

Perustuslakivaliokunnalle

Hallituksen esitys 203/2017 vp eduskunnalle laiksi sotilastiedustelusta sekä eräiksi siihen liittyviksi laeiksi

1 Arvioinnin lähtökohdat

Hallituksen esitys on osa tiedustelulainsäädäntöä koskevaa kokonaisuutta, jossa säädettäisiin siviili- ja sotilastiedustelusta sekä tiedustelun valvonnasta. Ehdotukseen laiksi sotilastiedustelusta sisältyy laaja valikoima sotilastiedusteluviranomaiselle annettavia tiedonhankintakeinoja sekä näiden keinojen käyttämiseen liittyviä muita säännöksiä. Esityksen mukaan viranomaisella saisi vastaavat tiedonhankintakeinot kuin mitä poliisilla on tällä hetkellä käytössään rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi. Tämän lisäksi sotilastiedusteluviranomaisella saisi uusia toimivaltuuksia muun muassa ulkomaan tietojärjestelmätiedusteluun ja tietoliikennetiedusteluun.

Ehdotettu laki sisältää useita viranomaistoimivaltuuksia, joilla rajoitettaisiin niiden kohteiden perusoikeuksia. Perusoikeusrajoitus kohdistuisi muun muassa perustuslain 10 §:ssä suojattuihin luottamuksellisen viestin suojaan, kotirauhan suojaan ja henkilötietojen suojaan. Osalla ehdotetuissa valtuuksista on yhteys liikkumisvapauteen (9 §).

Perustuslain 10 §:n 2 momentin mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. 15.10.2018 voimaan tulleella lailla (817/2018) perustuslakiin on lisätty 10 §:n 4 momentti, jonka mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Perustuslain muutosta koskevassa mietinnössään (PeVM 4/2018 vp) perustuslakivaliokunta viittasi sotilaallista toimintaa koskevan rajoitusedellytyksen osalta muun muassa tarpeeseen seurata Suomen turvallisuusympäristön kannalta merkityksellisen sotilaallisen toiminnan kehitystä tilannekuvan muodostamiseksi. Valiokunta kiinnitti huomiota siihen, että vaikka vieraan valtion sotilas- tai muun viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa, sotilastiedustelutoimivaltuuksia ei voida kohdistaa kaikissa tapauksissa niin täsmällisesti, ettei olisi vaaraa viranomaisten tilapäisestä pääsystä yksittäisten, tiedustelutehtävään liittymättömien henkilöiden viestintää koskeviin tietoihin, mikä tulee perustuslakivaliokunnan mielestä tavallisissa laeissa rajata mahdollisimman vähäiseksi. Valiokunta korosti, että säännöksen

soveltamisala rajautuu hallituksen esityksen perusteluissa kuvatuilla tavoin tiedon hankkimiseen vain Suomeen kohdistuvasta sotilaallisesta toiminnasta taikka Suomen turvallisuusympäristön kannalta merkityksellisestä sotilaallisesta toiminnasta. Muutoinkin valiokunta painotti tarvetta tulkita rajoitusperustetta suppeasti.

Muussa tulkintakäytännössään perustuslakivaliokunta on katsonut, että perusoikeusrajoitusten on oltava täsmällisiä ja tarkkarajaisia ja että rajoituksen olennaisen sisällön tulee ilmetä laista (PeVM 25/1994 vp, s. 5/I). Valiokunta on edellyttänyt, että perusoikeusrajoituksen perustelevalle käsitteelle tarkka merkityssisältö ilmenee myös lakitekstin sanamuodosta, ei pelkästään esityksen perusteluista (PeVL 5/1999 vp, s. 3/II). Valiokunta on suhtautunut kriittisesti käsitteiden laveaan tulkintaan (PeVL 30/2017 vp).

2 Sotilastiedustelun kohteet

Sotilastiedustelulakiehdotuksen 4 §:n 1 momentissa luetellaan sotilastiedustelun kohteet, joista tiedon saamiseksi tiedustelumenetelmiä voitaisiin käyttää. Säännöksessä ei rajata maantieteellisesti sitä, missä tiedusteltavan toiminnan on tapahduttava eli toiminta voi olla joko Suomessa tai ulkomailla. Luettelon perusteella tiedustelun ala olisi hyvin laaja, jolloin myös perusoikeusrajoitusten henkilöllinen ala kasvaa potentiaalisesti suureksi.

Esityksen perusteluiden (s. 183) mukaan tiedustelumenetelmän käytön edellytyksenä ei olisi, että toiminnan taustalla oleva taho olisi tunnistettu sillä hetkellä, kun tiedustelumenetelmän käyttöön ryhdytään. Tiedustelumenetelmiä voitaisiin käyttää uhkien havaitsemiseksi ja niiden aiheuttajina olevien tahojen tunnistamiseksi. Tiedustelumenetelmän kohteena voisi myös olla henkilö tai henkilöryhmä, jonka voidaan olettaa liittyvän kyseisessä pykälässä tarkoitettuun toimintaan. Tiedustelun lisäedellytyksenä olisi, että kohteena oleva toiminta on luonteeltaan sotilaallista.

Sotilaallisen toiminnan käsitettä ja luettelossa käytettyjä käsitteitä on selitetty pitkällisesti esityksen perusteluissa. Esityksen mukaan sotilaalliselle toiminnalle tyypillistä ovat suuret joukkokokonaisuudet, sotilaallisten toimenpiteiden valmistelu ja johtaminen, sotilaallinen järjestäytyminen, sotilaallinen kouluttautuminen ja varustautuminen vahvemmin kuin tavanomaisilla voimankäyttövälineillä. Lisäksi sotilaallinen toiminta vaatii usein vahvaa taloudellista resursointia. Usein tällaisen toiminnan taustalla on valtio. Sotilaallisen toiminnan käsitteen alaan luettaisiin niin valtiolliset kuin ei-valtiollisetkin toimijat.

Perustuslain muutosta koskevassa mietinnössään perustuslakivaliokunta korosti, että säännöksen soveltamisala rajautuu hallituksen esityksen perusteluissa kuvatuilla tavoin tiedon hankkimiseen vain Suomeen kohdistuvasta sotilaallisesta toiminnasta taikka Suomen turvallisuusympäristön kannalta merkityksellisestä sotilaallisesta toiminnasta. Muutoinkin valiokunta painotti tarvetta tulkita rajoitusperustetta suppeasti.

Tarkkarajaisuuden ja täsmällisyyden näkökulmasta voidaan todeta, että luettelon kohdat 1, 2, 3 ja 6 vaikuttavat tarkkarajaisilta. Kohdan 4 (vieraan valtion sotatarvikkeiden kehittäminen ja levittäminen) tulkinnassa on otettava huomioon perusteluissa (s. 188) esitetty raja, jonka mukaan kohta kattaa nimenomaan sellaisen teknologian kehittämisen ja levittämisen, jota ei kehitetä yksityisten ihmisten hankittavaksi.

Kohta 5 (kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi) on määritelty laveasti ja epäselvästi. Perustuslain muutosta koskevan hallituksen esityksen (HE 198/2017 vp) mukaan kriisinhallinta- ja avuntoantotehtävissä toimiviin henkilöihin voi kohdistua sotilaallista uhkaa, jolloin kyseessä voisi olla perustuslaissa tarkoitettu sotilaallinen toiminta. Tässä yhteydessä käsite "kriisi" viittaa jännitteiseen tilanteeseen, joka voi johtaa esimerkiksi aseelliseen selkkaukseen. Kyseessä ei ole kuitenkaan sellainen 1 momentin ensimmäisessä lauseessa tarkoitettu "toiminta", jonka taustalla olisi tietty toimija tai joka olisi luonteeltaan sotilaallista. Nähdäkseni myöskään perusteluissa (s. 189) viitatus demokraattisten instituutioiden toiminnan rajoittaminen ja perusvapauksien ja ihmisoikeuksien kaventaminen eivät itsessään ole säännöksessä edellytettyä luonteeltaan sotilaallista toimintaa. Kohta 5 on välttämätöntä täsmentää siten, että siinä määritellään tarkkarajaisemmin tiedustelun kohteena olevat toimijat ja sotilaallinen toiminta.

Kohta 7 on ongelmallinen siltä osin kuin tiedustelu liittyisi perusteluissa (s. 190) mainittuun terrorismi-iskuun, luonnononnettomuuteen, suuronnettomuuteen tai vastaavaan tapahtumaan, koska niissä ei ole kyse sotilaallisesta toiminnasta. Muutenkin kohdan 7 sanamuoto on erittäin lavea erityisesti kohdassa "kansainvälinen muu toiminta". Kohta 7 on syytä poistaa tai muotoilla tarkkarajaisemmin.

Ei-valtiolliset toimijat. Perusteluista selviää, että osa luettelon kohteista voisi olla myös ei-valtiollisia toimijoita. Tiedustelun kohdentamisen kannalta olennainen käsite on "valtiollinen toimija", jolla sotilastiedustelulakiehdotuksen 9 §:n 10 kohdan määritelmän mukaan tarkoitettaisiin vieraan valtion tunnistettua viranomaista tai sellaiseen rinnastuvaa toimijaa sekä näiden palveluksessa olevaa tai sen määräyksessä ja ohjauksessa toimivaa tahoa. Perustelujen (s. 201) mukaan käsite voisi tarkoittaa myös yksityistä yritystä, muuta ryhmittymää tai jopa yksittäistä henkilöä, mutta tällöin edellytyksenä olisi, että kyseinen taho toimii valtion määräysvallassa tai sen ohjauksessa.

Suhteellisuusperiaatteen näkökulmasta ei ole poissuljettua, että tiedustelu voisi jossain tapauksessa kohdistua esimerkiksi yksityiseen yritykseen, jos toiminta on luonteeltaan sotilaallista (esimerkiksi aseteknologian kehittäminen sotilaalliseen tarkoitukseen). Tällöin ei olla kuitenkaan enää sotilaallisen toiminnan käsitteen perusmerkityksen piirissä, mikä on käytännön soveltamistilanteissa otettava huomioon arvioitaessa tiedustelukeinojen oikeasuhtaisuutta.

Perustuslain muutosta koskevassa mietinnössään perustuslakivaliokunta totesi, että vaikka vieraan valtion sotilas- tai muun viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa, sotilastiedustelutoimivaltuuksia ei voida kohdistaa kaikissa tapauksissa niin täsmällisesti, ettei olisi vaaraa viranomaisten tilapäisestä pääsystä yksittäisten, tiedustelutehtävään liittymättömien henkilöiden viestintää koskeviin tietoihin, mikä tulee perustuslakivaliokunnan mielestä tavallisissa laeissa rajata mahdollisimman vähäiseksi.

