Puolustusministeriö
Försvarsministeriet
Ministry of Defence

EHDOTUS SOTILASTIEDUSTELUA KOSKEVAKSI LAINSÄÄDÄNNÖKSI

FÖRSLAG TILL LAGSTIFTNING OM MILITÄR UNDERRÄTTELSEVERKSAMHET

Työryhmän mietintö
Arbetsgruppsbetänkande

Puolustusministeriö | 2017

Ehdotus sotilastiedustelua koskevaksi lainsäädännöksi

Förslag till lagstiftning om militär underrättelseverksamhet

Työryhmän mietintö
Arbetsgruppsbetänkande

ISBN verkkojulkaisu: 978-951-25-2899-8

ISBN painettu: 978-951-25-2898-1

Painopaikka ja -aika
Lönnberg Print & Promo, Helsinki 2017

KUVAILULEHTI

<table>
<tr><td>Julkaisija</td><td colspan="2">Puolustusministeriö</td><td>Julkaisuaika
19.4.2017</td></tr>
<tr><td>Tekijä(t)</td><td colspan="3">Työryhmä
Hanna Nordström (puheenjohtaja)
Kosti Honkanen (sihteeri)
Juho Melaluoto (sihteeri)
Teija Pellikainen (sihteeri)
Minnamaria Nurminen (sihteeri)
Terhi Vira-Klockars (sihteeri)
Martti J. Kari (asiantuntija)</td></tr>
<tr><td>Julkaisun nimi</td><td colspan="3">Ehdotus sotilastiedustelua koskevaksi lainsäädännöksi. Työryhmän mietintö</td></tr>
<tr><td>Tiivistelmä</td><td colspan="3">Puolustusministeriö asetti 1.10.2015 hankkeen valmistelemaan ehdotus sotilastiedustelua koskevaksi lainsäädännöksi. Tavoitteena on ollut parantaa Puolustusvoimien tiedonhankintaa Puolustusvoimien tehtäviin liittyvistä vakavista kansainvälisistä uhkista ja ajanmukaistaa Puolustusvoimien tiedustelua koskevat toimivaltuudet.

Työryhmä ehdottaa, että säädettäisiin uusi laki sotilastiedustelusta.

Laissa ehdotetaan säädettäväksi sotilastiedustelun tarkoituksesta, kohteista ja tiedustelutoiminnassa noudatettavista periaatteista sekä tiedustelutoiminnan ohjauksesta ja valvonnasta puolustushallinnossa. Sotilastiedusteluviranomaisia olisivat Puolustusvoimien pääesikunta ja Puolustusvoimien tiedustelulaitos.

Sotilastiedusteluviranomaisille ehdotetaan toimivaltuuksia henkilötiedusteluun, radiosignaalitiedusteluun ja ulkomaan tietojärjestelmätiedusteluun sekä tietoliikennetiedusteluun Suomen rajan ylittävässä tietoliikenteessä. Toimivaltuudet olisivat viranomaisten käytettävissä Suomessa ja ulkomailla.

Laissa säädettäisiin myös sotilastiedusteluviranomaisten yhteistoiminnasta muiden viranomaisten kanssa, kansainvälisestä yhteistyöstä sekä tiedustelukielloista ja tietojen käsittelystä.

Laki ehdotetaan tulemaan voimaan mahdollisimman pian lakiehdotuksen säätämisjärjestystä koskevat seikat huomioon ottaen.</td></tr>
<tr><td>Asiasanat</td><td colspan="3">lainsäädäntö, sotilastiedustelu, Puolustusvoimat, henkilötiedustelu, tietoliikennetiedustelu, tietojärjestelmätiedustelu</td></tr>
<tr><td>Asianumerot</td><td colspan="3">HARE PLM004:00/2015</td></tr>
<tr><td></td><td colspan="2">ISBN (painettu)
978-951-25-2898-1</td><td>ISBN (verkkojulkaisu)
978-951-25-2899-8</td></tr>
<tr><td></td><td>Sivumäärä
391</td><td>Kieli
suomi</td><td>URN-tunnus
URN:ISBN: 978-951-25-2899-8</td></tr>
<tr><td>Julkaisujen myynti/ jakelu</td><td colspan="3">Julkaisu on saatavissa internetistä osoitteesta www.defmin.fi
Sähköinen versio: julkaisut.valtioneuvosto.fi
Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi</td></tr>
</table>

PRESENTATIONSBLAD

<table>
<tr><td>Utgivare</td><td colspan="2">Försvarsministeriet</td><td>Utgivningsdatum
19.4.2017</td></tr>
<tr><td>Författare</td><td colspan="3">Arbetsgruppen
Hanna Nordström (ordförande)
Kosti Honkanen (sekreterare)
Juho Melaluoto (sekreterare)
Teija Pellikainen (sekreterare)
Minnamaria Nurminen (sekreterare)
Terhi Vira-Klockars (sekreterare)
Martti J. Kari (sakkunnig)</td></tr>
<tr><td>Publikationens namn</td><td colspan="3">Förslag till lagstiftning om militär underrättelseverksamhet. Arbetsgruppsbetänkande</td></tr>
<tr><td>Referat</td><td colspan="3">Försvarsministeriet tillsatte 1.10.2015 ett projekt för att bereda ett förslag till lagstiftning om militär underrättelseverksamhet. Målet har varit att förbättra Försvarsmaktens underrättelseinhämtning om allvarliga internationella hot som sammanhänger med Försvarsmaktens uppgifter och att uppdatera Försvarsmaktens befogenheter som gäller underrättelseverksamhet.

Arbetsgruppen föreslår att en ny lag om militär underrättelseverksamhet ska stiftas.

Det föreslås att i lagen ska föreskrivas om syftet med och objekten för den militära underrättelseverksamheten och om de principer som ska iakttas i underrättelseverksamheten samt om styrningen och övervakningen av underrättelseverksamheten inom försvarsförvaltningen. Militärunderrättelsemyndigheter ska vara Försvarsmaktens huvudstab och Försvarsmaktens underrättelsetjänst.

Militärunderrättelsemyndigheterna föreslås få befogenheter gällande personbaserad underrättelseinhämtning, radiosignalspaning och underrättelseinhämtning som avser datasystem i utlandet samt underrättelseinhämtning som avser datatrafik i sådan datatrafik som överskrider Finlands gräns. Befogenheterna ska få användas av myndigheterna både i Finland och i utlandet.

I lagen ska också föreskrivas om militärunderrättelsemyndigheternas samverkan med andra myndigheter, om internationellt samarbete samt om förbud mot underrättelseinhämtning och behandling av uppgifter.

