostamaan saatavien tietojen perusteella.

Hakuehtojen määrittämisessä olisi kyse tietoliikennevirran analysoinnista sen konekielisessä muodossa, joka ei ole suoraan kielellisesti ymmärrettävässä muodossa. Tietoliikennevirrasta tunnistettaisiin kohteen käyttämien tietojärjestelmien tuottaman tietoliikennevirran säännönmukaisuuksia tai ominaispiirteitä ja tätä tietoliikennevirran osaa analysoimalla pystyttäisiin määrittämään tarkempia hakuehtoja.

Säännösehdotuksen mukaan määrittäminen voisi kohdistua korkeintaan viiteen prosenttiin kohteena olevan viestintäverkon osan kapasiteetista, eli käsittelyn kohteena voisi olla 5 prosenttia esimerkiksi tietyn Suomen rajan ylittävän valokuidun enimmillään kuljettamasta tietoliikenteen määrästä. Viidessä prosentissa olisi kyse reaaliaikaisuudesta, ei siitä, että määrällinen rajoite kumuloituisi ajan myötä; käsittelyn kohteen oleva tietoliikenteen määrä ei ole suurempi tietyn ajan jälkeen kuin mitä se on nyt.

Esityksen 1. lakiehdotuksen 67 b §:ssä olisi säädetty päätöksenteosta. Säännöksen voidaan katsoa vastaavan sitä, mitä jo nykyisellään on säädetty tietoliikennetiedustelun kokonaisuuteen liittyvistä toimivaltuuksista.

Hakuehtojen määrittämisen osalta keskeisiä elementtejä päätöksenteossa ovat sotilastiedustelun kohde sekä tietoliikenteen oletettu säännönmukaisuus tai ominaispiirre. Perustelujen olisi oltava kattavia ja tarkkoja, ja niiden olisi perustuttava saatuihin kokemuksiin ja tietoihin. Tuomioistuimessa sotilastiedustelun virkamies toimii virkavastuulla ja vastaa antamistaan tiedoista.

Hakuehtojen määrittämistä koskeva toimivaltuus on perusteltu tietoliikennetiedustelun täsmällisen kohdentamisen ja sivullisten viestinnän käsittelyn vähentämisen kannalta. Toimivaltuuden tarkoituksena ei ole laajentaa sotilastiedustelun aineellista kohdealaa eikä hankkia määrittämisvaiheessa itsenäisesti tiedustelutietoa, vaan muodostaa konekielisestä tietoliikenteestä sellaisia teknisiä hakuehtoja, joiden avulla varsinainen tietoliikennetiedustelu voidaan kohdistaa nykyistä tarkemmin

Ehdotus voidaan katsoa toteuttavan perustuslakivaliokunnan korostamaa perustuslain 10 §:n 4 momentin välttämättömyysvaatimusta, jonka mukaan viestin salaisuuteen puuttumisen tulee olla mahdollisimman kohdennettua ja rajoitettua eikä tietoliikennetiedustelu saa muodostua yleiseksi, kohdentamattomaksi ja kaikenkattavaksi tietoliikenteen seurannaksi (PeVM 4/2018 vp, s. 7–9; PeVL 35/2018 vp, s. 7–8 ja 23–24). Määrittämisvaiheen rajattu ja automatisoitu käsittely vähentää sivullisten viestinnän valikoitumista varsinaisen tietoliikennetiedustelun myöhempiin ja yksityisyyteen voimakkaammin puuttuviin käsittelyvaiheisiin.

Valtiosääntöoikeudellista hyväksyttävyyttä voidaan katsoa tukevan myös se, että hakuehdon käsite ja hyväksyttävyyden perusteet on määritelty laissa perustuslakivaliokunnan edellyttämällä tavalla ja että myös määritettävän hakuehdon tulee rajata tiedonhankinta välttämättömään (PeVL 35/2018 vp, s. 23–24; PeVL 36/2018 vp, s. 24; PeVL 76/2018 vp). Toimivaltuuden käyttö edellyttää tuomioistuimen lupaa, kohdistuu laissa tarkoitettuun tiedustelun kohteeseen ja on tiedusteluvalvontavaltuutetun riippumattoman valvonnan alaista. Näin sääntely muodostaa perustuslain 10 §:n kannalta hyväksyttävän ja oikeasuhtaisen keinon hankkia tietoa sotilaallisesta toiminnasta sekä kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.

Tietojen tallentaminen

Esityksen 1. lakiehdotuksen 66 §:n 3 momentin mukaan tietoliikenteen teknisessä käsittelyssä tietoja voitaisiin tallentaa 18 kuukauden ajaksi. Tallennettavien tietojen määrä ei voi ylittää viittä prosenttia kohteena olevan viestintäverkon osan kapasiteetista. Tallennus kohdistuisi niihin tietoihin ja määrä laskettaisiin siitä, mitä teknisten tietojen käsittelyyn tulee. Tallennettujen teknisten tietojen määrä saisi olla korkeintaan 5 prosenttia viestintäverkon osan kapasiteetista kunakin ajankohtana. Tiedot saisivat olla tallessa korkeintaan 18 kuukauden ajan tallentamisajankohdasta, jonka jälkeen ne hävitettäisiin automaattisesti järjestelmästä.

Esityksen 1. lakiehdotuksen 67 b §:n 3 momentin mukaan hakuehtojen määrittämisessä käytettävä tieto, joka voi vastata kunakin ajanhetkenä korkeintaan viittä prosenttia viestintäverkon osan tietoliikennekapasiteetista, voidaan tallentaa korkeintaan 12 kuukauden ajaksi sen tallentamisen ajankohdasta. Ajanjakson jälkeen tiedot hävitettäisiin automaattisesti.

Tallennettuja teknisiä tietoja voisi käyttää teknisten tietojen käsittelyssä, hakuehtojen määrittämisessä ja varsinaisessa tietoliikennetiedustelussa. Hakuehtojen määrittämisessä tallennettuja tietoja voisi käyttää hakuehtojen määrittämisessä ja varsinaisessa tietoliikennetiedustelussa. Jotta tallennettuja tietoja voitaisiin käyttää edellä mainittujen tiedustelumenetelmien osalta, edellyttää se aina tuomioistuimen lupaa.

Tietojen tallentamisen ja niiden käytön voidaan katsoa olevan välttämätöntä tiedonhankinnan tarkemmaksi kohdentamiseksi ja sen varmistamiseksi, että jo mahdollisimman varhaisessa vaiheessa tiedonhankinnassa pystyttäisiin erottelemaan tarpeeton tieto tiedonhankintaprosessin ulkopuolelle.

Tallennusajat on ehdotetussa sääntelyssä rajattu välttämättömään. Teknisten tietojen osalta 18 kuukauden ajanjakson aikana globaalissa viestintäverkossa ja tietoliikenteen reitittymisessä tapahtuu paljon muutoksia, joten 18 kuukautta vanhempia tietoja ei voida pitää enää tarpeellisina.

Hakuehtojen määrittämisessä tallennettavat tiedot voidaan katsoa välttämättömiksi myös 12 kuukauden ajanjakson ylittäviltä osin, mutta koska tallennuksen piiriin sisältyy myös viestin sisältöä, pidempää tallennusaikaa ei voida pitää perusteltuna.

Euroopan ihmisoikeustuomioistuin on viimeisimmissä tietoliikennetiedustelua lähellä olevia järjestelmiä koskevissa ratkaisuissa (Centrum för Rättvisa ja Big Brother Watch) katsonut, että tiedustelumenetelmän käytön eri vaiheissa yksityisyyden suojaan puuttumisen aste on erilainen. Pelkästään tietojen tallentaminen ei puutu syvällisesti henkilön yksityisyyden suojaan, kun taas loppuvaiheessa virkamiehen suorittama tietojen analysointi puuttuu jo syvällisesti suojattuun oikeuteen.

Perustuslakivaliokunta on katsonut lausuntokäytännössään Rajavartiolaitoksen radioteknisen valvonnan osalta, että radiolaitteisiin kohdistuva tietojen hankintaa ja niiden tallentamista voidaan pitää suhteellisen vähäisenä puuttumisena luottamuksellisen viestin salaisuuden suojaan tietyin edellytyksin (PeVL 15/2024, kohdat 12–13).

Lisäksi perustuslakivaliokunta on käytännössään 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.).

Osaltaan tietojen tallentamisen ja niiden käytön voidaan katsoa olevan lähellä ylimääräisen tiedon käyttöä. Perustuslakivaliokunta on katsonut, että ylimääräistä tietoa koskevan sääntelyn arvioinnissa on syytä ottaa huomioon yhtäältä perustuslaissa turvattu luottamuksellisen viestin salaisuuden suoja. Tämän lisäksi perustuslakivaliokunta on rikostorjunnan osalta katsonut, että huomioon on otettava yksityisyyden suojan rajoittamista puoltava vakavien rikosten selvittämisintressiin ja rikosoikeudelliseen järjestelmän uskottavuuteen liittyvät hyväksyttävät ja yhteiskunnallisesti painavat perusteet (PeVL 32/2013 vp., s. 7).

Perustuslakivaliokunta on katsonut viimeaikaisessa käytännössään, 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). Lisäksi Euroopan unionin tuomioistuin on vakiintuneesti arvioinut, että kansalliseen turvallisuuteen (mukaan lukien maanpuolustus) kohdistuva uhka eroaa luonteeltaan, vakavuudeltaan ja uhan muodostavien erityisten olosuhteiden vuoksi siitä yleisestä ja pysyvästä vaarasta, jonka muodostavat vakavat rikokset (tuomio Commissioner of An Garda Síochána, C-140/20, 61–62 kohta; tuomio La Quadrature du Net ym., C-511/18, C-512/18 ja C-520/18, 136–137 kohta).

Säännöksessä tarkoitettuja tietoja käytettäisiin tiedon hankkimiseen sotilastiedustelun kohteista. Nyt ehdotetut säännökset eivät anna sotilastiedusteluviranomaiselle rajoittamatonta pääsyä tallennettuihin tietoihin eivätkä tiedot ole muutenkaan sellaisessa muodossa, josta suoraan olisi selvitettävissä laitetta käyttäneiden henkilöllisyys.

Ehdotetut säännökset asettavat tarkat rajoitukset tietojen käytölle. Lisäksi tallennettujen tietojen käyttö edellyttää aina toisen tiedustelumenetelmän käyttöä, joka edellyttää tuomioistuimen lupaa, viime kädessä tuomioistuimen luvassa määritellyin hakuehdoin.

Valvonnan kannalta keskeiseksi muodostuu teknisten tietojen käsittelyyn ja hakuehtojen määrittämiseen käytettävän järjestelmän valvonta. Järjestelmän on tuotettava ja tallennettava ainoastaan lain asettamien rajoitteiden mukaisesti tietoa.

Lisäksi keskeiseksi valvonnan kohteeksi muodostuu se, että tallennettuja tietoja voidaan käsitellä ainoastaan tuomioistuimen luvan mukaisesti laissa säädettyihin tarkoituksiin. Keskeistä on se, että tallennettujen tietojen käsittelystä jää selvät lokitiedot ja käsittely pystytään yhdistämään selkeästi tiettyyn tuomioistuimen antamaan lupaan.

Viestin sisältöön menevät hakuehdot

Esityksen 1. lakiehdotuksen 70 §:ssä ehdotetaan, että hakuehtona voitaisiin käyttää nykyisin sallittujen hakuehtojen lisäksi myös viestin sisällössä olevaa kielellistä ilmaisua. Perustuslakivaliokunta on käytännössään katsonut, että välttämättömyyttä koskeva edellytys perustuslain 10 §:n 4 momentissa tarkoittaa, että luottamuksellisen viestin salaisuuteen kohdistunut rajoitus on sallittu vain, jos tiedonhankinta ei ole mahdollista vähemmän puuttuvin keinoin, ja että tiedonhankinnassa puututaan luottamuksellisen viestin salaisuuteen mahdollisimman kohdennetusti ja rajoitetusti (PeVM 4/2018 vp, s. 8 ja HE 198/2017 vp, s. 37—38). Edellä sanottu lähtökohta huomioiden perustuslakivaliokunta katsoi, että koska hakuehdon käsite on tietoliikennetiedustelun kohdentumisen kannalta ensiarvoisen tärkeä, sääntelyn tarkkarajaisuuden ja täsmällisyyden sekä tietoliikennetiedustelun perus- ja ihmisoikeusnäkökulmasta hyväksyttävän kohdentumisen vuoksi sotilastiedustelulaissa tulee säätää hyväksyttävän hakuehdon perusteista (PeVL 36/2018 vp.). Sotilastiedustelusta annetun lain 10 §:n 1 kohtaan säädettiin perustuslakivaliokunnan myötävaikutuksella hakuehdon määritelmä, jonka 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.

Toisaalta hallituksen esityksessä 202/2017 vp. ehdotettiin, että hakuehtona voisi käyttää viestin sisältöä kuvaavaa tietoa poikkeuksellisissa tilanteissa. Perustuslakivaliokunta ei ottanut suoraa kantaa siihen, olisiko viestin sisältöä kuvaavaa tietoa mahdollista käyttää hakuehtona (PeVL 35/2018 vp.). Perustuslakivaliokunta kuitenkin edellytti PeVL 36/2018 vp. vastaavasti, että lakiin tuli lisätä nimenomainen säännös yleiseen ja kohdentamattomaan tietoliikenteen seurantaan kohdistuvasta kiellosta ja että hakuehtojen määritelmästä säädettäisiin.