Valtiollisen toimijan käsitteen liian väljä tulkinta voi johtaa siihen, että tosiasiaassa tiedustelun kohteeksi tuleekin luonnollisia henkilöitä. Viestinnän kohteena olevan toimijan pitäisi olla etukäteen tunnistettu valtiolliseksi toimijaksi. Katson, että viranomaisen olisi pystyttävä esittämään tiedustelua valvovalle viranomaiselle ne perusteet, joihin nojautuen tämä tunnistaminen on tehty. Jos tiedustelun aikana osoittautuu, ettei kohde olekaan valtiollinen toimija, tiedustelu olisi keskeytettävä (11 §:n 4 momentin mukaan) ja kerätyt tiedot hävitettävä.

Esityksen perusteluissa vedotaan olettamukseen, jonka mukaan viranomaisen laitteita käytetään ainoastaan viranomaisten väliseen viestintään. En pidä oletusta kestäväenä, jos se ulotetaan kaikkiin viranomaisiin. Viranomaisilla on olemassa eri viestintävälineitä nimenomaan sitä varten, että kansalaiset voivat ottaa yhteyttä viranomaiseen. Tällöin viestinnän toisena osapuolena on luonnollinen henkilö, jonka yksityisyyden suoja tulee rajoitetuksi, jos viestintää seurataan. Esityksen mukaan joihinkin tiedustelumenetelmiin sovellettaisiin kevyempää hyväksymis- menettelyä ja kevyempiä oikeussuojakeinoja silloin jos tiedustelun kohteena on valtiollinen toimija. Katson, ettei näin voida toimia, ellei ole varmuutta siitä, ettei viestinnän toiseksi osapuoleksi voi tulla luonnollista henkilöä.

Nähdäkseni valtiollisena toimijana ei voitaisi myöskään pitää esimerkiksi vieraan valtion puolustusvoimien palveluksessa olevaa ammattisotilasta tai asevelvollista hänen käyttäessään omaa viestintälaitettaan yksityiseen viestintään.

Perus- ja ihmisoikeussuojan ala. Kun on kysymys valtion virkamiesten toiminnasta, perus- ja ihmisoikeussuojan kannalta ei ole merkitystä sillä, onko tiedustelutoimen kohde Suomen alueella vai sen ulkopuolella, koska perusoikeudet koskevat jokaista luonnollista henkilöä kansalaisuudesta riippumatta (HE 309/1993 vp, s. 23/II). Myöskään henkilön kansallisuudella ei ole tässä suhteessa merkitystä, sillä ihmisoikeussopimukset velvoittavat sopimusvaltiota kunnioittamaan ja takaamaan sopimusten sisältämät ihmisoikeudet pääsääntöisesti kaikille valtion oikeuspiiriin kuuluville henkilöille siitä riippumatta, ovatko he kyseisen valtion kansalaisia (HE 309/1993 vp., s. 21/II). Lisäksi perustuslain 22 §:n mukaan julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen.

Tästä näkökulmasta pidän hyvin ongelmallisena ulkomailla tapahtuvan sotilastiedustelun (62 §) suhteen otettua lähtökohtaa, jonka mukaan muun muassa tiedustelukieltoja ja jäljentämiskieltoja ei olisi velvollisuutta noudattaa ulkomailla tapahtuvaan sotilastiedusteluun vaan niitä ainoastaan "voidaan soveltaa" eli päätös jäisi viranomaisen omaan harkintaan. Pidän 62 §:n 1 momentin kirjoitusasua myös hyvin vaikeaselkoisena.

Uhan konkreettisuus ja etäisyys. Esityksen mukaan tiedusteltavan toiminnan ei tarvitsisi olla luonteeltaan konkreettista uhkaa aiheuttavaa eikä tiedustelua olisi rajattu Suomeen tai suomalaisiin joukkoihin kohdistuvaan toimintaan tai lähialueille. Ehdotettujen perusoikeusrajoitusten oikeasuhtaisuuden kannalta on olennainen ero sillä, kohdistuuko tiedustelu toimintaan, jonka suhteen Suomeen kohdistuvaa uhkaa voidaan pitää todennäköisenä vai onko tarkoituksena kerätä tietoa etäisemmästä kohteesta, jotta tietoja voidaan käyttää vaihdon välineenä kansainvälisessä yhteistyössä (ks. esimerkiksi esityksen s. 187). Yksityiselämän suojan rajoittaminen jälkimmäisellä perusteella ei nähdäkseni täyttäisi suhteellisuusperiaatteeseen sisältyvää rajoituksen välttämättömyyden vaatimusta. Ehdotettua lakia on syytä rajata tämän mukaisesti. Samoin tapauskohtaiseen oikeasuhtaisuusharkintaan vaikuttaa, onko kyseessä Suomeen kohdistuva uhka, muu uhka lähialueella vai hankitaanko tietoa etäisemmästä konfliktista (esim. s. 184).

Yleislauseke. 4 §:n 2 momenttia pidän muotoilultaan ongelmallisen väljänä. Säännöksen sanamuodon perusteella jää epäselväksi, koskisiko säännöksen loppuosan vaarantamisedellytys pelkästään "muuta sellaista toimintaa" vai myös "vieraan valtion toimintaa". Ilmausta "muu

sellainen toiminta" ei voi pitää täsmällisenä ja tarkkarajaisena. Kriteeriä "voi vaarantaa" pidän väljänä, koska siinä pelkkä vaarantumisen mahdollisuus riittäisi, eikä säännöksessä ole otettu kantaa siihen, kuinka vakavasta vaarasta olisi kyse. Käsite "yhteiskunnan elintärkeät toiminnot" on merkitykseltään lavea.

3 Yleiset periaatteet (5–8 §)

Sotilastiedustelulakiehdotukseen sisältyy pakkokeinolain (806/2011) ja poliisilain (872/2011) mallia seuraten säännökset suhteellisuusperiaatteesta (5 §), vähimmän haitan periaatteesta (6 §) ja tarkoitussidonnaisuuden periaatteesta (7 §). Lisäksi lakiin sisältyisi säännös syrjinnän kiellosta (8 §). Näiden periaatteiden merkitys on tärkeä sen varmistamisessa, että tiedustelutoiminnassa puuttuminen perusoikeuksiin rajoitetaan siihen mikä on välttämätöntä. Esityksen perusteluissa (s. 193) viitataan tiedustelulainsäädännön perus- ja ihmisoikeusmyönteiseen tulkintaan (vrt. PeVM 25/1994 vp, s. 4/I). Esikuvistaan huolimatta suhteellisuusperiaatetta koskevan säännöksen sanamuotoa kannattanee nykyaikaistaa siten, että "on oltava puolustettavia"-rakenteen sijasta käytettäisiin ilmaisua "on välttämätöntä" ja "oikeuksien loukkaamisen" sijasta puhuttaisiin oikeuksiin puuttumisesta.

Vakavampi puute on ehdotetussa 8 §:ssä, joka rajoittaisi niitä perusteita, joilla tiedustelutoimenpiteitä kohdennettaisiin. Esityksen perusteluissa (s. 195) syrjinnän kiello yhdistetään vähemmistöjen syrjinnän ehkäisemiseen. Siten syrjinnän kiello toteuttaa perustuslain 6 §:ssä suojattua oikeutta yhdenvertaisuuteen.

Kuitenkin vaikka kiellettyjen syrjintäperusteiden luettelo muistuttaa perustuslain 6 §:n 2 momentin luetteloa, pidän erikoisena, että kiellettyjen perusteiden luettelosta puuttuu perustuslakiin verrattuna henkilön sukupuoli ja yleisperuste "muu henkilöön liittyvä syy". Tältä osin luettelo on tarpeen korjata perustuslakia vastaavaksi. Vielä suurempana ongelmana pidän kiellon ehdotettua muotoilua, jonka mukaan kohdentaminen ei saa perustua *ainoastaan* lueteltuihin perusteisiin. Ainoastaan-kriteeri tekisi mahdolliseksi sellaisen kohdentamisen, jossa kielletyn perusteen rinnalle otettaisiin jokin keinotekoinen kriteeri tai toinen kielletty kriteeri niin, että tosiasiassa kohdentaminen olisi syrjivää. Tällöin säännös jäisi käytännössä merkityksettömäksi.

Tiedustelu, joka perustuu yksinomaan henkilön ominaisuuksiin kuten uskontoon tai alkuperään on ongelmallinen perustuslain 6 §:n 2 momentin kannalta. Voinee kysyä, onko ylipäänsä koskaan tarpeellista tai perusteltua kohdentaa tiedustelua edellä mainitun kaltaisten ominaisuuksien perusteella. Sen sijaan tiedustelun kohdentamisen tulee perustua henkilön käyttäytymiseen, esimerkiksi siihen millaisissa paikoissa ja missä seurassa hän liikkuu tai onko hän aktiivinen sotilaallisessa toiminnassa. Tästä syystä oikea ratkaisu on poistaa säännöksestä sana 'ainoastaan', jolloin kiellettyjen syrjintäperusteiden luettelo on ehdoton.

4 Yleiset edellytykset

5–8 §:ien yleisten periaatteiden lisäksi tiedustelumenetelmien käyttöä rajattaisiin 11 §:n yleisillä edellytyksillä. 11 §:n 1 momentin mukaan tiedustelumenetelmän käytön yleisenä edellytyksenä olisi, että sillä voidaan perustellusti olettaa saatavan tietoa tiedustelutehtävän kannalta. Säännöksen

loppuosa ("tiedustelutehtävän kannalta") on kielellisesti puutteellinen. Ehdotettu säännös olisi samankaltainen kuin poliisilain 5 luvun 2 §:n 1 momentti ja pakkokeinolain 10 luvun 2 §:n 1 momentti.

Arvioinnissa on otettava huomioon, että poliisi- ja pakkokeinolaeissa yksityisyyden suojaan puuttumisen taustalla on tarkkarajaisesti määritelty rikos tai (poliisilaissa) konkreettisen vaaran torjuminen (vrt. PeVL 11/2005 vp). Ehdotetut tiedustelutoimivaltuudet perustuvat laveasti määriteltyihin tiedustelun kohteisiin. Ehdotuksessa tietojen saamista ei ole sidottu siihen, kuinka merkittäviä tai käyttökelpoisia tietoja oletetaan saatavan. Ei kuitenkaan voida pitää suhteellisuusperiaatteen mukaisena sitä, että viranomaisen puuttuu kohdehenkilön yksityiselämän suojaan vain saadakseen tietoa, jolla on vähäinen merkitys.