Det föreslås att lagen ska träda i kraft så snart som möjligt med beaktande av de omständigheter som gäller den föreslagna lagens lagstiftningsordning.</td></tr>
<tr><td>Nyckelord</td><td colspan="3">lagstiftning, militär underrättelseverksamhet, Försvarsmakten, personbaserad underrättelseinhämtning, underrättelseinhämtning som avser datatrafik, underrättelseinhämtning i informationssystem</td></tr>
<tr><td>Ärendenummer</td><td colspan="3">HARE PLM004:00/2015</td></tr>
<tr><td></td><td colspan="2">ISBN (tryckt)
978-951-25-2898-1</td><td>ISBN (webbpublikation)
978-951-25-2899-8</td></tr>
<tr><td></td><td>Sidantal
391</td><td>Språk
finska</td><td>URN
URN:ISBN: 978-951-25-2899-8</td></tr>
<tr><td>Beställningar/
distribution</td><td colspan="3">Publikationen är tillgänglig på internet på adressen www.defmin.fi
Elektronisk version: julkaisut.valtioneuvosto.fi
Beställningar: julkaisutilaukset.valtioneuvosto.fi</td></tr>
</table>

DESCRIPTION

<table>
<tr><td>Published by</td><td colspan="2">Ministry of Defence</td><td>Date of publication
19.4.2017</td></tr>
<tr><td>Authors</td><td colspan="3">Working group
Hanna Nordström (Chair)
Kosti Honkanen (Secretary)
Juho Melaluoto (Secretary)
Teija Pellikainen (Secretary)
Minnamaria Nurminen (Secretary)
Terhi Vira-Klockars (Secretary)
Martti J. Kari (Specialist)</td></tr>
<tr><td>Title of publication</td><td colspan="3">Proposal for legislation on military intelligence. A working group report</td></tr>
<tr><td>Abstract</td><td colspan="3">On 1 October 2015, the Ministry of Defence launched a project to draft a proposal for legislation on military intelligence with the aim of improving the Defence Forces' intelligence gathering on serious international threats related to the Defence Forces' tasks and to modernise the Defence Forces' powers related to intelligence.

The working group proposes that a new act on military intelligence be passed.

It is proposed that provisions on the purpose and targets of military intelligence, the principles complied with in intelligence activities as well as the steering and oversight of intelligence activities in the defence administration be contained in the act. Military intelligence authorities would include the Defence Command of the Defence Forces and the Defence Force Intelligence Agency.

It is proposed that powers to gather human intelligence, signals intelligence and foreign information systems intelligence as well as telecommunications intelligence in traffic crossing the Finnish borders be granted to the military intelligence authorities. The authorities would have these powers both in Finland and abroad.

The act would also contain provisions on military intelligence authorities' cooperation with other authorities, international cooperation and prohibitions on intelligence gathering and data processing.

It is proposed that the act enter into force as soon as possible, taking issues related to the procedure for enactment into account.</td></tr>
<tr><td>Keywords</td><td colspan="3">legislation, military intelligence, Defence Forces, human intelligence, telecommunications intelligence, information systems intelligence</td></tr>
<tr><td>Reference numbers</td><td colspan="3">HARE PLM004:00/2015</td></tr>
<tr><td></td><td colspan="2">ISBN (print)
978-951-25-2898-1</td><td>ISBN (electronic version)
978-951-25-2899-8</td></tr>
<tr><td></td><td>Number of pages
391</td><td>Language
Finnish</td><td>URN
URN:ISBN: 978-951-25-2899-8</td></tr>
<tr><td>Sale/Distribution of publications</td><td colspan="3">The publication is available on the internet at www.defmin.fi
Online version: julkaisut.valtioneuvosto.fi
Publication sales: julkaisutilaukset.valtioneuvosto.fi</td></tr>
</table>

Puolustusministeriölle

Puolustusministeriö asetti 1.10.2015 työryhmän valmistelemaan ehdotus sotilastiedustelua koskevaksi lainsäädännöksi eli säännökset muun muassa puolustusvoimien tiedustelun tarkoituksesta, toimivaltaisista viranomaisista sekä niiden tehtävistä ja toimivaltuuksista, ohjauksesta ja valvonnasta, tietojen käsittelystä ja rekisteröinnistä sekä viranomaisten yhteistyöstä. Työryhmän tuli saada työnsä valmiiksi viimeistään 31.12.2016.

Puolustusministeriö jatkoi 7.12.2016 työryhmän määräaikaa 28.2.2017 saakka.

Sotilastiedustelua ja samanaikaisesti sisäministeriössä valmisteltavana olevien siviilitiedustelua koskevien säännösten tuli olla keskenään yhteen sovitettuja.

Hankkeessa tuli ottaa huomioon tiedonhankintalakityöryhmän mietintö ja siitä saatu lausuntopalaute.

Työryhmän mietintö tuli toimeksiannon mukaan laatia hallituksen esityksen muotoon.

Työryhmän puheenjohtajaksi määrättiin hallitusneuvos, lainsäädäntöjohtajana Hanna Nordström ja varapuheenjohtajaksi yksikön johtaja Timo Junttila (28.2.2016 saakka) ja yksikön johtaja Heikki Välivehmas (1.3.2016 lähtien) puolustusministeriöstä.

Työryhmän jäseniksi kutsuttiin oikeudellinen neuvonantaja Minna Hulkkonen tasavallan presidentin kansliasta, valtioneuvoston turvallisuusjohtaja Jari Ylitalo valtioneuvoston kansliasta, ulkoasiainneuvos Marja Lehto ulkoasiainministeriöstä, lainsäädäntöneuvos Liisa Vanhala oikeusministeriöstä (20.3.2016 saakka), lainsäädäntöneuvos Timo Kerttula (14.9.2016 saakka) ja poliisijohtaja Petri Knape (15.9.2016 lähtien) sisäministeriöstä sekä tiedustelupäällikkö, kenraalimajuri Harri Ohra-aho ja puolustusvoimien asessori Tuija Sundberg pääesikunnasta.

Työryhmän pysyviksi asiantuntijoiksi kutsuttiin asiantuntija Mika Susi Elinkeinoelämän keskusliitto EK:sta, OTT, kansainvälisen oikeuden dosentti Jarna Petman Helsingin yliopistosta, yksikön päällikkö Mikko Kinnunen ulkoasiainministeriöstä, apulaispäällikkö Olli Kolstela suojelupoliisista, eversti Pekka Turunen pääesikunnasta, kauppatieteiden maisteri Teemu Karnio puolustusvoimista, osastopäällikkö, ylijohtaja Juhapekka Ristola (31.12.2015 saakka), osastopäällikkö Olli-Pekka Rantala (1.1.2016 - 14.9.2016) ja osastopäällikkö Laura Vilkkonen liikenne- ja viestintäministeriöstä (15.9.2016 lähtien).

Työryhmän sihteerinä ovat toimineet hallitussihteeri Kosti Honkanen, vanhempi hallitussihteeri Minnamaria Nurminen ja hallitussihteeri Teija Pellikainen puolustusministeriöstä, sekä sotilaslakimies Juho Melaluoto (31.1.2017 saakka) ja sotilaslakimies Terhi Vira-Klockars pääesikunnasta. Sihteeristön työhön on osallistunut asiantuntijana apulaistiedustelupäällikkö, eversti Martti J. Kari pääesikunnasta.