Voimassa olevan sääntelyn on käytännössä osoittanut, että nykyisin sallitut hakuehdot, kuten IP-osoitteet, verkkotunnukset, puhelinnumerot ja muut tekniset tunnisteet, eivät kaikissa tilanteissa erottele tiedustelun kohteeseen liittyvää liikennettä muusta tietoliikenteestä riittävän tarkasti. Nykytilassa hakuehtojen mukaista tietoliikennettä voidaan käsitellä automaattisesta ja manuaalisesti, eli hakuehtovaiheen jälkeen tietoliikenteeseen voidaan kohdistaa myös sisältöön meneviä hakuehtoja. Vaikka hakuehdot sinänsä kohdistuvat tarkasti, tiedustelun kannalta epäolennaista tietoa joudutaan hävittämään vasta hakuehtovaiheen jälkeen.

Käytäntö on osoittanut, etteivät teknisiksi tiedoiksi katsottavat tiedot kaikissa tilanteissa rajaa tietomassaa tarkoitetulla tavalla. Tietoliikennettä olisi voitu rajata olennaisesti tarkemmin esimerkiksi käyttämällä tiettyä erityistä viestin sisällössä esiintyvää sanaa. Lisäksi teknisenä tietona pidettävä tunniste, kuten puhelinnumero, voi tietoliikenteen rakenteesta riippuen sijaita viestin sisällössä

Kielto määritellä hakuehtoa sen mukaan, missä tietoliikenteen teknisessä kerroksessa tieto sijaitsee, voi siten johtaa epäjohdonmukaiseen lopputulokseen: sama tunniste voidaan hyväksyä hakuehdoksi, jos se esiintyy otsake- tai ohjaustietona, mutta sitä ei voida käyttää, jos se sijaitsee esimerkiksi koteloidun tietoliikenteen sisällä.

Tietoliikennetiedustelu voidaan jakaa kolmeen vaiheeseen: 1) tietoliikenteen ohjaaminen tietoliikennetiedustelujärjestelmään, 2) hakuehtojen käyttöön ja 3) hakuehtoja vastaavan tietoliikenteen automaattiseen ja manuaaliseen käsittelyyn. Nyt käsiteltävä muutos koskisi nimenomaan toista vaihetta. Tietoliikennetiedustelussa hakuehto määrittelee, mikä osa tietoliikenteestä valikoituu jatkokäsittelyyn. Mitä tarkempi hakuehto on, sitä pienempi määrä viestintää päätyy viranomaisen varsinaisesti käsiteltäväksi. Nyt käsiteltävänä oleva ehdotuksessa viestin sisällössä oleva kielellinen hakuehtoa olisi käytettävä yhdessä muiden jo nykyisin sallittujen hakuehtojen kanssa. Sisältöön menevä hakuehto on automaattisen valikoinnin väline, ei itsenäinen valtuus viestinnän sisällön rajoittamattomaan tarkasteluun.

Ehdotus tarkoittaisi sitä, että osa tietoliikennetiedustelun vaiheessa kolme suoritettavista toimenpiteistä siirrettäisiin vaiheeseen kaksi. Ehdotuksen myötä vaiheessa käsiteltävä tietomassaa ei tarvitsisi käsitellä yhtä laajasti, koska sisällössä olevan kielellinen hakuehto on rajannut käsittelyn ulkopuolelle tiedustelutehtävän kannalta epäolennaista tietoliikennettä.

Sisältöön menevän hakuehdon tarkoituksena ei ole laajentaa tiedustelun kohteena olevan viestinnän määrää, vaan nimenomaisesti rajata tietoliikennemassasta aikaisempaa täsmällisemmin se osa, jolla olisi merkitystä tiedustelutehtävän kannalta.

Viestin sisältöön menevien hakuehtojen käytön mahdollistaminen on tarpeen tietoliikennetiedustelun täsmälliseksi ja teknologianeutraaliksi kohdentamiseksi. Voimassa olevassa sääntelyssä hakuehdon sallittavuus määräytyy osittain sen perusteella, missä tietoliikenteen teknisessä kerroksessa hakuehtona käytettävä tieto sijaitsee. Nykyaikaisessa tietoliikenteessä esimerkiksi järjestelmän, laitteen tai käyttäjän tunnistava teknisluonteinen tieto voi kuitenkin sijaita viestin sisällössä tai koteloidun tietoliikenteen sisällä. Tällöin sisältöön menevien hakuehtojen kategorinen kielto voi estää tietoliikenteen tehokkaan rajaamisen, vaikka hakuehtona käytettävä tieto ei luonteeltaan merkittävästi eroaisi sallituista teknisistä tunnisteista.

Ehdotus merkitsee siten laadullisesti uudenlaista mahdollisuutta kohdistaa automaattinen valikointi viestin sisältöön, mutta samalla se voi vähentää viestinnän salaisuuteen kohdistuvan puuttumisen määrällistä laajuutta. Toimivaltuuden käyttö olisi sidottu laissa säädettyyn tiedustelun kohteeseen, välttämättömyys- ja suhteellisuusvaatimuksiin, tuomioistuimen ennakkolupaan sekä riippumattomaan tiedusteluvalvontaan. Hakuehtoa ei saisi käyttää yleiseen aihepiiripohjaiseen seurantaan, vaan sillä olisi oltava riittävän yksilöity ja todennettavissa oleva yhteys luvassa tarkoitettuun sotilaalliseen toimintaan tai kansallista turvallisuutta vakavasti uhkaavaan toimintaan.

Ehdotuksen mukaan myös nykyisin sallittu hakuehto voisi olla viestin sisällössä. Tilanteissa on kyse siitä, että esimerkiksi kohde tallentaa puhelinnumeron tietyssä palvelussa olevaan puhelinluetteloonsa tai että hakuehto esiintyy esimerkiksi kohteena olevan toimijan käyttämän suojauksen takia koteloidun tietoliikenteen sisällä, eli varsinainen viestintä on toisen viestin sisällä. Hallituksen esityksessä katsotaan, että tieto ei muutu yksityisyyden suojan kannalta välttämättä olennaisesti arkaluonteisemmaksi vain siksi, että tietoliikenneprotokolla sijoittaa sen teknisesti viestin sisällöksi katsottavaan osaan.

Hallituksen esityksessä katsotaan, että sääntelyn olisi oltava tältäkin osin teknologianeutraalia. Hakuehdon sallittavuutta ei olisi perusteltua ratkaista yksinomaan sen perusteella, mihin osaan sähköistä viestintää tunniste sijoittuu, vaan arvioinnissa olisi otettava huomioon hakuehdon tietosisältö, yksilöivyys, yhteys tiedustelun kohteeseen ja vaikutus tietoliikennetiedustelun prosessiin tulevaan tietoliikenteeseen.

Joka tapauksessa esityksessä ei ehdoteta, että tietoliikennetiedustelun päätöksentekoprosessia muutettaisiin, vaan edelleen tuomioistuimelle esitettävässä vaatimuksessa ja päätöksessä olisi esitettävä hakuehdot tai hakuehtojen luokat sekä perustelut sille. Lisäksi sotilastiedustelutoimintaan kohdistuisi jatkuva tiedusteluvalvontavaltuutetun valvonta, jossa valtuutettu voi ottaa jo ennen tuomioistuimelle tehtävää vaatimusta kantaa hakuehtoihin.

Ehdotuksen tarkoituksena ei ole mahdollistaa viestien sisällön yleistä tai kohdentamatonta seulontaa, vaan parantaa tietoliikennetiedustelun tarkkuutta sellaisissa tilanteissa, joissa tietoliikenteen tekniset tiedot eivät yksin mahdollista tiedustelutehtävän kannalta merkityksellisen liikenteen luotettavaa erottamista. Hallituksen esityksen mukaan sisältöön meneviä hakuehtoja koskeva kielto poistettaisiin osana muutoksia, joiden tavoitteena on määrittää hakuehdot aikaisempaa paremmin ja kohdentaa tietoliikennetiedustelu tarkemmin.

Esityksen mukaan sisältöön menevä hakuehto voisi olla huomattavasti yksilöivämpi. Esimerkiksi tiettyyn vieraan valtion sotilaalliseen järjestelmään tai yksilöityyn operaatioon liittyvä erityinen merkkijono, koodisana tai muu poikkeuksellinen sisällöllinen ominaisuus voi erotella merkityksellisen tietoliikenteen täsmällisemmin kuin esimerkiksi toimijan käyttämä IP-osoite, verkkotunnus tai muu tekninen tunniste. Sisältöön menevän hakuehdon salliminen voi tällöin vähentää järjestelmään valikoituvan tietoliikenteen kokonaismäärää ja samalla pienentää sivullisten viestinnän käsittelyä.

Ehdotus ei merkitsisi yleistä oikeutta hakea tietoa viestien aiheen, mielipiteiden tai muun väljästi määritellyn sisällön perusteella. Hakuehtojen olisi edelleen liityttävä välittömästi tuomioistuimen luvassa tarkoitettuun sotilastiedustelun kohteeseen, ja sen olisi rajattava käsiteltävä tieto tiedustelutehtävän kannalta välttämättömään. Sisältöön menevää hakuehtoa ei siten voitaisi käyttää yleisenä temaattisena hakuna tai uusien tiedustelukohteiden kartoittamiseksi.

Sisältöön menevän hakuehdon käyttäminen ei myöskään sellaisenaan merkitsisi, että yksittäinen virkamies lukisi tai muuten tarkastelisi kaikkien vertailun kohteena olevien viestien sisältöä. Hakuehdon tekninen käyttäminen tapahtuisi automaattisena vertailuna, jonka tarkoituksena olisi erotella suuresta tietoliikennevirrasta vain hakuehtoa vastaava liikenne. Ihmisen tarkasteltavaksi tulisi siten lähtökohtaisesti vain hakuehdon perusteella eroteltu ja tiedustelutehtävän kannalta mahdollisesti merkityksellinen aineisto.

Sisältöön menevien hakuehtojen käyttöä rajoittaisivat tiedustelutoiminnan tarkoitussidonnaisuus, välttämättömyys- ja suhteellisuusvaatimus, vähimmän haitan periaate, syrjintäkielto, tiedustelukiellot, tarpeettomien tietojen hävittämisvelvollisuus sekä tuomioistuimen ja tiedusteluvalvontavaltuutetun harjoittama riippumaton valvonta. Näin rajattuna ehdotus ei laajentaisi tietoliikennetiedustelua kohdentamattomaksi sisällön tarkkailuksi, vaan antaisi mahdollisuuden käyttää joissakin tilanteissa yhdessä muiden hakuehtojen kanssa ja siten toteuttaa tiedon minimointia tehokkaammin.

Sisältöön menevän hakuehdon käytön mahdollistamisella pyritään vähentämään yksityisyyteen kohdistuvan puuttumisen kokonaislaajuutta silloin, kun hakuehdot ovat riittävän yksilöiviä, niitä käytetään yhdessä muiden kohdentavien hakuehtojen kanssa ja sen avulla vähennetään tosiasiallisesti jatkokäsittelyyn valikoituvan sivullisen viestinnän määrää. Sisältöön menevän hakuehdon valtiosääntöoikeudellista hyväksyttävyyttä ei tule arvioida yksinomaan sen perusteella, mihin tietoliikenteen kenttään hakuehto teknisesti kohdistuu, vaan ennen kaikkea sen perusteella, kuinka täsmällisesti se rajaa tiedonhankinnan laissa tarkoitettuun toimintaan ja kuinka tehokkaasti se vähentää sivullisten viestinnän käsittelyä.

Edellä sanotun perusteella, hallituksen esityksessä on katsottu, että esitysehdotuksen voidaan katsoa täyttävän perustuslain 10 §:n 4 momentin asettamat vaatimukset.

Suomessa olevaan telepäätelaitteeseen tai teleosoitteeseen kohdistuva hakuehto

Esityksen 1. lakiehdotuksen 68 ja 70 §:ssä ehdotetaan, että tietoliikennetiedustelussa käytettävä hakuehto voisi kohdistua myös Suomen rajan sisäpuolelle tilapäisesti. Vallitseva turvallisuuspoliittinen tilanne on osoittanut, että Suomen turvallisuusympäristön kannalta keskeiset valtiot käyttäytyvät aiempaa arvaamattomammin ja aggressiivisemmin. Voimassa olevassa laissa oleva kategorinen kiellon mukaisesti tiedonhankinta on lopetettava välittömästi silloin, kun kohde siirtyy Suomeen, vaikka tiedustelun kohteena oleva toiminta jatkuisi muuttumattomana, hakuehto kohdistuisi edelleen samaan yksilöityyn laitteeseen tai teleosoitteeseen. Tiedonhankinnan tarve usein myös edellä kuvatussa tilanteessa muuttuu aiempaa akuutimmaksi, koska kohde on saapunut Suomeen, ja tiedonhankinnan tarve kasvaa. Telepäätelaitteen tai -osoitteen siirtyminen Suomeen ei kuitenkaan muuta sitä toimintaa, jonka perusteella tietoliikennetiedustelu on alun perin aloitettu.

Ehdotuksen tarkoituksena ei ole laajentaa tietoliikennetiedustelua yleisesti Suomessa tapahtuvaan tiedonhankintaan, vaan estää jo lainmukaisesti aloitetun ja täsmällisesti kohdennetun tiedustelun äkillinen katkeaminen, kun tiedustelun kohteena oleva toimija tai tämän käyttämä telepäätelaite saapuu kesken tiedustelun Suomeen. Laitteen maantieteellinen siirtyminen ei itsessään muuta tiedustelun kohteena olevaa toimintaa eikä poista tiedonhankinnan välttämättömyyttä. Tiedonhankinnan tarve voi päinvastoin korostua toiminnan saadessa välittömän yhteyden Suomeen.

Hakuehdon käyttäminen Suomessa olisi sallittua vain tilapäisesti ja saman tiedustelutehtävän yhteydessä, kunnes käyttöön voidaan ottaa kohdennetumpi tiedustelumenetelmä. Kyse olisi siten jatkuvuutta turvaavasta siirtymätoimivallasta, ei Suomessa tapahtuvan tiedustelun itsenäisestä tai vaihtoehtoisesta muodosta. Yksilöidyn telepäätelaitteen tai teleosoitteen käyttäminen hakuehtona voi lisäksi rajata tiedonhankintaa tarkemmin kuin väljemmät tunnisteet ja siten vähentää sivullisten viestinnän käsittelyä.