Näitä puutteita on mahdollista korjata muuttamalla säännöksen loppuosa muotoon "saatavan tiedustelutehtävän kannalta tärkeää tietoa", jolloin tiedustelukeinon käyttöedellytyksen kynnyksenousee korkeammalle.

5 Ehdotetut tiedustelumenetelmät

5.1 Valtuuksien laajuudesta

Lakiehdotuksessa on otettu lähtökohdaksi, että tiedusteluviranomainen saisi tiedonhankinta-toimivaltuudet, jotka olisivat samantyyppisiä kuin jo poliisilla ja Puolustusvoimilla voimassa olevat rikoksen ennalta estämisen tiedonhankintatoimivaltuudet (esityksen s. 218). Lisäksi ehdotukseen sisältyy uusina toimivaltuuksina muun muassa radiosignaalitiedustelu, ulkomaan tietojärjestelmä-tiedustelu ja tietoliikennetiedustelu.

Esityksen perusteluiden (s. 219) mukaan tiedusteluviranomaisen toimivaltuuksien käyttökynnykset olisivat samat kuin poliisilain 5 luvussa tiedustelutoimintaan sopeutettuna. Arvioinnissa tulee kuitenkin huomata, että ehdotetut tiedustelumenetelmät ovat paikoin laveampia ja niiden edellytykset väljempiä kuin poliisi- tai pakkokeinolaeissa. Tämä on syytä ottaa huomioon menetelmien muissa piirteissä kuten kestoajassa. Toimivaltuuksien käytössä ei olisi kyse rikoksen ennalta estämisestä ja torjunnasta kuten poliisilaissa, vaan paljon abstraktimmasta ja vaikeammin kohdennettavasta tiedustelutiedon hankinnasta.

Perustuslain muutosta koskevassa mietinnössään perustuslakivaliokunta katsoi, että vaara viranomaisten tilapäisestä pääsystä yksittäisten, tiedustelutehtävään liittymättömien henkilöiden viestintää koskeviin tietoihin tulee rajata mahdollisimman vähäiseksi ja muutoinkin valiokunta painotti tarvetta tulkita perustuslain 10 §:n 4 momentin rajoitusperustetta suppeasti (PeVM 4/2018 vp). Tiedusteluviranomaisille annettavia valtuuksia on tarpeen arvioida muun muassa perusoikeuksien rajoitusedellytyksiin kuuluvan välttämättömyysvaatimuksen näkökulmasta. Kunkin esitetyn toimivaltuuden kohdalla on erikseen arvioitava, onko se välttämätön ja onko sen taustalla painava yhteiskunnallinen tarve (vrt. PeVL 6/2018 vp). Esityksen mahdollisen hyväksymisen jälkeen lakien toimeenpanoa on syytä seurata muun muassa sen suhteen, minkä verran eri tiedustelumenetelmiä on käytetty ja mikä niiden tuloksellisuus on ollut.

5.2 Tiedustelumenetelmien käyttöedellytykset

Sotilastiedustelulakiehdotuksen 4 luvussa on kuvattu sotilastiedusteluviranomaisen tiedustelumenetelmät. Osaa menetelmistä voidaan käyttää tiedustelutehtävän suorittamiseksi ilman tarkempia edellytyksiä tai välttämättömyysedellytyksellä. Näissä menetelmissä vaikuttaa yleensä olevan kyse siitä, että menetelmä ei ole sellainen, että se rajoittaisi yksityisyyttä tai se kohdistuu valtiolliseen toimijaan.

Osa tiedustelumenetelmistä rajoittaa kohteen yksityisyyden suojaa ja näiden menetelmien käytön edellytyksenä on, että menetelmällä *voidaan perustellusti olettaa olevan erittäin tärkeä merkitys* tietojen saamiseksi tiedustelutehtävän kannalta. Käsitykseni on, että perustellun olettamuksen edellytyksestä seuraa, että tiedusteluviranomaisen on pystyttävä esittämään tiedusteluluvulle niin hyvät perusteet, että asiaa käsittelevä tuomioistuimien tulee itse vakuuttuneeksi tiedustelumenetelmän tarpeellisuudesta eikä sen tarvitse nojautua pelkkään lupaa pyytävän viranomaisen arvioon.

Pidän ehdotettuja edellytyksiä pääosin perusteltuina rajoituksen oikeasuhtaisuuden kannalta. Jostain syystä kuitenkin televalvontaa, ulkomaan tietojärjestelmätiedustelua ja valtiollisen toimijan tietoliikenteeseen kohdistuvaa tiedustelua koskevissa säännöksissä (35, 60 ja 67 §) edellytys on muodossa "voidaan olettaa" ilman perustellusti-määrettä. Säännökset tulee korjata yhdenmukaisiksi muiden kanssa. Lisäksi tukiasematietojen hankkimista koskeva toimivaltuus (37 ja 38 §) puuttuu jäljempänä kuvatuista syistä siinä määrin yksityiselämän suojaan, että perustellun olettamuksen edellytys tulee liittää siihenkin. Teknisten tietojen käsittelyä koskevaan säännökseen (63 §) tulee mielestäni sisällyttää vähintään "tiedustelutehtävän suorittamiseksi"-tyyppinen edellytys.

5.3 Päätöksenteko tiedustelumenetelmien käytöstä

Esityksen mukaan tiedustelumenetelmien käytöstä päättäisi joko tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies, pääesikunnan tiedustelupäällikkö tai tuomioistuimien. Päätöksenteko on pääosin verrannollista poliisilain vastaaviin säännöksiin.

Ulkomaan tietojärjestelmätiedustelun (60 ja 61 §) suhteen katson kuitenkin, että koska ulkomaan tietojärjestelmätiedustelu – jäljempänä selitetyin tavoin – voisi kohdistua myös yksityisen henkilön omistamaan tietojärjestelmään, tämä tiedustelumenetelmä voi rajoittaa kohteensa yksityiselämän suojaa ja siksi siihen on liitettävä etukäteinen tuomioistuinarviointi.

Poliisilakia koskevassa lausunnossaan (PeVL 67/2010 vp) perustuslakivaliokunta kiinnitti huomiota siihen, että toimivalta peitetoiminnasta ja valeostosta päättämisestä oli osoitettu poliisiyksikön päällikölle ja piti aiheellisena harkita ratkaisutoimivallan osoittamista tuomioistuimelle. Sama huomio voidaan esittää myös sotilastiedustelulaista.

5.4 Sähköiseen viestintään kohdistuvat tiedustelumenetelmät

5.4.1 Yksilöön kohdistuvat tiedonhankintakeinot

Lakiesitys sotilastiedustelusta sisältää useita tiedustelukeinoja, jotka kohdistuvat tietoliikenteeseen tai tietojärjestelmään. Henkilötiedusteluun luettavista keinoista tällaisia ovat tekninen laitetarkkailu (30 §), telekuuntelu (32 §), tietojen hankkiminen telekuuntelun sijasta (33 §), televalvonta (35 §),

tukiasematietojen hankkiminen (37 §) ja teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen (39 §).

Valiokunnan aiempi käytäntö on perustunut tuolloin voimassa olleeseen perustuslain 10 §:n 3 momentin sanamuotoon, jonka mukaan välttämättömistä rajoituksista luottamuksellisen viestin salaisuuteen voidaan säätää lailla muun muassa yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa. Yksilön tai yhteiskunnan turvallisuutta vaarantavien rikosten piiriin kuuluvat perusoikeusuudistuksen esitöiden mukaan esimerkiksi huumausainerikokset, törkeät väkivaltarikokset sekä maan- ja valtiopetosrikokset (HE 309/1993 vp, s. 54/II). Valiokunta on pitänyt lisäksi mahdollisena, että tunnistamistietojen saaminen jätetään sitomatta tiettyihin rikostyyppeihin, jos sääntely muutoin täyttää perusoikeuksien yleiset rajoitusedellytykset (PeVL 26/2001 vp, s. 3/II, PeVL 37/2002 vp, s. 3/I; PeVL 66/2010 vp).

Poliisilaissa (5 luvun 5 §) telekuuntelun käyttö on sidottu laissa lueteltuihin törkeisiin ja ylitörkeisiin rikoksiin. Ehdotetussa sotilastiedustelulaissa ei-valtiolliseen toimijaan kohdistuvaan telekuunteluun voitaisiin antaa lupa, jos sillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Telekuuntelun lupaperusteita ei ole siten rajattu samalla tavoin yksiselitteisesti kuin poliisilaissa, vaan käytännössä 32 §:n 3 momentissa vain toistetaan 11 §:n 1 momentin yleinen tuloksellisyysedellytys. Telekuuntelun edellytyksenä on kyllä tiedonhankinnan liittyminen tiedustelutehtävään, mutta nekin on laissa määritelty hyvin laveasti. Tiedustelukeinon käyttöala jäisi siten pelkästään yleisten periaatteiden varaan, mikä on ongelmallista tarkkarajaisuuskriteerin kannalta.

Erona poliisilakiin tiedusteluperusteilla tehtävän telekuunteluluvan ei tarvitsisi perustua tiettyyn teleosoitteeseen tai telepäätelaitteeseen, vaan se voisi perustua tiettyyn henkilöön. Tämä on olennainen edellytysten lavennus poliisilakiin verrattuna. Kun lupa perustuu teleosoitteeseen tai telepäätelaitteeseen, pakkokeinolla on objektiiviset rajat. Jos lupa perustuu henkilöön, joudutaan paljon helpommin tilanteeseen, jossa mitä tahansa teleosoitetta tai telepäätelaitetta ryhdytään kuuntelemaan pelkällä tiedusteluviranomaisen omalla päätöksellä. Näin lakea toimivaltaisuus on ongelmallinen perusoikeusrajoituksen ennakoitavuuskriteerin kannalta.

Poliisilaissa telekuuntelua koskeva lupa voidaan antaa enintään kuukaudeksi. Sotilastiedustelulaissa telekuuntelua koskeva lupa voitaisiin antaa enintään 3–6 kuukauden kerrallaan. Lupaedellytysten väljyys ja siten perusoikeusrajoitusten potentiaalisesti laajempi henkilöllinen ala puoltavat pikemminkin lyhyttä enimmäisaikaa.

