21.2.2018

Eduskunnan lakivaliokunnalle

Hallituksen esitys siviilitiedustelua koskevaksi lainsäädännöksi

1 Yleistä

Sisäministeriö asetti 1.10.2015 hankkeen, jonka tehtävänä oli valmistella ehdotukset siviilitiedustelua koskevaksi lainsäädännöksi, jolla luotaisiin säädösperusta ulkomaan henkilötiedustelulle, tietojärjestelmätiedustelulle ja tietoliikennetiedustelulle. Lisäksi tehtävänä on selvittää ja arvioida suojelupoliisin salaisten tiedonhankintakeinojen toimivuutta ja riittävyyttä sekä erilaisia tiedustelutiedon hankintakeinoja vaihtoehtoineen. Siviilitiedustelulainsäädännön keskeisimmäksi tavoitteeksi asetettiin Suomen kansallisen turvallisuuden parantaminen.

Siviilitiedustelulakityöryhmä luovutti mietintönsä (Siviilitiedustelulainsäädäntö, Siviilitiedustelulakityöryhmän mietintö, Sisäministeriön julkaisu 8/2017) sisäministeri Paula Risikolle 19.4.2017. Työryhmä ehdotti, että säädettäisiin uusi laki tietoliikennetiedustelusta siviilitiedustelussa sekä muutettaisiin poliisilakia niin, että siihen lisättäisiin uusi 5 a luku, jossa säädettäisiin tiedustelumenetelmistä ja niiden käytöstä siviilitiedustelussa. Lisäksi työryhmä ehdottaa muutettavaksi lakia poliisin hallinnosta, lakia henkilötietojen käsittelystä poliisitoimessa, esitutkintalakia, pakkokeinolakia ja lakia oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa. Liitelakiehdotuksissa esitetään muun muassa poistettavaksi suojelupoliisin esitutkinta- ja pakkokeinotoimivaltuudet. Suojelupoliisi jäisi edelleen sisäministeriön alaiseksi poliisin yksiköksi.

Ehdotus lähetettiin lausunnolle 24.4.2017. Lausuntoaika oli kahdeksan viikkoa. Lausuntopyyntö lähetettiin 96 taholle, joista lausunnon antoivat 59 tahoa. Lausuntopyynnön vastaanottajien lisäksi lausuntonsa antoi seitsemän tahoa, joten mietinnöstä saatiin lausunnot yhteensä 66 taholta. Luonnos hallituksen esitykseksi oli lisäksi käsiteltävänä lainsäädännön arviointineuvostossa, joka antoi asiassa lausunnon.

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.

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

Siviilitiedustelulainsäädäntöä koskeva hallituksen esitys (HE 202/2017 vp) liittyy seuraaviin eduskunnassa käsiteltävänä oleviin hallituksen esityksiin: 1) Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta (HE 198/2017 vp); 2) Hallituksen esitys eduskunnalle laiksi sotilastiedustelusta sekä eräiksi siihen liittyviksi laeiksi (HE 203/2017 vp); 3) Hallituksen esitys eduskunnalle laiksi tiedustelutoiminnan valvonnasta ja laiksi valtion virkamieslain 7 §:n muuttamisesta (HE 199/2017 vp). Edellä mainitut esitykset muodostavat tiedustelulakipaketin kokonaisuudessaan.

2 Suomen turvallisuusympäristön muutos

2.1 Muutoksen vaikutuksista

Sisäisen turvallisuuden strategia hyväksyttiin valtioneuvostossa 5.10.2017. Strategia pohjautuu toukokuussa 2016 eduskunnalle annettuun sisäisen turvallisuuden selontekoon. Hallitus vahvisti keväällä 2017 uuden turvallisuuden painopistealueen. Strategian ja selonteon mukaan Suomen turvallisuusympäristö on kiistatta monimutkaistunut. Uudet haasteet ja tehtävät edellyttävät viranomaisilta asianmukaista suorituskykyä.

Suojelupoliisin havainnoissa korostuu omaan toimialaan liittyvä voimakas turvallisuusympäristön muutos, joka kytkeytyy Suomen kokonaisturvallisuuteen laajemmin. Vakavimmat Suomen kansallista turvallisuutta uhkaavat tekijät liittyvät nykyään usein Suomen ulkopuolisiin tapahtumiin. Yleisen globalisoitumiskehityksen seurauksena yksittäisten valtioiden turvallisuuskysymykset ovat kansainvälistyneet. Ulkomaista alkuperää olevan ja siellä syntyvän uhan seuraukset saattavat näkyä Suomessa aiempaa nopeammin. Suomen turvallisuutta merkittävimmällä tavalla uhkaavat ilmiöt ja niiden taustatekijät liittyvät lähes poikkeuksetta maamme ulkopuolisiin ja osin vaikeasti hahmotettaviin tapahtumiin, ilmiöihin ja kehityssuuntiin.

Negatiiviset tapahtumat ja jännitteet kansainvälisessä politiikassa heijastuvat myös Suomen turvallisuus-ympäristöön. Näitä muutoksia ja niiden nopeutta on aiempaa vaikeampi ennakoida ja arvioida. Kansalliseen turvallisuuteen kohdistuville ulkoisille uhkille on yhteistä se, että niiden taustalla olevien valtiollisten ja ei-valtiollisten tahojen tunnistaminen ja erottaminen toisistaan on yhä vaikeampaa.

Turvallisuusympäristön muutoksiin on pystyttävä vastaamaan ajanmukaistamalla turvallisuusviranomaisten toimivaltuuksia sekä parantamalla viranomaisten suorituskykyä, jotta Suomen valtion johdolle ja kansallisesta turvallisuudesta vastaaville viranomaiselle pystytään luomaan parempi tilannekuva Suomen turvallisuusympäristöstä ja siihen kohdistuvista vakavista uhkista. Tällä hetkellä suomalaisen yhteiskunnan mahdollisuudet reagoida kansalliseen turvallisuuteen kohdistuviin uhkiin ovat merkittävässä epäsuhdassa uhkien toteutumisesta aiheutuvien vahinkojen kanssa. Vahinkojen mittavuudesta voidaan mainita esimerkiksi Ranskassa tapahtuneet terrori-iskut, jotka Ranskan viranomaisten mukaan aiheuttivat Ranskalle arviolta 750 miljoonan euron menetykset pelkästään turismin vähentymisenä (Reuters in Paris 23.8.2016). Brysselin terroristi-iskujen arvioitiin maksaneen Belgian taloudelle lähes miljardin verran (Politico 26.7.2016).

2.2 Terrorismi

Suomen terrorismitilanne on tiiviisti kytköksissä kansainvälisen terrorismin kehityskulkuihin ja trendeihin. Konfliktialueilla on keskeinen rooli radikaali-islamistisen terrorismin kehityksessä. Viime vuosina erityisesti Syyrian ja Irakin konfliktialue on toiminut terrorismin kasvualustana. Konfliktialue on nyt murroksessa, ja sen seurauksena radikaali-islamistiset verkostot myös Euroopassa arvioivat toimintaansa uudelleen.

Vierastaistelijailmiö vaikuttaa merkittävästi Suomen terrorismin uhkaan. Vaikutus on sekä suoraa että epäsuoraa. Suoran turvallisuusuhan aiheuttavat mahdollisesti palaavat tai palaamaan pyrkivät vierastaistelijat tai heidän verkostonsa. Epäsuora uhka nousee propagandan, värväyksen ja vaikuttamisen kautta. Lisäksi vierastaistelijailmiö on aiempaa vahvemmin sitonut myös Suomessa toimivat ja Suomeen kytkeytyvät radikaaliverkostot osaksi kansainvälisiä verkostoja. Tämä nostaa suomalaisten tai Suomeen sidoksissa olevien henkilöiden terrorihankkeisiin kytkeytymisen todennäköisyyttä joko maassamme tai ulkomailla.

Syyrian ja Irakin konfliktialueella oleskelee tällä hetkellä kymmeniä Suomesta matkustaneita henkilöitä, heidän joukossaan useita lapsia. Syyrian ja Irakin alueella toimivien terroristijärjestöjen hallinnoimilla alueilla on kasvamassa uusi jihadistisukupolvi, jossa on mukana myös suomalaisia. Tästä johtuen ilmiö tulee

vaikuttamaan Suomessa vielä pitkään. Suomesta lähteneiden taistelijoiden vuoksi myös ulkomaiset radikaali-islamistit tuntevat Suomen entistä paremmin.