Toimivallan käyttöä rajoittaisivat tiedustelutehtävän muuttumattomuus, hakuehdon yksilöitävyys, tapauskohtainen välttämättömyys, suhteellisuusperiaate, vähimmän haitan periaate, tietojen minimointi sekä riippumaton laillisuusvalvonta. Käyttö olisi lopetettava heti, kun kohdennetumpi menetelmä on käytettävissä, hakuehdon yhteys tiedustelun kohteeseen katkeaa tai tiedonhankinnan jatkaminen ei enää ole välttämätöntä. Näin rajattuna ehdotus ei murenna kotimaisen viestinnän suojaa, vaan poistaa nykyisestä sääntelystä ennakoimattomissa siirtymätilanteissa syntyvän tiedustelukatkoksen.

Laitteen siirtyminen Suomeen muuttaa tiedonhankinnan alueellista asetelmaa, mutta ei välttämättä puuttumisen tosiasiallista kohdetta tai intensiteettiä. Sama yksilöity hakuehto kohdistuu edelleen samaan telepäätelaitteeseen tai teleosoitteeseen ja samaan tiedustelun kohteena olevaan toimintaan. Perustuslakivaliokunta on pitänyt hakuehdon käsitettä tietoliikennetiedustelun hyväksyttävän kohdentumisen kannalta ensiarvoisen tärkeänä ja edellyttänyt, että hyväksyttävän hakuehdon perusteista säädetään laissa (PeVL 35/2018 vp, s. 23–24; PeVL 36/2018 vp). Esimerkiksi yksilöityyn telepäätelaitteeseen tai teleosoitteeseen perustuvan hakuehdon tilapäinen käyttäminen voi siten toteuttaa tiedonhankinnan mahdollisimman täsmällistä kohdentamista ja vähentää sivullisten viestinnän käsittelyä.

Perustuslain 10 §:n 4 momentti ei kategorisesti kiellä Suomessa tapahtuvaa sotilaalliseen toimintaan tai kansallista turvallisuutta vakavasti uhkaavaan toimintaan kohdistuvaa tiedonhankintaa. Säännös edellyttää, että viestin salaisuuteen kohdistuva rajoitus on välttämätön. Perustuslakivaliokunta on katsonut, että välttämättömyysvaatimuksen perusteella tiedonhankinnan tulee olla mahdollista vain, jos tietoa ei voida hankkia vähemmän puuttuvin keinoin, ja että viestinnän salaisuuteen tulee puuttua mahdollisimman kohdennetusti ja rajoitetusti. Välttämättömyyttä on arvioitava myös tiedustelumenetelmän käytön edellytyksenä yksittäistapauksessa (PeVM 4/2018 vp, s. 8–9; PeVL 35/2018 vp, s. 7–8 ja 23–24; PeVL 36/2018 vp).

Perustuslakivaliokunta on lisäksi katsonut, että perustuslain 10 §:n 4 momentissa tarkoitetulla toiminnalla tulee olla kytkentä Suomeen ja sen tulee uhata nimenomaan Suomen kansallista turvallisuutta, vaikka toiminta voisi maantieteellisesti tapahtua Suomen rajojen ulkopuolella (PeVM 4/2018 vp, s. 8; PeVL 35/2018 vp). Tämä tukee sitä, ettei tiedonhankinnan valtiosääntöoikeudellista hyväksyttävyyttä ratkaise yksinomaan telepäätelaitteen kulloinenkin maantieteellinen sijainti, vaan ennen kaikkea tiedonhankinnan kohteena olevan toiminnan luonne, sen yhteys Suomen kansalliseen turvallisuuteen sekä tiedonhankinnan välttämättömyys ja oikeasuhtaisuus

Ehdotuksen hyväksyttävyyttä on näin ollen arvioitava sen perusteella, onko saman yksilöidyn hakuehdon lyhytaikainen käyttäminen Suomessa yksittäistapauksessa välttämätöntä tiedonhankinnan katkeamisen estämiseksi ja voidaanko tavoiteltava tieto saada viivytyksettä vähemmän puuttuvalla keinolla. Kun käyttö rajataan samaan tiedustelutehtävään, tilapäiseen siirtymävaiheeseen ja aikaan, joka tarvitaan kohdennetumman tiedustelumenetelmän käyttöön ottamiseksi, ehdotusta voidaan pitää perustuslain 10 §:n 4 momentin välttämättömyys- ja oikeasuhtaisuusvaatimusten mukaisena.

4. Ilmoitusvelvollisuudesta luopuminen

Esityksen 1. lakiehdotuksen 89 a §:ssä ehdotetaan, että tietoliikennetiedustelun kohteeksi joutuneelle ei tarvitsisi tehdä ilmoitusta. Tietoliikennetiedustelun erityisluonteen vuoksi jälkikäteinen henkilökohtainen ilmoittaminen ei ole tarkoitukseen soveltuva oi-

keusturvamekanismi ja että sen tehtävä voidaan tässä rajatussa tilanteessa korvata tehokkaalla, riippumattomalla ja jatkuvalla valvonnalla.

Tietoliikennetiedustelun kohteena ei lähtökohtaisesti ole nimetty henkilö samalla tavoin kuin esimerkiksi telekuuntelussa. Tiedustelu kohdistuu tietoliikenteeseen, teknisiin tunnisteisiin, organisaation viestintään tai tiettyyn sotilastiedustelun kohteena olevaan toimintaan. Tiedustelujärjestelmään voi tämän vuoksi tulla myös sellaisten henkilöiden viestintään liittyviä tietoja, jotka eivät ole varsinaisia tiedustelun kohteita vaan esimerkiksi viestivät kohteena olevan organisaation kanssa.

Voimassa oleva ilmoitusvelvollisuus voi siten ulottua esimerkiksi 1) varsinaiseen tiedustelun kohteeseen, 2) kohteen kanssa viestineeseen henkilöön, 3) henkilöön, jonka tunniste on tullut järjestelmään satunnaisesti tai 4) henkilöön, jonka tietoja on käsitelty vain sen selvittämiseksi, onko tiedolla merkitystä. Ilmoitusvelvollisuus ei tällaisessa ympäristössä kohdistu luontevasti vain siihen, jonka toimintaan viranomainen on tarkoituksellisesti puuttunut, vaan se voi johtaa ilmoittamiseen myös sivullisille, joiden viestintä on tullut käsiteltäväksi satunnaisesti ja tieto on poistettu välittömästi.

Voimassa olevan lain mukaan ilmoittamatta jättämistä tai ilmoituksen lykkäämistä voidaan hakea tuomioistuimelta. Mahdollisuutta on jouduttu käyttämään, koska sotilastiedustelun kohteena olevaan toimintaan voi liittyä myös muita kuin valtiollisia toimijoita. Viranomainen ja tuomioistuin joutumat käyttämään resursseja ilmoittamatta jättämistä koskevien asioiden käsittelyyn. Näin ollen lainsäädännön selkeyden ja läpinäkyvyyden vuoksi hallituksen esityksessä katsotaan, että selkeämpää olisi säätää suoraan ilmoittamatta jättämisestä.

Tietoliikennetiedustelua koskevasta ilmoitusvelvollisuudesta luopuminen ei merkitse oikeusturvasta luopumista, vaan oikeusturvan järjestämistä tietoliikennetiedustelun erityispiirteisiin paremmin soveltuvalla tavalla. Tietoliikennetiedustelu kohdistuu ensisijaisesti tietoliikenteeseen ja laissa tarkoitettuun toimintaan, ei ennalta yksilöityyn luonnolliseen henkilöön. Menetelmän yhteydessä käsiteltäväksi voi tulla myös sellaisten sivullisten tietoja, jotka eivät ole tiedustelun varsinaisia kohteita. Ilmoitusvelvollisuuden toteuttaminen voisi tällöin edellyttää henkilön tunnistamista ja häntä koskevien lisätietojen hankkimista yksinomaan ilmoituksen tekemistä varten, vaikka henkilöllisyydellä ei olisi tiedustelutehtävän kannalta merkitystä. Tämä lisäisi tarpeettomasti henkilötietojen käsittelyä ja voisi olla ristiriidassa tietojen minimointia ja viivytyksetöntä hävittämistä koskevien vaatimusten kanssa.

Ilmoittaminen voisi lisäksi paljastaa tiedustelun kohdentamista, menetelmiä ja teknisiä kykyjä sekä vaarantaa samaan toimintaan tai toimijaverkostoon kohdistuvan pitkäkestoisen tiedonhankinnan. Tietoliikennetiedustelun tarve ei välttämättä pääty yksittäisen luvan tai tiedustelutoimenpiteen päättyessä. Ilmoittamatta jättämisen perusteet liittyvät siten maanpuolustuksen ja kansallisen turvallisuuden suojaamiseen sekä tiedustelutoiminnan edellytysten turvaamiseen.

Ilmoitusvelvollisuuden poistamista tasapainottavat tietoliikennetiedustelun tuomioistuinkontrolli, tiedusteluvalvontavaltuutetun riippumaton ja koko tiedusteluprosessin kattava valvonta, mahdollisuus tehdä valtuutetulle tutkimispyyntö sekä tietojen käsittelyä, minimointia ja hävittämistä koskevat velvoitteet. Euroopan ihmisoikeustuomioistuimen oikeuskäytännöstä ei seuraa ehdotonta velvollisuutta ilmoittaa jokaiselle tietoliikennetiedustelun kohteeksi joutuneelle, vaan järjestelmän hyväksyttävyyttä arvioidaan oikeusturvatakeiden kokonaisuuden perusteella. Perustuslakivaliokunta on edellyttänyt,

että tiedusteluvalvontavaltuutetun valvonta ulottuu yksittäisten tiedustelumenetelmien lisäksi yleisesti tiedustelutoimintaan ja tiedustelutiedon käyttöön (PeVM 9/2018 vp). Tämä mahdollistaa sen, että valvonnassa arvioidaan paitsi tiedon hankkimisen myös sen säilyttämisen, jatkokäsittelyn, luovuttamisen ja hävittämisen lainmukaisuutta.

Perustuslakivaliokunta on pitänyt riippumattoman laillisuusvalvojan asemaa ilmoittamiskysymyksissä merkityksellisenä ja edellyttänyt tiedusteluvalvontavaltuutetulle oikeutta hakea muutosta myös ilmoituksen lykkäämistä ja tekemättä jättämistä koskeviin ratkaisuihin (PeVL 35/2018 vp, s. 32). Ehdotetussa järjestelmässä ilmoitusvelvollisuuden poistuminen korostaa vastaavasti valtuutetun oma-aloitteisen valvonnan, tiedonsaantioikeuksien ja puuttumistoimivaltuuksien merkitystä.

Perustuslakivaliokunta on pitänyt tiedustelumenetelmän käytöstä ilmoittamista lähtökohtana ja edellyttänyt ilmoittamista koskevien poikkeusten tiukkaa lakisääteistä rajaamista. Toisaalta valiokunta on hyväksynyt sen, ettei tietoliikennetiedustelun ilmoitusvelvollisuus ulotu kaikkiin teknisluonteisen käsittelyn tilanteisiin, kuten pelkkään tunnistamistietojen käsittelyyn tai välittömästi hävitettyihin tietoihin (PeVL 35/2018 vp, s. 27). Valiokunta on lisäksi pitänyt tehokasta, kattavaa ja riippumatonta valvontajärjestelmää tiedustelutoimivaltuuksien hyväksyttävyyden välttämättömänä edellytyksenä sekä edellyttänyt valvonnan ulottamista koko tiedustelutoimintaan ja tiedustelutiedon käyttöön (PeVM 4/2018 vp, s. 9; PeVL 35/2018 vp, s. 30–31; PeVL 36/2018 vp, s. 35; PeVM 9/2018 vp).

Ehdotettua ilmoitusvelvollisuudesta luopumista voidaan puoltaa tietoliikennetiedustelun erityisluonteella, sivullisten tietojen välittömällä hävittämisellä, tarpeettoman henkilötietojen käsittelyn välttämisellä ja tiedustelumenetelmien suojaamisella. Koska muutos poikkeaa valiokunnan ilmoittamista koskevasta lähtökohdasta, sen hyväksyttävyys edellyttää kuitenkin, että riippumaton valvonta on oma-aloitteista, kattavaa ja tosiasiallisesti tehokasta ja että henkilöllä säilyy todellinen mahdollisuus saattaa epäilynsä tiedusteluvalvontavaltuutetun tutkittavaksi.

5. Viranomaisen ulkopuolisen suorittamat toimenpiteet

Esityksen 1. lakiehdotuksen 42 §:ssä ehdotetaan, että viranomaisen ulkopuolinen henkilö voisi suorittaa tiettyjä asennustoimenpiteitä tiedustelumenetelmän käytön mahdollistamiseksi.

Tilanteessa voidaan katsoa olevan osittain kyse lähellä ohjattua tietolähdetoimintaa lähellä olevasta toiminnasta, jossa henkilö viranomaisen ohjauksessa toteuttaa omassa sosiaalisessa verkostossaan ja tiloihin pääsymahdollisuuksiensa rajoissa viranomaisen ohjeistaman toimenpiteen. Kyse ei ole tiedonhankinnasta, vaan sotilastiedusteluviranomaisella olisi oltava varsinaisen tiedustelumenetelmän käyttämiseen tarvittava lupa tai päätös.

Voimassa olevassa laissa tarkoitettu tietolähdetoiminta perustuu vahvasti rikostorjunnassa säädettyyn tietolähdetoimintaan, joka on säädetty perustuslakivaliokunnan myötävaikutuksella (PeVL 66/2010 vp). Tietolähdetoimintaa ei ole arvioitu perustuslakivaliokunnan tähänastisessa lausuntokäytännössä erityisesti minkään perusoikeuden kannalta.