Vastaavat huomiot voidaan esittää televalvonnasta (35 §).

Ehdotuksen 100 §:n mukaan sähköisen viestinnän palveluista annetun lain 157 §:n 1 momentin mukaisesti säilytettyjä tietoja voitaisiin käyttää myös tiedustelutarkoituksessa. Huomautan, että jäljempänä kuvattavan Euroopan unionin *Tele2/Watson*-tuomion jälkeen voidaan perustellusti kysyä, onko 157 §:n tarkoittama säilytysvelvollisuus ylipäänsä Euroopan unionin oikeuden mukainen.

5.4.2 Yleisluontoista valvontaa koskevasta tulkintakäytännöstä

Osa ehdotetuista tiedonhankintakeinoista ei kohdistu tiettyyn henkilöön, vaan niillä seurataan tietoliikennettä laajemmin. Tällaisia keinoja ovat tukiasematietojen hankkiminen (37 §), radiosignaalitiedustelu (58 §), teknisten tietojen käsittely (63 §), valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu (65 §) ja muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu (67 §).

Erona yksilöön kohdistuviin tiedonhankintakeinoihin, tietoliikenteeseen yleisesti kohdistuvat tiedonhankintakeinot ovat luonteeltaan spekulatiivisempia ja ne eivät perustu tietyn henkilön seuraamiseen vaan yleisempään tiedonhankintaan. Saatujen tietojen perusteella voidaan myös suunnata yksilöön kohdistuvia muita tiedonhankintakeinoja. Tietoja voidaan yhdistellä muista lähteistä saatuihin tietoihin ja niistä voidaan tilastollisilla menetelmillä luoda henkilöprofiileja.

Perustuslakivaliokunta on teletunnistetietoja koskevassa yhteydessä katsonut, että kun lainsäädäntö antaa mahdollisuuden tietojen kokoamiseen ja yhdistämiseen, huomiota on kiinnitettävä rajoitusten merkittävyyteen (PeVL 18/2014 vp). Oikeasuhtaisuusvaatimuksen vastaisena voidaan pitää ainakin sellaista sääntelyä, joka merkitsee laajamittaista, erittelemätöntä, pitkäaikaista ja rajoittamatonta tietojen säilyttämistä yhdistettynä viranomaisten erittelemättömään ja rajoittamattomaan pääsyyn näihin tietoihin (PeVL 18/2014 vp; PeVL 20/2016 vp; PeVL 26/2016 vp). Valiokunta on kiinnittänyt huomiota EU-tuomioistuimen oikeuskäytännön merkitykseen (erityisesti asioissa *Digital Rights Ireland*, *Schrems* ja *Tele2/Watson*; PeVL 9/2017 vp).

Mietinnössään PeVM 4/2018 vp perustuslakivaliokunta painotti, että perustuslain 10 §:n 4 momentin rajoissa säädettävien valtuuksien, esimerkiksi siviili- ja sotilastiedustelua koskevissa hallituksen esityksissä tiedusteluviranomaisille ehdotettavien toimivaltuuksien, on oltava sopusoinnussa myös Suomen kansainvälisten ihmisoikeusvelvoitteiden, erityisesti Euroopan ihmisoikeussopimuksen, ja EU-oikeuden kanssa. Valiokunta on korostanut myös, että perustuslaissa turvattu perusoikeussuojan taso voi olla korkeampi kuin suojan vähimmäistason asettavista ihmisoikeusvelvoitteista johtuu (PeVL 59/2017 vp, PeVL 43/2016 vp, PeVL 24/2016 vp, PeVL 59/2014 vp).

Euroopan unionin perusoikeuskirjan 7 artiklassa turvataan yksityiselämän suoja, mukaan lukien luottamuksellisen viestinnän suoja. Perusoikeuskirjan 8 artiklassa turvataan henkilötietojen suoja. 51 artiklan mukaan perusoikeuskirjan määräykset koskevat jäsenvaltioita ainoastaan silloin, kun ne soveltavat unionin oikeutta. Euroopan unionista tehdyn sopimuksen toimivallanjakoa koskevan 4 artiklan 2 kohdan mukaan kansallinen turvallisuus säilyy yksinomaan kunkin jäsenvaltion vastuulla, joten perusoikeuskirjan soveltuvuus riippuu siitä, pidetäänkö muun muassa ehdotettuja sähköiseen viestintään puuttuvia toimia Euroopan unionin lainsäädännön alaan kuuluvina. Euroopan unionin tuomioistuimessa on käsiteltävänä ennakkoratkaisupyyntö asiassa C-623/17, jossa on kysymys nimenomaan Euroopan unionin lainsäädännön soveltumisesta tiedustelutoiminnassa.

Euroopan unionin tuomioistuimen mukaan jos henkilön viestinnästä tai paikkatiedoista kerätään tietoja pitkäkestoisesti, syntyy tietojen kokonaisuus, joka "voi mahdollistaa hyvin tarkkojen päätelmien tekemisen niiden henkilöiden, joiden tietoja on säilytetty, yksityiselämästä, kuten elämäntavoista, vakituista tai tilapäisistä oleskelupaikoista, päivittäisestä tai muusta liikkumisesta,

tekemisestä sekä näiden henkilöiden sosiaalisista suhteista ja heidän sosiaalisesta ympäristöstään" (*Digital Rights Ireland*, kohta 27). Näiden tietojen perusteella voidaan laatia asianomaisten henkilöiden profiili, joka on yksityiselämän kunnioittamista koskevan oikeuden kannalta aivan yhtä arkaluonteista tietoa kuin itse viestinnän sisältö (*Tele2/Watson*, kohta 99). Tietojen säilyttäminen ja niiden myöhempi käyttö ilman, että sähköisten viestintäpalvelujen käyttäjille ilmoitetaan siitä, voi aiheuttaa kyseisille ihmisille tunteen siitä, että heidän yksityiselämänsä on jatkuvan tarkkailun kohteena (*Digital Rights Ireland*, kohta 27; *Tele2/Watson*, kohta 100). Tällä voi olla vaikutusta myös Euroopan unionin perusoikeuskirjan 11 artiklassa turvatun sananvapauden käyttämiselle (*Digital Rights Ireland*, kohta 25). Tuomioistuin on pitänyt viestinnän liikenne- ja paikkatietojen säilyttämistä vakavana puuttumisena perusoikeuksiin ja siten vain vakavan rikollisuuden torjuminen voi olla tällaisen toimenpiteen perusteena. Tuomioistuin katsoi, että välttämättömän puuttumisen rajat ylitti kansallinen lainsäädäntö, jonka mukaisesti kaikkien käyttäjien ja kaikkien sähköisten viestintävälineiden kaikki liikennetiedot tuli säilyttää ilman mitään erottelua tai rajoituksia taikka poikkeuksia asetetun tavoitteen perusteella. Lainsäädäntö ei myöskään edellyttänyt, että henkilöt, joiden tietoja säilytetään, olisivat edes epäsuorasti sellaisessa tilanteessa, joka voisi johtaa rikosoikeudellisiin toimiin. Lainsäädäntöä sovellettiin siis myös henkilöihin, joiden osalta ei ole mitään seikkaa, jonka perusteella voitaisiin olettaa, että heidän toimintansa voisi olla edes epäsuorasti tai kaukaisesti yhteydessä vakavaan rikollisuuteen. Laissa ei myöskään säädetty minkäänlaisesta poikkeuksesta, joten sitä sovelletaan jopa henkilöihin, joiden viestintään sovelletaan kansallisen lainsäädännön mukaan salassapitovelvollisuutta. Tällaisessa säännöstössä ei vaadittu minkäänlaista yhteyttä säilytettäväksi säädettyjen tietojen ja yleistä turvallisuutta koskevan uhan välillä eikä säilyttämistä ollut rajoitettu joko tiettyyn ajanjaksoon ja/tai maantieteellisesti määritellyn alueeseen ja/tai sellaisten tiettyjen henkilöiden piiriin, joilla on yhteys vakavaan rikollisuuteen tai rikollisuuden torjumiseen (*Tele2/Watson*, kohdat 102–107). Euroopan unionin oikeus on myös esteenä sellaiselle lainsäädännölle, jossa viranomaisille säädetään oikeus saada säilytettäviä tietoja, jos samalla ei rikollisuuden torjumisen puitteissa rajoiteta tätä tietojen saantia vain vakavan rikollisuuden torjumisen tarkoitukseen, eikä tietojen saannin edellytykseksi aseteta tuomioistuimen tai riippumattoman hallintoviranomaisten suorittamaa ennakkovalvontaa eikä vaadita, että kyseessä olevat tiedot säilytetään unionin alueella (*Tele2/Watson*, kohta 125).

Tuomioistuin toteaa kuitenkin, että tietojen säilyttäminen on mahdollista, jos se on kohdennettua ja sillä edellytyksellä, että näiden tietojen säilyttäminen on, siltä osin kuin kyse on säilytettävistä tietoluokista, tarkoitetuista viestintävälineistä, asianomaisista henkilöistä ja aiotun säilytyksen kestosta, rajoitettu täysin välttämättömään (*Tele2/Watson*, kohta 108).

Euroopan ihmisoikeussopimuksen 8 artikla edellyttää, että yksityiselämän suojaan kohdistuvien rajoitusten on perustuttava lakiin, niillä on oltava hyväksyttävä tavoite ja niiden on oltava välttämättömiä demokraattisessa yhteiskunnassa. Euroopan ihmisoikeustuomioistuin on salaisia tiedustelumenetelmiä koskevassa oikeuskäytännössään kiinnittänyt huomiota erityisesti menetelmiä koskevan lainsäädännön ennakoitavuuteen. Tuomioistuimen mukaan salaiseen valvontaan liittyvä ilmeinen väärinkäytösten riski, joten siihen on liitettävä selkeät ja yksityiskohtaiset säännöt. Laista tulee riittävällä selkeydellä ilmetä, millaisissa olosuhteissa ja millä edellytyksillä viranomaiset voivat käyttää salaisia tiedustelukeinoja. Mielivaltaisen oikeuksiin puuttumisen estämiseksi laista

tulee myös ilmetä viranomaisilla olevan harkintavallan ala ja miten sitä käytetään (*Big Brother Watch* ym. v. *Yhdistynyt kuningaskunta*, kohdat 305–306 ja viitattu oikeuskäytäntö).

