PUOLUSTUSMINISTERIÖ **Muistio** **HE 203/2017**
Lainsäädäntöjohtaja Hanna Nordström 14.2.2018
Hallitussihteeri Kosti Honkanen

Eduskunnan perustuslakivaliokunnalle

HALLITUKSEN ESITYS EDUSKUNNALLE LAIKSI SOTILATIEDUSTELUSTA SEKÄ ERÄIKSI SIIHEN LIITTYVIKSI LAEIKSI

1 Johdanto

Esityksen pääasiallinen sisältö

Esityksessä ehdotetaan säädettäväsi laki sotilastiedustelusta. Esitys liittyy hallituksen esityksiin, joissa ehdotetaan säädettäväksi siviilitiedustelutoiminnasta, siviili- ja sotilastiedustelun valvonnasta sekä perustuslain muuttamisesta koskien luottamuksellisen viestin suojan rajoittamista tiedon hankkimiseksi sotilaallisesta toiminnasta ja muusta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Esityksen tavoitteena on saattaa Puolustusvoimien tiedustelua koskeva lainsäädäntö ajan tasalle sekä täyttää perutuslaista ja Suomea sitovista kansainvälisistä velvoitteista johtuvat vaatimukset.

Suomen turvallisuusympäristön voidaan katsoa muuttuneen viime vuosina nopeassa tahdissa. Turvallisuuspoliittiseen toimintaympäristöön liittyvät haasteet ovat yhä monimuotoisempia ja ulkoisiin uhkiin varautumisen aikajänne on lyhentynyt. Oikean ja ajantasaisen tiedon merkitys on korostunut entisestään. Lisäksi Puolustusvoimien toiminnan kannalta keskeinen sotilastiedustelun kohteena oleva tieto on siirtynyt digitaaliseen muotoon.

Tämän esityksen tavoitteena on parantaa Puolustusvoimien tiedonhankintaa Puolustusvoimien tehtäviin liittyvistä vakavista kansainvälisistä uhista siten, että Puolustusvoimilla olisi Suomessa ja ulkomailla toimivaltuudet henkilötiedusteluun, radiosignaalitiedusteluun, tietojärjestelmätiedusteluun sekä tietoliikennetiedusteluun.

Sotilastiedustelun tarkoituksena on seurata turvallisuusympäristön kehitystä ja tuottaa tietoa ylimmän turvallisuuspoliittisen johdon ja sotilaallisen päätöksenteon tueksi. Sotilastiedustelu antaa ennakkovaroituksen Suomeen kohdistuvasta sotilaallisesta uhkasta ja tukee muita viranomaisia. Lisäksi sotilastiedustelu tukee Puolustusvoimien muuta kansainvälistä toimintaa ja sotilaallisiin kriisinhallintaoperaatioihin liittyvää päätöksentekoa sekä Puolustusvoimien toimintaa ja omasuojaa kansainvälisessä toiminnassa.

Esityksessä ehdotetaan säädettäväksi sotilastiedustelun kohteista ja tiedustelutoiminnassa noudatettavista periaatteista, toiminnan ohjauksesta sekä valvonnasta puolustushallinnossa. Sotilastiedusteluviranomaisia olisivat Puolustusvoimien pääesikunta ja Puolustusvoimien tiedustelulaitos. Laissa säädettäisiin viranomaisten käytössä olevista tiedustelumenetelmistä ja toimivaltuuksien käytöstä päättämisestä sekä yhteistyöstä muiden viranomaisten kanssa, tiedustelutiedon ilmoittamisesta, tiedustelukielloista ja kansainvälisestä yhteistyöstä.

Esityksessä ehdotetaan muutettavaksi lisäksi puolustusvoimista annettua lakia, julkisen hallinnon turvallisuusverkkotoiminnasta annettua lakia sekä tuloverolakia. Sotilaskurin-

pidosta ja rikostorjunnasta puolustusvoimissa annettua lakia muutettaisiin siviilitiedustelu koskevasta lainsäädännöstä eduskunnalle annetusta hallituksen esityksestä johtuen, jonka myötä suojelupoliisi luopuisi esitutkintatoimivaltuuksistaan.

Ehdotettu laki on tarkoitettu tulemaan voimaan mahdollisimman pian lakiehdotuksen säätämisjärjestystä koskevat seikat huomioon ottaen.

Lakiehdotuksia arvioidaan perustuslain 10 §:ssä säädetyn yksityiselämän suojan, 12 §:ssä säädetyn sananvapauden, 15 §:ssä säädetyn omaisuuden suojan, 21 §:ssä säädetyn oikeusturvan sekä vastuuta virkatoimista koskevan 118§:n ja hallintotehtävän antamista muulle kuin viranomaiselle koskevan 124 §:n kannalta. Lakiehdotuksia tulee lisäksi tarkastella perusoikeuksien yleisten rajoitusedellytysten kannalta (HE 1/1998 vp, PeVM 25/1994 vp).

Esitystä on arvioitu perusoikeussäännöksiin sisältyvien lakivarausten kannalta ottaen samalla huomioon perusoikeuksien yleiset rajoitusedellytykset kuten rajoituksen tarkkarajaisuus ja täsmällisyys, rajoittamisen perusteena olevien syiden hyväksyttävyys, suhteellisuusvaatimuksen täyttyminen perusoikeutta rajoitettaessa, oikeusturvajärjestelyjen riittävyys ja rajoituksen ristiriidattomuus Suomen kansainvälisten ihmisoikeusvelvoitteiden kannalta.

Esityksessä ehdotetaan säädettäväksi myös asevelvollisten osallistumisesta sotilastiedusteluun. Sotilastiedusteluviranomaista avustaessaan reserviläisillä olisi oikeus käyttää toimivaltuuksia ainoastaan tiedustelumenetelmän käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa. Heidän käytössään olevista tiedustelumenetelmistä säädettäisiin lailla. Heillä ei olisi käytettävinä tiedustelumenetelmiä, joilla voitaisiin hankkia tietoa viestin sisällöstä. Reserviläisillä tulisi olla tiedolliset ja taidolliset valmiudet tehtävien hoitamiseen. Kyse ei siten olisi asevelvollisten itsenäisen harkintavallan eikä merkittävästä julkisen vallan käytöstä.

Esitys on laadittu ottaen huomioon Euroopan ihmisoikeussopimuksen vaatimukset, joita on käsitelty Euroopan ihmisoikeustuomioistuimen (EIT) ratkaisukäytännössä. Vaikka Euroopan unionin toimivalta ei koske kansallista turvallisuutta, voidaan esityksen katsoa täyttävän Euroopan unionin oikeuden vaatimukset jo Suomen oikeusjärjestyksen ja perustuslain asettamien tarkkarajaisuus- ja täsmällisyysvaatimusten kautta.

Asian valmistelu

Puolustusministeriö asetti 1 päivänä lokakuuta 2015 työryhmän valmistelemaan ehdotuksen sotilastiedustelua koskevaksi lainsäädännöksi. Hanke perustui pääministeri Juha Sipilän hallituksen ohjelmaan, jonka mukaan hallitus esittää säädösperustaa ulkomaantiedustelulle ja tietoliikennetiedustelulle.

Työryhmän tehtävänä oli valmistella ehdotus säännöksiksi muun muassa Puolustusvoimien tiedustelun tarkoituksesta, toimivaltaisista viranomaisista sekä niidentehtävistä ja toimivaltuuksista, ohjauksesta ja valvonnasta, tietojen käsittelystä ja rekisteröinnistä sekä viranomaisten yhteistyöstä. Hankkeen keskeisin tavoite oli kansallisen turvallisuuden parantaminen.

Työryhmässä oli edustus puolustusministeriön lisäksi tasavallan presidentin kansliasta, valtioneuvoston kansliasta, ulkoasiainministeriöstä, oikeusministeriöstä, sisäministeriöstä sekä pääesikunnasta. Työryhmään oli myös kutsuttu pysyvät asiantuntijat Elinkeinoelämän keskusliitto EK:sta, Helsingin yliopistosta, ulkoasiainministeriöstä, liikenne-ja viestintäministeriöstä, suojelupoliisista ja Puolustusvoimista.

Työryhmän asettamispäätöksessä todetaan, että mietinnön valmistelussa on otettava huomioon tiedonhankintalakityöryhmän mietintö (Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö, 2015) ja siitä saatu lausuntopalaute.

Ehdotus sotilastiedustelua koskevaksi lainsäädännöksi oli laajalla lausuntokierroksella. Lausuntoa pyydettiin 119 eri taholta: eduskuntapuolueilta, viranomaisilta ja muilta tahoilta. Lausunnon antoi 72 eri tahoa. Lausuntopyyntö julkaistiin sähköisesti lausuntopavelu.fi – verkkopalvelussa sekä puolustusministeriön internet-sivulla. Lausunnoista laadittiin puolustusministeriössä lausuntotiivistelmä, jossa lausuntopalautteen kriittiset näkökohdat on tuotu esille.