Tietolähdetoiminta, ohjattu tietolähteen käyttö sekä esityksessä ehdotettava osallistuva tietolähteen käyttö perustuvat lähtökohtaisesti tietolähteen olemassa oleviin kontaktei-

hin ja ihmissuhteisiin sekä ihmisten väliseen tavanomaiseen kanssakäymiseen ja pääsyyn tiedon äärelle.

Nyt käsiteltävänä oleva säännösehdotusta ei kuitenkaan ole sidottu tiedonhankintaan eikä siinä oltaisi osana rikollista toimintaa. Ulkopuolisen suorittamia asentamistoimenpiteitä olisi arvioitava perusoikeussuojan rajoittamisen kannalta samoista lähtökohdista kuin esimerkiksi peiteltyä tiedonhankintaa tai peitetoimintaa koskevia toimivaltuuksia, koska toimivaltuudessa on kyse henkilön käytössä olevien verkostojen sekä tiettyihin tiloihin ja laitteistoihin pääsyn hyödyntämisestä, joihin viranomaisella ei lähtökohtaisesti ole vastaavaa pääsyä edes tiedustelumenetelmää käyttämällä.

Jos avustava henkilö ei kykenisi toimimaan tavalla, joka kuuluu hänen normaalin toimintaansa, voisi tämä johtaa jopa mahdollisiin vaaratilanteisiin.

Osaltaan nyt käsiteltävää säännöstä voidaan arvioida myös sen kautta, mitä perustuslakivaliokunta on lausunut peitetoiminnasta. Perustuslakivaliokunta on peitetoimintaan liittyen luonnehtinut epäsovinnaiseksi toimivaltuudeksi sellaista tutkintakeinoa, joka merkitsee poliisin oikeutta 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 uudenlaista toimivaltaa suorittaa toimia, jotka muutoin ovat rikosoikeudellisesti sanktioituja myös viranomaisen tekeminä (PeVL 5/1999 vp, s. 5). Esityksessä ehdotetaan säädettävän ulkopuolisen suorittamista toimenpiteistä, jotka voisivat täyttää tilanteen mukaan jonkin rikoksen tunnusmerkistön. Toimenpiteet vastaavat kuitenkin sitä, mitä sotilastiedustelusta annetun lain xx §:ssä on säädetty tiedustelumenetelmän käytön edellyttämästä laitteen, menetelmän tai ohjelmiston asentamisesta ja poisottamisesta.

Viranomaisen ulkopuolisen suorittamissa toimenpiteissä on kyse sotilastiedusteluviranomaiselle kuuluvasta toimivaltuudesta, ja avustamistoimia olisi mahdollista suorittaa yksinomaan viranomaisen valvonnassa ja ohjauksessa. Toimiessaan vastoin saamiaan ohjeita avustava henkilö olisi mahdollisesti rikosoikeudellisessa vastuussa toimistaan.

Ehdotetun sääntelyn ei katsota eroavan perusoikeusjärjestelmän näkökohdista, kun sitä arvioidaan sitä vasten, mitä perustuslakivaliokunta on todennut ja mitä on säädetty ohjatun tietolähteen käytöstä (PeVL 66/2010 vp. ja PeVL 67/2010 vp.).

Käsiteltävää sääntelyä on myös arvioitava merkittävän julkisen vallan käytön kannalta. Perustuslakivaliokunta on vakiintuneesti katsonut, että merkittävänä julkisen vallan käyttönä on pidettävä esimerkiksi sitä, että yksilön perusoikeuksiin puututaan merkittävällä tavalla itsenäiseen harkintaa perustuen (HE 1/1998 vp. s. 179/II, ks. myös PeVL 48/2001 vp. s. 3/II, PeVL 20/2002 vp. s. 3 ja PeVL 30/2010 vp. s.10/I, ks. myös PeVL 62/2010 vp. s. 6).

Esityksessä katsotaan, että avustavissa toimenpiteissä ei ole kyse yksityiselle henkilölle annettavasta julkisesta hallintotehtävästä eikä toimenpiteitä tulisi arvioida perustuslain 124 §:ssä tarkoitetuksi julkiseksi hallintotehtäväksi. Avustavat toimenpiteet voidaan arvioida tietyissä määrin tietolähdetoimintaa konkreettisemmiksi, avustavan henkilön suorittamia toimenpiteet eivät muodostu sellaisiksi tehtäviksi, jotka olisi arvioitava julkiseksi hallintotehtäväksi. Toimenpiteet eivät perustuisi henkilön itsenäiseen harkinta- ja päätöksentekovaltaan eikä henkilö tekisi itsenäisesti sellaisia ratkaisuja, jotka vaikuttaisivat yksityisten oikeuksiin tai velvollisuuksiin.

Säännöksen toimenpiteissä on kyse siitä, että avustava henkilö laittaa esimerkiksi sotilastiedusteluviranomaisen tiedonhankintaohjelmiston sisältävän muistitikun tiettyyn tiedustelun kohteena olevan toimijan laitteeseen sanotuksi ajaksi, ottaa sen pois ja palauttaa muistitikun sotilastiedusteluviranomaiselle tai muuten sovitulla tavalla hävittää sen. Jos henkilö laittaisi muistitikun täysin toiseen laitteeseen, kyse saattaisi olla jopa rikollisesta toiminnasta.

Joka tapauksessa sotilastiedusteluviranomaisella olisi aina vastuu siitä, että mahdollisesti esimerkiksi väärään laitteeseen asennettu ohjelmisto lopettaa tiedonhankinnan välittömästi tämän käytyä ilmi. Sotilastiedusteluviranomainen vastaa muutenkin varsinaisen tiedustelumenetelmän käytöstä ja tietojen käsittelystä.

On selvää, että avustajan käyttäminen tulisi perustua ennakolta tarkoin suunniteltuun ja ohjattuun sotilastiedusteluviranomaisen toimintaan. Mikäli tarkoin ennakoitu, suunniteltu ja ohjattu avustajan toiminta ei olisi mahdollista, keinoa ei saisi käyttää. Keinon käyttöä koskevassa tarkastelussa olisi arvioitava, onko avustajan käyttö mahdollista toteuttaa siten, että lähes täydellinen kontrolli toiminnasta säilyisi toimivaltaisella viranomaisella. Mikäli avustajan käyttö sisältäisi riskejä esimerkiksi väärinkäytöksistä, olisi itsestään selvää, ettei toimenpiteitä voisi toteuttaa tällaisen henkilön kanssa. Toisin sanoen suunniteltavan ja ohjattavan toiminnan olisi oltava niin yksinkertaista ja ennakoitavissa olevaa, että riski väärinkäytöksille ja viime kädessä avustajan niistä johtuva rikosoikeudellisen vastuun toteutumiselle olisi lähes olematon.

Avustavan henkilön käytössä olisi kyse viranomaisten harkinta- ja päätöksentekovaltaan perustuvasta toimivaltuuksien käyttämiseksi tehtävistä toimenpiteistä. Toimenpiteet olisivat jokaisessa tilanteessa ainoastaan sotilastiedusteluviranomaisen toimivaltuuksien käyttöön liittyviä, luonteeltaan avustavia toimia, joissa ei kuitenkaan olisi kyse julkisesta hallintotehtävästä tai julkisen vallan käyttämisestä. Myös virkavastuun osalta kyse olisi yksinomaan toimivaltuutta käyttävälle viranomaiselle kuuluvasta vastuusta, joka ei itsenäisenä vastuuna ulottuisi itse avustavaan henkilöön, vaan henkilön käyttö sisältyisi kokonaisuudessaan viranomaisen toiminnan kattavaan virkavastuuseen.

6. Valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuva tiedustelu

Esityksen 1. lakiehdotuksen 61 a §:ssä ehdotetaan uutta toimivaltuutta, valtiollisen toimijan tietojärjestelmään kotimaassa kohdistuvaa tietojärjestelmätiedustelua. Uusi toimivaltuus yhdistäisi osaltaan ennen kaikkea teknistä laitetarkkailua ja televalvontaa. Se, missä voimassa olevan lainsäädännön mukaan tietoa voidaan hankkia yksittäisistä laitteista, uudessa toimivaltuudessa tiedonhankintaa voitaisiin jatkaa tietojärjestelmän kokonaisuudessa edeten siihen kuuluvien laitteiden välillä. Uuden tietojärjestelmään liittyvän laitteen havaitsemisen jälkeen tiedon hankintaa voitaisiin kohdistaa tähän laitteeseen, ilman erillistä lupaa, jossa laite yksilöitäisiin.

Kotimaan tietojärjestelmätiedustelua koskevan toimivaltuuden tarkoituksena on mahdollistaa tiedon hankkiminen Suomessa sijaitsevasta valtiollisen toimijan tietojärjestelmästä silloin, kun järjestelmää käytetään sotilastiedustelun kohteena olevaan toimintaan. Toimivaltuus ei kohdistuisi yleisesti Suomessa sijaitseviin tietojärjestelmiin eikä se muodostaisi yleistä oikeutta päästä kotimaisten yritysten, yhteisöjen tai yksityishenkilöiden tietojärjestelmiin. Menetelmän käyttäminen edellyttäisi perusteltua yhteyttä laissa tarkoitettuun sotilastiedustelun kohteena olevaan toimintaan sekä tuomioistuimen lupaa.

Toimivaltuus on välttämätön, koska valtiollinen toimija voi käyttää Suomessa sijaitsevaa palvelinta, pilvipalvelua tai muuta tietojärjestelmää osana esimerkiksi ulkomailta johdettua tiedustelu-, vaikuttamis- tai kybertoimintaa. Tällöin toimivallan määräytyminen yksinomaan järjestelmän fyysisen sijainnin perusteella voisi muodostaa tiedustelukatvealueen ja antaa ulkomaiselle toimijalle mahdollisuuden välttää sotilastiedustelua sijoittamalla käyttämänsä teknisen infrastruktuurin Suomeen.

Ehdotetulla toimivaltuudella ei laajennettaisi sotilastiedustelun aineellisia kohteita. Tiedonhankinnan tulee edelleen koskea vain laissa tarkoitettua sotilaallista toimintaa tai kansallista turvallisuutta vakavasti uhkaavaa toimintaa, jonka taustalla on valtiollinen toimija. Menetelmän alueellinen ulottaminen Suomeen poistaisi teknologian ja verkkopalvelujen kansainvälisestä rakenteesta johtuvan toimivaltakatkoksen, mutta ei alentaisi tiedustelun aineellisia käyttöedellytyksiä. Ehdotus on osa sotilastiedustelulainsäädännön mukauttamista muuttuneen kybertoimintaympäristön vaatimuksiin.

Tietojärjestelmätiedustelu olisi tiettyyn järjestelmään ja siinä harjoitettavaan toimintaan täsmällisesti kohdistuva tiedustelumenetelmä. Valtiollisen toimijan käyttämä tietojärjestelmä muodostuisi siitä laitteita, palveluita ja tietoliikenneinfrastuktuuria käsittävästä kokonaisuudesta, johon valtiollisella toimijalla on käyttöoikeus. Tietojärjestelmätiedustelu kotimaassa voi siten olla perusoikeuksiin vähemmän puuttuva, kun tiedustelun kohteena oleva tietojärjestelmä voidaan yksilöidä ja yhdistää laissa tarkoitettuun toimintaan, jolloin tiedonhankinta voidaan rajata suoraan siihen järjestelmän osaan, tietoon tai toiminnallisuuteen, jolla on merkitystä tiedustelutehtävän kannalta. Tämä vähentää sivullisten tietojen käsittelyn tarvetta.

Menetelmän käyttäminen voi puuttua perustuslain 10 §:ssä turvattuun yksityiselämän, henkilötietojen ja luottamuksellisen viestin salaisuuden suojaan siltä osin kuin järjestelmässä käsitellään luonnollisia henkilöitä koskevia tietoja tai viestintää. Vieras valtio tai sen viranomainen ei sellaisenaan ole Suomen perustuslaissa turvattujen perusoikeuksien haltija. Järjestelmän valtiollinen luonne ei kuitenkaan poista velvollisuutta suojata sivullisten luonnollisten henkilöiden perusoikeuksia.

Puuttumista rajoittaisivat kuitenkin toimivaltuuden sidonnaisuus sotilastiedustelun kohteena olevaan toimintaan, tuomioistuimen ennakkolupa, tietojärjestelmän yksilöiminen, välttämättömyys- ja suhteellisuusvaatimus, vähimmän haitan periaate, tiedustelukiellot sekä tarpeettomien ja sivullisia koskevien tietojen hetihävittämisvelvollisuudet. Riippumaton tiedusteluvalvonta kattaisi menetelmän käytön koko tiedusteluketjun ajan.

Perustuslakivaliokunta on korostanut, että perustuslain 10 §:n 4 momentissa tarkoitetun kansallisen turvallisuuden käsitettä on tulkittava suppeasti, uhkan vakavuusaste on asetettava korkealle ja tiedustelutoimivaltuuksien kohdentumisesta on säädettävä laissa tyhjentävästi (PeVM 4/2018 vp, s. 8–9; PeVL 35/2018 vp, s. 15–17; PeVL 36/2018 vp). Ehdotettu toimivaltuus on näiden vaatimusten mukaisesti rajattu tiedon hankkimiseen yksilöidystä, valtiollisen toimijan käyttämästä tietojärjestelmästä, jolla on perusteltu yhteys laissa tarkoitettuun sotilastiedustelun kohteena olevaan toimintaan.