Siviili- ja sotilastiedustelua sekä perustuslakisääntelyä koskevia lainsäädäntöhankkeita varten asetettiin 10.12.2015 parlamentaarinen seurantaryhmä, jotta eduskunta olisi jatkuvasti tietoinen hankkeiden etenemisestä.

Työryhmä on pitänyt 30 kokousta. Työryhmä on työnsä aikana kuullut seuraavia henkilöitä.

oikeuskansleri Jaakko Jonkka
apulaisoikeuskanslerin sijainen Kimmo Hakonen, oikeuskanslerinvirasto
eduskunnan oikeusasiamies Petri Jääskeläinen
tietosuojavaltuutettu Reijo Aarnio
laamanni Tuomas Nurmi, Helsingin käräjäoikeus
laamanni Seppo Karvonen, Vantaan käräjäoikeus
professori emeritus (julkisoikeus) Teuvo Pohjolainen
professori Tuomas Ojanen, Helsingin yliopisto
yliopistonlehtori Jukka Viljanen, Tampereen yliopisto

Lisäksi työryhmä on kuullut asiantuntijoita tietoliikennetiedustelun teknisistä toteuttamisvaihtoehdoista.

Työryhmä on järjestänyt yleisen kuulemistilaisuuden elinkeinoelämän edustajille 23.11.2016 sekä kansalaisjärjestöille ja muille sidosryhmille 24.11.2016.

Työryhmän mietintö on laadittu hallituksen esityksen muotoon. Mietinnössä ehdotetaan säädettäväksi uusi laki sotilastiedustelusta, joka sisältäisi säännökset sotilastiedustelun tarkoituksesta, kohteista ja tiedustelutoiminnassa noudatettavista periaatteista, toiminnan ohjauksesta sekä valvonnasta puolustushallinnossa. Laissa säädettäisiin sotilastiedusteluviranomaisten toimivaltuuksista, sotilastiedusteluviranomaisten yhteistoiminnasta muiden viranomaisten kanssa, kansainvälisestä yhteis-työstä sekä tiedustelukielloista ja tietojen käsittelystä.

Mietinnön ehdotukset on sovitettu yhteen siviilitiedustelua koskevaa lainsäädäntöä valmistelemaan asetetun sisäministeriön työryhmän ehdotusten kanssa.

Ehdotuksia on tarpeellisilta osin sovitettu yhteen myös perustuslain tarkistamista selvittäneen oikeusministeriön asettaman asiantuntijatyöryhmän ehdotuksen (Luottamuksellisen viestin salaisuus. Perustuslakisäänteln tarkistaminen. Oikeusministeriö 41/2016) sekä siviili- ja sotilastiedustelutoiminnan valvonnan järjestämistä koskevan oikeusministeriön lainsäädäntöhankkeen kanssa.

Saatuaan työnsä valmiiksi työryhmä luovuttaa kunnioittavasti mietintönsä puolustusministeriölle.

Helsingissä 19.4.2017

Hanna Nordström Heikki Välivehmas

Minna Hulkkonen Petri Knape Marja Lehto

Harri Ohra-aho Tuija Sundberg Jari Ylitalo

Kosti Honkanen Minnamaria Nurminen

Teija Pellikainen Terhi Vira-Klockars

SISÄLLYS

TIIVISTELMÄ

Taustaa

Puolustusministeriö asetti 1.10.2015 työryhmän, jonka tehtävänä oli valmistella ehdotus sotilastiedustelua koskevaksi lainsäädännöksi eli perussäännökset puolustusvoimien tiedustelutoiminnan tarkoituksesta, toimivaltaisista viranomaisista sekä niiden tehtävistä ja toimivaltuuksista, tiedustelun ohjauksesta ja valvonnasta, tietojen käsittelystä sekä viranomaisten yhteistyöstä.

Sotilastiedustelua koskevan lainsäädännön valmistelu perustuu pääministeri Juha Sipilän hallituksen ohjelmaan, jonka mukaan hallitus esittää säädösperustaa ulkomaantiedustelulle ja tietoliikennetiedustelulle.

Sisäministeriö asetti tätä tarkoitusta varten siviilitiedustelua ja oikeusministeriö siviili- ja sotilasviranomaisten tiedustelutoiminnan valvontaa koskevaa lainsäädäntöä valmistelevat työryhmät.

Oikeusministeriön asettama asiantuntijatyöryhmä selvitti myöhemmin asetettavaa parlamentaarista valmistelua varten perustuslain tarkistamista siten, että lailla voitaisiin säätää tarpeellisiksi katsottavien edellytysten täyttyessä kansallisen turvallisuuden suojaamiseksi välttämättömistä rajoituksista luottamuksellisen viestin salaisuuden suojaan.

Sääntelyn tarkistamisen tarve

Suomen turvallisuusympäristö on muuttunut nopeasti muun muassa globalisoitumisesta ja digitalisaation kehityksestä johtuen. Sodankäynnin ja muun vaikuttamisen raja hämärtyy käytettäessä poliittisia ja taloudellisia painostuskeinoja, informaatio-operaatioita sekä hybridivaikuttamisen keinoja. Merkittäviin uhkiin liittyvä tieto siirtyy yhä enemmän tietoverkkoon.

Puolustusvoimien lakisääteisten tehtävien hoitaminen edellyttää tiedustelua. Sotilastiedustelu on keskeinen osa Suomen puolustusvalmiutta. Sotilastiedustelusta ei kuitenkaan ole nimenomaisia säännöksiä puolustusvoimia koskevassa lainsäädännössä. Suomessa ei ole myöskään sääntelyä siitä, mihin tiedustelutoiminnalla pyritään tai millaista tiedustelutoimintaa voidaan harjoittaa.

Puolustusvoimien viranomaisten salaiset tiedonhankintatoimivaltuudet rajoittuvat rikosten estämiseen ja paljastamiseen. Voimassa oleva lainsäädäntö ei mahdollista sitä, että tietoa voitaisiin hankkia muuten kuin silloin, kun on kyse rikoksesta ja tiedonhankinnan kohteena aina tietty henkilö ja tämän toiminta.

Puolustusvoimien nykyisillä toimivaltuuksilla ei voida riittävän tehokkaasti ja riittävän varhaisessa vaiheessa hankkia tietoa sotilaallisesta toiminnasta tai Suomeen kohdistuvista ulkoisista uhkista sotilaallisen ennakkovaroituksen antamiseksi. Puolustusvoimat ei voi ajoissa ryhtyä uhkien torjumisen edellyttämiin toimenpiteisiin. Ylimmän valtionjohdon ja sotilaallisen päätöksenteon tueksi on kyettävä tuottamaan objektiivista, varmennettua ja analysoitua tietoa. Puolustusvoimien tiedonhankintatoimivaltuudet ovat puutteellisia toiminnan yhteiskunnalliseen merkittävyyteen nähden sekä muihin maihin verrattuna. Tämän vuoksi sotilastiedusteluviranomaisten tiedonhankintamenetelmiä tulee kehittää.