2 Ohjaus ja seuranta

Lakiehdotuksen mukaan sotilastiedustelutoiminnan vuotoiset painopisteet käsittelisi valmistelevasti tasavallan presidentin ja ulko- ja turvallisuuspoliittisen ministerivaliokunnan yhteinen kokous. Painopisteissä olisi kyse ylätason linjauksista siitä, mistä sotilastiedustelun tulisi hankkia seuraavan vuoden aikana tietoa. Tarvittaessa painopisteitä voitaisiin käsitellä valmistelevasti myös useammin.

Painopisteissä ei olisi kyse operatiivisesta päätöksenteosta eikä ne perustaisi suoraan sotilastiedusteluviranomaiselle tiedustelutehtävää, vaan niitä koskeva päätöksenteko sotilastiedusteluviranomaisessa suoritettaisiin painopisteiden mukaisesti.

Painopisteiden valmistelu tapahtuisi vallitsevan käytännön mukaisesti, eli valmistelu tapahtuisi sotilastiedustelun osalta puolustusministeriössä.

Valmistelevasti käsitellyt painopisteet Puolustusvoimille antaisi puolustusministeriö.

Lisäksi tiedustelutehtäviä olisi mahdollista antaa sotilaskäskyinä.

Sotilastiedustelusta annettaisiin vähintään kerran vuodessa seurantaraportti tasavallan presidentin ja valtioneuvoston ulko- ja turvallisuuspoliittisen ministerivaliokunnan yhteiselle kokoukselle. Seurannassa ei olisi kyse laillisuusvalvonnasta, vaan siitä, minkälaista tietoa painopisteistä on saatu seurantakaudella. Tasavallan presidentti ja valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta voisivat tarvittaessa ryhtyä tarvittaviin toimiin saamiensa tietojen pohjalta.

3 Sotilastiedustelun kohteet

Lakiehdotuksessa esitettään, että sotilastiedustelussa voitaisiin hankkia tiedustelumenetelmällä tietoa tarkkaan rajatuista kohteista. Tiedustelumenetelmällä saataisiin hankkia tietoa seuraavasta toiminnasta, jos toiminta olisi luonteeltaan sotilaallista: 1) vieraan valtion asevoimien ja niihin rinnastuvien järjestäytyneiden joukkojen toiminta ja toiminnan

valmistelu; 2) Suomen maanpuolustukseen kohdistuva tiedustelutoiminta; 3) joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö; 4) vieraan valtion sotatarvikkeiden kehittäminen ja levittäminen; 5) kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi; 6) kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaava toiminta; 7) Suomen kansainvälisen avun antamisen ja kansainvälisen muun toiminnan turvallisuutta uhkaava toiminta.

Lisäksi lakiehdotuksen 4 §:n 2 momentin mukaan tiedustelumenetelmällä saadaan hankkia tietoa vieraan valtion toiminnasta tai muusta sellaisesta toiminnasta, joka voi vaarantaa Suomen maanpuolustusta tai vaarantaa yhteiskunnan elintärkeitä toimintoja.

Pykälän 1 momentissa tarkoitettu toiminta olisi luonteeltaan sellaista, ettei sen tarvitsisi välittömästi uhata Suomea. 1 momentissa luetellusta toiminnasta tiedon hankkiminen antaisi Suomelle tietoa, jonka perusteella erilaisiin kriisitilanteisiin voitaisiin varautua parhaalla mahdollisella tavalla.

Pykälän 1 momentin 1 kohdassa olisi mainittu vieraan valtion lisäksi vieraaseen valtioon rinnastuva järjestäytynyt joukko. Vieraaseen valtioon rinnastuvaa joukkoa olisi arvioitavat sen perusteella, miten järjestäytynyttä toiminta on, mitkä ovat sen käytössä oleva resurssit ja minkälaista toiminta on kokonaisuutena arvioituna.

Pykälän 2 momentti koskisi tilanteita, joissa tiedusteltava toiminta ei lähtökohtaisesti olisi sotilaallista. Valtiot saattavat pyrkiä käyttämään esimerkiksi sotilaallisen toiminnan valmistelemiseksi keinoja, joita ei voida katsoa sotilaallisiksi, esimerkiksi demokraattiseen yhteiskuntaan vaikuttamista. Lisäksi esimerkiksi sotilaallisissa kriisinhallintaoperaatioissa konfliktien moninaisuuden vuoksi operaatioalueella saattaa toimia ryhmittymiä, jotka voivat aiheuttaa merkittävää vahinkoa kriisinhallintajoukoille, vaikka ryhmittymät eivät ole valtiollisia toimijoita tai sellaiseksi rinnastuvia tai järjestäytyneitä.

Teknologian kehityksen myötä yhteiskunnan perustoiminnot ovat entistä riippuvaisempia yksityisistä toimijoista. Teknologian kehittyminen on myös johtanut tilanteeseen, jossa laaja-alaisen vahingon aiheuttaminen yhteiskunnalle on entistä helpompaa ja vahinkoa voidaan aiheuttaa maantieteellisesti suurienkin etäisyyksien päästä tietoverkkojen välityksellä. Esimerkkinä tällaisesta tilanteesta olisi tilanne, jossa toisesta valtiosta toimitettaisiin kehittynyt haittaohjelma yhteiskunnan kriittisiä perustoimintoja tuottavan ICT-palveluyrityksen palvelimelle. Jos haittaohjelma aktivoitaisiin, voisi tämä aiheuttaa esimerkiksi valtion ylimmän päätöksenteon pysähtymisen esimerkiksi kriisitilanteessa.

Toiminnan, joka ei olisi luonteeltaan sotilaallista, olisi oltava sellaista, joka laajuudeltaan voisi aiheuttaa vakavaa uhkaa kansalliselle turvallisuudelle. Toiminta voisi konkretisoituessaan esimerkiksi estää Suomen ylimmän valtiojohdon oikea-aikaisen päätöksenteon, estää Suomen toiminnan kriisitilanteessa tai olennaisesti vaikeuttaa Suomen mahdollisuuksia toimia kansainvälisessä yhteisössä.

Suhde perustuslakiin

Tukiasematietojen hankkimista, suunnitelmallista tarkkailua, peiteltyä tiedonhankintaa, teknistä katselua, teknistä seurantaa, peitetoimintaa, valeostoa ja paikkatiedustelua koskevassa sääntelyssä on otettu huomioon perusoikeuksien yleiset rajoitusedellytykset. Tä-

män vuoksi ja ottaen huomioon kyseisten menetelmien melko vähäisenä pidettävä puuttuminen luottamuksellisen viestin salaisuuteen tai tunnistamistietoihin, niitä on pidettävä ongelmattomina perustuslain 10 §:n 2 momentin kannalta.

Luottamuksellisen viestin salaisuuden suojan rajoittaminen olisi perustuslain 10 §:n ehdotetun uuden 4 momentin mukaan oltava välttämätöntä. Tämä edellytys seuraa myös perusoikeuksien yleisistä rajoitusedellytyksistä.

Arvioitaessa lakiehdotusten välttämättömyyttä on otettava huomioon, että ehdotettuja uusia tiedustelumenetelmiä olisi mahdollista käyttää tiedon hankkimiseen ainoastaan laissa tyhjentävästi luetelluista sotilastiedustelun kohteista (1. lakiehdotuksen 4 §). Sotilastiedustelun kohteet määriteltäisiin tyhjentävästi. Toisaalta kansallisen lain ei voida edellyttää täsmällisesti ja tyhjentävästi luetteloivan kaikkia niitä tilanteita, joissa viranomaiset saavat käyttää salaisia valtuuksia. Lain säännöksen, jonka mukaan salaisten valtuuksien käyttöperusteena on sotilaallinen uhka, on esimerkiksi katsottava täyttävän Euroopan ihmisoikeussopimuksen asettaman ennakoitavuusvaatimuksen. Tiedonhankinta näistä kohteista olisi Suomen ulkopuolisen turvallisuusympäristön seuraamisen ja Puolustusvoimien lakisääteisten, puolustusvalmiuden ylläpitämis- ja kehittämistehtävien kannalta välttämätöntä. Tiedustelumenetelmällä saataisiin hankkia tietoa vain sellaisesta toiminnasta, joka olisi luonteeltaan sotilaallista tai joka voisi vakavasti uhata kansallista turvallisuutta.

Ehdotetussa 4 §:ssä kuvattu toiminta olisi johdettavissa yhdestä tai useammasta sotilaallista toimintaa koskevasta suojeluintressistä. Sääntelyn arvioidaan siten täyttävän perustuslain 10 §:ään ehdotetun uuden 4 momentin edellytykset Näin ollen tiedonhankinnan kohteita koskevaa sääntelyä ei voisi pitää ongelmallisena yksityiselämän suojan kannalta. Sääntelyn arvioidaan täyttävän korostuneet vaatimukset välttämättömyydestä ja ennakoitavuudesta.

4 Tiedustelumenetelmien kohdentaminen

Tiedustelumenetelmän käytön tulisi olla aina kohdennettua. Ensinnäkin kohdentamista rajaisi sotilastiedustelun tarkoitus, jonka mukaan sotilastiedustelu olisi sidottu tiettyihin puolustusvoimista annetussa laissa tarkoitettuihin Puolustusvoimien tehtäviin.