Perustuslakivaliokunta on edelleen katsonut, että perustuslain 10 §:n 4 momentin välttämättömyysvaatimus edellyttää tiedonhankinnan olevan mahdollista vain, jos tietoa ei voida hankkia vähemmän puuttuvin keinoin, ja että viestin salaisuuteen puututaan mahdollisimman kohdennetusti ja rajoitetusti. Tiedonhankinnan välttämättömyys on voitava osoittaa kussakin yksittäistapauksessa (PeVM 4/2018 vp, s. 7–9; PeVL 35/2018 vp, s. 7–8; PeVL 36/2018 vp). Yksilöityyn tietojärjestelmään kohdistuva tiedonhankinta

voi toteuttaa näitä vaatimuksia, jos sen avulla tiedonhankinta voidaan rajata täsmällisemmin kuin käytettäessä laajempia tai välillisempiä tiedustelumenetelmiä

Menetelmän tuomioistuinlupa ja riippumaton laillisuusvalvonta muodostavat keskeiset oikeusturvatakeet. Perustuslakivaliokunta on katsonut, että oikeudellinen kontrolli tuomioistuimessa turvaa parhaiten ennakkovalvonnan itsenäisyyden ja puolueettomuuden. Tuomioistuinkontrolli ei kuitenkaan saa muodostua näennäiseksi, vaan tuomioistuimelle on annettava riittävät ja kattavat tiedot menetelmän kohteesta, edellytyksistä ja lupaasian taustalla olevista tosiseikoista (PeVL 35/2018 vp, s. 10–13 ja 29–30). Ehdotetussa toimivaltuudessa tämä edellyttää, että lupahakemuksessa määritellään riittävän täsmällisesti tietojärjestelmäkokonaisuus ja perusteet, joilla tiedonhankinta voidaan kohdistaa järjestelmässä havaittavaan uuteen laitteeseen ilman uutta lupaa

Perustuslakivaliokunta on lisäksi painottanut, ettei perustuslain 10 §:n 4 momentti mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa ja ettei pitkälle perusoikeuksiin puuttuvia tiedustelutoimivaltuuksia voida antaa ilman tehokasta valvontaa (PeVM 4/2018 vp, s. 7–9; PeVL 35/2018 vp, s. 14 ja 22–23; PeVL 36/2018 vp). Vaikka nyt arvioitava toimivaltuus koskee tietojärjestelmätiedustelua eikä tietoliikennetiedustelua, samat yleiset vaatimukset puoltavat menetelmän rajaamista yksilöityyn järjestelmään ja sen alistamista tiedusteluvalvontavaltuutetun koko käytön kattavaan valvontaan.

Näin rajattuna ehdotus toteuttaa perustuslain 10 §:n 4 momentissa nimenomaisesti hyväksyttyä tarkoitusta hankkia tietoa sotilaallisesta toiminnasta ja kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Toimivaltuus täydentää olemassa olevia tiedustelumenetelmiä tilanteessa, jossa tiedustelun kohteena oleva toiminta toteutetaan Suomessa sijaitsevaa teknistä infrastruktuuria hyödyntäen, eikä se mahdollista yleistä tai kohdentamatonta tietojärjestelmien seurantaa.

7. Rajavartiolaitoksen osallistuminen

Esityksen 1. lakiehdotuksen 18 a §:ssä ehdotetaan, että Rajavartiolaitos voi avustaa sotilastiedusteluviranomaista ja suorittaa tämän pyynnöstä tiettyjä yksittäisiä tiedustelumenetelmien käyttöön liittyviä toimenpiteitä sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa. Sotilastiedusteluun osallistuminen lisättäisiin samalla Rajavartiolaitoksen lakisääteiseksi tehtäväksi. Ehdotuksella ei siirrettäisi sotilastiedustelutehtävää tai tiedustelumenetelmien käyttöä koskevaa itsenäistä päätösvaltaa Rajavartiolaitokselle.

Perustuslain 2 §:n 3 momentin mukaan julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Perustuslakivaliokunnan käytännössä viranomaisten toimivaltuuksia koskevalta sääntelyltä on edellytetty täsmällisyyttä ja tarkkarajaisuutta erityisesti silloin, kun tehtävän hoitamiseen liittyy mahdollisuus puuttua perusoikeuksiin. Sääntelystä tulee käydä riittävän selvästi ilmi toimivaltainen viranomainen, toimivallan aineellinen sisältö, toimivallan käyttämisen edellytykset sekä vastuu toiminnan johtamisesta ja valvonnasta. Viranomaisten välinen yhteistyö ei itsessään laajenna kummankaan viranomaisen toimivaltaa, vaan toimivallan tulee perustua nimenomaiseen laintasoiseen säännökseen.

Ehdotuksen tarkoituksena on hyödyntää Rajavartiolaitoksen alueellista läsnäoloa, päivystysvalmiutta ja operatiivista osaamista tilanteissa, joissa tiedustelumenetelmän toteuttaminen edellyttää yksittäistä ja viivytyksetöntä toimenpidettä erityisesti rajanyli-

tyspaikalla tai muualla Rajavartiolaitoksen toiminnan yhteydessä. Järjestely tehostaisi viranomaisten voimavarojen käyttöä ja mahdollistaisi tiedustelumenetelmän oikea-aikaisen toteuttamisen ilman, että sotilastiedusteluviranomaisen olisi kaikissa tilanteissa siirrettävä omaa henkilöstöään kiireellisesti paikalle.

Perustuslakivaliokunta on turvallisuusviranomaisten välistä virka-apua arvioidessaan pitänyt hyväksyttävänä sitä, että toinen viranomainen antaa henkilöstöään ja erityisosaamistaan toimivaltaisen viranomaisen käyttöön. Valiokunnan arvioinnissa olennaista on ollut, että tehtävä suoritetaan sitä johtavan viranomaisen vastuulla ja että virka-apua antavan viranomaisen tehtävät ja toimivaltuudet määritellään laissa riittävän täsmällisesti. Virka-apua koskevassa sääntelyssä tulee lisäksi käydä selvästi ilmi avun pyytämistä, päätöksentekoa, johtamista, toimintojen yhteensovittamista ja toiminnan lopettamista koskeva vastuunjako (PeVL 3/2022 vp, ks. myös PeVL 10/2005 vp, PeVL 23/2005 vp ja PeVL 9/2014 vp).

Rajavartiolaitoksen osallistuminen olisi aina sidottu sotilastiedusteluviranomaisen pyyntöön eikä Rajavartiolaitos voisi itsenäisesti käynnistää sotilastiedustelutehtävää, valita tiedustelun kohdetta tai päättää tiedustelumenetelmän käyttämisestä. Menetelmän käytön edellytysten arviointi, kohdentaminen, päätöksenteko ja vastuu tiedustelutoiminnan lainmukaisuudesta säilyisivät sotilastiedusteluviranomaisella. Rajavartiolaitoksen tehtävä rajoittuisi yksittäisen, pyynnössä määritellyn toimeenpanotoimen suorittamiseen sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa.

Sotilastiedusteluviranomainen olisi asiassa toimivaltainen ja toimintaa johtava viranomainen. Rajavartiolaitoksen osallistuminen ei perustuisi sen omaan tiedustelulliseen arvioon, vaan sotilastiedusteluviranomaisen tekemään päätökseen, tämän esittämään yksilöityyn pyyntöön sekä pyyntöön sisältyviin määräyksiin. Avustavan viranomaisen mahdollisuus suorittaa käytännön toimenpide ei siten muuttaisi tiedustelumenetelmän käyttöä koskevan toimivallan tai vastuun oikeudellista kohdentumista.

Ehdotus ei alentaisi tiedustelumenetelmän käytön aineellisia tai menettelyllisiä edellytyksiä. Menetelmän käyttämiseen vaadittava tuomioistuimen lupa tai muu laissa säädetty päätös olisi hankittava samalla tavalla riippumatta siitä, suorittaako yksittäisen käytännön toimenpiteen sotilastiedusteluviranomaisen vai Rajavartiolaitoksen virkamies. Rajavartiolaitoksen avustamista ei siten voitaisi käyttää lupa-, välttämättömyys-, suhteellisuus- tai kohdentamisvaatimusten kiertämiseen.

Perustuslakivaliokunta on pitänyt perusoikeuksiin merkittävästi puuttuvien tiedustelutoimivaltuuksien kannalta olennaisena, että menetelmän käyttöä koskevat aineelliset edellytykset, päätöksenteko ja riippumaton valvonta säilyvät muuttumattomina toiminnan käytännön toteuttamistavasta riippumatta. Tiedustelutoimintaan tulee liittyä tehokas ja kattava valvontajärjestelmä, eikä pitkälle perusoikeuksiin puuttuvia toimivaltuuksia voida antaa ilman tehokasta valvontaa (PeVM 4/2018 vp, s. 9; PeVL 35/2018 vp, s. 30–31; PeVL 36/2018 vp, s. 35; PeVM 9/2018 vp).

Järjestely toteutettaisiin viranomaisten välisenä yhteistoimintana. Rajavartiolaitoksen virkamies toimisi laissa säädetyn toimivallan nojalla virkavastuulla, ja hänen toimintaansa koskisivat salassapitoa, tietoturvallisuutta, henkilötietojen käsittelyä ja virkamiehen vastuuta koskevat säännökset. Perustuslain 124 §:ssä tarkoitetusta julkisen hallintotehtävän antamisesta muulle kuin viranomaiselle ei olisi kyse.

Perusoikeuksiin puuttuvan toiminnan oikeudellinen määräysvalta säilyisi sotilastiedusteluviranomaisella. Rajavartiolaitoksen virkamiehelle ei siirtyisi itsenäistä harkintavaltaa siitä, kohdistetaanko tiedustelumenetelmää tiettyyn henkilöön, viestintään, laitteeseen tai muuhun kohteeseen. Vastuunjaon selkeyttäisi se, että sotilastiedusteluviranomainen vastaisi tiedustelumenetelmän käyttämisen edellytyksistä ja kokonaisuuden lainmukaisuudesta, kun taas Rajavartiolaitoksen virkamies vastaisi virkavastuulla oman konkreettisen menettelynsä asianmukaisuudesta.

Yhteistoiminnan voidaan katsoa olevan lähellä virka-apua ja johtoa voidaan hakea perustuslakivaliokunnan sitä koskevasta käytännöstä. Perustuslakivaliokunnan virka-apua koskevassa käytännössä on pidetty olennaisena, että avustavan viranomaisen tehtävät ja toimivaltuudet määritellään laissa täsmällisesti, toimintaa johtavan viranomaisen vastuu säilyy selkeänä ja virka-apua antava henkilöstö toimii virkavastuulla (PeVL 3/2022 vp, ks. myös PeVL 10/2005 vp, PeVL 23/2005 vp ja PeVL 9/2014 vp). Ehdotettu sääntely täyttää nämä lähtökohdat, koska Rajavartiolaitos voisi suorittaa ainoastaan sotilastiedusteluviranomaisen pyynnössä yksilöidyn toimeenpanotoimen tämän ohjauksessa ja valvonnassa.

Tiedustelumenetelmän käyttöä koskeva päätöksenteko, kohdentaminen ja vastuu kokonaisuuden lainmukaisuudesta säilyisivät sotilastiedusteluviranomaisella. Toiminta kuuluisi lisäksi kokonaisuudessaan riippumattoman tiedusteluvalvonnan piiriin, jonka tehokkuutta ja kattavuutta perustuslakivaliokunta on pitänyt perusoikeuksiin syvästi puuttuvien tiedustelutoimivaltuuksien välttämättömänä edellytyksenä (PeVM 4/2018 vp, s. 9; PeVL 35/2018 vp, s. 30–31; PeVL 36/2018 vp, s. 35; PeVM 9/2018 vp).

Rajavartiolaitoksen suorittamat toimenpiteet kuuluisivat tiedustelutoiminnan riippumattoman laillisuusvalvonnan piiriin. Sotilastiedusteluviranomaisen pyyntö, annetut määräykset, Rajavartiolaitoksen toteuttamat toimenpiteet ja toiminnan yhteydessä käsitellyt tiedot olisi dokumentoitava siten, että toimivallan käyttö, vastuunjako ja menettelyn lainmukaisuus voidaan todentaa jälkikäteen.

Perustuslakivaliokunta on tiedustelutoiminnan valvontaa koskevassa käytännössään edellyttänyt, että valvonta ulottuu yksittäisten tiedustelumenetelmien lisäksi yleisesti tiedustelutoimintaan ja tiedustelutiedon käyttöön. Valvonnan kattavuuden kannalta ei siten ole ratkaisevaa, minkä viranomaisen virkamies suorittaa yksittäisen käytännön toimenpiteen. Kun toimenpide tehdään osana sotilastiedustelutehtävää, sen tulee kuulua kokonaisuudessaan tiedusteluvalvontavaltuutetun valvontaan (PeVM 9/2018 vp)

Näin rajattuna ehdotus ei hajauta sotilastiedustelun päätösvaltaa eikä muodosta Rajavartiolaitoksesta uutta tiedusteluviranomaista. Kyse on tarkasti rajatusta viranomaisavusta, jolla voidaan hyödyntää Rajavartiolaitoksen olemassa olevaa toimintavalmiutta ja erityisosaamista muuttamatta tiedustelumenetelmien käytön oikeudellisia edellytyksiä tai niitä koskevia oikeusturvatakeita.

8. Ulkomaisen tietojärjestelmän toiminnan haittaaminen ja estäminen

Esityksen 1. lakiehdotuksen 62 §:n 5 momentin ehdotuksen tarkoituksena on mahdollistaa välitön ja kohdennettu puuttuminen Suomen maanpuolustusta tai kansallista turvallisuutta vakavasti uhkaavaan tietojärjestelmäperusteiseen toimintaan. Kyse olisi poikkeuksellisesta toimivaltuudesta, jota voitaisiin käyttää Suomen ulkopuolella olevaan yksilöityyn tietojärjestelmään, jos järjestelmällä tai sen kautta voidaan aiheuttaa vakavaa uhkaa Suomen maanpuolustukselle tai kansalliselle turvallisuudelle.