Työryhmän ehdotus

Työryhmä on valmistellut ehdotuksen uudeksi sotilastiedustelua koskevaksi laiksi. Lakia sovellettaisiin Puolustusvoimien tiedustelutoimintaan eli sotilastiedusteluun, jolla hankitaan, tutkitaan ja hyödynnetään puolustusvoimista annetussa laissa säädettyihin puolustusvoimien tehtäviin liittyvää tietoa Suomen ulko-, turvallisuus- ja puolustuspolitiikan tueksi ja Suomeen kohdistuvien ulkoisten uhkien kartoittamiseksi. Tietoa hankittaisiin julkisista ja ei-julkisista tietolähteistä. Toimivaltuuksien käytön tulisi olla laissa säädettyjen yleisten periaatteiden, kuten suhteellisuusperiaatteen ja vähimmän haitan periaatteen, mukaisia.

Sotilastiedustelun tehtävänä on muodostaa ja ylläpitää sotilaallisen päätöksenteon edellyttämää laaja-alaista sotilasstrategista tilannekuvaa. Tarvittaessa on kyettävä antamaan ennakkovaroitus Suomeen kohdistuvasta uhkasta. Sotilastiedustelutoiminnan ensisijaisena tarkoituksena ei ole hankkia tietoja rikosten estämiseksi taikka tiedon hankkiminen rikosten valmistelusta tai suunnittelusta. Yleistoimivalta rikosten ennalta estämisessä, selvittämisessä ja paljastamisessa on poliisilla.

Ainoastaan sotilasviranomaisella on riittävä tietotaito maanpuolustukseen kohdistuvista uhkista ja sotilaallisesta toimintakentästä sekä toimintakentän tapojen ja käytäntöjen tuntemus. Tiedustelutoiminnan asianmukainen toteuttaminen edellyttää tätä taustaosaamista, jotta sotilastiedustelu pääsee hyödyntämään maanpuolustuksen kannalta kaikkein kriittisintä tietoa, eikä siten ole mahdollista, että sotilastiedustelua suorittaisi muu viranomainen.

Sotilastiedustelulla hankittaisiin tietoa kotimaassa ja ulkomailla sotilaallisesta toiminnasta ja ulkomaisesta tiedustelutoiminnasta, valtio- ja yhteiskuntajärjestystä uhkaavasta toiminnasta, joukkotuhoaseista, sotatarvikkeiden kehittämisestä ja levittämisestä, valtioon tai yhteiskunnan elintärkeisiin toimintoihin kohdistuvista vakavista uhkista, vieraan valtion suunnitelmista tai toiminnasta, joka voisi aiheuttaa vahinkoa Suomen kansainvälisille suhteille taikka muille tärkeille eduille, kansainvälistä rauhaa ja turvallisuutta uhkaavista kriiseistä, kansainvälisten kriisinhallintaoperaatioiden turvallisuuteen kohdistuvista uhkista sekä puolustusvoimien kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuuteen kohdistuvista uhkista.

Ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteinen kokous käsittelisi valmistelevasti vuosittain sotilastiedustelun painopisteet.

Sotilastiedusteluviranomaisia olisivat pääesikunta ja Puolustusvoimien tiedustelulaitos. Palveluksessa olevat reserviläiset voisivat osallistua tiedustelutehtävän suorittamiseen sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa laissa säädetyin edellytyksin.

Tiedustelutehtävät antaa pääesikunnan tiedustelupäällikkö. Tietopyyntöjä sotilastiedusteluviranomaiselle voisivat tehdä tasavallan presidentti sekä valtioneuvoston kanslia, ulkoasiainministeriö ja puolustusministeriö. Sotilas- ja siviilitiedustelutoimintaa sovitettaisiin edellä mainittujen viranomaisten ja sisäministeriön sekä tarvittaessa muiden ministeriöiden ja viranomaisten kesken. Sotilastiedusteluviranomainen voisi toimia tiedustelutoiminnan asianmukaiseksi suorittamiseksi yhteistyössä suojelupoliisin kanssa. Laissa olisi säännökset kansainvälisen yhteistyön edellytyksistä.

Laissa säädettäisiin sotilastiedusteluviranomaisten toimivaltuuksista henkilötiedustelussa ja ulkomaan tietojärjestelmätiedustelussa. Lain kokonaisuuden kannalta olisi myös syytä säätää radiosignaalitiedustelusta. Turvallisuus - ja resurssinäkökulma huomioon ottaen ulkoisiin uhkiin liittyvää henkilötiedustelua tulisi olla mahdollista suorittaa myös Suomessa. Tiedustelumenetelmät vastaisivat nykyisin viranomaisilla käytössä olevia salaisia tiedonhankintakeinoja. Edellytykset toimivaltuuksien käyttämiselle ja käyttötarkoitus eroaisivat kuitenkin rikostorjunnasta.

Laissa ehdotetaan seuraavia toimivaltuuksia: suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen laitetarkkailu, telekuuntelu ja tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, teleosoitteen tai telepäätelaitteet tunnistamistietojen hankkiminen, peitetoiminta, tietolähdetoiminta, tietolähteen turvaaminen, valeosto, paikkatiedustelu, jäljentäminen ja kirjeen tai muun lähetyksen pysäyttäminen sekä jäljentäminen.

Tiedonhankintaa tulisi voida suojata siten, että se pidettäisiin salassa tiedon hankkijan tai tiedon luovuttajan turvallisuuden varmistamiseksi, tiedonhankinnan toteuttamisen edellyttämän luottamuksen hankkimiseksi ja tiedonhankintatoiminnan paljastumisen estämiseksi. Myös tiedustelua suorittavan virkamiehen henkilöllisyys ja taustaorganisaatio olisi tarpeen mukaan voitava pitää salassa.

Radiosignaalitiedustelussa tiedonhankinta kohdistuisi Suomen alueen ulkopuolelta lähtöisin olevaan tai Suomen alueen ulkopuolelle lähteviin radioaaltoihin, jolloin kyse ei olisi luottamuksellisen viestin salaisuuden suojaamasta viestiliikenteestä.

Ulkomaan tietojärjestelmätiedustelulla tarkoitettaisiin sotilastiedusteluviranomaisten aktiivista toimintaa tiedon hankkimiseksi tietoverkon välityksellä ulkomaisesta tietojärjestelmästä. Tietojärjestelmätiedustelu saattaisi tapauskohtaisesti edellyttää teknisen suojauksen ohittamista.

Lakiin ehdotetaan sisällytettäväksi säännökset tietoliikennetiedustelusta eli viestintäverkossa Suomen rajan ylittävään tietoliikenteeseen kohdistuvasta, tietoliikenteen automatisoituun erotteluun perustuvasta teknisestä tiedonhankinnasta sekä hankitun tiedon käsittelystä.