Suomen profiili radikaali-islamistisessa propagandassa on kohonnut. Suomalaisia on esiintynyt esimerkiksi terroristijärjestö "Islamilaisen valtion" (ISIL) propagandassa; propagandaa on julkaistu suomeksi ja iskuihin kehotetaan myös Suomessa. Sekä suomalaisten että Suomesta matkustaneiden tiedetään osallistuneen propagandan tuottamiseen, ja joissain tapauksessa he ovat pyrkineet nimenomaisesti suuntaamaan viestiä Suomeen. Tämä osaltaan kannustaa Suomessa oleskelevia radikaaleja henkilöitä myös väkivaltaiseen toimintaan. Virtuaaliset verkostot ovat nousseet yhä keskeisempään rooliin. Propagandan levitys on siirtynyt suojattuihin pikaviestisovelluksiin. Viranomaisten vastatoimien ja tiedustelun suhteen tämä on erityisen haasteellista.

Suojelupoliisin arvion mukaan Suomeen kohdistuva terrorismin uhka on neliportaisella tasolla ilmaistuna tällä hetkellä tasolla 2 - kohonnut. Uhka on vakavampi kuin koskaan aiemmin. Suojelupoliisin tietoon on tullut aiempaa vakavampia terrorismiin kytkeytyviä suunnitelmia ja hankkeita. Terrorismin uhka Suomessa on noussut muiden Pohjoismaiden tasolle, eikä terrorismin toimintaympäristössä ole nähtävissä lainkaan uhkaa laskevia kehityskulkuja. Päinvastoin uhkan kasvu on todennäköistä keskipitkällä aikavälillä. Suomen uhkatilanteen muutoksessa merkittävää on sen nopeus. Muissa Pohjoismaissa vastaava muutos tapahtui pidemmällä aikavälillä, jolloin siihen kyettiin varautumaan asteittain.

Suojelupoliisin terrorismin torjunnan kohdehenkilöiden määrä on kasvanut voimakkaasti viime vuosina. Kohdehenkilöiden lukumäärä on tällä hetkellä noin 370. Kohdehenkilöiden sidokset terroristiseen toimintaan ovat yhä suorempia. Muutos on ollut siis myös laadullista, ja Suojelupoliisin tietoon on tullut aiempaa vakavampia terrorismiin kytkeytyviä hankkeita sekä suunnitelmia. Useissa tapauksissa nämä hankkeet ja suunnitelmat kytkeytyvät Suomen ulkopuolella vaikuttaviin toimijoihin. Radikalisoitumisen ja uusien verkostojen paljastumisen seurauksena kohdehenkilöiden määrän arvioidaan kasvavan myös lähivuosina.

Suojelupoliisi kohdistaa jatkuvasti toimenpiteensä ja tiedonhankintansa korkeimman uhan muodostaviin henkilöihin. Kohdehenkilöiden määrän kasvun johdosta kohdentamisessa joudutaan noudattamaan voimakasta priorisointia. Erityisen tärkeää terroristisen uhkien osalta on hankkia tietoa mahdollisimman ennakoivasti, jotta uhkia kyettäisiin torjumaan ennen niiden muodostumista välittömiksi. Suojelupoliisin keskeisenä roolina on tämänkaltaisen tiedustelutiedon hankkiminen.

2.3 Tiedustelu

Laittoman tiedustelutoiminnan torjuminen on muuttunut nopeasti aiempaa monimutkaisemmaksi. Ulkomaisten tiedustelupalveluiden tiedustelutoiminta Suomessa on aktiivista. Valtiollinen tiedustelutoiminta on luonteeltaan pitkäjänteistä, ja sen keskeisiä kiinnostuksen kohteita Suomessa ovat muun muassa poliittisen johdon ja väestön suhtautuminen mahdolliseen Nato-jäsenyyteen, Suomen energiapoliittiset päätökset ja energiahuoltovarmuus sekä Suomen kyberturvallisuusrakenteet. Suojelupoliisin tietoon tulee konkreettisia tapauksia vieraiden valtioiden pyrkimyksistä hankkia Suomesta salaisia tietolähteitä toimittamaan tietoja, jotka eivät ole julkisesti saatavilla. Tiedusteluorganisaatiot pyrkivät hankkimaan avustajikseen lisäksi henkilöitä, joiden avulla on mahdollista vaikuttaa poliittiseen päätöksentekoon ja yleiseen mielipiteeseen. Valtiollisten tahojen suorittama laiton tiedustelu aiheuttaa vahinkoa myös suomalaisille korkeateknologian yrityksille ja tutkimuslaitoksille. Toiminta voi aiheuttaa yritystasolla kriittistä vahinkoa ja sillä on potentiaalisesti myös kansantaloudellista merkitystä.

Vastatiedustelun olennaisena peruslähtökohtana on löytää tiedustelutoimintaa harjoittavat henkilöt, joiden toiminta muodostaa vakavan uhkan kansalliselle turvallisuudelle. Nämä henkilöt eivät kuitenkaan ole aina tiedossa. Siksi

tiedustelutoimivaltuudet pitäisi käyttöperusteiden kohdalla irrottaa nykyisten toimivaltuuksien rikos- ja henkilöperusteista.

2.4 Kybertoimintaympäristö

Kybertoimintaympäristön merkitys kasvaa, eikä kyberkeinojen käyttöä poliittisten päämäärien saavuttamiseksi voida sulkea pois. Tietoliikenneverkkojen kautta tapahtuva rajat ylittävä vakoilu on noussut merkittäväksi uhaksi. Tällainen toiminta mahdollistaa suurten tietomäärien hankkimisen keskitetysti, mikä voi aiheuttaa korjaamatonta vahinkoa kohdevaltion turvallisuudelle ja sen eduille. Tietoverkoissa tapahtuva sabotaasi ja tiedon vääristäminen ovat myös merkittäviä uhkia kansalliselle turvallisuudelle. Kybervakoilulla saatua tietoa voidaan käyttää myös informaatiosodankäynnissä, josta esimerkkinä on Ranskan ja Yhdysvaltojen vaaleihin vaikuttaminen.

Suomen turvallisuusympäristön muutoksen kannalta olennaiset ulkovallat panostavat mittavasti hyökkäyksellisen kyberkapasiteettinsa rakentamiseen. Tämä vaatii näiltä valtioilta aiempaa enemmän tukea perinteisessä reaalimaailmassa tapahtuvalta tiedustelutoiminnalta, kuten tiedonkeräämistä henkilötiedustelun keinoin potentiaalisista kybervakoilun kohteista tai sellaisen henkilön löytämistä joka vahingossa tai tarkoituksellisesti auttaisi valtiollisen haittaohjelman viemisessä kohdeorganisaation tietojärjestelmään.

Kybervakoilu tarjoaa valtioille lähes riskittömän tavan hankkia tietoa riippumatta niiden taloudellisesta ja yhteiskunnallisesta kehitystasosta. Kybervakoilu on halpa tiedonhankintamenetelmä suhteessa potentiaalisesti saatavilla olevan tiedon määrään verrattuna.

Kybervakoilun ja -operaatioiden merkitys kasvaa tulevina vuosina entisestään. Syitä tälle ovat mahdollisuus toteuttaa kybertoimintaympäristössä tekoja alhaisin kustannuksin, suojautumisen vaikeus ja kalleus sekä vähäinen kiinnijäämisriski. Esimerkkeinä valtioihin kohdistuneesta kyberoperaatioista voidaan mainita muun muassa Ukrainan (2014), Georgian (2008) ja Viron (2007) suljettuihin viranomaisverkkoihin kohdistetut verkkohyökkäykset, jotka ovat osoittautuneet hyvin organisoiduiksi ja suunnitelluiksi operaatioiksi, joiden taustalla arvioidaan olevan valtiotoimija tai siihen hyvin läheisesti kytkeytyvät tahot.

Jo nykyisellään uutisoidaan globaalisti hakkeroinneista toisen valtion ohjusjärjestelmiin ja ydinvoimaloihin sekä niin sanottujen kyberpommien kätkemisestä. Myös Suomen kriittisen infrastruktuurin tietojärjestelmiä ja tietoliikenneyhteyksiä sekä avainhenkilöitä tiedustellaan ennakolta, jotta niihin voidaan tarvittaessa vaikuttaa.