Ihmisoikeustuomioistuin on luetellut oikeuskäytännössään kuusi vähimmäisvaatimusta, jotka viestintäsalaisuutta rajoittavasta lainsäädännöstä on ilmentävä: 1) millaisten tekojen perusteella viranomaiselle voidaan antaa oikeus puuttua viestintäsalaisuuteen, 2) ne henkilöryhmät, joihin kuulumisen altistaa viestinnän valvonnalle, 3) valvonnan kestolle asetetut rajat, 4) toimenpiteet, joiden mukaisesti hankittuja tietoja tutkitaan, käytetään ja tallennetaan, 5) turvatoimet, joita noudatetaan luovutettaessa tietoja muille osapuolille ja 6) olosuhteet, joissa saadut tiedot voidaan tai on velvollisuus poistaa tai tuhota. Tapauksissa, joissa viestintäsalaisuutta on rajoitettu kansallisen turvallisuuden nimissä, tuomioistuin on kiinnittänyt huomiota myös seuraaviin tekijöihin: 7) salaisen valvonnan valvonnan järjestäminen, 8) ilmoitusmenettelyt ja 9) kansalliseen lakiin sisältyvät oikeussuojakeinot (*Big Brother Watch* ym. v. *Yhdistynyt kuningaskunta*, kohta 307).

Euroopan ihmisoikeustuomioistuin on äskettäin arvioinut Ruotsin tietoliikennetiedustelua koskevaa lainsäädäntöä ja katsonut sen olevan ihmisoikeussopimuksen mukainen. Ruotsin järjestelmä on monin paikoin vastaava kuin sotilastiedustelulaissa nyt esitetty (*Centrum för rättvisa* v. *Ruotsi*).

5.4.3 Tukiasematietojen hankkiminen

Ehdotettuun sotilastiedustelulakiin sisältyy toimivaltuus tukiasematietojen hankkimiseen (37 §). Tällä toimivaltuudella viranomainen saa tiedon tiettyyn tukiasemaan kirjautuneista tai kirjautuvista telepäätelaitteista ja teleosoitteista. Ehdotettu toimivaltuus vastaisi poliisilain 5 luvun 11 §:n vastaavaa säännöstä sillä erotuksella, että poliisilaki edellyttää tietojen olevan "rikoksen estämiseksi merkityksellisiä", kun taas sotilastiedustelulain mukaan riittäisi, että tiedot ovat "tiedustelutehtävän kannalta tarpeellisia".

Toimivaltuus kohdistuu potentiaalisesti laajaan henkilöjoukkoon. Tukiasemia on erityisesti kaupungeissa varsin tiheässä, ja yhden tukiaseman piirissä voi olla kymmeniä tai satoja päätelaitteita. Toimivaltuuden perusteella viranomainen saa siis luettelon kaikista tukiaseman lähistöllä olevista päätelaitteista (esimerkiksi matkapuhelimista) ja käytännössä siis myös tiedon niiden omistajien summittaisista sijainneista. Jos viranomainen saa luvan useampaan tukiasemaan, se voi seurata tiettyjen henkilöiden liikkumista eri tukiasemien alueilla ja jos seuranta tehdään pitkällä aikavälillä, viranomaiselle muodostuu tietokanta niistä henkilöistä, jotka liikkuvat tietyllä alueella toistuvasti. Ehdotettu säännös ei aseta rajoituksia pitkäkestoiselle ja alueellisesti laajalle tukiasematietojen seurannalle.

Rikostutkinnassa tukiasematietojen hankkimisen hyöty perustuu siihen, että sen perusteella voidaan saada selville rikoksen tapahtumapaikalla oleskelleita henkilöitä. Sotilastiedustelulakia koskevan esityksen mukaan (s. 250) tiedustelukontekstissa tällä toimivaltuudella saataisiin tietoja siitä, keitä tietyllä alueella tai tilassa liikkuu. Viranomainen saisi siis haltuunsa luettelon kymmenistä tai sadoista alueella oleskelevista henkilöistä, joiden yhteydestä tiedustelun kohteeseen ei olisi tuossa vaiheessa tietoa.

Tukiasematietojen hankkiminen otettiin uutena toimivaltuutena pakkokeinolakiin lailla 646/2003 (HE 52/2002 vp). Perustuslakivaliokunta arvioi tuolloin ehdotusta perustuslain 10 §:n turvaaman

yksityiselämän suojan ja 9 §:ssä turvatun liikkumisvapauden kannalta. Valiokunta totesi, että ehdotettu sijaintitiedon hankkiminen eroaa rikoksesta epäiltyyn kohdistettavista pakkokeinoista siinä, että paikantaminen kohdistuu ennalta määräämättömään joukkoon matkaviestimiä ja koskee siten periaatteessa laajuudeltaan tuntematonta henkilöjoukkoa. Valiokunnan mukaan yksityiselämän suojan lähtökohtana on yksilön oikeus elää omaa elämäänsä ilman viranomaisten ja ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista ja tähän oikeuteen sisältyy muun muassa yksilön oikeus solmia ja ylläpitää suhteita muihin ihmisiin ja ympäristöön (PeVL 36/2002 vp).

Ehdotuksessa tietojen hankkiminen oli sidottu laissa lueteltuihin rikoksiin, joita perustuslakivaliokunta piti "verraten törkeinä". Valiokunta antoi lausuntonsa mukaan suurta painoa sille, että kysymyksessä oleva yksityiselämän suojan rajoitus oli "varsin vähäinen verrattuna rajoituksen perusteena olevan yhteiskunnallisen intressin tärkeyteen". Tästä lähtökohdasta valiokunta arvioi myös uutta pakkokeinolakia (PeVL 66/2010 vp).

Valiokunnan käytännön mukaan paikkatiedot kuuluvat perustuslain 10 §:n 1 momentissa turvatun yksityiselämän suojan piiriin ja niitä koskevia rajoituksia on arvioitava perustuslain yleisten rajoitusedellytysten kannalta (PeVL 24/2001; PeVL 53/2005 vp; PeVL 66/2010 vp). Valiokunnan arvioissa paikkatiedoille on annettu samankaltainen asema kuin viestinnän tunnistamistiedoille (PeVL 9/2004 vp; PeVL 11/2005 vp; PeVL 3/2006 vp). Euroopan unionin yleisen tietosuoja-asetuksen 4 artiklan mukaan sijaintitietoa pidetään henkilötietona (ks. PeVL 1/2018 vp), joten paikkatietojen käsittelyä on tarkasteltava myös henkilötietojen suojaa koskevan perusoikeuden kannalta.

Pakkokeinolain säätämisen jälkeen valiokunta on arvioinut uudelleen linjaansa koskien massaluontoista viestintätietojen keräämistä. Kuten edellä on todettu, valiokunta on katsonut, että kun lainsäädäntö antaa mahdollisuuden tietojen kokoamiseen ja yhdistämiseen, huomiota on kiinnitettävä rajoitusten merkittävyyteen (PeVL 18/2014 vp). Oikeasuhtaisuusvaatimuksen vastaisena voidaan pitää ainakin sellaista sääntelyä, joka merkitsee laajamittaista, erittelemätöntä, pitkäaikaista ja rajoittamatonta tietojen säilyttämistä yhdistettynä viranomaisten erittelemättömään ja rajoittamattomaan pääsyyn näihin tietoihin (PeVL 18/2014 vp; PeVL 20/2016 vp; PeVL 26/2016 vp).

Esitetty 37 § on sanamuotonsa puolesta varsin lavea. Lupa tukiasematietojen hankkimiseen voidaan antaa tarpeellisuusperusteella. Säännös ei rajoittaisi tietojen keruuta esimerkiksi ajallisesti, henkilömäärän suhteen tai maantieteellisen alueen suhteen. 38 §:ssä ei tietojen keruulle ei olisi – muista tiedustelumenetelmistä poiketen – säädetty lainkaan enimmäiskesto. Mielestäni tällä tavoin säänneltynä ehdotus ei täytä edellä viitattuja perustuslakivaliokunnan periaatteita eikä Euroopan unionin *Tele2*-tuomiossa todettuja linjauksia ja sitä tulee rajata ja täsmentää.

5.4.4 Radiosignaalitiedustelu

Radiosignaalitiedustelu koskee sähkömagneettisiin aaltoihin kohdistuvaa tiedonhankintaa. Radiosignaalitiedustelulla ei saisi hankkia tietoa muun kuin valtiollisen toimijan viestin sisällöstä. Tiedustelu voisi kohdistua ihmisten väliseen (COMINT) tai laitteiden väliseen viestintään (ELINT, FISINT).

Esityksen perusteluiden mukaan valtioiden hallitsemista radiotaajuuksalueista on usein varattu tietyt taajuudet pelkästään asevoimien käyttöön, eikä näillä taajuuksalueilla tapahtuvan viestinnän voitaisi perusteluissa esitetyn näkemyksen mukaan katsoa nauttivan yksityisen viestin suojasta. Nähdäkseni näin suoraviivaista tulkintaa ei voida tehdä. Perusoikeus luottamuksellisen viestin salaisuuteen ei väisty pelkästään sillä perusteella, että viestintä tapahtuu taajuuksalueella, joka tiedusteluviranomaisen käsityksen mukaan on varattu pelkästään asevoimien käyttöön. Kuitenkin jos tiedusteluviranomaisella on hyvin perusteltu käsitys siitä, että taajuuksalueella liikkuu vain valtiollisen toimijan viestintää, nähdäkseni perusoikeussuoja ei ole tiedustelun esteenä edellyttäen että tiedustelu keskeytetään välittömästi 82 §:n mukaisesti, jos ilmenee, ettei kyse ole valtiollisesta toimijasta.

5.4.5 Ulkomaan tietojärjestelmätiedustelu (60 §)

Esitetty tiedustelukeino antaisi viranomaiselle oikeuden hankkia tietoja tietoteknisin menetelmin Suomen ulkopuolella olevasta tietojärjestelmästä. Esityksen perustelujen (s. 270) mukaan tiedustelu voisi kohdistua tietokoneen lisäksi myös muuhun vastaavaan tekniseen laitteeseen. Perustelujen mukaan tiedustelun kohteena voisi olla laitteen ohjelmiston toiminnan, sen sisältämien tietojen ja yksilöintitietojen hankkiminen sekä sellaisen viestin kuuntelu, tallentaminen ja muu käsittely, joka ei ole tarkoitettu ulkopuolisten tietoon.