Tietoliikennetiedustelun keskeisenä edellytyksenä voidaan pitää sitä, että ne uhat, joita tiedonhankinta saa koskea, määritellään mahdollisimman selkeästi ja suppeasti. Kansainvälisten ihmisoikeussopimusten mukaan tietoliikennetiedustelu ei voi olla keino hankkia tietoa mistä tahansa uhasta tai riskistä. Tästä syystä ne uhat ja tilanteet, joita tiedustelu saa koskea, olisi lueteltu laissa niin täsmällisesti kuin mahdollista. Euroopan ihmisoikeustuomioistuimen ratkaisukäytännön mukaan lainsäädännöstä on riittävän selkeästi käytävä ilmi, missä olosuhteissa ja millä edellytyksellä kansalaiset voivat joutua viranomaisten salaisesti toteutettavan tarkkailun kohteeksi. Nämä reunaehdot otettaisiin huomioon tietoliikennetiedustelun toteuttamista harkittaessa. Tietoliikenteestä on kyettävä erottamaan ne tiedot, joilla on merkitystä itse tiedustelutehtävän kannalta.

Tietoliikennetiedustelu käsittäisi kolme eri toimivaltuutta: teknisten tietojen käsittely, valtiolliseen toimijaan ja muuhun kuin valtiolliseen toimijaan kohdistuva tietoliikennetiedustelu. Tietoliikennetiedusteluun vaadittaisiin aina tuomioistuimen lupa.

Valtiollisen toimijan tietoliikenteeseen kohdistuvan tiedustelun edellytyksenä olisi, että sillä voitaisiin olettaa saatavan tietoa tiedustelutehtävän kannalta. Muuhun kuin valtiolliseen toimijaan kohdistuvan tietoliikennetiedustelun edellytyksenä olisi, että sillä saatavien tietojen voitaisiin olettaa olevan välttämättömiä tiedustelutehtävän kannalta.

Yksityisille tahoille ei ehdotettaisi velvollisuutta luovuttaa salausavaimia tai asentaa ohjelmistoihin ja laitteistoihin takaportteja. Tietoliikennetiedustelu edellyttäisi, että rajat ylittävien viestintäverkon osien omistajille asetetaan velvoite osoittaa liityntäpisteet sekä antaa tiedot tietoliikennetiedustelun kohdistamiseksi tietoliikennetiedustelun toteuttamisesta vastaavalle viranomaiselle. Viestintäverkon osien omistajilla olisi oikeus saada valtion varoista korvaus viranomaisten avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista.

Koska sotilastiedustelun tehtävänä olisi hankkia tietoa ainoastaan laissa määritellyssä, puolustusvoimien lakisääteisiin tehtäviin liittyvässä tarkoituksessa, tiedustelutietojen antamisen muuhun käyttöön olisi tarkoin rajattua. Esitutkintaviranomaiselle olisi velvollisuus ilmoittaa, jos on syytä epäillä, että on tapahtunut erittäin vakava rikos. Tietoja voidaan ilmoittaa turvallisuutta vaarantavan rikoksen estämiseksi. Sotilastiedusteluviranomaisella olisi oikeus tietyissä tilanteissa ilmoittaa havaitsemistaan haitallisesta tietokoneohjelmasta tai antaa tietoja huomattavan varallisuusvahingon estämiseksi yksityiselle toimijalle.

Sotilastiedustelutoiminnan lainmukaisuutta ohjaisi ja valvoisi puolustusvoimissa puolustusvoimien asessori. Sisäisen valvonnan lisäksi toiminnan lainmukaisuutta valvoisi erityinen puolustushallinnon ulkopuolinen valvontaviranomainen. Toimintaa valvottaisiin myös parlamentaarisesti. Sotilas- ja siviilitiedustelun yhteisen ulkoisen valvontaviranomaisen tehtävistä ja toimivaltuuksista sekä parlamentaarisesta valvonnasta säädettäisiin erikseen. Puolustusministeriöllä olisi oikeus saada puolustusvoimilta tietoa merkittävistä sotilastiedusteluun liittyvistä asioista ja tarkastaa tiedonhankintamenetelmien käyttöä koskevia asiakirjoja. Tarkoituksena ei olisi rajoittaa ylimpien laillisuusvalvojien valvontatehtäviä.

Lakiehdotuksen henkilörekisterejä koskevat säännökset tullaan jatkovalmistelussa siirtämään vireillä olevan henkilötietojen käsittelyä puolustushallinnossa koskevan lainsäädännön kokonaisuudistuksen yhteydessä laadittavaan sääntelyyn.

Laki ehdotetaan tulemaan voimaan mahdollisimman pian lakiehdotuksen säätämisjärjestystä koskevat seikat huomioon ottaen.

SAMMANDRAG

Bakgrund

Försvarsministeriet tillsatte den 1 oktober 2015 en arbetsgrupp, som fick till uppgift att bereda ett förslag till lagstiftning om militär underrättelseverksamhet, dvs. grundläggande bestämmelser om syftet med försvarsmaktens underrättelseverksamhet, behöriga myndigheter samt deras uppgifter och befogenheter, styrningen och övervakningen av underrättelseverksamheten, behandlingen av uppgifter samt myndigheternas samarbete.

Beredningen av lagstiftningen om den militära underrättelseverksamheten grundar sig på statsminister Juha Sipiläs regeringsprogram, enligt vilket regeringen föreslår att underrättelse utomlands och datatrafikspaning ska basera sig på lagstiftning.

För detta syfte tillsatte inrikesministeriet en arbetsgrupp för att bereda lagstiftning om civil underrättelseinhämtning och justitieministeriet en arbetsgrupp för att bereda lagstiftning om övervakningen av de civila och de militära myndigheternas underrättelseinhämtning.

En sakkunnigarbetsgrupp som tillsatts av justitieministeriet har för den parlamentariska beredning som tillsätts senare utrett en revision av grundlagen så att det för att trygga den nationella säkerheten genom lag kan föreskrivas om nödvändiga begränsningar i skyddet för hemligheten i fråga om förtroliga meddelanden, när de förutsättningar som ska anses behövliga uppfylls.

Behovet att justera regelverket

Finlands säkerhetspolitiska omgivning har förändrats snabbt bl.a. till följd av globaliseringen och utvecklingen inom digitaliseringen. Gränsen mellan krigföring och annan påverkan blir diffusare när politiska och ekonomiska påtryckningsmetoder, informationsoperationer samt metoder för hybridpåverkan används. Information som anknyter till betydande hot flyttar i allt högre grad över till datanätet.

För att Försvarsmakten ska kunna sköta sina lagstadgade uppgifter förutsätts underrättelseverksamhet. Den militära underrättelseverksamheten är en central del av Finlands försvarsberedskap. Det finns emellertid inga uttryckliga bestämmelser om militär underrättelseverksamhet i den lagstiftning som gäller Försvarsmakten. I Finland finns inte heller något regelverk om vad man eftersträvar med underrättelseverksamheten eller hurdan underrättelseverksamhet som får bedrivas.