Ehdotettu toimivaltuus ei oikeuttaisi vaikutuksiltaan sotilaalliseen voimankäyttöön rinnastettavaan toimenpiteeseen. Jos suunnitellun toimenpiteen luonne, laajuus tai seuraukset ylittäisivät tiedustelullisen ja teknisen haittaamisen rajat, toimenpidettä ei voitaisi toteuttaa ehdotetun 62 §:n 5 momentin nojalla.

Suomen turvallisuuteen kohdistuva haitallinen toiminta voidaan toteuttaa ulkomailta käsin nopeasti, automatisoidusti ja tavalla, jossa hyökkäyksen vaikutukset voivat toteutua ennen kuin uhkaan voidaan vastata tavanomaisin hallinnollisin, oikeudellisin tai teknisin keinoin. Esimerkiksi kyberuhkien torjumisessa pelkkä tiedon hankkiminen, varoituksen antaminen tai puolustautuminen oman tietojärjestelmän sisällä ei kaikissa tilanteissa riitä. Vakavan vahingon estäminen voi edellyttää, että uhkaa aiheuttavan tietojärjestelmän toimintakykyyn vaikutetaan suoraan.

Perustuslakivaliokunta on korostanut, että valtion tulee pyrkiä takaamaan kansallinen turvallisuus ja yleinen järjestys kaikissa olosuhteissa. Perusoikeuksien välisessä intressipunninnassa on otettava huomioon rajoitusten taustalla olevat turvallisuusintressit erityisesti silloin, kun torjuttava uhka voi palautua myös perustuslain 7 §:ssä turvattuun henkilökohtaiseen turvallisuuteen (PeVL 16/2022 vp, kappale 10; PeVL 37/2022 vp, kappale 8). Ehdotetulla toimivaltuudella toteutettaisiin samalla perustuslain 22 §:ssä julkiselle vallalle asetettua velvollisuutta turvata perus- ja ihmisoikeuksien toteutuminen ehkäisemällä Suomen maanpuolustukseen, kriittiseen infrastruktuuriin ja yhteiskunnan välttämättömiin palveluihin kohdistuvia vakavia kyberuhkia.

Perustuslakivaliokunta on tiedustelulainsäädäntöä arvioidessaan edellyttänyt, että kansallisen turvallisuuden käsitettä tulkitaan suppeasti, uhkan vakavuusaste asetetaan korkealle ja tiedustelutoimivaltuuksien kohdentumisesta säädetään täsmällisesti. Valiokunta on lisäksi korostanut, että toimivaltuuden käyttämisen välttämättömyys on voitava osoittaa yksittäistapauksessa ja tavoite on pyrittävä saavuttamaan vähemmän puuttuvalla keinolla (PeVM 4/2018 vp, s. 7–9; PeVL 35/2018 vp, s. 7–8; PeVL 36/2018 vp). Ehdotetun toimivaltuuden korkea käyttökynnys, kohdistaminen yksilöityyn tietojärjestelmään, viimesijaisuus ja sivullisvaikutusten minimointi vastaavat näitä lähtökohtia.

Toimivaltuuden avulla voitaisiin ehkäistä tai rajoittaa esimerkiksi Puolustusvoimien toimintakykyyn, kriittiseen infrastruktuuriin, välttämättömiin palveluihin tai laajasti yhteiskunnan turvallisuuteen kohdistuvaa vakavaa kybertoimintaa. Toimenpiteellä saavutettava perusoikeuksien suoja voisi siten olla huomattavasti suurempi kuin yksilöityyn ulkomaiseen tietojärjestelmään kohdistuva rajattu haitta.

Ehdotuksella ei annettaisi yleistä toimivaltaa vaikuttaa ulkomaisiin tietojärjestelmiin eikä sitä voitaisi käyttää tavanomaisen haitallisen verkkotoiminnan torjumiseen; toimenpiteet liittyisivät aina sotilastiedustelun kohteisiin. Toimivallan käyttö olisi sidottu erityisen korkeaan aineelliseen kynnykseen, vakavaan uhkaan Suomen maanpuolustukselle tai kansalliselle turvallisuudelle. Toimenpiteen kohteena tulisi olla yksilöity tietojärjestelmä, jolla on konkreettinen yhteys uhkaa aiheuttavaan toimintaan. Toimivaltuutta ei siten voitaisi käyttää yleiseen tietoverkkotoiminnan valvontaan, ennakoimattomaan varautumiseen tai pelkästään tiedustelutoiminnan tehostamiseksi.

Tietojärjestelmän toimintaa voitaisiin haitata vain, jos tavoiteltavaa lopputulosta ei voida saavuttaa riittävän nopeasti muulla lievemmällä keinolla. Ennen toimenpidettä olisi arvioitava muun muassa uhkan vakavuus ja välittömyys, toimenpiteen odotettavissa oleva tehokkuus, kohdejärjestelmän käyttötarkoitukset, sivullisille aiheutuvat vaikutukset sekä toimenpiteen ulko- ja turvallisuuspoliittiset seuraukset.

Toimivaltuutta rajoittaisivat välttämättömyys- ja suhteellisuusvaatimus. Toimenpide olisi toteutettava siten, että sillä vaikutetaan ainoastaan siinä määrin ja niin kauan kuin vakavan uhkan ehkäiseminen edellyttää. Jos uhka voidaan torjua järjestelmän toimintaa tilapäisesti hidastamalla tai rajoittamalla, sitä ei voitaisi tehdä kokonaan käyttökelvottomaksi. Toimenpide olisi lopetettava heti, kun sen edellytykset lakkaavat tai tavoite on saavutettu. Tarkoituksena ei olisi aiheuttaa rangaistusluonteista vahinkoa, hankkia taloudellista etua tai puuttua vieraan valtion toimintaan yleisesti. Toimenpiteen ainoa hyväksyttävä tarkoitus olisi estää tai rajoittaa Suomen maanpuolustukseen tai kansalliseen turvallisuuteen kohdistuvan vakavan uhkan toteutumista.

Toimivaltuuden käyttäminen ei myöskään vapauttaisi Suomea kansainvälisen oikeuden noudattamisesta**.** Säännös muodostaisi kansallisen toimivaltaperustan, mutta jokaisen toimenpiteen kansainvälisoikeudellinen hyväksyttävyys olisi arvioitava erikseen. Arvioinnissa olisi otettava huomioon kohdejärjestelmän sijaintivaltio, toiminnan vaikutukset sen alueella, uhkan alkuperä ja vakavuus sekä kansainvälisen oikeuden asettamat välttämättömyys- ja suhteellisuusvaatimukset. Kotimainen toimivaltasäännös ei siten merkitsisi yleistä oikeutta ryhtyä tietoteknisiin toimenpiteisiin toisen valtion alueella.

Toimivaltuuden käytön mahdolliset ulko- ja turvallisuuspoliittiset sekä eskalaatioon liittyvät vaikutukset edellyttäisivät asianmukaisen korkean tason päätöksenteon lisäksi toiminnan jatkuvaa riskinarviointia. Arviointia olisi tehtävä ennen toimenpiteeseen ryhtymistä ja koko sen toteuttamisen ajan. Toimenpide olisi keskeytettävä, jos sen vaikutukset muodostuvat ennakoitua laajemmiksi tai jos sivullisille taikka Suomen turvallisuuseduille aiheutuva riski kasvaa suhteettomaksi.

Näin rajattuna toimivaltuus täydentäisi sotilastiedustelua tilanteissa, joissa tiedustelun avulla tunnistettu vakava kyberuhka edellyttää viipymätöntä vaikuttamista ennen vahingon toteutumista. Kyse ei olisi sotilastiedusteluviranomaisen yleisestä toimivallasta toteuttaa hyökkäyksellisiä kyberoperaatioita, vaan tarkasti kohdennetusta, viimesijaisesta ja puolustuksellisesta keinosta Suomen maanpuolustuksen ja kansallisen turvallisuuden suojaamiseksi.

9. Ulkomaisen toimivaltaisen virkamiehen osallistuminen

Ulkomaisen toimivaltaisen virkamiehen rajattu osallistuminen sotilastiedustelutoimintaan on perusteltua Suomen kansallisten etujen, maanpuolustuksen ja kansallisen turvallisuuden suojaamiseksi. Rajat ylittävien sotilaallisten ja muiden turvallisuusuhkien tunnistaminen edellyttää kykyä yhdistää Suomen ja sen liittolaisten erityisosaamista, teknisiä suorituskykyjä ja tiedustelutietoja. Sääntely parantaa Suomen mahdollisuuksia hyödyntää kansainvälistä yhteistyötä ilman, että sotilastiedustelun aineellista kohdealaa tai tiedustelumenetelmien käyttöedellytyksiä laajennetaan.

Ehdotus ei merkitse itsenäisen toimivallan antamista ulkomaiselle viranomaiselle eikä Suomen julkisen vallan käyttöä koskevan päätösvallan siirtämistä toiselle valtiolle. Ulkomaisen virkamiehen osallistuminen edellyttää Pääesikunnan tiedustelupäällikön päätöstä ja tapahtuu aina suomalaisen sotilastiedusteluviranomaisen virkamiehen kanssa sekä tämän välittömässä ohjauksessa ja valvonnassa. Ulkomainen virkamies on velvollinen noudattamaan suomalaisen viranomaisen määräyksiä, rajoituksia ja ohjeita, eikä hän voi päättää tiedustelutehtävästä, sen kohteesta tai tiedustelumenetelmän käytöstä.

Perustuslakivaliokunnan käytännössä ulkomaisten virkamiesten rajattua toimimista Suomessa ei ole pidetty täysivaltaisuuden kannalta ongelmallisena, kun toiminta perus-

tuu lakiin, tapahtuu suomalaisen viranomaisen johdolla ja valvonnassa ja on sidottu tarkasti määriteltyihin tehtäviin (PeVL 9/2009 vp). Ehdotetussa sääntelyssä sotilastiedusteluviranomainen vastaa aina tiedustelumenetelmän käytön lainmukaisuudesta, menetelmän käyttöön sovelletaan Suomen lain mukaisia päätös- ja lupamenettelyjä ja toiminta kuuluu tiedusteluvalvontavaltuutetun riippumattoman valvonnan piiriin.

Kun ulkomaisen virkamiehen osallistuminen on avustavaa, ajallisesti ja asiallisesti rajattua sekä suomalaisen viranomaisen tosiasiallisen määräysvallan alaista ja kun vastuusta ja valvonnasta säädetään kattavasti, ehdotus ei puutu merkittävästi perustuslain 1 §:ssä turvattua Suomen täysivaltaisuutta eikä perustuslain 2 §:n 3 momentissa säädettyä oikeusvaltioperiaatetta. Sääntely voidaan käsitellä tavallisen lain säätämisjärjestyksessä.

10. Sivullisen laitteen tai tietojärjestelmän käyttäminen

Esityksen 1. lakiehdotuksen 42 §:ssä ehdotetaan, että sotilastiedusteluviranomainen voisi käyttää sivullisen laitetta tai tietojärjestelmää tiettyjen toimenpiteiden suorittamiseksi. Toimivaltuuden tarkoituksena on mahdollistaa tiedustelumenetelmän tekninen toteuttaminen tilanteessa, jossa pääsy tiedustelun varsinaiseen kohteeseen ei muutoin ole mahdollinen tai turvallisesti toteutettavissa. Sivullisen laitetta tai tietojärjestelmää voitaisiin käyttää vain, jos se olisi välttämätöntä tiedustelumenetelmän tai siinä tarvittavan ohjelmiston asentamiseksi kohteena olevaan laitteeseen tai järjestelmään taikka sen poistamiseksi. Sivullisen oma laite ei tällöin olisi tiedustelun varsinainen kohde, vaan tekninen väline, jonka kautta laissa säädetty ja asianmukaisesti luvitettu tiedustelumenetelmä toteutetaan.

Perustuslain 2 §:n 3 momentista seuraa, että julkisen vallan käytön tulee perustua lakiin. Perustuslakivaliokunnan vakiintuneen käytännön mukaan viranomaisen toimivaltuuksien tulee olla täsmällisiä ja tarkkarajaisia, ja sääntelystä tulee käydä ilmi ainakin toimivallan sisältö, käyttämisen edellytykset ja käytön enimmäislaajuus. Vaatimukset korostuvat silloin, kun toimivaltuus mahdollistaa salaisen puuttumisen sivullisen yksityiselämän tai omaisuuden suojaan (PeVL 66/2010 vp ja PeVL 67/2010 vp).

Toimivaltuuden tarvetta puoltaa se, että nykyisessä verkottuneessa toimintaympäristössä tiedustelun kohteena olevaan laitteeseen tai järjestelmään ei aina voida päästä suoraan. Kohde voi olla teknisesti eristetty, suojattu tai saavutettavissa vain muun laitteen tai tietojärjestelmän välityksellä. Jos sivullisen laitetta ei voitaisi käyttää edes tarkasti rajattuna teknisenä välivaiheena, muutoin lainmukainen ja välttämätön tiedustelumenetelmä voisi jäädä toteuttamatta tai sen toteuttaminen voisi edellyttää laajempaa ja sivullisten oikeuksiin voimakkaammin puuttuvaa vaihtoehtoista menettelyä.

Perustuslakivaliokunta on tiedustelulainsäädäntöä arvioidessaan katsonut, että perustuslain 10 §:n 4 momentin välttämättömyysvaatimus merkitsee tiedonhankinnan sallimista vain, jos tietoa ei voida hankkia vähemmän puuttuvin keinoin. Viestin salaisuuteen on lisäksi puututtava mahdollisimman kohdennetusti ja rajoitetusti, ja välttämättömyys on arvioitava kussakin yksittäistapauksessa. Valiokunta on myös pitänyt tiedustelumenetelmien käytön yleistä välttämättömyysedellytystä edellytyksenä sääntelyn käsittelemiselle tavallisessa lainsäätämisjärjestyksessä (PeVM 4/2018 vp, s. 8–9; PeVL 35/2018 vp, s. 7–8; PeVL 36/2018 vp).