Tiedustelumenetelmää voitaisiin esityksen mukaan käyttää, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Säännöksessä ei tehdä erottelua valtiollisen toimijan ja ei-valtiollisen toimijan tietojärjestelmien välillä, joten toimivaltuus sallisi tunkeutumisen myös yksityisen henkilön tietokoneeseen tai muuhun laitteeseen. Ehdotetulla toimivaltuudella on siten merkitystä yksityiselämän suojaa, henkilötietojen suojaa ja luottamuksellisen viestin salaisuutta koskevien perusoikeuksien kannalta. (Esityksen mukaan (s. 271) muun kuin valtiollisen toimijan osalta lisäedellytyksenä olisi se, että kohteena oleva toiminta aiheuttaisi vakavaa vaaraa kansalliselle turvallisuudelle, mutta tällaista edellytystä ei ole säädöstekstissä.)

Yksityisen henkilön tietokoneeseen kohdistuessaan tietojärjestelmätiedustelu voisi tarkoittaa esimerkiksi puuttumista luottamuksellisen viestin salaisuuteen. Tiedustelumenetelmän käytöstä päättäisi esityksen mukaan pääesikunnan tiedustelupäällikkö, eikä siihen liittyisi etukäteistä tai jälkikäteistä tuomioistuinkontrollia tai velvollisuutta ilmoittaa kohteelle 86 §:n mukaisesti. Perustuslakivaliokunta piti poliisilakia ja pakkokeinolakia käsitellessään tavallisen lain säätämisyjärjestyksen käyttämisen edellytyksenä, että telekuuntelun tulee aina olla sidottu tuomioistuimen lupaan eikä tästä periaatteesta voida poiketa kiireellisessä tilanteessa (PeVL 67/2010 vp, PeVL 66/2010 vp). Ottaen huomioon tiedustelumenetelmän merkityksen yksityiselämän suojalle, katson että päätöksenteon tulee olla tuomioistuimella.

Tiedustelumenetelmää voi verrata rikoslaissa kriminalisoituun tietomurtoon (RL 38 luvun 8 §). Perustuslakivaliokunta on todennut, että tietojärjestelmään kohdistuvilla tietomurroilla voi olla yksilöiden yksityiselämän suojaan ja luottamuksellisen viestin salaisuuden suojaan ulottuvia haitallisia vaikutuksia (PeVL 33/2013 vp, PeVL 32/2013 vp).

Yksityiseen tietojärjestelmään tunkeutumisen merkitys yksityiselämän suojan kannalta riippuu tietojärjestelmän käyttötarkoituksesta. Yksityinen matkapuhelin tai henkilökohtainen tietokone voi sisältää omistajansa yksityiselämän kannalta hyvin merkityksellisiä tai arkaluonteisia tietoja. Viranomaisen tunkeutumisella tällaisen laitteen tietoihin voi yksityisen henkilön kokeman yksityisyyden kannalta olla sama merkitys kuin puuttumisella kotirauhan suojaan. Tietojärjestelmä ei kuulu kotirauhan piiriin, mutta perusoikeussuojan kohteesta voitaisiin tässä yhteydessä käyttää nimitystä *tietojenkäsittelyrauha* tai *tietojenkäsittelyn luottamuksellisuuden suoja*.

Perusteluiden mukaan toimivaltuuden käytön kannalta tarkoituksenmukaista ei olisi tietyn tietojärjestelmän kaiken tiedon hankkiminen tai tietojärjestelmään satunnaisen käyttäjän tallentamien tietojen hankkiminen. Perusteluissa myös todetaan, että tiedustelumenetelmän kohteena olevaa tietojärjestelmää ei välttämättä voida määritellä etukäteen kovinkaan tarkkaan. Tästä johtuen suunnitelmassa voitaisiin määritellä tiedustelumenetelmän kohde väljemmin kuin esimerkiksi teknisen laitetarkkailun kohdalla on asian laita. Hankittujen tietojen pohjalta suunnitelmaa voitaisiin tarkentaa ja tiedustelumenetelmää kohdistaa tarkemmin. Toisaalta voi olettaa, että useissa tapauksissa tiedusteluviranomaisella on pyrkimys saada kohteestaan mahdollisimman paljon tietoa, koska tarvittavaa tietoa ei voida etukäteen täsmällisesti rajata. Tämä tarve ohjaa helposti viranomaisen harkintaa erityisesti kiiretilanteessa siihen suuntaan, että tietoa kerätään paljon. Tiedustelun oikeasuhtaisuuden vuoksi on tärkeää, että sekä tiedusteluviranomainen että tuomioistuin kiinnittää erityistä huomiota tiedustelun rajaamiseen tiedusteluluvasta päätettäessä.

5.4.6 Teknisten tietojen käsittely

Sotilastiedustelulakiehdotuksen 63 §:n 1 momentin mukaan tiedusteluviranomainen voisi viestintäverkon tietoliikenteestä hetkellisesti kerätä ja tallentaa tietoliikenteen teknisiä tietoja ja automaattisen tietojenkäsittelyn avulla käsitellä niitä tilastollista analyysiä varten.

Ehdotuksen perusteluiden mukaan tietoliikenteen käsittely ei kohdistuisi viestin sisältöön vaan viestinnän teknisiin tietoihin, joiden avulla tietoliikennetiedustelua voitaisiin kohdistaa paremmin vain niihin viestintäverkon osiin, joissa liikkuisi tiedustelutehtävän kannalta olennaista viestintää. Esityksen arvion mukaan koska tiedonhankinta kohdistuisi vain lyhytaikaisesti viestin tunnistamistietoihin tai muihin tietoliikenteen teknisiin tietoihin eikä sotilastiedusteluviranomaisella olisi pääsyä edes yksittäisten viestien teknisiin tietoihin, sotilastiedusteluviranomainen ei voisi siten selvittää viestinnän osapuolena olevaa luonnollista henkilöä. Teknisten tietojen käsittely ei näin ollen olisi ongelmallista perustuslain luottamuksellisen viestin salaisuuden suojan kannalta (s. 352).

Hallituksen esityksen mukaan viestinnän teknisillä tiedoilla tarkoitettaisiin muun muassa viestien välitystietoja. Ehdotuksen 9 §:n 1 momentin 8 kohdassa tietoliikenteen teknisillä tiedoilla tarkoitetaan "muita kuin viestin sisältöön kuuluvia tietoliikenteen tietoja". Käsittelyn kohteeksi voisivat siten tulla luottamuksellisen viestin tunnistamistiedot. Kuitenkin esityksen mukaan teknisten tietojen kerääminen voitaisiin toteuttaa esimerkiksi ottamalla teknisen analyysin kohteeksi lyhytaikainen näyte tietyssä viestintäverkon osassa liikkuvasta tietoliikenteestä tai ottamalla tietyssä viestintäverkon osassa liikkuvista IP-paketeista esimerkiksi joka kymmenestuhannes paketti (s. 279). Esityksen 2 momentin mukaan tilastollisen analyysin tulokseen ei saisi sisältyä tietoa, josta

voidaan tunnistaa yksittäinen luonnollinen henkilö ja 3 momentin mukaan tiedot olisi hävitettävä välittömästi sen jälkeen, kun tilastollisen analyysin tulos on valmistunut.

Aiemmassa käytännössään perustuslakivaliokunta katsoi tunnistamistietojen jäävän luottamuksellisen viestin salaisuutta suojaavan perusoikeuden ydinalueen ulkopuolelle (ks. esim. PeVL 33/2013 vp, s. 3/I, PeVL 6/2012 vp, s. 3—4, PeVL 29/2008 vp, s. 2/II ja PeVL 3/2008 vp, s. 2/I). Lausunnossaan PeVL 18/2014 vp valiokunta katsoi, että käytännössä sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat kuitenkin olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen. Myös Euroopan ihmisoikeustuomioistuin on todennut, että viestien tunnistamistiedoilla voi olla yhtä suuri merkitys yksityiselämän suojan kannalta kuin viestien sisältöä koskevilla tiedoilla (*Big Brother Watch ym. v. Yhdistynyt kuningaskunta*, kohta 356). Lisäksi on syytä muistaa, että ihmisoikeustuomioistuimen oikeuskäytännön mukaan kaikessa viestintätietojen käsittelyssä on kysymys artiklassa 8 suojattujen oikeuksien rajoituksesta, vaikka käsittely tapahtuisikin koneellisesti.

Yksityisyyden suojaan liittyvää ongelmaa ei nähdäkseni ole, jos tietojen keräämisessä toimitaan ottamalla lyhytaikaisia tai satunnaisia näytteitä kuten hallituksen esityksessä on kuvattu. Tietojen kerääminen alkaa kuitenkin saada massavalvonnan piirteitä, jos tietoja tallennetaan laajasti tai pitkälti ajalta. Tämän estämiseksi 63 §:n 1 momenttia on mielestäni tarpeen täsmentää siten, että keräämisen lyhytaikaisuus tai satunnaisuus tulee ilmi.

5.4.7 Tietoliikennetiedustelu

65 ja 67 §:issä sallittaisiin tietoliikenteeseen kohdistuva tiedustelu. Hallituksen esityksen mukaan viestitietojen kerääminen tapahtuisi hakuehtojen käyttöön perustuvan automaattisen tietojen käsittelyn avulla. Tietojen kerääminen toteutettaisiin tunnistamalla tietty viestintäverkon osa, jossa valtiollisen toimijan tietoliikenne kulkee ja tarvittaessa vertailemalla tietoliikennettä hakuehdoiksi kutsuttaviin ennakkoon asetettuihin kriteereihin. Tietoliikennetiedustelun yhtenä tarkoituksena olisi myös tunnistaa yksittäisiä telepäätelaitteita ja teleosoitteita telekuuntelun tai televalvonnan toteuttamisen mahdollistamiseksi (s. 281). Esityksen mukaan kukaan luonnollinen henkilö ei näkisi tiedustelujärjestelmän läpi kulkenutta tietoliikennettä. Ainoastaan hakuehtoja vastaava liikenne tallentuisi järjestelmään niin, että sotilastiedusteluviranomaisen virkamies voisi sitä käsitellä. Viestintää käsittelevällä virkamiehellä olisi pääsy sekä viestin välitystietoihin että sen sisältöön (s. 282). Esityksen 65 § koskee valtiollisen toimijan tietoliikenteeseen kohdistuvaa tiedustelua ja 67 § muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvaa tiedustelua.