Kohdentamista rajaa sotilastiedustelun tarkoituksen ja kohteiden lisäksi tasavallan presidentin ja valtioneuvoston ulko- ja turvallisuuspoliittisen ministerivaliokunnan valmistelevasti käsittelemät painopisteet. Painopisteiden pohjalta pääesikunnan tiedustelupäällikkö laatisi tiedustelutehtävän, joka olisi konkreettisempaa kohteiden rajaamista, esimerkiksi osoittamalla sotilastiedusteluviranomaiselle tietyn maantieteellisen alueen tai ilmiön, josta hankittavalla tiedolla painopisteiden mukainen tiedon tarve täytettäisiin. Tiedustelutehtävän pohjalta sotilastiedusteluviranomainen suorittaisi operatiiviset toimet tiedonhankkimiseksi parhaaksi katsomillaan tiedustelumenetelmillä ja analysoimalla tiedon.

Sotilastiedustelutoimintaa ja tiedustelumenetelmien käyttöä rajaisi yleiset periaatteet. Näitä olisivat suhteellisuusperiaate, vähimmän haitan periaate ja tarkoitussidonnaisuuden periaate. Lisäksi laissa säädettäisiin erikseen syrjinnän kiellosta, jonka perusteella tiedustelumenetelmän käyttö ei saisi perustua ainoastaan yhteen kriteeriin, esimerkiksi poliittiseen toimintaan.

Laajasti tarkasteltuna myös laissa säädettäväksi esitetty ilmoitusvelvollisuus rajaisi osaltaan tiedustelumenetelmien käyttöä. Tiedustelutoiminnan vaivihkaisen luonteen vuoksi sotilastiedusteluviranomaisen voidaan olettaa käyttävän ensisijaisesti tiedustelumenetelmiä, jotka puuttuisivat perusoikeuksiin mahdollisimman vähäisessä määrin.

Tiedustelutehtävän perusteella käytettäviä tiedustelumenetelmää kohdennettaisiin edelleen tiedustelumenetelmien käytön yleisellä ja erityisellä edellytyksellä. Tiedustelumenetelmän käytön yleisenä edellytyksenä olisi 1. lakiehdotuksen 11 §:n 1 momentin mukaan se, että tiedustelumenetelmän käytöllä voitaisiin perustellusti olettaa saatavan tietoa tiedustelutehtävän kannalta.

EIT on ottanut kantaa ratkaisuissaan kohdentamisen osalta muun muassa Amann v. Sveitsi, Kopp v. Saksa, Kruslin v. Ranska, Huvig v. Ranska. Ratkaisuissa on todettu, että lain on oltava tarpeeksi selkeä antaakseen riittävän osoituksen siitä, missä olosuhteissa ja millä edellytyksillä kansalaiset voivat joutua salaisten viranomaistoimenpiteiden kohteeksi. Lisäksi laki ei voi olla sellainen, että se mahdollistaa salaisen tarkkailun kohdistamisen sattumanvaraisesti keneen tahansa.

Edellä tarkoitetun pykälän 2 momentissa olisi erikseen rajaus siitä, että luottamuksellisen viestin suojan alaan puuttuvia tiedustelumenetelmiä voitaisiin käyttää tiedustelumenetelmän käytön kohdistuessa muuhun kuin luonteeltaan sotilaalliseen toimintaan ainoastaan silloin, kun tällaisen toiminnan taustalla oleva toimija voi aiheuttaa vakavaa vaaraa kansalliselle turvallisuudelle ja jos toiminnassa on kyse sotilastiedustelun kohteita koskevan 4 §:n 2 momentin tarkoittamasta toiminnasta.

Tiedustelumenetelmä kohtaisesti olisi säädetty siitä, keneen tai keihin sekä mihin tiedustelumenetelmän käyttöä saisi kohdentaa.

Suhde perustuslakiin

Sotilastiedustelussa tulisi kunnioittaa perus- ja ihmisoikeuksia sekä noudattaa sotilastiedustelutoiminnan yleisiä periaatteita, jotka ohjaisivat kaikkea toimintaa.

Sotilastiedustelun toimenpiteiden kohdentaminen on toteutettava syrjimättömästi syrjinnän kiellon mukaisesti. Sääntely vahvistaisi perustuslain 6 §:n 2 momentin yhdenvertaisuusperiaatetta tiedustelutoiminnassa.

5 Tiedustelumenetelmät

5.1 Tiedustelumenetelmän käytön edellytykset

Tiedustelumenetelmän käytön yleisestä edellytyksestä säädettäisiin 1. lakiehdotuksen 11 §:n 1 momentissa. Säännöksen mukaan tiedustelumenetelmän käytön yleisenä edellytyksenä on, että tiedustelumenetelmän käytöllä voitaisiin perustellusti olettaa saatavan tietoa tiedustelutehtävän kannalta. Kuten edellä on todettu, kyseessä olisi niin sanotusta perustellusta tuloksellisuusodotuksesta. Tiedustelumenetelmän käytön hyödyllisyys olisi perusteltava yksittäistapauksellisesti niin, että ulkopuolinen tarkastelija voisi päätyä samaan lopputulokseen. Perustelu voisi liittyä esimerkiksi siihen, miksi nimenomaan tiettyä henkilöä tai henkilöryhmää tulisi voida tarkkailla ja miksi näin pystyttäisiin oletetusti saamaan hyödyllistä tietoa.

Mainitun pykälän 2 momentissa olisi erikseen rajaus siitä, että luottamuksellisen viestin suojan alaan puuttuvia tiedustelumenetelmiä voitaisiin käyttää tiedustelumenetelmän käytön kohdistuessa muuhun kuin luonteeltaan sotilaalliseen toimintaan ainoastaan silloin, kun tällaisen toiminnan taustalla oleva toimija voi aiheuttaa vakavaa vaaraa kansalliselle turvallisuudelle ja jos toiminnassa on kyse sotilastiedustelun kohteita koskevan 4 §:n 2 momentin tarkoittamasta toiminnasta.

Yleisen edellytyksen lisäksi olisi tiedustelumenetelmä kohtaisesti säädetty erityisistä edellytyksistä. EIT on ottanut kantaa ratkaisuissaan Amann v. Sveitsi, Kopp v. Saksa, Kruslin v. Ranska ja Huvig v. Ranska siihen, että lainsäädännöstä on käytävä riittävän selkeästi ilmi olosuhteet, joissa kansalainen voi joutua salaisen viranomaistoiminnan kohteeksi.

Tiedustelumenetelmäkohtaisia erityisiä edellytyksiä olisivat ”perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta” tai ”välttämätöntä tietojen saamiseksi tiedustelutehtävän kannalta”.

Vaatimus erittäin tärkeästä merkityksestä täyttyisi silloin, kun tiedustelutehtävän suorittaminen muulla tavalla olisi hyvin työlästä tai tiedustelutehtävän pitkittymisestä aiheutuisi erityistä vaaraa tai kohtuuttomia kustannuksia.

Välttämättömyysedellytyksellä tarkoitettaisiin viimesijaisuutta eli käytännössä sitä, että tietojen hankkiminen muulla keinolla ei olisi mahdollista tai esimerkiksi vaatisi oleellisesti enemmän voimavaroja tai viivästyttäisi tiedonhankintaa kohtuuttomasti. Välttämättömyys olisi myös muuhun kuin valtiolliseen toimijaan kohdistuvan tietoliikennetiedustelun edellytyksenä. EIT on ottanut tietoliikennetiedustelun osalta välttämättömyyteen kantaa ratkaisussaan Szabó ja Vissy v. Unkari. Ratkaisussa todetaan, että menetelmän käytön tulee olla yleisellä tasolla ehdottoman välttämätöntä demokraattisten instituutioiden suojaamiseksi ja menetelmän käytön tulee yksittäisen tiedusteluoperaation yhteydessä olla ehdottoman välttämätöntä olennaisen tärkeän tiedon saamiseksi.

Suomen perustuslain mukaan valtio ei nauti perusoikeussuojaa. Esityksessä ehdotetaan, että valtiolliseen toimijaan kohdistuvia tiedustelumenetelmiä voitaisiin käyttää alemmalla edellytyksellä. Valtiollinen toimija olisi 1. lakiehdotuksen 9 §:ssä määritelty vieraan valtion tunnistetuksi viranomaiseksi tai sellaiseen rinnastuvaksi toimijaksi sekä tarkoitetun tahon palveluksessa olevaksi tai sen määräyksessä ja ohjauksessa toimivaksi tahoksi.

5.2 Tarkkailu, tekninen tarkkailu, tiedustelu televerkoissa, peitetoiminta ja valeosto sekä tietolähdetoiminta

Laissa säädettäisiin sotilastiedusteluviranomaisen käytössä olevista tiedustelumenetelmistä. Tiedustelumenetelmät vastaisivat pääosin jo poliisilain 5 luvussa säädettyjä salaisia tiedonhankintakeinoja. Näistä käytössä olisivat tarkkailua, suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen laitetarkkailu, telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen, peitetoiminta, valeosto ja tietolähdetoiminta.

Telekuuntelu poikkeaisi poliisilain 5 luvun määritelmästä siltä osin, että telekuuntelua voitaisiin kohdistaa henkilöön, eli tietyn henkilön luvan voimassaolon aikana käyttämiin kaikkiin teleosoitteisiin ja telepäätelaitteisiin.