Yksityisten yritysten tietopääoman anastamiseen pyrkivistä hyökkäyksistä iso osa jää kokonaan pimentoon, koska yrityksillä tai kolmannella sektorilla ei ole valmiutta tunnistaa valtiollisen toimijan uhkaa. Erityisen kriittisiä uhkia ovat kyberoperaatiot, joissa hyökkääjä on hyväksikäyttänyt suoraan organisaation luotettuja palveluketjutoimintoja. Tieto hyökkäyksistä tulee suojelupoliisille lähes poikkeuksetta ulkomaisten kumppanien vinkkeinä. Viedyn tietopääoman arvo keskisuuren yrityksen tapauksessa on kymmeniä miljoonia euroja vuodessa. Hyökkäystoiminnan nopea havainnointi minimoisi viedyn tiedon määrän ja sen aiheuttamat potentiaaliset menetykset yritykselle.

Vaikka luotetuilta kumppaneita saadut vinkit auttavat Suomea vastaan kohdistuvien yksittäisten hyökkäysten torjunnassa, tulee huomioida, että ulkomaisten kumppaneiden toiminnan pääprioriteetti on niiden kansallisten toimijoiden suojaaminen. Tiedon välitys Suomen kaltaisille kumppaneille on toissijaista ja aiheuttaa siten välillä merkittävän, kuukausienkin viiveen tiedon saannissa ja edelleen suojautumisessa.

Tietoverkkoihin kohdistuvat hyökkäykset ovat erittäin vaarallinen uhka kahdesta syystä: niihin soveltuva teknologia kehittyy jatkuvasti, ja niissä on usein valtiotoimijoiden apuna järjestäytyneen rikollisuuden edustajia ja hakkereita.

Valtiollinen toiminta, kansalaisyhteiskunta ja rikollisuus sulautuvat toisiinsa, joten uhkien torjumiseksi turvallisuusviranomaisten teknisen suorituskyvyn olisi oltava hyökkääjää parempi. Suorituskyvyn käyttämiseen tarvittavien valtuuksien tulisi olla käyttöperusteeltaan olla sellaiset, että uhkien muodostuminen voidaan havaita mahdollisimman aikaisin. Jos viranomaiset kykenevät pelkään reagoimiseen vahinkojen jo tapahduttua, yhteiskunnan elintärkeät toiminnot ovat erittäin suuressa vaarassa.

Tietoliikennetiedustelu mahdollistaa ennakoivan puolustautumisen seuraamalla valtiollisten kybervakoiluoperaatioiden kartoitus- ja hyökkäystoimintaa tietoverkoissa ei vain omaa valtiota kohti, vaan myös muihin maihin kohdistuneena. Toiminnan käynnistämiseksi tarvittava tieto ja osaaminen ovat jo valtaosin olemassa.

2.5 Hybridivaikuttaminen

Hybridivaikuttaminen on osa suurvaltojen sekä vahvojen poliittisten tai aseellisten ryhmien toimintaa oman vaikutusvallan lisäämiseksi, vastapuolen toiminnan häiritsemiseksi ja omien poliittisten ja/tai sotilaallisten tavoitteiden saavuttamiseksi. Hybridivaikuttamisen toimijat on tapana jakaa valtiollisiin ja ei-valtiollisiin toimijoihin. Vieraiden valtioiden hybridivaikuttamisen keinot ovat aiempaa monimuotoisemmat (sotilaallinen, poliittinen, taloudellinen, infrastruktuuri, informaatio, kulttuuri, muut keinot). Suojelupoliisin kiinnostuksen kohteen hybridiuhista ovat erityisesti vaikuttaminen informaation ja propagandan avulla sekä kybertoiminta. Nykyisillä rikos- ja henkilöperusteisilla toimivaltuuksilla ei läheskään kaikissa tapauksissa ole mahdollisuuksia tunnistaa tai torjua ulkomaisia valtiollisia hybridiuhkia, jotka voivat vakavasti vaarantaa Suomen kansallista turvallisuutta.

Informaatiovaikuttamiseen voi liittyä esimerkiksi disinformaation levittämistä, kulttuuriin liittyvän vaikutusvallan kasvattamista, tietojärjestelmäkatkosten aiheuttamista tai hämmennyksen ja epävakauden ruokkimista. Tiedotusvälineet ja sosiaalinen media, mukaan lukien ns. trollien käyttö, on vain pieni osa toiminnasta. Teknisesti vaikuttamiskeinoille kehittyy aivan uusia mahdollisuuksia informaatio- ja kyberteknologian ansiosta. Esimerkiksi Yhdysvaltain presidentinvaaleissa erään globaalin sosiaalisen mediayhtiön tiedotteen mukaan sen palvelimelle laaditut valetilit olivat kahden vuoden aikana julkaisseet noin 80 000 päivitystä, joiden tarkoitus oli ollut vaikuttaa Yhdysvaltain politiikkaan. Presidentinvaalien alla levinneet viestit tavoittivat arviolta jopa 126 miljoonaa amerikkalaista.

Osa informaatio-operaatioista tapahtuu kyberhyökkäysten avulla. Tavoitteena voi olla sellaisten tietojen saaminen, joita voidaan käyttää informaatio-operaatioissa, tai vaikkapa haittaohjelmien asettaminen, jotta saadaan valmius toisen maan tietoliikenneyhteyksien katkaisemiseen tarvittaessa. Uudempi ilmiö on kyberhyökkäysten käyttäminen vaalikampanjoiden aikana ehdokkaiden mustamaalaukseen. Valtiollisten toimijoiden lisäksi huolena on kyberrikollisten kasvava kyky aiheuttaa merkittävää haittaa erilaisille yhteiskunnan kriittisille toiminnoille.

Valtioneuvoston kanslia julkaisi 17.2.2017 riippumattoman tutkimuksen Suomen kyberturvallisuuden tilasta (Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017). Tutkimuksen mukaan kansallinen kyberturvallisuustapahtumien havainnointikyky on puutteellinen. Siksi tilannetietoisuus on heikko ja edellytykset estää, rajoittaa ja toipua vakavista kyberhyökkäyksistä on rajallinen. Suomalaisen yhteiskunnan kaikkia elintärkeitä toimintoja sekä huoltovarmuuskriittisiä yrityksiä ei ole tällä hetkellä suojattu riittävällä tavalla erilaisia kyberuhkia vastaan ja myös häiriötilanteiden resilienssi (sietokyky) on edelleen osassa suojattavia kohteita heikolla tasolla. Suomen lainsäädäntöä ei ole kyetty ajanmukaistamaan kyberturvallisuuden vaatimuksia vastaaviksi. Tiedustelulainsäädännön uudistaminen arvioidaan välttämättömäksi havainnointikyvyn parantamiseksi.

3 Nykyisten toimivaltuuksien käytön oikeudelliset rajoitteet tiedustelutoiminnassa

Suojelupoliisin nykyisten toimivaltuuksien (salaisten tiedonhankintakeinojen) yhteinen piirre on se, että ne on määritelty henkilö- ja rikoslähtöisesti. Niitä voidaan kohdistaa vain sellaiseen henkilöön tai käyttää hankittaessa tietoa vain sellaisen henkilön toiminnasta, jonka voidaan perustellusti olettaa tulevaisuudessa syyllistyvän tai jo syyllistyneen tietyn rangaistusuhan ylittävään rikokseen, rikoksen yritykseen tai joissain tapauksissa sellaisen valmisteluun.

Rikostorjuntatoimivaltuuden käyttö tulee lähtökohtaisesti pystyä kohdistamaan aina tiettyyn henkilöön, vaikka henkilön henkilöllisyys ei tarvitse olla viranomaisen tiedossa. Telekuuntelu tai televalvonta voidaan kohdistaa myös tuntemattomaan henkilöön esimerkiksi IP-osoitteen perusteella, vaikka tiedusteluviranomaisella tulee olla tietty varmuus siitä, että kyseinen IP-osoite on tuntemattoman henkilön käyttämä. Jos tällaista tiettyyn henkilöön liittyvää rikostorjunnallista perustetta ei ole olemassa, ei poliisilain mukaisen salaisen tiedonhankintakeinon käyttö ole mahdollista.

Tiedustelutoiminnalle tyypillistä on, ettei tietty henkilö ole aina tiedossa, vaan tiedustelun olennaisena tavoitteena olisi löytää sellaiset henkilöt, joiden toiminta vakavasti uhkaa kansallista turvallisuutta. Siksi tiedustelutoimivaltuuksien käyttöperusteiden kohdalla tulisi irtaantua nykyisten toimivaltuuksien rikos- ja henkilöperustaisuudesta.