Försvarsmaktens myndigheters hemliga informationsinhämtningsbefogenheter begränsar sig till att förebygga och avslöja brott. Gällande lagstiftning möjliggör inte att underrättelseinformation kan inhämtas, utom när det är fråga om ett brott och föremål för informationsinhämtningen är alltid en viss person och dennes agerande.

Med Försvarsmaktens nuvarande befogenheter kan man inte tillräckligt effektivt och på ett tillräckligt tidigt stadium inhämta information om militära aktiviteter eller yttre hot som riktas mot Finland för att en militär förvarning ska kunna ges. Försvarsmakten kan inte i tid vidta de åtgärder som avvärjning av hot förutsätter. Som stöd för beslutsfattandet i den högsta statsledningen och det militära beslutsfattandet måste man kunna producera objektiv, säkerställd och analyserad information. Försvarsmaktens befogenheter till informationsinhämtning är bristfälliga i relation till verksamhetens samhälleliga betydelse samt i jämförelse med andra länders. På grund av detta bör militärunderrättelsemyndigheternas informationsinhämtningsmetoder utvecklas.

Arbetsgruppens förslag

Arbetsgruppen har berett ett förslag till en ny lag om militär underrättelseverksamhet. Lagen ska tillämpas på Försvarsmaktens underrättelseverksamhet, dvs. på militär underrättelseverksamhet, genom vilken information med anknytning till Försvarmaktens uppgifter om vilka föreskrivs i lagen om försvarsmakten inhämtas, undersöks och utnyttjas som stöd för den finska utrikes-, säkerhets- och försvarspolitiken och för att kartlägga yttre hot som riktas mot Finland. Information ska inhämtas ur offentliga och icke-offentliga informationskällor. Användningen av befogenheterna ska stå i överensstämmelse med de allmänna principer, om vilka föreskrivs i lagen, såsom proportionalitetsprincipen och principen om minsta olägenhet.

Den militära underrättelseverksamheten har till uppgift att forma och upprätthålla en vidsträckt militärstrategisk lägesbild som krävs för det militära beslutsfattandet. Vid behov måste man kunna ge en förvarning om ett hot som riktas mot Finland. Det främsta syftet med den militära underrättelseverksamheten är inte att inhämta information för att förebygga brott eller att inhämta information om förberedelse eller planering av brott. Den allmänna behörigheten att förebygga, utreda och avslöja brott har polisen.

Endast de militära myndigheterna har tillräcklig kunskap om de hot som riktas mot försvaret och om det militära verksamhetsfältet samt kännedom om verksamhetsfältets sätt och praxis. För att underrättelseverksamhet ska kunna bedrivas ändamålsenligt förutsätts detta bakgrundskunnande, för att den militära underrättelseverksamheten ska kunna utnyttja den information som är allra mest kritisk med tanke på försvaret. Därför kan inte någon annan myndighet bedriva militär underrättelseverksamhet.

Genom militär underrättelseverksamhet ska man inhämta information om militära aktiviteter inom landet och utomlands och om utländsk underrättelseverksamhet, verksamhet som hotar stats- och samhällsordningen, massförstörelsevapen, utvecklande och spridning av krigsmateriel, allvarliga hot som riktas mot staten eller mot samhällets vitala funktioner, en främmande stats planer eller verksamhet som kan orsaka skada för Finland internationella relationer eller andra viktiga intressen, kriser som hotar internationell fred och säkerhet, hot som riktas mot säkerheten vid internationella krishanteringsoperationer samt hot som riktas mot säkerheten när Försvarsmakten ger internationellt bistånd och i annan internationell verksamhet.

Det ministerutskott som behandlar utrikes- och säkerhetspolitik och republikens president ska vid ett gemensamt sammanträde årligen förberedande behandla prioriteringarna för den militära underrättelseverksamheten.

Huvudstaben och Försvarsmaktens underrättelsetjänst ska vara militärunderrättelsemyndigheter. Reservister i tjänstgöring ska kunna delta i fullgörandet av ett underrättelseuppdrag under styrning och övervakning av militärunderrättelsemyndigheten med de förutsättningar om vilka ska föreskrivas i lagen.

Huvudstabens underrättelsechef ger underrättelseuppdragen. Republikens president samt statsrådets kansli, utrikesministeriet och försvarsministeriet ska kunna begära upplysningar av militärunderrättelsemyndigheten. Den militära och den civila underrättelseverksamheten ska samordnas mellan de ovan nämnda myndigheterna och inrikesministeriet samt vid behov mellan andra ministerier och myndigheter. Militärunderrättelsemyndigheten ska kunna agera i samarbete med skyddspolisen för att underrättelseverksamheten ska skötas på korrekt sätt. I lagen ska finnas bestämmelser om förutsättningarna för internationellt samarbete.

I lagen ska det föreskrivas om militärunderrättelsemyndigheternas befogenheter vid personbaserad underrättelseinhämtning och underrättelseinhämtning som avser utländska informationssystem. Med tanke på lagen som helhet finns det också skäl att föreskriva om radiosignalspaning. Med beaktande av säkerhets- och resursaspekten bör det vara möjligt att utföra personbaserad underrättelseinhämtning med anknytning till yttre hot också i Finland. Underrättelsemetoderna ska motsvara de hemliga informationsinhämtningsmetoder som myndigheterna för närvarande har i bruk. Förutsättningarna för att använda befogenheterna och syftet med användningen av dem ska dock skilja sig från dem som gäller vid brottsbekämpning.

I lagen föreslås följande befogenheter: systematisk observation, förtäckt inhämtande av information, teknisk avlyssning, optisk observation, teknisk spårning, teknisk observation av utrustning, teleavlyssning och inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning, täckoperation, användning av informationskällor, tryggande av en informationskälla, bevisprovokation genom köp, platsspecifik underrättelseinhämtning, kopiering och kvarhållande samt kopiering av ett brev eller en annan försändelse.

Informationsinhämtning bör kunna skyddas så att den hemlighålls för att säkerheten för den som inhämtar eller den som överlåter informationen ska kunna tryggas, för att det förtroende som genomförandet av informationsinhämtning förutsätter ska kunna förvärvas och för att avslöjandet av informationsinhämtningen ska kunna förhindras. Också identiteten och bakgrundsorganisationen i fråga om en tjänsteman som bedriver underrättelseverksamhet ska vid behov kunna hemlighållas.

Vid radiosignalspaning ska informationsinhämtningen inriktas på radiovågor som sänds från platser utanför finskt territorium eller till platser utanför finskt territorium, varvid det inte är fråga om sådan meddelandetrafik som skyddas av den hemlighet som gäller för ett förtroligt meddelande.

Med underrättelseinhämtning som avser utländska datasystem ska avses militärunderrättelsemyndigheternas aktiva verksamhet för att inhämta information från ett utländskt datasystem genom datanätets förmedling. Underrättelseinhämtning som avser datasystem kan i något fall förutsätta att det tekniska skyddet kringgås.