Lisäksi telekuuntelua voitaisiin kohdistaa myös viestintäyhteyteen, joka ei käyttäisi yleistä viestintäverkkoa. Tällaisia viestintäyhteyksiä voisivat olla esimerkiksi satelliittipuhelut. Tiedustelumenetelmänä käytettävän telekuuntelun laajennusta voidaan pitää perusteltuna muun muassa sillä, että satelliittiteknologia kehittyy kiihtyvällä vauhdilla, minkä voidaan myös olettaa lisäävän satelliittiteknologiaa käyttävien sovellutusten määrää.

Tekninen laitetarkkailu poikkeaisi poliisilain 5 luvun määritelmästä siinä, että teknisellä laitetarkkailulla voitaisiin hankkia tietoa myös viestin sisällöstä. Voimassaolevan poliisilain ja pakkokeinolain mukaan teknisellä laitetarkkailulla ei voitaisi hankkia tietoa tietokoneen tai muun vastaavan teknisen laitteen taikka sen ohjelmiston sisältämistä viesteistä.

5.3 Paikkatiedustelu, jäljentäminen ja lähetyksen jäljentäminen

Edellä sanottujen toimivaltuuksien lisäksi säädettäisiin uusista toimivaltuuksista, jotka mukailisivat pakkokeinolain eräitä salaisia pakkokeinoja. Näitä olisivat paikkatiedustelu, jäljentäminen ja lähetyksen jäljentäminen. Jäljentäminen ja lähetyksen jäljentäminen voisivat kohdistua myös viestiin. Lähetyksen jäljentämiseen liittyisi myös olennaisena lähetyksen pysäyttäminen jäljentämistä varten.

5.4 Radiosignaalitiedustelu ja ulkomaan tietojärjestelmätiedustelu

Erityisesti sotilastiedustelulle säädettäviä toimivaltuuksia olisivat radiosignaalitiedustelu ja ulkomaan tietojärjestelmätiedustelu.

Radiosignaalitiedustelusta säädettäisiin nimenomaisesti oikeusjärjestelmän kehityksen asettamista vaatimuksista johtuen. Radiosignaalitiedustelu kohdistuu joko Suomen alueelle tulevaan tai Suomesta lähtöisin olevaan radiosignaaliin, jonka lähettävä tai vastaanottava laite on Suomen rajan ulkopuolella. Keskeisiä radiosignaalien käyttäjiä ovat sotilaalliset toimijat omassa operatiivisessa viestinnässään ja johtamisjärjestelmissä. Lisäksi esimerkiksi ohjuksien liikkuminen perustuu keskeisesti radiosignaaleihin. Radiosignaalitiedustelusta olisi tarkoituksen mukaista säätää nimenomaisesti sen merkittävyyden kannalta Puolustusvoimille.

Ulkomaan tietojärjestelmätiedustelussa olisi kyse teknisin menetelmin hankittavasta tiedosta Suomen rajan ulkopuolella olevasta tietojärjestelmästä. Tietojärjestelmällä tarkoitettaisiin laajasti eri laitteiden yhdistelmästä muodostuvaa kokonaisuutta ja tiedustelumenetelmän käyttö voisi kohdistua niin järjestelmän ja siinä käytettävien ohjelmistojen teknisiin tietoihin kuin järjestelmän sisältämiin tietoihin ja viesteihin.

Ulkomaan tietojärjestelmätiedustelussa käytettävien menetelmien voidaan katsoa vastaavan osaltaan teknistä kuuntelua ja teknistä laitetarkkailua, mutta sen merkittävyyden kannalta ja etenkin ulkopoliittisten näkökohtien kannalta, toimivaltuudesta olisi tarkoituksenmukaista säätää nimenomaisesti.

5.5 Ulkomailla tapahtuva sotilastiedustelu

Edellä tarkoitettuja tiedustelumenetelmiä voitaisiin käyttää myös ulkomailla. Ulkomailla tapahtuvassa sotilastiedustelussa voitaisiin ottaa huomioon tiedustelumenetelmiä koskevat rajoitukset. Kaikissa tilanteissa tämä ei kuitenkaan olisi aina mahdollista olosuhteiden ollessa moninaisia. Toiminnassa olisi kuitenkin otettava huomioon Euroopan ihmisoikeustuomioistuimen tulkintakannanotto toimintaa ohjaavina suuntaviivoina.

5.6 Tietoliikennetiedustelu

Teknisten tietojen käsittely

Merkittävä uusi toimivaltuuskokonaisuus olisi tietoliikennetiedustelu. Tietoliikennetiedustelu käsittäisi tiedonhankinnan valtiollisen toimijan sekä muun kuin valtiollisen toimijan tietoliikenteestä. Lisäksi tietoliikennetiedustelua tukevana toimivaltuutena olisi teknisten tietojen käsittely.

Käsiteltävänä olevan hallituksen esityksen mukaan tekniseksi tiedoksi määriteltäisiin tieto, joka on muuta kuin viestin sisältöä koskevaa semanttista tietoa. Teknisten tietojen käsittelyssä yleisen viestintäverkon osasta otettaisiin joko ajallisesti lyhyt kestoisia näytteitä tai satunnaisotannalla viestintäverkon osassa kulkevia IP-paketteja. Näiden pohjalta tehtäisiin tekninen analyysi, jonka tuloksena voitaisiin arvioida sitä, onko tietty viestintäverkon osa sellainen, josta mahdollisimman tehokkaasti voitaisiin saada tietyltä alueelta tulevaa tietoliikennettä.

Teknisen analyysin tuloksena ei saa syntyä tietoa, josta voitaisiin tunnistaa yksittäisiä henkilöitä.

Tietoliikenteeseen kohdistuva tiedustelu

Tietoliikennetiedustelussa olisi kyse kohteena olevan toimijan tietoliikenteen tiedustelusta Suomen alueella. Suomen alueen kautta kulkee merkittäviä tietoliikennekaapeleita, joissa voidaan arvioida reitittyvän sotilastiedustelun kannalta merkittävien kohteiden tietoliikennettä internet-verkon toiminnan vuoksi.

Koska valtiollisen toimijan ei voida katsoa nauttivan perusoikeussuojaa, voitaisiin tällaisen toimijan tietoliikenteeseen puuttua lievemmin ehdoin kuin muun toimijan tietoliikenteeseen.

Tietoliikennetiedustelussa tietoliikenteen tiedustelu tapahtuisi hakuehtojen perusteella, jotka tuomioistuin olisi hyväksynyt lupaa antaessaan. EIT on ratkaisussaan Liberty ja muut v. Yhdistynyt kuningaskunta katsonut tällaisen menettelyn hyväksyttäväksi.

Hakuehtoina käytettäisiin teknisiä tietoja tai niiden luokkia. Internet-verkossa lähetettävä viesti jakautuu IP-paketeiksi, jotka ohjautuvat tietoliikennevirrassa vastaanottajalle. Vastaanottajan päätelaitteessa IP-paketit kasaantuvat taas ymmärrettäväksi viestiksi. Jotta tämä olisi mahdollista, IP-paketit sisältävät teknistä tietoa muun muassa siitä, mistä IP-paketti on lähtöisin ja mitä kautta IP-paketti on reitittynyt. Näihin tietoihin kohdistuvilla hakuehdoilla tietoliikenteestä voitaisiin seuloa tiedusteluoperaation kohteena olevaa tietoliikennettä.

Tietoliikennetiedustelunprosessissa tietyssä tuomioistuimen myöntämän luvan tarkoittamassa viestintäverkon osassa, käytännössä tietyssä aallonpituudessa, kulkeva tietoliikenne peilattaisiin tietoliikennetiedustelujärjestelmän välimuistiin, jossa tietoliikenteeseen kohdistettaisiin hakuehtoja. Tässä vaiheessa sotilastiedusteluviranomaisella ei olisi pääsyä tietoliikenteeseen, mikä ei olisi käytännössä teknisesti eikä käsiteltävänä olevan tietomäärän takia mahdollista. Välimuistissa oleva tieto ylikirjoitetaan saman tien sen jälkeen, kun se on todettu hakuehtoja vastaamattomaksi, joten sotilastiedusteluviranomainen ei voi palata käsittelemään tietoja enää jälkikäteen.

Hakuehtojen mukainen tietoliikenne ohjautuisi jatkokäsittelyyn, missä tietoliikenteen sisältöön menevillä hakuehdoilla tietoliikenteestä edelleen haettaisiin tiedusteluoperaation kannalta merkityksellistä tietoa. Automaattisessa jatkokäsittelyssä tietomäärä on edelleen niin suuri, ettei olisi tarkoituksen mukaista, että yksittäinen virkamies vielä tässä vaiheessa puuttuisi viestinnän sisältöön. Automaattisen käsittelyn vaihe vertautuisi esimerkiksi telekuuntelulla hankittuihin tallenteisiin, joista voidaan jo nykyisellään automatisoidusti poistaa irrelevantti tieto tallenteita tarkastettaessa. Edelleen tässä vaiheessa manuaaliseen jatkokäsittelyyn valikoitumaton tieto ylikirjoitetaan, joten sotilastiedusteluviranomainen ei pysty palaamaan tähän tietoon jälkikäteen.