Kun nykyisten tiedonhankintatoimivaltuuksien käytön erityiset edellytykset on määritelty rikosten ja niiden vakavuuden perusteella, niin suojelupoliisin käytössä olevat toimivaltuudet eivät mahdollista nykyisellääänkään sille säädetyn tehtävän suorittamista muutoin kuin rikosten torjunnan ja selvittämisen osalta. Mutta sellaisten hankkeiden torjumiseksi, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta, ei salaisia tiedonhankintakeinoja voida lainkaan käyttää.

Käsiteltävänä olevan lakiehdotuksen sekä edellä kerrotun perusteella tiedustelutoimivaltuuksien käytön edellytykset määritellään uhkalähtöisesti. Salainen tiedonhankinta ehdotetaan mahdollistettavaksi sellaisen laissa tyhjentävästi määritellyn toiminnan osalta, joka vakavasti uhkaa Suomen kansallista turvallisuutta joko suoraan tai välillisesti. Kansallista turvallisuutta vakavasti uhkaava toiminta voi ensinnäkin olla sellaista, joka konkretisoituessaan olisi rikos, mutta johon ei vielä voida kohdistaa konkreettista ja yksilöityä rikosepäilyä taikka tekijä ei ole tiedossa. Toiseksi kyse voi olla sellaisesta kansallista turvallisuutta uhkaavasta toiminnasta, joka on tiedossa, mutta se tapahtuu toisen valtion alueella eikä siitä ole mahdollista saada tietoa kuin julkisista lähteistä. Kolmanneksi kyse voi olla toiminnasta, joka ei ole Suomen lain mukaan rikos eikä voi sellaiseksi muodostuakaan. Esimerkkeinä voidaan mainita Suomen huoltovarmuuden kannalta merkityksellisten kiinteistöjen siirtyminen ulkomaiseen omistukseen tai toiminta, jolla suomalaiseen ja ulkomaiseen kansalaismielipiteeseen pyritään vaikuttamaan levittämällä järjestelmällisesti väärää tietoa Suomen politiikasta julkisuudessa.

4 Siviilitiedustelu

4.1 Siviilitiedustelun kohteet

Lakiehdotuksessa siviilitiedustelulla tarkoitetaan suojelupoliisin suorittamaa tiedonhankintaa ja tiedon hyödyntämistä kansallisen turvallisuuden suojaamiseksi, ylimmän valtiojohdon päätöksenteon tukemiseksi ja muiden viranomaisten lakisääteisiä kansalliseen turvallisuuteen liittyviä tehtäviä varten.

EIT:n ratkaisukäytännön mukaan laki ei voi olla sellainen, että se mahdollistaa salaisen tarkkailun kohdistamisen sattumanvaraisesti keneen tahansa (Amann v. Sveitsi). Esimerkiksi pelkkä laissa oleva maininta siitä, että salaisia valtuuksia saadaan käyttää kansallisen turvallisuuden suojaamiseksi, ei ole riittävä ennakoitavuusvaatimuksen täyttämiseksi (Zakharov v. Venäjä). Toisaalta kansallisen lain ei voida edellyttää täsmällisesti ja tyhjentävästi luetteloivan kaikkia niitä tilanteita, joissa viranomaiset saavat käyttää salaisia valtuuksia. Lain säännöksen, jonka

mukaan salaisten valtuuksien käyttöperusteena on terrorismin uhka, on esimerkiksi katsottava täyttävän ihmisoikeussopimuksen asettaman ennakoitavuusvaatimuksen (Szabo & Vissy v. Unkari).

Siviilitiedustelussa käytettävillä toimivaltuuksilla, tiedustelumenetelmillä saataisiin hankkia tietoa ainoastaan laissa tyhjentävästi luetelluista siviilitiedustelun kohteista. Niistä ehdotetaan säädettäväksi niin yksilöidysti kuin tiedustelutoiminnan erityispiirteistä johtuen on mahdollista. Siviilitiedustelun kohteita lakiehdotuksen mukaan ovat:

1) terrorismi,
2) ulkomainen tiedustelutoiminta,
3) joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö,
4) kaksikäyttötuotteiden vientivalvonnasta annetun lain (562/1996) 2 §:ssä tarkoitettujen kaksikäyttötuotteiden suunnittelu, valmistaminen, levittäminen ja käyttö,
5) kansanvaltaista yhteiskuntajärjestystä uhkaava toiminta,
6) suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaava toiminta,
7) vieraan valtion toiminta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille tai taloudellisille tai muille tärkeille eduille,
8) kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi,
9) kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaava toiminta,
10) Suomen kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuutta uhkaava toiminta,
11) yhteiskuntajärjestystä uhkaava kansainvälinen järjestäytynyt rikollisuus.

4.2 Tiedustelumenetelmät ja niiden käyttöä ohjaavat periaatteet

Tiedustelumenetelmiä ovat telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen laitetarkkailu, teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen, peitetoiminta, valeosto, ohjattu tietolähdetoiminta, paikkatiedustelu, jäljentäminen, lähetyksen pysäyttäminen jäljentämistä varten, tietojen saanti yksityiseltä yhteisöltä ja tietoliikennetiedustelu (Poliisilaki 5 a luku 2 §).

Tiedustelumenetelmän käytön kohdistaminen henkilöön tai henkilöryhmään muodostaa poikkeuksetta puuttumisen kyseisen henkilön tai henkilöiden yksityisyyden suojaan. Tiedustelumenetelmää lähtökohtaisesta käytetään sen kohteelta salassa. Tiedustelutoiminnan ja tiedustelumenetelmien vaivihkaisen luonteen vuoksi ei tiedustelumenetelmän käyttäminen ja sillä saatu tieto itsessään aiheuta vastaavantyyppistä vahinkoa tai haittaa mitä esimerkiksi useiden pakkokeinojen (pidättäminen, vangitseminen tai vakuustakavarikko). Tiedustelumenetelmillä saatua tietoa ei myöskään lähtökohtaisesti käytetä henkilön syyllisyyttä tukevana selvityksenä eikä niillä puututa vastaavalla tavalla henkilön koskemattomuuteen tai vapauteen mitä pakkokeinoilla. Sitä vastoin tiedustelumenetelmillä saadun tiedon käyttäminen syyttömyyttä tukevana selvityksenä mahdollistetaan melko alhaisella kynnyksellä.

Perusoikeuksien ja ihmisoikeuksien kunnioittamiseen on tiedustelumenetelmien käytön kohdalla syytä kiinnittää erityistä huomiota. Tiedustelumenetelmillä lähtökohtaisesti puututaan perustuslaissa suojattuihin perusoikeuksiin. Tämä koskee erityisesti yksityiselämän ja luottamuksellisen viestin suojaa. Perus- ja ihmisoikeuksien suojaa on toisaalta punnittava kansallisen turvallisuuden suojaamisintressiä vasten. Sinällään nämä vastinintressit eivät ole toisensa poissulkevia, koska kansallisen turvallisuuden suojaamisella ja yhteiskunnan kannalta vahingollisten tapahtumien estämisellä suojataan samalla jokaisen perus- ja ihmisoikeuksia.

Tiedustelumenetelmän käyttö ei saa olla syrjivää eikä sen kohdentaminen saisi perustua esimerkiksi etniseen profilointiin eli siihen, että henkilöstä hankittaisiin tietoa

yksinomaan tai pääasiallisesti henkilön etnisen taustan, ihonvärin tai uskonnon perusteella.

Myös muilla poliisioikeudellisilla periaatteilla, suhteellisuusperiaatteella, vähimmän haitan periaatteella ja tarkoitussidonnaisuusperiaatteella, on korostunut merkitys tiedustelumenetelmiä käytettäessä. Suhteellisuusperiaate edellyttää aina arviointia toimenpiteiden oikeasuhtaisuutta ja siten käytettyjen keinojen ja niillä aiheutettujen haittojen, kuten esimerkiksi yksityisyyden suojaan puuttumisen, tulee aina olla järkevässä suhteessa tavoiteltuun päämäärään nähden. Oikeasuhtaisuus ei siis tarkoita vain sitä, ettei toimenpide saa olla ylimitoitettu tiedustelun kohteensa olevan henkilön näkökulmasta, vaan kyse on myös siitä, että toimenpiteen on oltava riittävän tehokas tavoitellun päämäärän, kuten esimerkiksi tietyn tiedon saamisen saavuttamiseksi. Suhteellisuusperiaatetta osaltaan ilmentää poliisilain 1 luvun 3 §:ssä säädetyn lisäksi myös saman luvun 9 §:n 1 momentissa säädetty oikeus luopua toimenpiteestä, jos sen loppuun suorittaminen voisi johtaa kohtuuttomaan lopputulokseen tavoiteltavaan päämäärään nähden.