Det föreslås att i lagen ska inbegripas bestämmelser om underrättelseinhämtning som avser datatrafik, dvs. teknisk informationsinhämtning som riktas mot datatrafik i kommunikationsnät som överskrider Finlands gräns, vilken baserar sig på automatiserad avskiljning av datatrafik samt om behandling av den inhämtade informationen.

Som en central förutsättning för underrättelseinhämtning som avser datatrafik kan det anses att de hot som informationsinhämtningen får gälla definieras så klart och snävt som möjligt. Enligt de internationella människorättsfördragen får underrättelseinhämtning som avser datatrafik inte vara en metod att inhämta information om vilket hot eller vilken risk som helst. Av denna orsak ska de hot och situationer som underrättelseverksamheten får gälla räknas upp så exakt som möjligt i lagen. Enligt Europeiska människorättsdomstolens avgörandepraxis ska det av lagstiftningen tillräckligt klart framgå i vilka förhållanden och under vilken förutsättning medborgarna kan bli föremål för hemlig observation från myndigheternas sida. Dessa specialvillkor ska beaktas när det övervägs om underrättelseinhämtning som avser datatrafik ska genomföras. I datatrafiken måste man kunna avskilja de uppgifter som är av betydelse med tanke på själva underrättelseuppdraget.

Underrättelseinhämtning som avser datatrafik omfattar tre olika befogenheter: behandling av tekniska data, underrättelseinhämtning som avser datatrafik och som riktas mot en statlig aktör och sådan som riktas mot någon annan än en statlig aktör. För underrättelseinhämtning som avser datatrafik ska alltid krävas tillstånd av domstol.

En förutsättning för underrättelseinhämtning som riktas mot en statlig aktörs datatrafik ska vara att man genom detta kan antas få information med tanke på ett underrättelseuppdrag. En förutsättning för underrättelseinhämtning som avser datatrafik, vilken riktas mot någon annan än en statlig aktör, ska vara att den information som man får genom detta kan antas vara nödvändig med tanke på ett underrättelseuppdrag.

Det föreslås inte att privata parter ska ges en skyldighet att överlåta krypteringsnycklar eller installera bakdörrar i programvara eller anordningar. Underrättelseinhämtning som avser datatrafik ska förutsätta att ägarna av delar av ett kommunikationsnät, vilka överskrider landets gränser, ska ges en skyldighet att anvisa accesspunkterna samt lämna uppgifter till den myndighet som genomför underrättelseinhämtning i datatrafik så att den underrättelseinhämtning som avser datatrafik kan inriktas. Ägarna till kommunikationsnätsdelarna ska ha rätt att få ersättning av statens medel för direkta kostnader som orsakats av att de har biträtt myndigheterna och lämnat uppgifter.

Eftersom den militära underrättelseverksamheten ska ha till uppgift att inhämta information endast i det syfte som definieras i lagen och som anknyter till Försvarsmaktens lagstadgade uppgifter, ska lämnandet av underrättelseuppgifter för annat bruk vara exakt avgränsat. Om det finns skäl att misstänka att ett synnerligen allvarligt brott har begåtts, ska man vara skyldig att meddela detta till förundersökningsmyndigheten. Uppgifter kan meddelas för att förebygga ett brott som äventyrar säkerheten. Militärunderrättelsemyndigheten ska ha rätt att i vissa situationer till en privat aktör meddela om skadliga datorprogram som myndigheten har upptäckt eller ge uppgifter för att förhindra en ansenlig förmögenhetsskada.

Militärunderrättelseverksamhetens lagenlighet ska vid Försvarsmakten styras och övervakas av försvarsmaktens assessor. Utöver den interna övervakningen ska också en särskild övervakningsmyndighet, som står utanför försvarsförvaltningen, övervaka lagenligheten. Verksamheten ska också övervakas parlamentariskt. Särskilda bestämmelser ska finnas om uppgifterna och befogenheterna för den militära och civila underrättelseverksamhetens gemensamma externa övervakningsmyndighet samt om den parlamentariska övervakningen. Försvarsministeriet ska ha rätt att av Försvarsmakten få information om betydande frågor som anknyter till den militära underrättelseverksamheten samt att granska de handlingar som gäller användningen av informationsinhämtningsmetoderna. Syftet ska inte vara att begränsa de högsta laglighetsövervakarnas tillsynsuppgifter.

De bestämmelser i den föreslagna lagen som gäller personregister kommer i den fortsatta beredningen att flyttas över till ett regelverk som ska upprättas i samband med en total översyn av den lagstiftning som gäller behandlingen av personuppgifter inom försvarsförvaltningen, vilken pågår just nu.

Det föreslås att lagen ska träda i kraft så snart som möjligt med beaktande av de omständigheter som gäller den föreslagna lagens lagstiftningsordning.

ABSTRACT

Background

On 1 October 2015, the Ministry of Defence appointed a working group to draft a proposal for legislation on military intelligence comprising basic provisions on the purpose of the Defence Forces' intelligence activities, the competent authorities and their tasks and powers, steering and oversight of intelligence gathering, processing of data and cooperation between authorities.

The drafting of legislation on military intelligence is based on the Government Programme of Prime Minister Sipilä, according to which the Government will propose a statutory base for foreign intelligence and telecommunications intelligence.

For this purpose, a working group on civilian intelligence was appointed by the Ministry of the Interior, while the Ministry of Justice nominated a working group to prepare legislation on the oversight of intelligence activities conducted by civilian and military authorities.

To facilitate parliamentary preparation by a group to be appointed later, an expert working group nominated by the Ministry of Justice investigated the possibility of amending the Constitution by making it possible to pass an act with provisions on limitations to the protection of the secrecy of confidential communications that are essential for safeguarding national security when the preconditions regarded as necessary are met.

Legislation needs to be reviewed

Finland's security environment has changed rapidly as a result of such factors as globalisation and advancing digitalisation. The line between warfare and other exertion of influence has been blurred by application of political and economic pressure, information operations and means of hybrid warfare. Intelligence related to significant threats is increasingly transitioning to information networks.

Without intelligence activities, the Defence Forces cannot perform their statutory duties. Military intelligence is a key part of Finland's defence readiness. However, the legislation on the Defence Forces contains no specific provisions on military intelligence. Neither are the objectives of intelligence activities or the kind of intelligence activities that are permissible regulated under any statute in Finland.

The powers of covert intelligence gathering granted to Defence Force authorities are limited to preventing and detecting offences. The valid legislation only permits the gathering of intelligence in case of an offence, and the target of intelligence activities always is a certain person and his or her activities.

The current powers of the Defence Forces do not allow the efficient and timely gathering of intelligence on military activities or external threats against Finland in order to provide military advance warning. The Defence Forces are thus unable to take timely action to prevent threats. An ability to produce objective, confirmed and analysed information is required to support decision-making by the highest levels of government and military authorities. The Defence Forces' powers to gather intelligence are inadequate compared to the societal significance of these activities and their scope in other countries. The military intelligence authority's intelligence gathering methods must thus be improved.