Vasta automaattisen käsittelyn jälkeen sotilastiedusteluviranomaisen virkamies pääsisi analysoimaan tietoja.

5.7 Suhde perustuslakiin

Tiedustelumenetelmistä ehdotetaan säänneltäväksi mahdollisimman täsmällisesti ja tarkkarajaisesti 1. lakiehdotuksen 4 luvussa. Tiedustelumenetelmän käytön yleisistä edellytyksistä ja noudatettavista periaatteista säädettäisiin 1 luvussa. Lisäksi erityisistä edellytyksistä säädettäisiin tiedustelumenetelmä kohtaisesti.

Suhteellisuusperiaate edellyttäisi arvioimaan, onko tiedustelumenetelmän käyttö puolustettavaa suhteessa tiedustelua koskevan toimeksiannon tärkeyteen, kiireellisyyteen, tavoiteltavaan päämäärään ja muihin tilanteen kokonaisarviointiin vaikuttaviin seikkoihin. EIT ja EU-tuomioistuin ovat ratkaisukäytännössään korostaneet suhteellisuusperiaatteen noudattamisen tärkeyttä erityisesti tietoliikennetiedustelun yhteydessä (esimerkiksi Zakharov v. Venäjä, Weber ja Saravia v. Saksa, Digital Rights Ireland). Esimerkiksi tietoliikennetiedustelu edellyttäisi siksi viimesijaisuutta, eli sitä, että tietojen hankkiminen muulla menetelmällä olisi mahdotonta tai kohtuuttoman vaikeaa.

Vähimmän haitan periaatteesta johtuu, että sotilastiedusteluviranomaisen toimenpiteillä ei kenenkään oikeuksiin saisi puuttua enempää eikä kenellekään saisi aiheuttaa suurempaa vahinkoa tai haittaa, kuin on välttämätöntä tiedustelutehtävän suorittamiseksi. Sotilastiedusteluviranomainen saisi tarkoitussidonnaisuuden periaatteen mukaisesti käyttää tiedustelutoimivaltuuksiaan vain säädettyyn tarkoitukseen.

Ehdotetut tiedonhankintamenetelmät ovat suurelta osin sellaisia, joista on muissa yhteyksissä säädetty perustuslakivaliokunnan myötävaikutuksella (muun muassa PeVL 67/2010 vp, PeVL 33/2013 vp). Näin ollen perusoikeussääntelyn kehittyminen on voitu esityksessä huomioida. Toimivaltuuksien koskevasta sääntelystä käy ilmi, mitä valtuuksia käytettäessä saa tehdä ja miten tällöin on menetelmät, vaatimuksen tai päätöksen tietosisältö, kuka tiedustelusta päättää, tiedustelua koskevan luvan, päätöksen tai määräyksen kesto,

mahdolliset tiedustelumenetelmän käytön rajoitukset ja ehdot, kuuntelu-, katselu-, jäljentämis- ja tiedustelukiellot samoin kuin tiedustelun käytöstä ilmoittaminen.

Perustuslain 9 §:n kannalta merkityksellisiä tiedustelumenetelmiä olisivat tukiasematietojen hankkiminen, suunnitelmallinen tarkkailu, tekninen katselu ja tekninen seuranta. Kyseiset menetelmät merkitsisivät melko vähäistä puuttumista liikkumisvapauteen suhteessa siihen rajoitusperusteen välttämättömyyteen, jota kansallinen turvallisuus kansanvaltaisessa yhteiskunnassa edustaa. Näin ollen tässä mainittuja tiedustelumenetelmiä koskevan sääntelyn ei arvioida olevan ongelmallinen liikkumisvapauden kannalta.

Jokaisen kotirauha on perustuslain 10 §:n 1 momentin mukaan turvattu. Lailla voidaan pykälän 3 momentin mukaan säätää perusoikeuksien turvaamiseksi tai rikoksen selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimista.

Perustuslaissa turvattu kotirauhan piiri kattaa lähtökohtaisesti kaikenlaiset pysyväisluonteiseen asumiseen käytetyt tilat (PeVL 43/2010 vp, s. 2, PeVL 40/2010 vp, s. 4, PeVL 18/2010 vp, s. 7, PeVL 6/2010 vp, s. 4, PeVL 8/2006 vp, s. 2, PeVL 39/2005 vp, s. 2, PeVL 16/2004 vp, s. 5, PeVL 69/2002 vp, s. 2, PeVL 48/2001 vp, s. 2, PeVL 46/2001 vp, s. 3–4).

Tiedustelumenetelmä kohtaisesti olisi säädetty kielloista kohdistaa tiedustelumenetelmän käyttöä vakituiseen asumiseen käytettävään tilaan. Peitetoiminta ja valeosto asunnossa olisi sallittua vain, jos sisäänkäynti tai oleskelu tapahtuu asuntoa käyttävän aktiivisella myötävaikutuksella. Tiedustelumenetelmillä ei näin ollen puututtaisi perustuslaissa tarkoitetun kotirauhan suojan ydinalueelle.

Lähtökohtana olisi, ettei tiedustelumenetelmää saisi kohdistaa asuntoon myöskään ulkomailla. Asunnon käyttötarkoituksen selvittäminen saattaa kuitenkin osoittautua mahdottomaksi tai kohtuuttoman vaikeaksi erilaisissa toimintaympäristöissä.

Perustuslain 10 §:n 3 momentin nojalla ei ole mahdollista säätää sellaisista rajoituksista viestin salaisuuteen, joiden tarkoituksena ei olisi yksilöidyn rikoksen torjuminen tai selvittäminen, vaan laajemmalti Puolustusvoimien lakisääteisten tehtävien suorittamiseksi välttämättömän tiedon hankkiminen vakavista ulkoisista uhkista.

Näin ollen tiedon hankkimisesta teknisen kuuntelun, teknisen laitetarkkailun, telekuuntelun ja sen sijasta tehtävän tietojen hankkimisen, televalvonnan, viestin jäljentämisen, viestiin kohdistuvan lähetyksen jäljentämisen ja tietoliikennetiedustelun menetelmin sotilaallisesta toiminnasta tai sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta, jos tiedonhankinta kohdistuu muuhun kuin valtiolliseen toimijaan, olisi mahdollista säätää tavallisen lain säätämisjärjestyksessä vain perustuslain 10 §:n 4 momenttiin ehdotetun tiedon hankkimista koskevan uuden rajoitusperusteen nojalla ja edellyttäen, että sääntely täyttää perusoikeuksien yleiset rajoitusedellytykset. Uusi rajoitusperuste ei mahdollista yleisestä, kohdentamattomasta ja kaiken kattavasta tietoliikenteen seurannasta säätämistä.

Lähetyksen pysäyttäminen jäljentämistä varten ei voida katsoa puutuvan perusoikeussuojaan merkittävällä tavalla.

Tiedusteluviranomaisella ei voisi olla suoraa ja rajoittamatonta pääsyä tietoliikenneverkkoihin. Etenkin tietoliikennetiedustelun osalta tätä voidaan ehkäistä sillä, että tietoliikennetiedustelun edellyttämän tuomioistuimen luvan mukaisen kytkennän tietoliikenneverkkoon tekisi jokin muu taho kuin tiedusteluviranomainen itse.

6 Päätöksenteko

Päätöksentekijänä tiedustelumenetelmien käytön osalta olisi tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies, pääesikunnan tiedustelupäällikkö tai Helsingin käräjäoikeus. Eräiden tiedustelumenetelmien osalta olisi tarkoituksenmukaista turvallisuusnäkökohtien kannalta, että päätöksenteko pysyisi sotilastiedustelunviranomaisen sisällä.

Nyt käsiteltävänä olevassa esityksessä tuomioistuinlupaa edellyttäviä tiedustelumenetelmiä olisivat telekuuntelu ja tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen laitetarkkailu, paikkatiedustelu ja tietoliikennetiedustelu. Lupa voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan lukuun ottamatta telekuuntelussa ja sen sijasta toimitettavassa tietojen hankkimisessa, jos kohteena on henkilö. Näissä tilanteissa lupa voitaisiin antaa enintään kolmeksi kuukaudeksi kerrallaan.

Päätöksenteko olisi porrastettu sen mukaan kuinka vahvasti tiedustelumenetelmän käytöllä puututaan perusoikeuksiin. Esimerkiksi televerkoissa tapahtuvan tiedustelun osalta tuomioistuimelle esitettävässä lupavaatimuksessa olisi esitettävä 1) toimenpiteen perusteena oleva tiedustelutehtävä; 2) toimenpiteen kohteena oleva henkilö, teleosoite tai telepäätelaite; 3) tosiseikat, joihin telekuuntelun tai tietojen hankkimisen telekuuntelun sijasta edellytykset ja kohdistaminen perustuvat; 4) telekuuntelua tai tietojen hankkimista telekuuntelun sijasta koskevan luvan voimassaoloaika kellonajan tarkkuudella; 5) telekuuntelua tai tietojen hankkimista telekuuntelun sijasta johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies; 6) mahdolliset telekuuntelun tai tietojen hankkimisen telekuuntelun sijasta rajoitukset ja ehdot.

Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvan tiedustelun osalta tuomioistuimelle esitettävässä lupavaatimuksessa olisi esitettävä 1) tiedustelutehtävä, jota varten tietoliikennettä hankitaan; 2) tiedustelun kohdetta koskevat tosiseikat; 3) tosiseikat, joihin tietoliikennetiedustelun käytön edellytykset perustuvat; 4) tiedonhankinnassa käytettävät hakuehdot tai hakuehtojen luokat sekä perustelut niille 5) viestintäverkon osa, johon tiedustelu kohdistetaan sekä perustelut kohdistamiselle; 6) luvan voimassaoloaika kellonajan tarkkuudella; 7) viestinnän keräämistä ja tallentamista johtava ja valvova Puolustusvoimien tiedustelulaitoksen virkamies; 8) mahdolliset tietoliikennetiedustelun rajoitukset ja ehdot. Tietoliikennetiedustelun osalta säädettäisiin erikseen siitä, mitä hakuehtoja ei saisi käyttää tietoliikennetiedustelua käytettäessä.

EIT on ratkaisukäytännössään, muun muassa tapauksissa Weber ja Saravia v. Saksa sekä Liberty ja muut v. Yhdistynyt kuningaskunta, asettanut minivaatimuksia salaista viranomaistoimintaa koskevalle lainsäädännölle, jotta vallan väärin käyttöä voitaisiin ehkäistä. Lainsäädännöstä on käytävä ilmi muun muassa ne tilanteet, joissa perusoikeuksiin puuttuminen on mahdollista, kohteiden määrittely ja toimivaltuuksien käytön keston rajoitukset.

Ulkomailla tapahtuvasta sotilastiedustelusta ja siinä käytettävistä tiedustelumenetelmistä päätöksen tekisi aina pääesikunnan tiedustelupäällikkö. Suomalaisella tuomioistuimella ei ole toimivaltaa tehdä päätöksiä, jotka ulottuisivat toisen valtion lainkäyttöpiiriin. Lisäksi pääesikunnan tiedustelupäällikön olisi otettava päätöksessään huomioon ulkopoliittiset näkökohdat, mikä varmistettaisiin tiedustelutoiminnan yhteensovittamisen kautta.

Suhde perustuslakiin

Tiedustelutoiminnassa korostuvat oikeusturvajärjestelyjen ja valvonnan tehokkuus sekä asianmukaisuus. Myös ihmisoikeusvelvoitteet ja Euroopan unionin oikeusjärjestys edellyttävät luottamuksellisen viestin salaisuuden suojaan puuttuvien toimivaltuuksien käytön valvonnalta tehokkuutta ja riippumattomuutta. On tärkeää, että tiedusteluviranomaisella ei ole rajoittamatonta harkintavaltaa tiedonhankinnan kohdentamisessa. Yksi tapa rajoittaa viranomaisen harkintavaltaa on osoittaa vakavinta puuttumista perusoikeussuojaan tarkoittava tiedustelumenetelmien käytöstä päättäminen tuomioistuimelle (muun muassa EIT:n ratkaisu Weber ja Saravia v. Saksa).

Harkintavaltaa voidaan rajoittaa myös yksittäisiä toimivaltuuksia koskevissa säännöksissä. Sääntelystä käy ilmi, kuka tiedustelumenetelmän käyttämisestä päättää, tiedustelua koskevan luvan, päätöksen tai määräyksen tietosisältö.

7 Tietojen luovuttaminen

Esitetyssä laissa olisi tarkasti säädetty tilanteista, joissa tiedustelumenetelmin saatua tietoa voitaisiin luovuttaa rikosten selvittämiseen ja estämiseen. Jos rikoksesta säädetty ankarin rangaistus olisi vähintään kuusi vuotta vankeutta, olisi sotilastiedusteluviranomaisen ilmoitettava siitä toimivaltaiselle viranomaiselle.

Mahdollisuus luovuttaa tietoa rikosten selvittämiseksi olisi sidottu rikoksiin, joista säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta. Jos kyseessä olisi vielä estettävissä oleva rikos, tietoa voitaisiin luovuttaa, jos rikoksesta säädetty ankarin rangaistus olisi vähintään kaksi vuotta vankeutta.

Esityksessä säädettäisiin lisäksi tiedustelutiedon luovuttamisesta kansainvälisessä yhteistyössä. Esityksessä tarkoitettu tietojen luovuttaminen koskisi muuta kuin henkilötietoa, josta säädettäisiin erikseen valmisteltavana olevassa henkilötietojen käsittelystä Puolustusvoimissa annettavassa laissa, joka on tarkoitus antaa eduskunnalle lähiaikoina.

EIT on ratkaisussaan Weber ja Saravia v. Saksa katsonut, että tilanteissa, joissa tiedusteluviranomaisen tietoon tulee rikoksia koskevaa tietoa, tieto on annettavissa edelleen rikosten torjuntaa ja selvittämistä suorittaville viranomaisille, jos kyseessä on riittävän vakava rikollisuus. Puolustusministeriössä valmisteltavana olevassa Puolustusvoimien henkilötietojen käsittelystä annetussa laissa säädettäisiin kattavasti ja yksityiskohtaisesti myös sotilastiedustelua koskevista henkilörekistereistä, niiden käyttötarkoituksesta ja tietosisällöstä sekä henkilötietojen luovuttamisesta toiselle valtiolle ja kansainväliselle järjestölle.

Koska Puolustusvoimien kansainvälinen toiminta on luonteeltaan hyvin erilaista kuin muiden viranomaisten, eikä henkilötietojen vapaa liikkuvuus unionin alueella koske Puolustusvoimien toimintaa, asiasta olisi syytä säätää Puolustusvoimien osalta erikseen.

Edellä mainitussa laissa säädettäisiin tyhjentävästi niistä tarkoituksista, joiden vuoksi tietoja saisi luovuttaa sekä tietyistä luovutuksiin liittyvistä suojatoimista. Laissa erikseen kiellettäisiin Suomen kansalaisten ja Suomessa asuvien henkilöiden arkaluonteisten henkilötietojen laajamittainen luovuttaminen ulkomaille. Sääntelyn voidaan katsoa täyttävän perustuslain vaatimuksen riittävästä yksityiskohtaisuudesta ja tarkkarajaisuudesta.

Hallituksen esitys laiksi Puolustusvoimien henkilötietojen käsittelystä ja eräiksi siihen liittyviksi laeiksi on tarkoitus antaa eduskunnalle viikolla 10. Siten se olisi eduskunnan käsiteltävänä samaan aikaan tiedustelulainsäädäntöä koskevien hallitusten esitysten kanssa.

Suhde perustuslakiin

Sotilastiedusteluviranomaisen tehtävistä ja toimivaltuuksista on säädettävä yleisen laillisuusperiaatteen nojalla selkeästi. Kuitenkin tiedustelutoiminnassa voi tulla vastaan tilanteita, joissa saadaan tietoa rikosepäilystä tai suhteellisen vakavista vielä estettävissä olevista rikoksista. Oikeusjärjestyksen kannalta ei voida pitää perusteltuna tilannetta, jossa vakaviin rikoksiin liittyvää tietoa ei voitaisi luovuttaa edelleen kyseisten rikosten selvittämisestä tai ennalta estämisestä vastaavalle viranomaiselle.

Sääntelyä voidaan pitää tältä osin selkeänä ja tarkkarajaisena.

8 Tiedustelukiellot ja tietojen hävittäminen

Lakiesityksen 79 §:ssä olisi säädetty tiedustelukielloista (muun muassa EIT:n ratkaisu Weber ja Saravia v. Saksa). Pykälän 1 momentissa luetelluilla tiedustelumenetelmillä ei saisi hankkia tietoa tiettyjen ammattityhmien toiminnasta, joita koskevista velvollisuuksista tai oikeudesta kieltäytyä todistamasta säädetään oikeudenkäymiskaaren 17 luvun 13, 14, 16, 20 §:ssä tai 22 §:n 2 momentissa.

Erityinen tiedustelukielto koskisi tietoliikennetiedustelua. Kiellon mukaan tietoliikennetiedustelua ei saisi kohdistaa viestintään, jonka lähettäjä ja vastaanottaja olisivat Suomessa.

Tiedustelukiellosta poikkeuksena olisivat tilanteet, joissa tiedustelukiellon piirissä olevat ammattiryhmän edustajan osalta olisi tehty tiedustelumenetelmän käyttöä koskeva päätös. Toisin sanoen edellytyksenä olisi se, että myös tämä henkilö osallistuisi sotilastiedustelun kohteena olevaan toimintaan.

Jäljentämiskielloista säädettäisiin erikseen 80 §:ssä.

Tiedustelutietojen hävittämisestä (muun muassa EIT:n ratkaisu Weber ja Saravia v. Saksa) säädettäisiin 81 §:ssä. Lähtökohtaisesti tiedustelumenetelmällä saatu tieto olisi hävitettävä viipymättä sen jälkeen, kun on käynyt ilmi, ettei tietoa tarvittaisi tai tietoa ei saisi käyttää sotilastiedustelun tehtävien hoitamiseksi taikka tietoa ei tarvittaisi maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi. Erityisistä tiettyjä tiedustelumenetelmiä koskevista keskeyttämisvelvollisuuksista ja tiedustelumenetelmällä hankitun tiedon hävittämisestä säädettäisiin 82 §:ssä.