Poliisilain 1 luvun 4 §:ssä säädetään vähimmän haitan periaatteesta, jonka mukaan kenenkään oikeuksiin ei saa puuttua enempää eikä kenellekään saa aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi. Oikeuksilla tarkoitetaan perustuslaissa säädettyjä perusoikeuksia. Vähimmän haitan periaate velvoittaa suojelupoliisia minimoimaan tiedustelumenetelmän kohteeksi joutuneelle henkilölle toimenpiteestä aiheutuvaa perusoikeuspuuttumista. Ilmaisulla ”kenellekään” tarkoitetaan, että vähimmän haitan periaate suojaa kaikkia, joihin (suojelu)poliisin toimenpide ulottaa vaikutuksensa. Kuten vähimmän haitan periaatteesta ilmenee, niin sen rakenneosiin kuuluvat välttämättömyysedellytys ja sitä seuraava vaihtoehtoisia (tässä yhteydessä) tiedustelumenetelmiä koskeva optimointivelvollisuus. Nämä elementit ohjaavat suojelupoliisin toimintaa siviilitiedustelussa ja tiedustelumenetelmän valinnassa sekä sen kohdistamisessa. Kun siviilitiedustelua ja siinä valittuja tiedustelumenetelmiä ryhdytään käyttämään, toiminta on toteutettava siten, että se aiheuttaa tiedustelun kohteena olevalle mahdollisimman vähäisen puuttumisen perusoikeuksiin. Tällä tarkoitetaan kohteelle aiheutuvan vahingon tai haitan minimointivelvollisuutta.

Tarkoitussidonnaisuuden periaatteesta säädetään lain 1 luvun 5 §:ssä, jonka mukaan poliisi saa käyttää toimivaltuuttaan vain säädettyyn tarkoitukseen. Periaate liittyy tässä yhteydessä sekä poliisin hallinnosta annetun lain 10 §:n että poliisilain 1 luvun 1 §:n muutoksiin, mutta myös niiden perusteluissa todettuihin seikkoihin. Tällä tarkoitetaan, että suojelupoliisin asiallisen toimivallan tulee aina perustua nimenomaiseen säännökseen. Puututtaessa yksilön oikeuksiin tai velvollisuuksiin säännöksen tulee olla laissa. Tarkoitussidonnaisuuden periaate koskee kaikkea poliisitoimintaa, ja tässä yhteydessä sillä olisi merkitystä ainakin siviilitiedustelutoimivaltuuksien ja erityisesti niillä saatujen tietojen käyttämisessä.

4.3 Tiedustelumenetelmien käytön edellytykset

Siviilitiedustelun kohde ei yksistään mahdollista tiedustelumenetelmän käyttöä. Laissa ehdotetaan säädettäväksi kaikille tiedustelumenetelmille yhteisestä yleisestä käyttöedellytyksestä ”voidaan perustellusti olettaa saatavan tietoja sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta”. Kyse olisi perustelua edellyttävästä tuloksellisuusvaatimuksesta, jolloin tiedustelumenetelmän käytön odotusarvona on sen perusteltu hyödyllisyys. Tiedustelumenetelmän käytön hyödyllisyys tulisi pystyä yksittäistapauksellisesti perustelemaan, mitä ilmentäisi ilmaisu ”perustellusti”. Perustelu voisi liittyä esimerkiksi siihen, miksi nimenomaan tiettyä henkilöä tai henkilöryhmää taikka tiettyä tilaa tai muuta paikkaa tulisi voida tarkkailla ja miksi näin pystyttäisiin oletetusti saamaan kansallisen turvallisuuden kannalta hyödyllistä tietoa. Tämä voisi liittyä esimerkiksi henkilön tai henkilöryhmän käyttäytymiseen taikka muutoin siitä saatuihin tietoihin.

Kansallista turvallisuutta vakavasti uhkaavan toiminnan vaatimus johtuu ehdotettavan perustuslain 10 §:n 4 momentista. Kyseisen perustuslain kohdan perusteella

vakavuusedellytys nostaa luottamuksellisen viestin suojaan puuttuvien keinojen soveltamiskynnystä asettaessaan kvalifioinnin uhkan laadusta. Siten pelkästään jonkinasteisen uhkan kansalliselle turvallisuudelle muodostava toiminta ei vielä täyttäisi säännöksessä asetettua vaatimusta. Uhkan vakavuusaste kytkeytyy myös edellä 3 §:ssä käsiteltyihin sisällöllisiin määrittelyihin siitä, millainen siviilitiedustelun kohteena oleva toiminta muodostaa vakavan uhkan kansalliselle turvallisuudelle. Kansallista turvallisuutta vakavasti uhkaavan toiminnan vaatimus koskee myös muiden kuin luottamuksellisen viestin salaisuuden suojaan puuttuvien tiedustelumenetelmien käyttöä.

Kansallista turvallisuutta vakavasti uhkaavan toiminnan lajit tyhjentyisivät 3 siviilitiedustelun kohteisiin (Poliisilaki 5 a luku 3 § ja Laki tietoliikennetiedustelusta siviilitiedustelussa 3 §). Tiedustelumenetelmän käytön perusteeksi ei kuitenkaan riittäisi pelkkä abstraktin tason uhka, vaan yksittäistapauksellisesti tulisi pystyä osoittamaan, että siviilitiedustelun kohteena oleva toiminta muodostaisi vakavan uhkan tai sen voitaisiin olettaa vakavasti uhkaavan kansallista turvallisuutta. Tätä ilmentäisi relatiivilause ”joka vakavasti uhkaa kansallista turvallisuutta”. Ilmaisulla ”uhkaa” tarkoitettaisiin sitä, ettei säännöksessä edellytettäisi kansallisen turvallisuuden olevan välittömästi vaarantumassa. Näin ollen säännöksessä tarkoitettu tiedonhankinta voisi koskea myös siviilitiedustelun kohteena olevaa toimintaa, joka jatkuessaan vakavasti uhkaisi kansallista turvallisuutta. Uhkalta kuitenkin edellytettäisiin tietynasteista ajallista läheisyyttä tai sillä tulisi olla ainakin välillinen liityntä Suomen kansalliselle turvallisuudelle.

EIT:n ratkaisukäytännön perusteella on selvää, että ainakin sotilaallinen maanpuolustus, terrorismin torjunta ja laittoman tiedustelutoiminnan torjunta kuuluvat kansallisen turvallisuuden piiriin (mm. Klass v. Saksa, Weber ja Saravia v. Saksa). Kansalliseen turvallisuuteen saattaa kuitenkin kohdistua monenlaisia uhkia, joita on vaikea ennakoida tai määritellä etukäteen. Tästä seuraa, että käsitteen selventäminen on ensisijaisesti jätettävä kansallisen käytännön varaan (Kennedy v. Yhdistynyt Kuningaskunta).

Kansallisella turvallisuudella säännöksessä viitataan viime kädessä valtion oikeudenkäyttöpiirissä olevien ihmisten kollektiiviseen turvallisuuteen välittömästi tai välillisesti väkivaltaista ulkoista uhkaa vastaan. Kansallista turvallisuutta vakavasti uhkaavaa on tyypillisesti sellainen yleisvaarallinen ja siihen liittyvä toiminta, joka uhkaa suuren ja ennalta arvaamattoman, sattumanvaraisesti määräytyvän ihmisjoukon henkeä tai terveyttä (HE 198/2017 vp, s. 35).