Valtiollinen toimija ei nauti perus- ja ihmisoikeuksien suojaa (HE 309/1993 vp, s. 23/II), joten 65 §:ssä tarkoitettu tiedustelu on ongelmaton perustuslain kannalta. Tämänkin tiedustelumenetelmän perusoikeusriskit liittyvät kuitenkin valtiollisen toimijan käsitteeseen, joten tiedusteluluvan myöntävä tuomioistuin on keskeisessä roolissa tämän henkilöpiirin rajaamisessa.

65 §:n 3 momentissa säädettäisiin nimenomainen kielto käyttää hakuehtona Suomessa oleskelevan henkilön hallussa olevaa tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen

yksilöiviä tietoja. Säännöksessä ei kuitenkaan kiellettäisi käsittelemästä Suomessa oleskelevan henkilön viestintätietoja, jos hän on viestinnän lähettävänä tai vastaanottavana osapuolena. Tulkitseen, että viestinnän molempien osapuolten tulisi olla valtiollisia toimijoita, jotta viestinnän seuranta 65 §:n mukaisesti olisi sallittua. Tämä on kuitenkin syytä täsmentää säännökseen.

Esityksen 67 § koskee muuhun kuin valtiolliseen toimijaan kohdistuvaa tiedustelua. Tiedustelun edellytyksenä olisi, että tiedustelun voidaan olettaa olevan *välttämätöntä* tiedon saamiseksi tiedustelutehtävän kannalta. Jostain syystä säännöksessä ei puhuta perustellusta olettamasta niin kuin useimmissa muissa ehdotetun lain säännöksissä. Edellytystä perustellusta olettamasta tulisi lisätä sanamuotoon. Edellytys tiedustelun välttämättömyydestä on osin tiukempi edellytys kuin muissa säädettäväksi ehdotetuissa luottamuksellisen viestin salaisuuden suojaan puuttuvissa tiedustelumenetelmissä, joissa puhutaan tiedustelun erittäin tärkeästä merkityksestä.

Tietoliikennetiedustelussa on kysymys toimivaltuudesta, joka puuttuu kaikkien välitettävänä olevien viestinnän osapuolten luottamuksellisen viestinnän suojaan ja henkilötietojen suojaan. Ehdotuksen mukaan viranomaisen voisi puuttua myös viestien sisältöön. Tiedustelu voi periaatteessa olla laajamittaistakin ja koskea suurta viesti- tai ihmisjoukkoa. Potentiaalisesti kyseessä on sitten erittäin merkittävä rajoitus, joka sellaisenaan merkitsisi puuttumista perusoikeuden ydinalueeseen.

Euroopan ihmisoikeustuomioistuimen mukaan Euroopan ihmisoikeussopimuksesta ei seuraa periaatteellista estettä massamuotoisen tiedustelujärjestelmän käyttämiselle. Olennaista on, täyttääkö tiedustelua koskeva lainsäädäntö muut ihmisoikeussopimuksesta seuraavat, muun muassa tarkkarajaisuutta ja ennakoitavuutta koskevat vaatimukset (*Big Brother Watch ym. v. Yhdistynyt kuningaskunta*, kohdat 314–315). Lisäksi ehdotettua sääntelyä on tietenkin arvioitava erikseen perustuslain ja mahdollisesti Euroopan unionin oikeuden kannalta.

Ehdotetussa muodossaan tietoliikennetiedustelussa seulottaisiin koneellisesti vain osa viesteistä virkamiehen tutkittavaksi, mikä olennaisesti vähentää puuttumisen intensiteettiä. Toisaalta seulonnan tekninen epäonnistuminen, liian väljät seulontakriteerit tai tahallinen väärinkäytös voivat johtaa hyvinkin merkittävään perusoikeusloukkaukseen. On olennaista arvioida, pystytäänkö tätä riskiä hallitsemaan riittävässä määrin teknisesti, ehdotetuilla säännöksillä ja ehdotetulla valvontajärjestelmällä.

Luvan tietoliikennetiedusteluun myöntäisi tuomioistuin. Tuomioistuimelle tehtävään hakemukseen sisällytettävät tiedot on kuvattu 66 §:n 3 momentissa ja 68 §:n 3 momentissa. Pidän luetteloa varsin kattavana. Tietoliikennetiedustelua koskevissa säännöksissä ei tosin rajata sitä, kuinka suureen viesti- tai ihmisjoukkoon tiedustelu voi kohdistua. Tuomioistuin voi kuitenkin asettaa tällaisia rajoituksia luettelon 6 kohdan perusteella. Tiedustelun oikeasuhtaisuus jää muutenkin merkittävässä määrin tuomioistuimen arvion varaan. Oikeasuhtaisuutta arvioitaessa on syytä kiinnittää huomiota perustuslakivaliokunnan mietinnössään esittämään näkemykseen, jonka mukaan perustuslain 10 §:n uusi 4 momentti ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa. Valiokunta arvioi lisäksi välttämättömyys-kriteeriä siten, että luottamuksellisen viestin salaisuuteen kohdistunut rajoitus on sallittu vain, jos tiedonhankinta ei ole mahdollista vähemmän puuttuvien keinoin, ja että tiedon hankkimisessa puututaan luottamuksellisen viestin salaisuuteen mahdollisimman kohdennetusti ja rajoitetusti (PeVM 4/2018 vp).

Tuomioistuimen tehtävänä on myös arvioida luvan oikeasuhtaista kestoaikaa. Luvan kesto on suhteutettava tiedustelutoimen välttämättömyyteen. Lähtökohtana ei voi olla, että luvat ovat aina maksimikeston mittaisia.

Ehdotus sisältää mahdollisuuden siihen, että kiiretilanteessa päätöksen tietoliikennetiedustelusta tekee pääesikunnan tiedustelupäällikkö. Tällöin asia on kuitenkin vietävä 24 tunnin kuluessa tuomioistuimen päätettäväksi. Vastaava menettely sisältyy poliisi- ja pakkokeinolakeihin, jotka on perustuslakivaliokunnan myötävaikutuksella säädetty (PeVL 66/2010 vp ja 67/2010 vp). Euroopan ihmisoikeustuomioistuin arvioi vastaavaa Ruotsin tiedustelulainsäädäntöön sisältyvää menettelyä ja katsoi sen olevan ihmisoikeussopimuksen mukainen, mutta muistutti että tällaisen menettelyn tulee pysyä poikkeuksellisenä (*Centrum för rättvisa v. Ruotsi*, kohta 140).

6 Lupapäätöskäsittely

Arvioidessaan luottamuksellisen viestinnän suojan rajoituksia poliisi- ja pakkokeinolakien yhteydessä perustuslakivaliokunta on pitänyt oleellisena oikeusturvakysymyksenä, että kuunteluvaltuuden edellytyksenä on aina riippumattoman tuomioistuimen yksittäistapauksessa konkreettisen rikosepäilyn johdosta antama lupa (PeVL 8/1994 vp, s. 2/II; PeVL 36/2002 vp; PeVL 37/2002 vp). Valiokunta on korostanut, että tuomioistuimen on huolellisesti harkittava luvan myöntämisen tarvetta ja laajuutta erityisesti kun hakemuksen perusteena on törkeysasteeltaan suhteellisen vähäinen rikos (PeVL 32/2013 vp, s. 4/II; PeVL 33/2013 vp, s. 4/II). Valiokunta on myös edellyttänyt tuomioistuimen antamaa lupaa edellytyksenä telepakkokeinolla saadun ylimääräisen tiedon käyttämiselle (PeVL 66/2010 vp, s. 10/II; PeVL 67/2010 vp, s. 5/I).

Tuomioistuinkontrollilla on siis ollut keskeinen asema luottamuksellisen viestin suojan rajoitusten oikeutuksena. Kuitenkin voi kysyä, toimiiko tuomioistuinkontrolli sillä tavoin rajoittimena kuin perustuslakivaliokunta sen olettaa toimivan. Oikeuspoliittinen tutkimuslaitos on tutkinut käräjäoikeuksien telepakkokeinopäätöksiä vuonna 2006. Tutkimuksen kohteena olevien lupapäätösten perustelut olivat tavallisesti hyvin kaavamaisia ja ne oli perusteltu suppeasti tai ei lainkaan. Noin kolmanneksessa hakemuksista konkreettinen peruste jäi jossain määrin epäselväksi. Pelkistetyimmillään käräjäoikeuden perusteluissa vain toistettiin pakkokeinolain sanamuodot ja viitattiin hakemuksessa esitettyihin perusteluihin ilman päätökseen kirjattua arviointia siitä, miten hakemus konkreettisesti täyttää pakkokeinoluvan edellytykset.

Eduskunnan oikeusasiamies on toistuvasti ainakin vuodesta 2001 lähtien kiinnittänyt huomiota ongelmiin telepakkokeinohakemuksissa ja niitä koskevien päätösten käsittelyssä ja perusteluissa. Ongelmia on ollut muun muassa pakkokeinohakemusten sekä niitä koskevien päätösten perusteluissa. Hakemusten käsittely vaikuttaa summaariselta, mitä kuvastaa muun muassa hylättyjen vaatimusten hyvin vähäinen osuus. Vaatimuksia hylätään vuosittain kymmenkunta, mikä on 0,2–0,4 % vuosittaisesta hakemusmäärästä (noin 3 000).

Tiedustelutoiminnan lupia ei voida samalla tavoin sitoa perusterikoksiin kuin poliisi- ja pakkokeinolakien tapauksessa. Lisäksi tiedustelu koskee potentiaalisesti suurempaa viesti- ja henkilökuntaa kuin poliisitutkinta. Tiedustelulupien tuomioistuinkäsittely ei ole julkinen etu- eikä

jälkikäteen. Nämä seikat korostavat tuomioistuimen erityisen keskeistä roolia oikeusturvan takaajana luvista päätettäessä.

Jotta tuomioistuinkäsittely ei jää muodollisuudeksi, vaan jotta luvan edellytykset tulevat aidosti tutkituksi, tuomioistuimelle on varmistettava riittävät henkilö- ja aikaresurssit ja koulutus. Lisäksi tuomioistuinprosessia tulee kehittää siten, että tuomioistuin ei ole vain hakijan esittämien arvioiden varassa, vaan prosessissa on mukana myös osapuoli, joka tarkastelee lupahakemusta kriittisesti tiedustelun kohteena olevien henkilöiden perus- ja ihmisoikeuksien näkökulmasta.