Käsiteltävänä olevan lakiehdotuksen 83 §:ssä säädettäisiin tietoliikennetiedustelua koskevista erityisistä tietojen hävittämisvelvollisuuksista. Säännöksen mukaan tieto olisi hävitettävä viipymättä, kun kävisi ilmi, että viestinnän lähettäjä ja vastaanottaja olivat Suomessa. Lisäksi tieto olisi hävitettävä välittömästi, jos lähettäjällä, vastaanottajalla tai tallentajalla olisi oikeus tai velvollisuus kieltäytyä todistamasta kyseisestä tiedosta tiedustelukieltojen mukaisesti.

Tiedustelukieltoja ja tietojen hävittämisvelvollisuuksia olisi toteutettava tiedustelumenetelmän käytön aikana sekä tiedustelumenetelmän käytöstä syntyneiden tallenteiden tarkastamisen (1. lakiehdotuksen 106 §) yhteydessä.

Suhde perustuslakiin

Tiedustelukielloilla, tietojen hävittämisvelvollisuudella ja hetihävittämisvelvollisuudella rajataan yksityiselämän suojaan puuttumista sen jälkeen, kun tiedustelumenetelmän edellytysten on katsottu täyttyneen ja niitä varsinaisesti käytetään. Edellä tarkoitetut kiellot ja velvollisuudet toteuttavat lainsäädännön ennakoitavuutta, koska ne rajaavat tiedustelumenetelmien käyttöä siten, että niitä kohdistetaan vain sotilastiedustelun kannalta merkityksellisiin tietoihin ja niiden avulla pyritään välttämään sivullisiin kohdistuvaa tiedustelumenetelmien käyttöä. Kun tiedonhankinta rajataan vain sotilastiedustelun kannalta merkityksellisiin tietoihin, yksilöt voivat ennakoida, missä tilanteissa he saattavat joutua tiedustelumenetelmien käytön kohteeksi ja missä tilanteissa heistä hankittua tietoa käytettäisiin.

Tiedustelukielloilla ja hävittämisvelvollisuuksilla on tärkeä merkitys yksilön oikeusturvan takeena ja viranomaisen mielivallan ehkäisemisessä.

9 Ilmoittaminen tiedustelumenetelmän käytöstä

Ilmoituksen tekeminen tiedustelumenetelmän käytöstä on yhdistetty siihen, että yksilöllä on mahdollisuus haastaa viranomaisten toiminnan laillisuus (muun muassa EIT:n ratkaisut Klass ym. v. Saksa, Weber ja Saravia v. Saksa). Ilmoitusvelvollisuus ei ole kuitenkaan absoluuttinen, koska ilmoittaminen voisi vaarantaa niitä pitkäntähtäimen tavoitteita, joiden vuoksi tiedustelumenetelmän käyttö aloitettiin.

Käsiteltävänä olevan esityksen 1. lakiehdotuksen 86 §:ssä säädettäisiin ilmoitusvelvollisuudesta tiedustelumenetelmän käytön kohteelle (muun muassa EIT:n ratkaisut Zakharov v. Venäjä, Klass ym. v. Saksa, Weber ja Saravia v. Saksa). Pykälän 1 momentin mukaan telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta ja teknisestä tarkkailusta sekä viestiin kohdistuvasta jäljentämisestä ja viestiin kohdistuvasta lähetyksen jäljentämisestä olisi viipymättä ilmoitettava tiedonhankinnan kohteena olleelle henkilölle kirjallisesti sen jälkeen, kun tiedustelumenetelmän käytön tarkoitus olisi saavutettu. Ilmoitus olisi tehtävä viimeistään vuoden kuluttua tiedustelumenetelmän käytön lopettamisesta.

Ilmoitusta voitaisiin lykätä tai jättää se tekemättä, mikäli tuomioistuin antaisi siihen luvan. Lykkäys voitaisiin myöntää korkeintaan kahdeksi vuodeksi kerrallaan, jos se olisi perusteltua käynnissä olevan tiedustelumenetelmän turvaamiseksi, maanpuolustuksen kannalta tai kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi.

Ilmoitus voitaisiin jättää kokonaan tekemättä tuomioistuimen päätöksellä, jos se on välttämätöntä maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi taikka hengen tai terveyden suojaamiseksi. EIT on katsonut ratkaisuissaan Klass ym. v. Saksa sekä Weber ja Saravia v. Saksa, ettei ilmoitusvelvollisuus ole absoluuttinen, sillä se voisi vaarantaa niitä pitkäntähtäimen tavoitteita, joiden vuoksi tiedustelumenetelmän käyttö aloitettiin. Lisäksi ratkaisussa Weber ja Saravia v. Saksa todetaan, että päätös kokonaan ilmoittamatta jättämisestä tulisi tapahtua ulkopuolisen toimielimen toimesta.

Tietoliikennetiedustelun osalta ilmoitusvelvollisuus alkaisi siitä ajankohdasta, kun tiedustelumenetelmän käyttö olisi lopetettu ja tietoliikennetiedustelun jatkokäsittelyssä olisi manuaalisesti selvitetty viestin sisältö. Ennen manuaalista käsittelyä sotilastiedusteluviranomaisen virkamiehellä ei olisi mahdollisuutta perehtyä kerätyn tietoliikenteen sisältöön eikä sotilastiedusteluviranomaisella olisi näin ollen myöskään mahdollisuutta hyödyntää tietoa. EIT on ratkaisussaan Weber ja Saravia v. Saksa todennut, että tieto, jota ei ole käytetty ja on tuhottu, ei edellytä ilmoittamista tiedustelumenetelmän käytön kohteelle.

Ilmoitusvelvollisuus ei koskisi suunnitelmallista tarkkailua, peiteltyä tiedonhankintaa, peitetoimintaa, valeostoa, tietolähteen ohjattua käyttöä, paikkatiedustelua, muuhun viestiin kohdistuvaa jäljentämistä ja muuhun kuin viestiin kohdistuvaa lähetyksen jäljentämistä. Tätä voidaan pitää perusteltuna kyseisten tiedustelumenetelmien käytön vaarantumisena, työturvallisuusnäkökohdilla tai lievällä puuttumisella perusoikeuksiin.

Poikkeus ilmoitusvelvollisuudesta koskisi myös tilanteita, joissa tiedustelumenetelmän käytön kohteena olisi valtiollinen toimija.

Suhde perustuslakiin

Perustuslain 118 §:n 3 momentissa säädetään, että jokaisella, joka on kärsinyt oikeudenloukkauksen tai vahinkoa virkamiehen tai muun julkista tehtävää hoitavan henkilön lainvastaisen toimenpiteen tai laiminlyönnin vuoksi, on oikeus vaatia tämän tuomitsemista rangaistukseen sekä vahingonkorvausta julkisyhteisöltä taikka virkamieheltä tai muulta julkista tehtävää hoitavalta sen mukaan kuin lailla säädetään.

Tiedustelumenetelmän käytön kannalta yksilön oikeusturvan takeena on, että tiedustelumenetelmän käytöstä ilmoitetaan lähtökohtaisesti tiedustelumenetelmän käytön kohteena olevalle henkilölle. Näin yksilöllä on mahdollisuus haastaa viranomaisten toiminnan laillisuus.

Lisäksi jo ennen ilmoituksen saamista itseään tiedustelumenetelmän käytön kohteeksi epäilevä voi tehdä pyynnön perustettavaksi esitettävälle tiedusteluvaltuutetulle ryhtyä toimiin sen osalta, onko hänen kohdallaan tiedustelumenetelmiä käytetty tai onko niitä mahdollisesti käytetty lainmukaisesti sekä ryhtymään väärinkäytöksen edellyttämiin toimiin.

10 Valvonta ja oikeusturvajärjestelyt

Tiedustelumenetelmien käyttö perustuisi aina viranomaisomaispäätökseen. Kuten edellä tämän muistion kohdassa *Päätöksenteko* on todettu, päätöksentekijänä olisi aina joko tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies, tiedustelumenetelmien käyttöön erityisesti perehtynyt muu virkamies, pääesikunnan tiedustelupäällikkö tai

tuomioistuin. Edellä tarkoitetut tahot suorittaisivat tiedustelumenetelmien käytön valvontaa ennakollisesti.

Tiedustelumenetelmien käyttöä valvoisi aina ensisijaisesti lähiesimies, kuten asianlaita on muussakin viranomaistoiminnassa. Jo voimassa olevan lainsäädännön mukainen viranomaistoiminnan valvonta säilyisi ennallaan. Eduskunnan oikeusasiamies, valtioneuvoston oikeuskansleri ja tietosuojavaltuutettu suorittaisivat jatkossakin valvontatehtäviään, joiden alaan myös sotilastiedustelu kuuluisi jatkossa. Myös Euroopan ihmisoikeustuomioistuin valvoisi osaltaan Suomen lainsäädännön ihmisoikeussopimuksen mukaisuutta.

Elimellisenä osana valvontaa olisi myös sotilastiedusteluviranomaisen velvollisuus laatia pöytäkirja ilman aiheetonta viivytystä tiedustelumenetelmän käytöstä.