Ilmaisu ”kansallinen turvallisuus” tarkoittaisi sitä, ettei säännöksessä tarkoitettu uhkaava toiminta kohdistuisi ensisijaisesti kehenkään yksilönä vaan yleisemmin yhteiskuntaan ja sen ihmisyhteisöön. Kuitenkin myös esimerkiksi yksityishenkilöihin kohdistuvat väkivallanteot voisivat olla säännöksessä tarkoitettua toimintaa, jos ne laajuudeltaan tai merkitykseltään olisivat kansallisen turvallisuuden kannalta merkittäviä ja voisivat siten muodostaa vakavan uhan sille. Esimerkiksi valtiojohtoon tai yhteiskunnan perustoiminnoista huolehtiviin henkilöihin samoin kuin heidän turvallisuusjärjestelyistään vastaaviin kohdistuvat uhat voivat muodostaa vakavan uhan kansalliselle turvallisuudelle.

Kansallisen turvallisuuden määritelmää käsitellään tarkemmin perustuslain 10 §:n muuttamista koskevassa hallituksen esityksessä (HE 198/2017 vp). Merkityksellistä tiedustelumenetelmän käytön edellytyksen osalta on, että siviilitiedustelun kohteilla täsmennettäisiin niitä toiminnan lajeja, jotka voivat muodostaa vakavan uhkan Suomen kansalliselle turvallisuudelle. Yksittäinen siviilitiedustelun kohde ei kuitenkaan itsessään ole sellainen, että se sellaisenaan muodostaa vakava uhkan kansalliselle turvallisuudelle, vaan suojelupoliisin tulisi perustella kohteena olevaan toimintaan liittyvien tosiseikkojen avulla, miksi se muodostaa vakavan uhan Suomen kansalliselle turvallisuudelle.

Laissa ehdotetaan säädettäväksi tiedustelumenetelmäkohtaisista erityisistä käyttöedellytyksistä. Telekuuntelua, tietojen hankkimista telekuuntelun sijasta, suunnitelmallista tarkkailua, teknistä kuuntelua, teknistä katselua, henkilön teknistä seurantaa, teknistä laitetarkkailua, peitetoimintaa, valeostoa, tietolähteen ohjattua käyttöä ja paikkatiedustelua saadaan käyttää vain, jos niillä voidaan perustellusti

olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Peitetoiminnan ja valeoston käyttäminen edellyttäisi lisäksi, että menetelmän käyttö olisi välttämätöntä. Peitetoiminnan käytön edellytyksenä olisi myös sen kohdistuminen järjestäytyneeseen kansallista turvallisuutta vakavasti uhkaavaan toimintaan. Järjestäytyneeseen toimintaan liittyy usein suunnitelmallisuus. Suunnitelmallisuuden mainitseminen säännöksessä tarkoittaisi myös sitä, että menetelmää olisi mahdollista kohdistaa jatkossakin esimerkiksi saman yksittäisen toimijan suunnitelmalliseen toimintaan. Peitetoiminnan käytön edellytyksenä olisi myös, että tiedonhankintaa on toiminnan suunnitelmallisuuden, järjestäytyneisyyden tai ammattimaisuuden taikka ennakoitavissa olevan jatkuvuuden tai toistuvuuden vuoksi pidettävä tarpeellisena.

Erittäin tärkeä" merkitys” ja ”välttämätöntä” vastaisivat salaisten tiedonhankintakeinojen käytön edellytyksiä koskevia ilmaisuja, joista säädetään 5 luvun 2 §:ssä. Nykyistä poliisilakia koskevassa hallituksen esityksessä (HE 224/2010 vp, s. 38–43 ja 90 ja 91) tiedonhankintakeinojen käytön edellytyksiä koskevassa yleisperustelujen jaksossa on selostettu tarkemmin käsitteiden ”erittäin tärkeä merkitys” ja ”välttämätöntä” merkityssisältöä.

Jos tiedustelumenetelmä kohdistetaan valtiolliseen toimijaan tai siihen rinnastuvan tahoon, tiedustelumenetelmän käytön edellytyksiin sovelletaan perusteltua tuloksellisuusodotusta riippumatta siitä, mitä tiedustelumenetelmää käytetään. Tämä johtuu siitä, ettei vieraan valtion viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa (HE 198/2017 vp, s. 35).

Tiedustelumenetelmää ei saa kohdistaa vakituiseen asumiseen käytettävään tilaan. Peitetoiminta ja valeosto ovat kuitenkin asunnossa sallittuja, jos sisäänkäynti tai oleskelu tapahtuu asuntoa käyttävän aktiivisella myötävaikutuksella.

Perustuslaissa turvattu kotirauhan piiri kattaa lähtökohtaisesti kaikenlaiset pysyväisluonteiseen asumiseen käytetyt tilat (esim. 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). Kotirauhan suojaama piiri määritellään kuitenkin eri tavoin perustuslaissa kuin esimerkiksi rikoslaissa. Tästä johtuen tiedustelumenetelmän käyttöä ei saa kohdistaa rikoslain 24 luvun 11 §:ssä tarkoitettuun kotirauhan suojaamaan asuntoon tai muuhun asumiseen tarkoitettuun tilaan, jollei voitaisi osoittaa paikkaa tosiasiallisesti käytettävän muuhun kuin pysyväluonteiseen asumiseen (PeVL 36/1998 vp, KKO 2009:54). Ainoa poikkeus tästä on peitetoiminta ja valeosto, jolloin peitetoimintaa tai valeostoa suorittavalla suojelupoliisin virkamiehellä tulisi olla oikeus paljastumisen estämiseksi mennä kyseisiin tiloihin käyttämällä hyväkseen luotua peitettä. Siksi peitetoiminta ja valeosto kuitenkin on asunnossa sallittua, jos sisäänkäynti tai oleskelu tapahtuisi asuntoa käyttävän aktiivisella myötävaikutuksella. Puheena olevan sääntelyn ulottaminen koskemaan myös valeostoa on oikeusturvasyistä perusteltua, koska valeosto voidaan toteuttaa myös asunnossa.

Tiedustelumenetelmän käyttö on lopetettava ennen päätöksessä mainitun määräajan päättymistä, jos käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole. Tällä korostetaan sitä, ettei tiedustelumenetelmiä voida missään tapauksessa käyttää kauempaa kuin on tarpeen, vaikka lupa olisikin vielä voimassa.

Vaikka tiedonhankinta siviilitiedustelussa on luonteeltaan pitkäkestoista, jokaisen tiedustelumenetelmän osalta tulisi erikseen säätää luvan tai päätöksen kestosta, joka voisi olla enintään kuusi kuukautta. Luvan tai päätöksen mentyä umpeen olisi tiedustelumenetelmän käytöstä päätettävä uudelleen tai sen käyttö olisi lopetettava. Lisäksi tiedustelumenetelmän tarpeellisuutta ja sen perusteita olisi harkittava koko ajan sitä käytettäessä ja keinon käyttö olisi lopetettava ennen päätöksessä mainitun määräajan päättymistä, jos käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole.

4.4 Päätöksentekijä

Siviilitiedustelun hoitaminen ja tiedustelumenetelmien käyttö siviilitiedustelussa ehdotetaan osoitettavaksi yksinomaan yhden viranomaisen, suojelupoliisin tehtäväksi.

Siviilitiedustelussa käytettävien tiedustelumenetelmien päätöksentekoa koskeva sääntely perustuisi pääosin poliisilain salaisia tiedonhankintakeinoja koskevaan lukuun. Tuomioistuimen päätettäväksi esitettäisiin perus- ja ihmisoikeuksiin merkittävimmin puuttuvien tiedustelumenetelmien käyttäminen.

Päätöksentekotoimivaltaan liittyvät perus- ja ihmisoikeuspuuttumiset keinokohtaisesti on arvioitu esitutkinta- ja pakkokeinolainsäädännön uudistamisen yhteydessä (Oikeusministeriön komiteanmietintö 2009:2) perustuslakivaliokunnan kannanotot mukaan lukien. Siksi myös 5 a luvussa tiedustelumenetelmien päätöksentekoa koskevien perusratkaisujen kohdalla on perusteltua seurata mahdollisimman pitkälle 5 luvussa omaksuttua sääntelyä.

Tietoliikennetiedustelusta päättäisi tuomioistuin. Tuomioistuin päättäisi myös paikkatiedustelusta, jos se kohdistuu muuhun kotirauhan suojaamaan paikkaan kuin vakituiseen asumiseen käytettävään paikkaan tai paikkaan, johon ei ole yleistä pääsyä tai johon yleinen pääsy on rajoitettu tai estetty paikkatiedustelun toimittamisajankohtana.