Telepakkokeinojen yhteydessä valiokunta on toistuvasti ehdottanut, että telekuuntelussa otettaisiin käyttöön julkinen asiamies, jonka tehtävänä olisi valvoa telekuuntelun kohteena olevan rikoksesta epäillyn ja muiden kuuntelun kohteeksi mahdollisesti joutuvien etuja (PeVL 36/2002 vp, s. 7/II; PeVL 66/2010 vp, s. 10/I). Tehtävä voisi olla kuitenkin tarkoituksenmukaista antaa hallituksen esityksessä HE 199/2017 vp tarkoitetulle tiedusteluvaltuutetulle, jolla olisi oikeus tulla kuulluksi tuomioistuimen käsitellessä tiedustelulupaa. Valtuutetulla tulisi olla myös oikeus kannella käräjäoikeuden päätöksestä hovioikeuteen.

7 Ylimääräinen tieto

Ehdotuksen 76 § ja 77 § sallivat tai velvoittavat tiedusteluviranomaisen ilmoittamaan poliisille tai muulle toimivaltaiselle viranomaiselle tiedustelumenetelmää käytettäessä ilmi tulleesta tehdystä rikoksesta tai tekeillä olevasta rikoksesta, joka on vielä estettävissä. Koska tiedustelumenetelmistä seuraavia perusoikeusrajoituksia perustellaan tarpeella hankkia tietoa sotilaallisesta toiminnasta ja tästä syystä tiedustelumenetelmät ovat vaikutuksiltaan kenties laveampia ja pitkäkestoisempia kuin mikä olisi mahdollista rikoksentutkinta- tai torjuntakontekstissa, on ongelmallista, jos tiedustelumenetelmillä hankittua tietoa käytetään kovin vähäisten rikosten torjumiseen.

77 §:n 2 momentin mukaan tietoa saisi luovuttaa sellaisen rikoksen estämiseksi, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta. Rikoslain noin 450:stä nimikkeestä 58 % tulisi tämän säännöksen piiriin. Pidän näin alhaista rajaa ongelmallisena ehdotuksen oikeasuhtaisuuden kannalta.

8 Tiedustelusta ilmoittaminen

Sotilastiedustelulakiehdotuksen 86 §:ssä säädeltäisiin tiedustelumenetelmän käytöstä ilmoittamisesta. Koska tiedustelu tapahtuu kohteiltaan salassa, jälkikäteisellä ilmoituksella on tärkeä rooli siinä, että kohde voi saattaa tiedustelun laillisuuden valvontaviranomaisen tutkittavaksi.

Säännöksen 2 momentin mukaan muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta tarvitsisi ilmoittaa vain, jos käsittelyssä on manuaalisesti selvitetty tietyn Suomessa olevan henkilön luottamuksellisen viestin sisältö. Velvollisuutta ilmoittaa ei olisi, jos tieto on hävitetty 83 §:n perusteella eli käytännössä jos on käynyt ilmi, että viestinnän molemmat osapuolet olivat Suomessa viestinnän tapahtuessa tai jos kyseessä on viestintä asianajajan, lääkärin, papin tai toimittajan kanssa.

Ottaen huomioon, että perus- ja ihmisoikeudet antavat suojaa henkilölle suomalaista viranomaista vastaan heidän kansalaisuudestaan ja olinpaikastaan riippumatta, pidän yhdenvertaisuuden kannalta ongelmallisena sitä, että vain Suomessa oleva henkilö saisi tietää häneen kohdistuneesta tiedustelusta. Rajausta on syytä poistaa. Toki jos ulkomailla oleskelevan henkilön henkilöyttä tai yhteystietoja ei ole, hänelle ei käytännössä voida toimittaa tietoa tiedustelusta.

Asianajajan, lääkärin, papin ja toimittajan viestinnän nauttima erityinen suoja on tärkeä muiden perus- ja ihmisoikeuksien toteutumisen kannalta. On erityisen tärkeää, että nämä henkilöryhmät saavat tiedon tiedustelun kohteena olemisesta, joten säännöstä on mielestäni muutettava myös tältä osin.

9 Yhteistyö muiden viranomaisten ja yhteisöjen kanssa (17 §) ja kansainvälinen yhteistyö (19 §)

17 §:n mukaan tiedusteluviranomainen voisi luovuttaa muille viranomaisille ja yhteisöille salassapitosäännösten estämättä tietoja, jos tietojen luovuttaminen on välttämätöntä maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi. Ehdotetussa laissa ei ole määritelty, millaisista yhteisöistä on kyse. Esityksen perusteluissa viitataan yhteisöihin, jotka ovat keskeisessä osassa Suomen kokonaismaanpuolustuksessa (s. 139). Yhteisöllä saatettaisiin tarkoittaa myös yritystä (s. 213).

Esityksessä ei ole rajattu tai määritelty luovutettavia tietoja. Perustelujen (s. 213) mukaan kyse olisi muista kuin laissa henkilötietojen käsittelystä Puolustusvoimissa (HE 13/2018 vp) tarkoitetuista tiedoista. Ottaen huomioon ehdotetun sotilastiedustelulain tarkoituksena (3 §) ja mainitun Puolustusvoimien henkilötietolain soveltamisalan (1 §), kaikki sotilastiedustelussa kerättävät henkilötiedot näyttäisivät kuuluvan kyseisen henkilötietolain soveltamisalaan, jolloin herää kysymys, onko 17 §:n 2 momentissa tarkoitettu tiedoilla sellaisia tietoja, jotka eivät täytä henkilötiedon määritelmää, esimerkiksi teknisiä tai valtiollisiin toimijoihin liittyviä tietoja. Henkilötietojen suojan varmistamiseksi säännöstä on rajattava ja täsmennettävä tämän mukaisesti.

19 §:n 1 momentin mukaan kansainvälinen yhteistyö käsittäisi muun muassa tiedustelutietojen vaihtamista. Esityksen perusteluiden (s. 215) mukaan tiedonvaihto voisi koskea esimerkiksi vieraan valtion aseteollisuutta. Tietoihin voisi kuulua kuitenkin myös henkilötietoja ja tähän liittyen säännöksen 5 momentissa viitataan ehdotettuun lakiin henkilötietojen käsittelystä Puolustusvoimissa.

Kansainväliseen tietojenvaihtoon liittyen perustuslain näkökulmasta ongelmallista on, jos viranomainen voi tietojenvaihdon kautta kiertää sille kansallisessa lainsäädännössä asetettuja rajoituksia. Tällainen tilanne voisi tulla kyseeseen esimerkiksi silloin, jos viranomainen vaihtaa tietoja sellaisen valtion kanssa, jossa tiedustelumenetelmiä koskeva perus- ja ihmisoikeussuoja on heikompi kuin Suomessa (vrt. *Centrum för rättvisa v. Ruotsi*, kohta 150).

Puolustusvoimien henkilötietolakia koskevan esityksen 32 §:n mukaan Puolustusvoimat saisi luovuttaa henkilötietoja muun muassa sotilastiedustelutehtävässä, jos se on välttämätöntä kansallisen turvallisuuden varmistamiseksi. Säännöksen mukaan päätettäessä tietojen luovuttamisesta on lisäksi otettava huomioon henkilötietoja vastaanottavan valtion

ihmisoikeustilanne, luovutuksen merkitys Suomen kansainvälisille suhteille sekä Suomea sitovat kansainväliset sopimukset ja muut velvoitteet. Lisäksi on otettava huomioon henkilötietoja vastaanottavan valtion tietosuojan taso ja luovutuksen merkitys rekisteröidyn oikeuksille.

Ehdotukseen ei siten sisälly vaatimusta esimerkiksi siitä, että vastaanottavan valtion ihmisoikeussuojan taso olisi Suomea vastaava. Toisaalta ehdotettujen lakien puitteissa olisi mahdollista myös se, että Suomi vastaanottaa ja käyttää hyväkseen tietoa, joka on hankittu ihmisoikeuksia loukkaamalla, esimerkiksi kidutuksella. Mielestäni 19 §:n sääntelyä tulee tiukentaa tästä näkökulmasta.

19 §:n 3 momentin mukaan vieraan valtion toimivaltainen virkamies voisi sotilastiedusteluviranomaisen virkamiehen kanssa ja tämän ohjauksessa ja valvonnassa käyttää säännöksessä lueteltuja tiedustelumenetelmiä eli tarkkailua ja suunnitelmallista tarkkailua (20 §), peiteltyä tiedonhankintaa (22 §), peitetoimintaa (41 §), valeostoa (45 §), tietolähdetoimintaa (49 §) ja tietoliikenteen teknisten tietojen käsittelyä (63 §).

Valiokunta on tarkastellut tämäntapaisia toimivaltuuksia perustuslain 1 §:n 1 momentissa tarkoitetun Suomen täysivaltaisuuden kannalta. Asialla on merkitystä myös julkista hallintotehtävää koskevan 124 §:n kannalta.

Valiokunta on pitänyt perustuslain näkökulmasta ongelmattomana lainsäädäntöä, jossa kansainvälisoikeudelliseen sopimukseen perustuen toisen valtion virkamiehelle annetaan toimivalta toimia Suomen alueella pakkokeinolain ja poliisilain mukaisissa peitetoiminta- ja valeostotehtävissä rikosten selvittämiseksi. Edellytyksenä tällöin on, että Suomi on hyväksynyt asiaa koskevan oikeusapupyynnön tai on itse pyytänyt sitä. Vieraan valtion virkamiehellä on tuolloin vastaava rikos- ja yksityisoikeudellinen vastuu ja oikeudet kuin suomalaisilla virkamiehillä. Lisäksi hänen toimintansa on suomalaisen virkamiehen johdon ja valvonnan alaista. (PeVL 9/2003 vp.)

Sotilastiedustelulakia koskevan esityksen mukaan vieraan valtion virkamiehet käyttäisivät edellä mainittuja toimivaltuuksia yhteistoiminnassa sotilastiedusteluvirkamiehen kanssa ja tämän ohjauksessa ja valvonnassa. Lainsäädännössä on tarpeen varmistaa, että vieraan valtion virkamiehiä sitoo toimivaltuuksia käytettäessä Suomen lainsäädäntö ja että he ovat Suomessa toimiessaan rikosoikeudellisen vastuun piirissä. (Vrt. PeVL 56/2006 vp.)

Helsingissä 16.10.2018

Niklas Vainio
OTM, FM