Ehdotuksella ei annettaisi yleistä oikeutta käyttää sivullisten laitteita tai käsitellä niiden sisältämiä tietoja. Toimivaltuus olisi sidottu yksittäiseen tiedustelutehtävään ja nimenomaan tiedustelumenetelmän teknisen toteuttamisen välttämättömyyteen. Sivullisen laitteen käyttäminen ei laajentaisi tiedustelumenetelmän kohdetta, tarkoitusta tai aineellisia käyttöedellytyksiä. Laitteessa olevia sivullisen tietoja ei saisi käsitellä muutoin kuin siltä osin kuin se olisi teknisen toimenpiteen toteuttamiseksi väistämätöntä.

Perustuslakivaliokunta on tiedustelulainsäädännön yhteydessä korostanut, ettei perustuslain 10 §:n 4 momentti mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa. Sama täsmällisen kohdentamisen vaatimus puoltaa nyt käsiteltävän toimivaltuuden rajaamista vain ennalta suunniteltuun tekniseen toimenpiteeseen. Sivullisen laitteen käyttäminen ei saisi muodostua keinoksi hankkia tietoja sivullisesta tai hänen viestinnästään eikä laajentaa alkuperäisen tiedusteluluvan kohdealaa (PeVM 4/2018 vp, s. 7–9; PeVL 35/2018 vp; PeVL 36/2018 vp).

Ehdotuksessa sivulliselle aiheutuvaa puuttumista rajoittaa olennaisesti vaatimus siitä, ettei laitteen tai tietojärjestelmän käyttämisestä saa aiheutua vähäistä suurempaa haittaa. Toimenpide olisi suunniteltava ja toteutettava siten, ettei se vaaranna laitteen käyttöturvallisuutta, tietoturvallisuutta tai tavanomaista toimintaa eikä aiheuta tietojen häviämistä, muuttumista tai paljastumista. Hallituksen esityksen perusteluissa toimivaltuus on kuvattu yksittäiseen laitteeseen tai järjestelmän osaan kohdistuvaksi, eikä sitä ole tarkoitettu toteutettavaksi esimerkiksi teleyrityksen kriittistä tuotantoinfrastruktuuria hyödyntämällä. Esityksessä toimenpiteen arvioidaan olevan kestoltaan lyhyt, ja siitä aiheutuvan haitan olisi jäätävä vähäiseksi.

Sivullisen laitetta voitaisiin käyttää vain, jos tiedustelumenetelmää ei voida toteuttaa yhtä tehokkaasti ja turvallisesti muulla, sivullisen oikeuksiin vähemmän puuttuvalla keinolla. Käytettävissä olevista vaihtoehdoista olisi valittava se, joka aiheuttaa sivulliselle vähiten haittaa. Toimenpiteen olisi lisäksi oltava ajallisesti lyhyt, teknisesti rajattu ja mahdollisuuksien mukaan täysin palautettava.

Perustuslain 15 §:ssä turvattu omaisuudensuoja kattaa omistajan oikeuden käyttää ja hallita omaisuuttaan. Sivullisen laitteen käyttäminen merkitsee siten omaisuudensuojan kannalta omaisuuden käyttöön kohdistuvaa rajoitusta, vaikka sivullinen ei menettäisi laitteen omistusta tai hallintaa. Perustuslakivaliokunta arvioi omaisuuden käyttörajoituksia perusoikeuksien yleisten rajoitusedellytysten perusteella kiinnittäen huomiota erityisesti rajoituksen hyväksyttävään tarkoitukseen, täsmällisyyteen, välttämättömyyteen ja oikeasuhtaisuuteen. Omaisuudensuojan rajoituksen hyväksyttävyyteen vaikuttavat myös rajoituksen tosiasiallinen vaikutus, kesto ja se, säilyykö omistajalla mahdollisuus käyttää omaisuuttaan normaalisti. Valiokunnan omaisuudensuojaa koskevassa käytännössä rajoitusten hyväksyttävyyttä on arvioitu juuri tällaisena kokonaisuutena, ei siten, että jokainen omaisuuden käyttöön kohdistuva puuttuminen olisi sellaisenaan kielletty.

Ehdotuksella suojataan maanpuolustusta ja kansallista turvallisuutta sellaisilta vakavilta uhkilta, joiden selvittämiseen tiedustelumenetelmän käyttäminen on välttämätöntä. Perustuslakivaliokunta on korostanut valtion velvollisuutta pyrkiä takaamaan kansallinen turvallisuus ja yleinen järjestys kaikissa olosuhteissa. Perusoikeuksien välisessä punninnassa on otettava huomioon toimenpiteiden taustalla olevat turvallisuusintressit erityisesti silloin, kun suojattava etu voi palautua myös perustuslain 7 §:ssä turvattuun henkilökohtaiseen turvallisuuteen (PeVL 16/2022 vp, kappale 10; PeVL 37/2022 vp, kappale 8).

Puuttuminen sivullisen omaisuudensuojaan jäisi ehdotuksessa vähäiseksi, koska sivullinen ei menettäisi laitteen hallintaa tai käyttömahdollisuutta, toimenpiteen kesto olisi rajattu eikä siitä saisi aiheutua vähäistä suurempaa haittaa. Omaisuudensuojan rajoituksen vastapainona on erityisen painava yhteiskunnallinen intressi eli maanpuolustuksen ja kansallisen turvallisuuden suojaaminen. Sääntelyn hyväksyttävyyttä tukee myös perustuslain 22 §:ssä julkiselle vallalle säädetty velvollisuus turvata perus- ja ihmisoikeuksien toteutuminen. Valiokunta on pitänyt tätä turvaamisvelvollisuutta merkityksellisenä arvioitaessa sääntelyä, jolla varaudutaan vakaviin turvallisuus- ja häiriötilanteisiin.

Sääntelyssä otettaisiin samalla huomioon mahdollisuus, että toimenpiteestä aiheutuu ennakoimaton vahinko. Esityksen mukaan tällainen vahinko tulisi korvattavaksi vahingonkorvauslain mukaisesti. Vahingonkorvausvastuu täydentää toimenpiteen ennakollisia rajoituksia, vaikka toimivaltuuden hyväksyttävyyden ensisijaisena takeena on vahingon estäminen eikä sen jälkikäteinen korvaaminen.

Toimivaltuuden käyttö olisi osa asianmukaisesti päätettyä tiedustelumenetelmää ja kuuluisi tiedusteluvalvontavaltuutetun riippumattoman valvonnan piiriin. Sivullisen laitteen käyttämisen perusteet, käytetty laite, toimenpiteen tarkoitus, toteuttamistapa ja havaitut vaikutukset olisi dokumentoitava siten, että toiminnan välttämättömyys, oikeasuhtaisuus ja lainmukaisuus voidaan todentaa jälkikäteen.

Perustuslakivaliokunta on pitänyt tiedustelutoiminnan tehokasta ja kattavaa valvontajärjestelmää välttämättömänä. Valiokunnan mukaan ilman tehokasta valvontaa viranomaisille ei voida antaa pitkälle perusoikeuksiin puuttuvia tiedustelutoimivaltuuksia. Valvonnan tulee ulottua yksittäisten tiedustelumenetelmien lisäksi tiedustelutoimintaan yleisesti ja tiedustelutiedon käyttöön (PeVM 4/2018 vp, s. 9; PeVL 35/2018 vp, s. 30–31; PeVL 36/2018 vp, s. 35; PeVM 9/2018 vp).

Näin rajattuna toimivaltuus ei merkitsisi sivullisen omaisuuden ottamista yleisesti tiedusteluviranomaisen käyttöön. Kyse olisi yksittäisestä, lyhytaikaisesta ja teknisesti rajatusta toimenpiteestä, joka on välttämätön laissa säädetyn tiedustelumenetelmän toteuttamiseksi ja josta ei saa aiheutua sivulliselle vähäistä suurempaa haittaa. Sääntelyllä voidaan siten katsoa olevan hyväksyttävä, painava ja perusoikeusjärjestelmän kannalta oikeasuhtainen peruste.

11. Tiedonhankinta yleisesti saatavilla olevista lähteistä

Esityksen 2. lakiehdotuksen 8 b §:ssä säädettäisiin tiedonhankinnasta yleisesti saatavilla olevista lähteistä. Sääntely olisi uudentyppistä.

Ehdotetun sääntelyn tarkoituksena on luoda selkeä lakisääteinen perusta Puolustusvoimien tehtäviin liittyvälle tiedonhankinnalle yleisesti saatavilla olevista lähteistä sekä tällaisen tiedonhankinnan suojaamiselle. Tiedonhankintaa voitaisiin toteuttaa sekä manuaalisesti että automaattisesti. Yhteys Puolustusvoimiin voitaisiin tarvittaessa peittää käyttämällä vääriä, harhauttavia tai peiteltyjä tietoja. Ehdotuksella ei annettaisi oikeutta hankkia tietoja lähteistä, jotka eivät ole yleisesti saatavilla, eikä kiertää tietojärjestelmien käyttörajoituksia tai teknisiä suojauksia.

Perustuslain 2 §:n 3 momentin mukaan julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Perustuslakivaliokunta on pitänyt viranomaisen toimivaltuuksien nimenomaista lakiperustaa sekä sääntelyn täsmällisyyttä ja tarkkarajaisuutta erityisen tärkeinä silloin, kun toiminnassa käsitellään henkilötietoja tai käytetään salaisen tiedonhankinnan menetelmiä. Ehdotettu säännös parantaa toiminnan valtiosääntöoikeudellista perustaa saattamalla tiedonhankinnan tarkoituksen, tiedonlähteet, toteuttamistavat ja peitteen käytön nimenomaisen laintasoisen sääntelyn piiriin (PeVL 66/2010 vp ja PeVL 67/2010 vp).

Yleisesti saatavilla oleviin lähteisiin kohdistuva tiedonhankinta on tarpeen, koska sotilaallista toimintaa ja kansalliseen turvallisuuteen vaikuttavia ilmiöitä koskevaa merkityksellistä tietoa julkaistaan yhä enemmän avoimissa tietoverkoissa, verkkopalveluissa ja muissa julkisissa lähteissä. Tällaisen tiedon järjestelmällinen hankkiminen, yhdistäminen ja analysointi tukee turvallisuusympäristön muutosten havaitsemista, tilannekuvan muodostamista ja Puolustusvoimien lakisääteisten tehtävien hoitamista. Avoimista lähteistä saatava tieto voi myös vähentää tarvetta käyttää yksityisyyteen voimakkaammin puuttuvia salaisia tiedonhankintakeinoja.

Perustuslakivaliokunta on tiedustelulainsäädäntöä arvioidessaan katsonut, että tiedonhankinnassa on käytettävä ensisijaisesti perusoikeuksiin vähemmän puuttuvaa keinoa ja että puuttuminen on rajattava mahdollisimman kohdennetuksi. Välttämättömyyttä on arvioitava tiedustelumenetelmän käytön edellytyksenä yksittäistapauksessa. Avoimista lähteistä tapahtuva tiedonhankinta voi toteuttaa näitä vaatimuksia, jos sen avulla tarvittava tieto voidaan hankkia ilman salaisen tiedustelumenetelmän käyttämistä (PeVM 4/2018 vp, s. 8–9; PeVL 35/2018 vp, s. 7–8; PeVL 36/2018 vp).

Tiedon yleinen saatavuus ei merkitse sitä, että tiedon käsittely jäisi perustuslain 10 §:ssä turvatun yksityiselämän ja henkilötietojen suojan ulkopuolelle. Julkisista lähteistä koottujen tietojen laajamittainen yhdistäminen ja analysointi voi antaa henkilöstä sellaisen kokonaiskuvan, jota yksittäisistä tiedoista ei ole mahdollista muodostaa. Ehdotuksen hyväksyttävyyttä tukee kuitenkin se, että tiedonhankinta olisi sidottu Puolustusvoimien laissa säädettyihin tehtäviin eikä yleisesti saatavilla olevia tietoja voitaisi kerätä tai käsitellä ilman tällaista tehtäväkohtaista yhteyttä.

Perustuslakivaliokunta on henkilötietojen käsittelyä koskevassa käytännössään katsonut henkilötietojen suojan kuuluvan osittain perustuslain 10 §:ssä turvatun yksityiselämän suojan piiriin. Lainsäätäjän tulee turvata henkilötietojen suoja tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa. Arvioinnissa on kiinnitettävä huomiota erityisesti käsittelyn tarkoitukseen, tietosisältöön, käsittelyn laajuuteen, säilytysaikaan ja rekisteröidyn oikeusturvaan (ks. esimerkiksi PeVL 51/2018 vp ja siinä viitattu käytäntö).

Perustuslakivaliokunta on henkilötietojen käsittelyä koskevassa käytännössään edellyttänyt laintasoista sääntelyä käsittelyn tavoitteista, tietosisällöistä ja sallituista käyttötarkoituksista sekä korostanut henkilötietojen käyttötarkoitussidonnaisuutta ja tarpeettomien tietojen poistamista. Tietojen kerääminen on jo itsessään henkilötietojen käsittelyä, joten myös yleisesti saatavilla olevia tietoja voidaan kerätä vain tiettyä ja nimenomaista tarkoitusta varten. Erityisesti arkaluonteisten tietojen käsittely on rajattava täsmällisillä ja tarkkarajaisilla säännöksillä vain välttämättömään (PeVL 51/2018 vp, s. 7–8, 13–16; PeVL 3/2017 vp, s. 5; PeVL 15/2018 vp, s. 40 ja 45)

Hallintopoliittinen osasto
Lainvalmistelu- ja oikeusyksikkö
Vanhempi hallitussihteeri Kosti Honkanen

Ehdotetussa sääntelyssä tiedonhankinnan yhteys Puolustusvoimien tehtäviin muodostaa näin keskeisen aineellisen rajauksen. Tiedonhankinta ei saisi muodostua yleiseksi verkkoympäristön kartoittamiseksi, vaan kerättävällä tiedolla tulisi olla riittävä yhteys laissa säädettyyn tehtävään. Tieto, jonka tarpeellista yhteyttä tehtävään ei voida todeta, olisi poistettava ilman aiheetonta viivytystä.