Tuomioistuimella ei lähtökohtaisesti ole toimivaltaa päättää toimivaltuuden käytöstä muualla kuin Suomessa. Operatiivista päätöksentekoa ei myöskään ole tarkoituksenmukaista viedä oikeudellisessa järjestelmässä uusille toimijoille ulkomaan tiedusteluun liittyvien ulkopoliittisesti sensitiivisten elementtien takia. Kansainväliseen vertailuun kuuluvien joidenkin maiden kohdalla ulkomaan tiedustelusta päättää tiedusteluviraston päällikkö. Ulkomaan tiedustelua koskevasta päätöksenteosta siviilitiedustelussa käytettävien tiedustelumenetelmien osalta on perusteltua säätää vastaavalla tavalla. Suojelupoliisin päällikkö päättäisi myös kansainväliseen yhteistyöhön osallistumisesta.

4.5 Luottamuksellisen viestin salaisuuden suojaan puuttuvat tiedustelumenetelmät

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 poliisilain 5 a lukuun esitettävä 6 § (telekuuntelu ja tietojen hankkiminen telekuuntelun sijasta), 7 § (televalvonta), 11 § (tekninen kuuntelu), 31 § (lähetyksen jäljentäminen) ja lakiehdotuksessa tietoliikennetiedustelusta siviilitiedustelussa tarkoitettu tietoliikennetiedustelu.

4.6 Siviilitiedustelussa saadun tiedon luovuttaminen rikostorjuntaan

Poliisilain 5 a luvun 44 §:ssä ehdotetaan säädettäväksi niin sanotusta palomuurista. Tiedustelutoimivaltuuksilla saatuja tietoja ei lähtökohtaisesti saisi käyttää muuhun tarkoitukseen kuin kansallisen turvallisuuden suojaamiseksi. Palomuurisäännöksessä säädettäisiin eräistä poikkeuksista käyttötarkoitussidonnaisuuteen. Pykälä sisältäisi osin myös suojelupoliisin poliisimiehen toimimisvelvollisuuden piiriin kuuluvia asioita.

Kyse olisi poikkeuksesta tiedustelumenetelmillä saadun tiedon käyttötarkoitussidonnaisuudesta. Asiaa koskeva sääntely on laadittu siten, että siinä tasapainoisella tavalla tulisi huomioitua yhtäältä tiedustelun rikostorjunnasta poikkeava käyttötarkoitus sekä toisaalta vakavien rikosten selvittämiseen ja etenkin sellaisten rikosten estämiseen liittyvä huomattava yhteiskunnallinen intressi.

Tiedustelussa ilmitulleiden lievien rikosten ilmoittaminen rikostorjuntaan ei saisi olla sillä tavalla automaattista, että tiedustelu tosiasiassa muodostuu tällaisten rikosten

estämisen ja selvittämisen keinoksi. Toisaalta verrattain lieviäkin rikoksia on voitava ilmoittaa rikostorjuntaviranomaisille, jos tämä tapauskohtaisesti on välttämätöntä tiedustelun tarkoituksena olevan kansallisen turvallisuuden suojaamiseksi. Kaikkein vakavimpien rikosten selvittäminen ja erityisesti ennalta estäminen puolestaan on yhteiskunnan kokonaisedun mukaista, mistä johtuen niiden ilmoittaminen rikostorjuntaan on syytä laajasti sallia. Ilmoittamista perustelee myös oikeudenmukaisuus ja vakavan rikoksen uhrin näkökulman huomioonottaminen.

Tietyin 44 §:ssä säädetyin edellytyksin tiedustelumenetelmällä saatua tietoa voisi luovuttaa esitutkintaviranomaiselle tai muulle toimivaltaiselle viranomaiselle. Rajoituksetta tietoliikennetiedustelulla saatua tietoa saataisiin luovuttaa syyttömyyttä tukevaksi selvitykseksi sekä hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi.

Tietyin 44 §:ssä säädetyin edellytyksin tiedustelumenetelmällä saatua tietoa voisi luovuttaa esitutkintaviranomaiselle tai muulle toimivaltaiselle viranomaiselle. Tiedustelumenetelmän käytöllä saatua tietoa saisi aina luovuttaa syyttömyyttä tukevaksi selvitykseksi sekä hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi

4.7 Ulkomaan tiedustelu ja kansainvälinen yhteistyö

Suomen turvallisuusympäristössä viime vuosina tapahtuneiden muutosten taustalla on sisäiseen ja kansalliseen turvallisuuteen kohdistuvien uhkien ja niihin liittyvien ilmiöiden kiihtyvä kansainvälistyminen ja tietoteknistyminen. Turvallisuusympäristössä tapahtuneet muutokset osaltaan ovat johtaneet siihen, ettei yksittäinen valtio kaikissa tilanteissa kykene torjumaan itseensä kohdistuvia uhkia vain omin toimenpitein. Muutos korostaa kansainvälisen tiedustelu- ja turvallisuustyön sekä siinä saatavan operatiivisen ja strategisen tiedon merkitystä. Toimialan operatiivinen ja strateginen kansainvälinen tiedonvaihto on lähes nelinkertaistunut 2000-luvulla.

Jos yhteiskuntaa halutaan menestyksellisesti turvata, suomalaisten turvallisuusviranomaisten on voitava hankkia tietoa myös ulkomaisilta toimijoilta. Ulkomaantiedustelulla tarkoitetaan kansallisen turvallisuuden kannalta olennaisen tiedon hankkimista ulkomaisista olosuhteista ja kohteista. Ulkomaantiedustelun tarkoituksena on tuottaa ylimmän valtionjohdon turvallisuuspoliittisen päätöksenteon sekä vakavien ulkoisten turvallisuusuhkien torjunnan kannalta välttämätöntä tietoa.

Ulkomaantiedustelun luonteesta johtuen toiminnan lähtökohtana on, että tarvittavat tiedot pyritään hankkimaan kevyimmällä mahdollisella keinolla. Käytännössä tiedustelu perustuu usein yhteistoimintaa läheisesti muistuttaviin toimintamalleihin. Kyse on kahden valtion viranomaisten välisestä vapaaehtoisuuteen perustuvasta tietojen ja näkökantojen vaihdosta, joka hyödyttää molempia osapuolia. Tiedonvaihto voi koskea esimerkiksi yhteisen mielenkiinnon kohteena olevia ilmiötä, yksittäisiä tapahtumia, havaintoja tai poliittisia mielialoja, joista tietoja antava osapuoli tarjoaa oman tulkintansa pyrkien vaikuttamaan vastaanottajaosapuolen näkemyksiin. Tällaisen molemminpuolisen tiedonvaihdon ohella ulkomaantiedustelutoiminta voi perustua tiedustelevan valtion yksipuoliseen toimintaan. Perustilanteessa toiminta pitää sisällään sen, että tiedustelevan valtion ulkomaille lähettämä henkilöstö virka-asemaansa perustuen tekee yleisiä havaintoja asemavaltion oloista sekä käy keskusteluja asemavaltion edustajien tai kansalaisten kanssa. Vaikka kyse ei tällöin ole asemavaltion kanssa nimenomaisesti sovitusta tietojenvaihdosta, tapahtuu toiminta monesti asemavaltion hiljaisen hyväksynnän turvin. Kaikki valtiot joutuvat tosiasiassa tiettyyn rajaan saakka sietämään maaperällään tapahtuvaa tiedustelua.

Tietyissä poikkeuksellisiksi luonnehdittavissa tilanteissa edellä kuvattu yhteistyötä korostava tai hiljaiseen hyväksyntään perustuva tiedustelu ei ole riittävää. Suomen kansallisen turvallisuuden kannalta kriittisen tärkeitä tietoja olisi tällaisissa tapauksissa voitava hankkia tarvittaessa myös salassa käytettävien tiedustelumenetelmien avulla.

Useat Euroopan valtiot ovat säätäneet ulkomaan tiedustelutoiminnastaan ja siinä käytettävistä toimivaltuuksista. Maittain vaihtelee, millä tarkkuudella yksittäisistä toimivaltuuksista on katsottu aiheelliseksi säätää. Ulkomaan tiedustelulla tarkoitettaisiin turvallisuusviranomaisten aktiivista toimintaa tiedon hankkimiseksi sellaisista ulkomailla oleskelevista yksittäisistä tai valtiollisista toimijoista, jotka saattavat uhata Suomen kansallista turvallisuutta tai muita yhteiskunnan elintärkeitä etuja.