Sotilastiedustelutoimintaa kokonaisuudessaan valvoisi pääesikunnan päällikkö ja puolustusvoimien asessori, joiden suorittamaa valvontaa täydentäisi puolustusministeriön harjoittama valvonta.

Edellä sanotun lisäksi tiedustelutoimintaa varten ehdotetaan perustettavaksi oma laillisuusvalvontaa suorittava viranomainen, tiedusteluvaltuutettu, jolla olisi riippumaton ja sillä olisi laajat tiedonsaantioikeudet sekä mahdollisuus keskeyttää tiedustelumenetelmän käyttö. Nyt käsiteltävänä olevassa esityksessä sotilastiedusteluviranomaiselle olisi myös säädetty velvollisuus toimittaa tieto kaikista tiedustelumenetelmiä koskevista päätöksistä tiedusteluvaltuutetulle. EIT on edellyttänyt muun muassa tapauksissa Amann v. Sveitsi, Liberty ja muut v. Yhdistynyt kuningaskunta ja Weber ja Saravia v. Saksa edellyttänyt, että lain tulee sisältää säännökset tarkkailuvaltuuksien valvonnasta ja niitä koskevista oikeussuojakeinoista.

Riippumattoman tiedusteluvaltuutetun lisäksi eduskuntaan on esitetty perustettavaksi tiedustelunvalvontavaliokunta. EIT on muun muassa ratkaisuissaan Campbell v. Yhdistynyt kuningaskunta ja Leander v. Ruotsi katsonut, että demokratian suojelemisen kannalta merkitystä on annettava myös sillä, että kansanedustuslaitos osaltaan osallistuu salaisten tarkkailuvaltuuksien valvontaan.

Valvonnan toteuttaminen voidaan nähdä myös laajempana. Valvontaa suorittavat myös edellä kuvatun ensisijaisen valvonnan lisäksi välillisesti kansalaiset, tiedustelumenetelmän käytöstä ilmoituksen saaneet henkilöt, tiedotusvälineet, kansalaisjärjestöt sekä kansanedustajat.

Kattavan ja tehokkaan valvonnan lisäksi yksilön oikeusturvasta huolehditaan esityksessä monessa eri kohdin, kuten säätämällä yksityiskohtaisesti sotilastiedustelun tarkoituksesta ja kohteista, tiedustelutoiminnan ohjauksesta ja toiminnassa noudatettavista periaatteista, tiedonhankinnan menetelmistä ja niiden edellytyksistä, luvanvaraisuudesta, tiedustelukielloista, tietojen luovuttamisesta, tiedustelutietojen hävittämisestä ja tiedustelumenetelmän käytöstä ilmoittamisesta tiedustelun kohteelle.

Suhde perustuslakiin

Tiedustelutoiminnan valvonnan tehokkuus edellyttää, että valvontaelimillä on oikeus tarkastaa tietoja ja asiakirjoja. Siksi tiedustelumenetelmiä koskisi viivytyksetön pöytäkirjaamisvelvoite.

Tiedustelutoiminnan ulkoisesta laillisuusvalvonnasta huolehtisi ylimpien laillisuusvalvojien lisäksi uusi viranomainen, tiedusteluvaltuutettu, joka valvoisi tiedustelutoimintaa reaaliaikaisesti (Klass ym. v. Saksa). Reaaliaikaisen valvonnan mahdollistamiseksi säädettäisiin velvoitteesta antaa tieto tiedusteluvaltuutetulle tiedustelumenetelmiä koskevista tuomioistuimen päätöksistä ja luvista mahdollisimman pian tuomioistuimen päätöksen jälkeen. Lisäksi sotilastiedusteluviranomaisen olisi mahdollisimman pian ilmoitettava tiedusteluvaltuutetulle päätöksestä, joka koskee muuta kuin tuomioistuimen päätöksentekotoimivaltaan kuuluvaa tiedustelumenetelmää, tiedustelun suojaamista, ilmaisukieltoa sekä rikostorjuntaan luovutettavan tiedon siirtämisen lykkäämisestä (1. lakiehdotuksen 104 §).

Valtuutetulla olisi laajat tiedonsaantioikeudet ja oikeus saada selvityksiä viranomaisilta ja muilta julkista hallintotehtävää hoitavilta. Valtuutettu voisi tehdä tarkastuksia tiedustelutoiminnan laillisuuden valvomiseksi, minkä lisäksi sille ehdotetaan oikeutta päästä valvonnan kannalta välttämättömiin tiloihin ja tietojärjestelmiin. Tiedusteluvaltuutettu voisi lisäksi määrätä tiedustelumenetelmän käytön keskeytettäväksi tai lopetettavaksi, jos hän katsoo valvottavan menetelleen lainvastaisesti tiedustelutoiminnassa.

11 Säätämisjärjestyksen arviointi

Tässä esityksessä ehdotettavan lainsäädännön arvioidaan täyttävän EIT:n ratkaisukäytännön ja perustuslakivaliokunnan tulkintakäytännön asettamat vaatimukset perus- ja ihmisoikeuksien huomioon ottamisesta. Esitykseen sisältyvät lakiehdotukset voidaan hallituksen käsityksen mukaan käsitellä tavallisen lain säätämisjärjestyksessä lukuun ottamatta sellaisia toimivaltuuksia koskevia säännösehdotuksia, jotka merkitsevät puuttumista perustuslain 10 §:n 2 momentissa turvattuun luottamuksellisen viestin salaisuuteen.

Tällaisia säännösehdotuksia ovat 1. lakiehdotuksen 24 § (tekninen kuuntelu), 30 § (tekninen laitetarkkailu), 32 §:n 3 momentti (muuhun kuin valtiolliseen toimijaan kohdistuva telekuuntelu), 33 § (muun kuin valtiollisen toimijan tietojen hankkiminen telekuuntelun sijasta), 35§:n 3 momentti (muuhun kuin valtiolliseen toimijaan kohdistuva televalvonta), 55 § (muun kuin valtiollisen toimijan lähetyksen jäljentäminen) ja 67 § (muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu). Niistä olisi kuitenkin mahdollista säätää tavallisen lain säätämisjärjestyksessä perustuslain 10 §:n 4 momenttiin ehdotetun tiedon hankkimista koskevan uuden rajoitusperusteen nojalla.

12 Voimaantulo

Lait ehdotetaan tulemaan voimaan mahdollisimman pian.

Suomen toimintaympäristön muutos on ollut nopea ja jatkuu edelleen. Sen vuoksi maanpuolustukselle kriittisen tärkeän sotilastiedustelun suorituskyvyn turvaamiseksi ehdotetut säännökset tulisi saattaa kokonaisuudessaan voimaan mahdollisimman nopeasti. Tällöin

olisi mahdollista välttää sotilastiedustelun kyvyn liiallinen heikkeneminen suhteessa Suomen nopeasti muuttuvaan turvallisuusympäristöön ja mahdollistaa Suomen puolustusratkaisun tarvitsema ennakkovaroituskyky ja toimintaympäristötietoisuus.

Esityksen 1. lakiehdotukseen sisältyvät säännösehdotukset, jotka koskevat teknistä kuuntelua (24 §), teknistä laitetarkkailua (30 §), muuhun kuin valtiolliseen toimijaan kohdistuvaa telekuuntelua (32 §:n 3 momentti), tietojen hankkimista telekuuntelun sijasta (33 §), muuhun kuin valtiolliseen toimijaan kohdistuvaa televalvontaa (35 §:n 3 momentti), lähetyksen jäljentämistä (55 §) ja muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvaa tiedustelua (67 §), edellyttävät perustuslain muuttamista ja liittyvät siten oikeusministeriössä valmisteltuun hallituksen esitykseen yksityiselämän suojaa koskevan perustuslain 10 §:n sääntelyn tarkistamiseksi (HE 198/2017 vp), joka on käsiteltävä perustuslain 73§:ssä säädetyssä järjestyksessä.

Jos perustuslain muutosehdotus käsiteltäisiin pääsäännön mukaan perustuslain 73 §:n 1 momentin mukaisessa niin sanotussa normaalissa perustuslain säätämisjärjestyksessä, edellä mainitut säännökset voisivat tulla voimaan mahdollisesti 1.1.2020. Sen sijaan, jos perustuslain muutosehdotus käsiteltäisiin perustuslain 73 §:n 2 momentin mukaisessa nopeutetussa menettelyssä, edellä mainitut säännökset voisivat tulla voimaan vuonna 2018 tai vuoden 2019 alusta.

Jos perustuslain muuttamiselle kiireellisessä menettelyssä ei katsota olevan edellytyksiä ja perustuslain muutos käsiteltäisiin normaalissa menettelyssä, muut kuin perustuslain muuttamista edellyttävät säännösehdotukset ehdotetaan kuitenkin tulevaksi voimaan mahdollisimman pian tavallisessa lainsäätämisjärjestyksessä eikä niitä jätettäisi teknisesti lepäämään eduskuntavaalien yli.

Esityksellä on lisäksi kiinteä yhteys hallituksen esityksiin HE 202/2017 vp ja HE 199/2017 vp, joissa ehdotetaan säädettäväksi siviilitiedustelusta ja tiedustelutoiminnan valvonnasta. Sen vuoksi kaikkien edellä mainittujen esitysten voimaantuloajankohdan tulisi olla sama.