Automaattisen tiedonhankinnan salliminen ei merkitsisi rajoittamatonta verkkoympäristön seurantaa. Automatisointi koskisi tiedon hankkimisen teknistä toteuttamistapaa, eikä se laajentaisi tiedonhankinnan aineellista käyttötarkoitusta tai sallittujen tietolähteiden piiriä. Automaattisen käsittelyn olisi oltava tarpeellista laissa säädetyn tehtävän suorittamiseksi, ja hankittavan tiedon määrä olisi rajattava tarkoituksen kannalta tarpeelliseen.

Tiedonhankinnassa tulisivat sovellettaviksi henkilötietojen käsittelyä koskeva lainsäädäntö, tarkoitussidonnaisuus, tarpeellisuus- ja suhteellisuusperiaatteet, tietojen minimointi, tietojen laatua koskevat vaatimukset, käyttöoikeuksien rajaaminen sekä tarpeettomien tietojen poistaminen. Yleisesti saatavilla olevan tiedon käsittely ei siten tarkoittaisi, että tieto voitaisiin säilyttää pysyvästi tai käyttää myöhemmin mihin tahansa tarkoitukseen.

Puolustusvoimiin olevan yhteyden peittäminen on tarpeen tiedonhankinnan toteuttajan turvallisuuden, tiedonhankinnan tarkoituksen ja viranomaisen toimintamenetelmien suojaamiseksi. Jos verkkopalvelun käyttäjälle, palvelun ylläpitäjälle tai ulkomaiselle toimijalle ilmenisi välittömästi, että tietoa hankkii Puolustusvoimat, tiedonhankinnan kohteena oleva toimija voisi muuttaa käyttäytymistään, poistaa tietoja, estää pääsyn palveluun tai ryhtyä vastatoimiin tiedonhankintaa suorittavaa henkilöä tai Puolustusvoimien tietojärjestelmiä vastaan.

eitteen käyttöä voidaan puolestaan arvioida soveltuvin osin valiokunnan peitetoimintaa koskevan käytännön valossa. Valiokunta on hyväksynyt peitteen käytön osana salaista tiedonhankintaa, kun toiminnan edellytyksistä, rajoista, vastuusta ja valvonnasta säädetään täsmällisesti laissa (PeVL 67/2010 vp; PeVL 66/2010 vp). Ehdotettu peite olisi tätä lievempi, koska se ei muodostaisi itsenäistä tiedonhankintamenetelmää eikä mahdollistaisi pääsyä ei-julkisiin tietoihin.

Peitteen käyttäminen voisi olla tarpeen myös viranomaisen tietotarpeiden ja tiedonhankinnan painopisteiden suojaamiseksi. Pelkästään tieto siitä, mitä verkkosivustoja, käyttäjätilejä, keskusteluryhmiä tai ilmiöitä Puolustusvoimat seuraa, voi paljastaa Suomen puolustuskykyyn, uhka-arvioihin tai tiedustelullisiin tietotarpeisiin liittyviä seikkoja.

Peitteen laatu ja laajuus olisi suhteutettava suojattavaan tiedonhankintaan. Mahdollisimman vähäistä peitettä olisi käytettävä silloin, kun tiedonhankinnan tarkoitus voidaan turvata esimerkiksi pelkällä organisaatioyhteyden salaamisella. Väärien henkilötietojen tai laajemman peiteprofiilin käyttäminen edellyttäisi tätä painavampaa perustetta.

Toiminnan lainmukaisuus olisi voitava todentaa jälkikäteen. Tiedonhankinta, automaattisesti kerätyt aineistot ja peitteen käyttö olisi dokumentoitava ja lokitettava riittävästi. Valvonnassa olisi voitava arvioida erityisesti tiedonhankinnan yhteys Puolustusvoimien lakisääteiseen tehtävään, kerättyjen tietojen tarpeellisuus, automaattisen käsittelyn kohdentuminen sekä peitteen käytön asianmukaisuus.

Yleisesti saatavilla oleviin lähteisiin kohdistuva tiedonhankinta ja siinä käytettävä peite eivät muodosta uutta salaista tiedonhankintamenetelmää eivätkä laajenna Puolustusvoimien pääsyä ei-julkisiin tietoihin. Sääntelyllä luodaan täsmällinen oikeusperusta avoimista lähteistä tapahtuvaan tehtäväsidonnaiseen tiedonhankintaan ja mahdollistetaan Puolustusvoimiin olevan yhteyden suojaaminen silloin, kun se on välttämätöntä tiedonhankinnan tarkoituksen, menetelmien tai henkilöstön turvallisuuden turvaamiseksi.

12. Tietolähteen rajaylityksessä avustaminen

Esityksessä ehdotetaan sääntelyä täsmennettäväksi siten, että sotilastiedusteluviranomainen voisi poikkeuksellisessa tilanteessa avustaa tietolähdettä Suomen rajan ylittämisessä, jos tämä on välttämätöntä tietolähteen hengen tai terveyden suojaamiseksi. Avustaminen voisi tulla kyseeseen esimerkiksi silloin, kun ulkomailla toimineen tietolähteen turvallisuutta ei voida enää turvata asemamaassa ja tietolähde on tämän vuoksi saatava Suomeen tai Suomen kautta kolmanteen valtioon. Erityistilanteessa raja voitaisiin joutua ylittämään muualla kuin virallisella rajanylityspaikalla tai virallisen rajanylityspaikan kautta peitellysti.

Nykyisessä sääntelyssä sotilastiedusteluviranomaisen virkamiehen osallistumista epätavalliseen rajanylitykseen voitaisiin arvioida rikoslain 17 luvun 8 §:ssä tarkoitettuna laittoman maahantulon järjestämisenä. Myös tietolähteen toiminta voisi tulla arvioitavaksi rikoslain 17 luvun 7 §:ssä tarkoitettuna valtionrajarikoksena. Ehdotuksen tarkoituksena on poistaa tämä epäselvyys säätämällä nimenomaisesti niistä tarkkarajaisista tilanteista, joissa viranomainen voi suojelutarkoituksessa avustaa tietolähdettä rajanylityksessä.

Ehdotus täydentäisi sotilastiedustelusta annetun lain 78 §:ssä säädettyä tietolähteen turvaamista. Voimassa olevan sääntelyn mukaan tietolähteen turvallisuudesta on huolehdittava tarpeen mukaan sekä tiedonhankinnan aikana että sen jälkeen. Pääesikunnan tiedustelupäällikkö voi lisäksi päättää väärien, harhauttavien tai peiteltyjen tietojen, rekisterimerkintöjen tai asiakirjojen antamisesta tietolähteelle, jos se on välttämätöntä tämän hengen tai terveyden suojaamiseksi. Ehdotettu sääntely mahdollistaisi turvaamisvelvoitteen tehokkaan toteuttamisen myös silloin, kun tietolähteen turvallinen poistuminen asemamaasta edellyttää viranomaisen aktiivista avustamista rajanylityksessä

Tietolähde voi sotilastiedusteluviranomaisen kanssa tekemänsä yhteistyön vuoksi altistua vainolle, väkivallalle, vapaudenmenetykselle tai muulle vakavalle vaaralle. Kun vaara liittyy tietolähteen toimintaan Suomen viranomaisen hyväksi, valtiolle muodostuu korostunut velvollisuus ryhtyä kohtuudella käytettävissä oleviin toimiin tietolähteen suojaamiseksi. HE 104/2026 vp:ssä muutoksella arvioidaan olevan myönteisiä vaikutuksia tietolähteen perus- ja ihmisoikeuksien suojaan.

Perustuslakivaliokunta on korostanut, että perustuslain 7 § turvaa siinä mainittuja oikeushyviä paitsi julkisen vallan omilta toimenpiteiltä myös edellyttää valtiolta lainsäädännöllisiä toimia niiden suojaamiseksi muiden tahojen loukkauksia vastaan. Valiokunta on lisäksi pitänyt ihmisten henkeä, terveyttä ja turvallisuutta vakavasti vaarantavan toiminnan estämistä painavana perusoikeusjärjestelmän mukaisena tavoitteena. Näille turvallisuusintresseille voidaan antaa merkitystä myös käytettävien keinojen oikeasuhtaisuutta arvioitaessa (ks. esim. PeVL 26/2014 vp, s. 2; PeVL 37/2016 vp, s. 2; PeVL 20/2018 vp, s. 2; PeVL 11/2026 vp, kappaleet 1 ja 2).

Tietolähteen avustaminen Suomen rajan yli olisi poikkeuksellinen ja viimesijainen suojelutoimi, jonka ainoana hyväksyttävänä tarkoituksena olisi tietolähteen hengen tai terveyden turvaaminen. Toimivaltuus täydentäisi sotilastiedusteluviranomaiselle jo säädettyä velvollisuutta huolehtia tietolähteen turvallisuudesta tiedonhankinnan aikana ja sen jälkeen.

Perustuslain 8 §:ssä säädetty rikosoikeudellinen laillisuusperiaate edellyttää, että rikosoikeudellisen vastuun perusteet määräytyvät lain nojalla. Samanaikaisesti perustuslain 2 §:n 3 momentti edellyttää, että viranomaisen toimivaltuus poiketa yleisesti sovellettavista velvoitteista perustuu täsmälliseen lakiin. Perustuslakivaliokunta on korostanut, että sekä rikosoikeudellisen rangaistusvastuun että muun rikosoikeudellisen seuraamuksen tulee perustua lakiin.

Ehdotus toteuttaisi perustuslain 7 ja 22 §:stä johtuvaa julkisen vallan aktiivista turvaamisvelvollisuutta. Samalla nimenomainen laintasoinen sääntely selkeyttäisi perustuslain 2 §:n 3 momentin ja 8 §:n kannalta virkamiehen toimivallan sekä tietolähteen ja virkamiehen rikosoikeudellisen aseman. Kun toimivaltuus rajataan yksittäistapaukseen, konkreettiseen hengen tai terveyden vaaraan, välttämättömyyteen, korkeatasoiseen päätöksentekoon, kattavaan dokumentointiin ja riippumattomaan valvontaan, ehdotusta voidaan pitää perusoikeusjärjestelmän kannalta hyväksyttävänä ja oikeasuhtaisena.

13. Muita huomioitavia seikkoja

Esityksen 1. lakiehdotuksen 91 §:ssä ehdotetaan, että reserviläisten lisäksi vapaaehtoiseen maanpuolustuksen harjoitukseen osallistuvia voitaisiin käyttää sotilastiedustelutoiminnassa. Henkilöpiirin laajennusta ei voida pitää perustuslain kannalta merkittävänä. Keskeistä on se, että kyse ei ole perustuslain 124 §:n mukaisesta julkisen vallan käytön siirtämisestä yksityiselle. Lisäksi virkavastuusta ja vahingonkorvausvastuusta olisi säädetty tarkasti.

Esityksen 1. lakiehdotuksen 11 §:ssä ehdotetaan, että puolustushaarat voisivat radiosignaalitiedustelun lisäksi käyttää perusmuotoista tietolähdetoimintaa. Toiminnassa on kyse passiivisesta tietojen vastaanottamisesta eikä tietojen vastaanottaminen ole satunnaista.

Esityksessä laajennettaisiin sotilastiedusteluviranomaisen ja eräiden muiden viranomaisten tietojen vaihtoa. Tietoja voitaisiin käyttää muun muassa velvoitteidenhoitoselvitysten laatimiseen ja tilanteissa, joissa tiedot ovat välttämättömiä tiedustelutehtävän suorittamiseksi. Ehdotus vastaa sitä, mitä muun muassa suojelupoliisille on säädetty kansallisen turvallisuuden osalta.

Esityksessä ehdotetaan muutettavaksi henkilötietojen käsittelyä Puolustusvoimissa annettua lakia niin, että henkilötietoja voitaisiin päivittää vertaamalla niitä muiden viranomaisten henkilörekistereihin. Sääntely vastaisi sitä, mitä suojelupoliisille on säädetty.

Esityksen 2. lakiehdotuksen 36 a §:ssä Puolustusvoimien virkojen hakumenettelyä muutettaisiin siten, että tiettyihin sotilastiedustelutehtäviin hakevien tai nimitettävien henkilöiden henkilöllisyys voitaisiin suojata. Sääntely vastaisi sitä, mitä suojelupoliisille on säädetty.

14. Lopuksi

2.9.2026

Hallintopoliittinen osasto
Lainvalmistelu- ja oikeusyksikkö
Vanhempi hallitussihteeri Kosti Honkanen

Hallituksen esityksessä katsotaan, että lait on säädettävissä tavallisen lain säätämisjärjestyksessä.

Esityksen 1. laki

Esityksen 1. lakiehdotuksessa

Liitteet Napsauta tähän hiirellä ja kirjoita liitteiden nimet kukin omalle rivilleen. Rivinvaihto enterillä.

Postiosoite
Postadress
Postal Address
Puolustusministeriö
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
kirjaamo@defmin.fi
www.defmin.fi

2.9.2026

Hallintopoliittinen osasto
Lainvalmistelu- ja oikeusyksikkö
Vanhempi hallitussihteeri Kosti Honkanen

Jakelu Napsauta tähän hiirellä ja kirjoita jakelun saajat kukin omalle rivilleen (henkilönimet muodossa Etunimi Sukunimi). Rivinvaihto enterillä.

Tiedoksi Napsauta tähän hiirellä ja kirjoita tiedoksisaajat kukin omalle rivilleen (henkilönimet muodossa Etunimi Sukunimi). Rivinvaihto enterillä.

Postiosoite
Postadress
Postal Address
Puolustusministeriö
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
kirjaamo@defmin.fi
www.defmin.fi