Suomalaisilla tiedusteluviranomaisilla ei ole säädettyjä toimivaltuuksia hankkia tietoa ulkomailla. Turvallisuusympäristön muutoksesta johtuen ja hallituksen esityksessä HE 202/2017 vp mainituilla perusteilla olisi kuitenkin tarpeen säätää ulkomaantoimivaltuuksista eli ulkomaantiedustelusta. Ulkomaantoimivaltuudet ehdotetaan siviilitoiminnassa säädettäväksi suojelupoliisille ja ulkomaantiedustelussa ehdotettaisiin käytettäväksi poliisilakiehdotuksen 5 a luvussa säädettäviä keinoja. Kansainvälisestä yhteistyöstä ja sen yhteydessä käytettävistä tiedustelumenetelmistä säädettäisiin erikseen.

Esityksen kansainvälisestä vertailusta voidaan havaita, että ulkomailla tehtävää tiedonhankintaa koskeva päätöksenteko vaihtelee maittain. Päätöksenteosta voi vastata esimerkiksi tiedusteluviranomainen itse tai jokin poliittisesti vastuunalainen taho. Jos päätöksenteosta vastaa tiedusteluviranomainen, tapahtuu se yleensä valtiojohdon linjausten puitteissa. Tiedustelussa käytettävät menetelmät kohdistuvat vieraan valtion suvereniteettiin kohdemaassa ja myös mahdollisesti kolmannessa valtiossa, jonka kautta tiedonhankintaa tehdään. Tämän vuoksi ulkomaan tiedustelun poliittinen ulottuvuus korostuu. Tiedustelun mahdolliset vaikutukset ja riskit vaikuttaisivat päätöksentekomenettelyyn.

Ulkomailla tehtävästä siviilitiedustelusta ja tiedustelumenetelmän käytöstä päättäisi aina suojelupoliisin päällikkö. Suomalaisilla tuomioistuimilla ei ole toimivaltaa päättää menetelmien käytöstä Suomen alueen ulkopuolella eikä se tästä syystä tule kyseeseen päätöksentekotahona. Lisäksi ulkomaantiedustelun ulkopoliittisten herkkyyksien vuoksi on perusteltua, että riskin menetelmien käyttämisestä kantaisi ulkomaantiedustelua suorittava taho eli suojelupoliisi.

Siviili- ja sotilastiedustelutoiminnan yhteensovittamisesta säädettäisiin erikseen. Ulkomaantiedustelun ulkopoliittisia ulottuvuuksia käsiteltäisiin siten myös siviili- ja sotilastiedustelun yhteensovittamisen yhteydessä, jolloin mukana olisivat keskeiset ulkopoliittiset tahot.

Kansainvälisestä yhteistyöstä säädettäisiin erikseen ja tällöinkin ulkomailla suoritettavassa operaatiossa käytettävistä tiedustelumenetelmistä päättäisi suojelupoliisin päällikkö.

5 Oikeusturvajärjestelyt ja valvonta

Tiedustelutoiminnassa korostuvat oikeusturvajärjestelyjen riittävyys ja valvonnan tehokkuus. On tärkeää, että tiedusteluviranomaisella ei ole rajoittamatonta harkintavaltaa tiedonhankinnan kohdentamisessa. Yksi tapa rajoittaa viranomaisen harkintavaltaa on edellä kerrotulla tavalla osoittaa vakavinta puuttumista perusoikeussuojaan tarkoittava tiedustelumenetelmien käytöstä päättäminen tuomioistuimelle (muun muassa Weber ja Saravia v. Saksa). Ehdotuksen mukaan 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 pois lukien telekuuntelu ja sen sijasta toimitettava tietojen hankkiminen, jos kohteena on henkilö. Näissä tilanteissa lupa voitaisiin antaa enintään kolmeksi kuukaudeksi kerrallaan.

Säännösehdotuksilla kuuntelu- ja katselukiellosta, jäljentämis- ja tiedustelukiellosta, tiedustelutietojen hävittämisestä ja tiedustelumenetelmän käytöstä ilmoittamisesta turvattaisiin niin ikään oikeusturvan toteutumista. Oikeus saada tieto tiedustelun kohteeksi joutumisesta on tärkeää, jotta henkilö ylipäätään ymmärtäisi hakea

oikeussuojaa (Poliisilaki 5 a luku 47 § ja Laki tietoliikennetiedustelusta siviilitiedustelussa 20 §). Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta ja teknisestä tarkkailusta sekä tietoliikennetiedustelusta olisi viipymättä ilmoitettava kohteelle, kun tiedonhankinnan tarkoitus on saavutettu. Muiden menetelmien käytöstä olisi ilmoitettava, jos asiassa aloitetaan esitutkinta. Ehdotettu sääntely antaisi mahdollisuuden jokaiselle, joka epäilee joutuneensa yksityiselämän suojan loukkauksen kohteeksi, saada asiansa käsitellyksi asianmukaisesti siten kuin perustuslain 21 §:ssä edellytetään. Kyseistä ilmoitusta voitaisiin tuomioistuimen päätöksellä lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedustelumenetelmän käytön turvaamiseksi, kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus voitaisiin myös tuomioistuimen päätöksellä jättää tekemättä, jos e on välttämätöntä kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi.

Asianosaisjulkisuus on tiedonhankinnan kohteen kannalta tärkeä oikeusturvatae. Kaikkien tiedustelumenetelmien käyttö olisi asianosaisjulkista siitä lähtien, kun henkilö on saanut ilmoituksen menetelmän käytöstä. Kaikkia tiedustelumenetelmäasioita koskisi oikeudenkäynnissä diaari-, asiakirja-, käsittely-, ratkaisu- ja asianosaisjulkisuus.

Tiedustelutoiminnan valvonnan tehokkuus edellyttää, että valvontaelimillä on pääsy kaikkeen tiedustelussa kertyneeseen aineistoon sekä oikeus tarkastaa tietoja ja asiakirjoja. Siksi tiedustelumenetelmiä koskisi viivytyksetön pöytäkirjaamisvelvoite. Tästä säädettäisiin tarkemmin asetuksella vastaavalla tavalla kuin mitä pöytäkirjaamisesta säädetään esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta annetussa asetuksessa (122/2014).

Tiedustelutoiminnan ulkoisesta laillisuusvalvonnasta huolehtisi ylimpien laillisuusvalvojien lisäksi uusi viranomainen, tiedusteluvaltuutettu, joka valvoisi tiedustelutoimintaa reaaliaikaisesti. Reaaliaikaisen valvonnan mahdollistamiseksi säädettäisiin velvoitteesta antaa tieto tiedusteluvaltuutetulle tiedustelumenetelmiä koskevista tuomioistuimen päätöksistä ja luvista mahdollisimman pian niiden antamisen päätöksen jälkeen. Lisäksi suojelupoliisin olisi mahdollisimman pian ilmoitettava tiedusteluvaltuutetulle päätöksestä, joka koskee muuta kuin tuomioistuimen päätöksentekotoimivaltaan kuuluvaa tiedustelumenetelmää, siviilitiedustelun suojaamista, ilmaisukieltoa, rikostorjuntaan luovutettavan tiedon siirtämisen lykkäämistä.

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.

Tiedustelutoiminnan oikeudellisesta valvonnasta sisäasiainhallinnossa huolehtisivat suojelupoliisi ja sisäministeriö. Näiden harjoittamaa laillisuusvalvontaa olisi tarkoitus vahvistaa uusilla henkilöstöresursseilla ja tehostaa valvontatoimia reaaliaikaistamalla. Sisäministeriön tulisi antaa eduskunnan oikeusasiamiehelle ja tiedusteluvaltuutetulle vuosittain kertomus tiedustelumenetelmien ja niiden suojaamisen käytöstä ja valvonnasta.

EIT on pitänyt tärkeänä, että tiedustelun valvontaan osallistuvat myös kansanedustuslaitoksen jäsenet. Tiedustelutoiminnan parlamentaarinen valvonta ehdotetaan annettavaksi uuden tiedusteluvalvontavaliokunnan tehtäväksi. Tiedusteluvalvontavaliokunta toimisi osana eduskunnan valiokuntalaitosta. Tiedusteluvaliokunnalla olisi valvontatehtävänsä hoitamiseksi tiedonsaantioikeuksien lisäksi oikeus saada selvityksiä muun muassa tiedusteluvaltuutetulta ja muilta viranomaisilta.