Working group proposal

The working group has prepared a proposal for a new act on military intelligence. The act would apply to the Defence Forces' intelligence activities: military intelligence work aiming to obtain, investigate and use intelligence related to the Defence Forces' tasks laid down in the Act on the Defence Forces in order to support Finland's foreign, security and defence policy and to map external threats against Finland. Intelligence would be gathered from public and non-public information sources. The powers to gather intelligence should be used in compliance with general principles laid down in the act, including the principle of proportionality and the least harm principle.

The purpose of military intelligence is to broadly create and maintain military strategic situational awareness required for making military decisions. If necessary, obtaining advance warning of a threat against Finland must be possible. The primary purpose of military intelligence activities is not to obtain information for preventing offences or to gather information on offences being prepared or planned. General powers to prevent, investigate and detect offences belong to the police.

Only military authorities have sufficient know-how regarding threats against national defence and the military field of activity, as well as knowledge of the customs and practices in this field. This underlying expertise is needed to carry out intelligence activities appropriately, ensuring that military intelligence can access the most critical information in terms of national defence, and it is thus not possible for military intelligence to be gathered by some other authority.

The purpose of military intelligence would be to gather information in Finland and abroad on military activities and foreign intelligence activities, activities that threaten governmental and social order, weapons of mass destruction, development and distribution of war materials, serious threats against the state or vital functions of society, a foreign state's plans or activities that could damage Finland's international relations or other vital interests, crises that undermine international peace and security, threats to the safety of international crisis management operations as well as threats that undermine safety related to the provision of international assistance and other international activities of the Defence Forces.

An initial discussion on the priorities of military intelligence would be held at an annual meeting between the Cabinet Committee on Foreign and Security Policy and the President of the Republic.

Military intelligence authorities would include the Defence Command and the Defence Force Intelligence Agency. When in service, reservists could participate in intelligence tasks under the guidance and supervision of the military intelligence authority and on the conditions laid down in the act.

Tasks related to intelligence would be assigned by the Chief of Defence Intelligence at the Defence Command. Information requests to the military intelligence authority could be made by the President of the Republic as well as the Prime Minister's Office, the Ministry for Foreign Affairs and the Ministry of Defence. Military and civilian intelligence activities would be coordinated in cooperation by the aforementioned authorities and the Ministry of the Interior and, where necessary, other ministries and authorities. To ensure that intelligence activities are conducted appropriately, the military intelligence authority could work together with the Finnish Security Intelligence Service. The act would contain provisions on the preconditions for international cooperation.

The act would lay down provisions on the powers of military intelligence authorities regarding human intelligence and foreign information systems intelligence. To ensure that the scope of the act is broad enough as a whole, it should also contain provisions on signals intelligence. Taking the perspectives of security and resource allocation into account, it should also be possible to conduct human intelligence activities in Finland. The methods of intelligence gathering would be the same

as the means of covert intelligence gathering currently available for the authorities. However, the criteria for exercising these powers and their purpose would be different from what is applicable to crime prevention.

The following powers are proposed in the act: surveillance, covert intelligence gathering, on-site interception, technical observation, technical tracking, technical surveillance of a device, telecommunications interception and obtaining data other than through telecommunications interception, traffic data monitoring, obtaining base station data, gathering data identifying a network address or a terminal end device, undercover activities, the use of covert human intelligence sources, the securing of an intelligence source, pseudo purchases, intelligence related to a certain location, copying, and interception and copying of a letter or other consignment.

It should be possible to protect intelligence-gathering so as to keep it secret in order to ensure the safety of the person acquiring or disclosing information, to gain the trust necessary for acquiring the information, or to prevent the discovery of the intelligence-gathering. Where necessary, it should also be possible to keep secret the identity and background organisation of the official gathering intelligence.

In signals intelligence, the object of the intelligence gathering would be traffic that originates outside Finland or that originates in Finland and terminates outside Finland's borders, which would thus not involve telecommunications protected by the secrecy of confidential communications.

Foreign information systems intelligence would mean active measures taken by military intelligence authorities to obtain information through the information network from a foreign information system. In individual cases, information systems intelligence could necessitate circumventing technical protection.

It is proposed that provisions on telecommunications intelligence, or technical intelligence work based on automatic screening of cross-border traffic in the telecommunications network, and the processing of the gathered information be included in the act.

As an essential precondition for telecommunications intelligence can be regarded that the threats concerning which intelligence gathering may be pursued are defined as clearly and narrowly as possible. Pursuant to international human rights conventions, telecommunications intelligence may not be a means used to obtain information on any threat or risk whatsoever. For this reason, the threats and situations that the intelligence gathering may concern would be listed in the act as precisely as possible. Pursuant to the case-law of the European Court of Human Rights, the relevant legislation must specify in sufficient detail under what circumstances and according to which criteria citizens may be subjected to secret surveillance by the authorities. These parameters would be taken into account when considering how to execute telecommunications intelligence. It must be possible to isolate from the telecommunications traffic flow the information that is relevant for the actual intelligence-related mission.

Telecommunications intelligence would involve three different powers: processing of technical data, intelligence gathering on a government actor and intelligence gathering on a non-governmental actor. The permission of a court would always be required for telecommunications intelligence activities.

The precondition for gathering intelligence on the telecommunications of a governmental actor would be that it can be assumed to result in gaining information relevant to the intelligence task. The precondition for gathering intelligence on a non-governmental actor would be that the information gained as a result can be presumed to be essential for the intelligence task.

The proposal does not contain an obligation placed on private parties to disclose encryption keys or to install back doors in software and hardware. It would be a prerequisite for organising telecommunications intelligence that the owners of cross-border telecommunications cables have an obligation to notify the competent authorities of their connection points and to provide information needed to target telecommunications intelligence activities to the authority responsible for the intelligence gathering. Owners of telecommunications network components would have the right to be compensated for any direct costs incurred in assisting the authorities and providing the information.

As the purpose of military intelligence gathering would only be to gather information for purposes defined in this act associated with the statutory tasks of the Defence Forces, any disclosures of intelligence information for other uses would be strictly limited. A duty to notify pre-trial investigation authorities would apply if there is reason to suspect that a highly serious offence has been committed. Information may be disclosed to prevent an offence that endangers safety or security. In certain situations, military intelligence authorities would have the right to report malicious computer software detected by them, or to provide information to a private actor to prevent significant property damage.

The legality of military intelligence activities in the Defence Forces would be directed and overseen by the Chief Legal Advisor of the Defence Forces. In addition to internal oversight, the legality of the activities would be supervised by a designated authority external to the defence administration. The activities would also be subject to parliamentary oversight. Provisions on the tasks and powers of the joint external supervisory authority of military and civilian intelligence and parliamentary oversight would be enacted separately. The Ministry of Defence would be entitled to obtain information on significant issues related to military intelligence from the Defence Forces and to inspect documents on the use of intelligence gathering methods. The intention of the act would not be to limit the supervisory tasks of the supreme overseers of legality.

In the course of further drafting, the provisions on personal data files in the proposal will be included in the regulation to be drafted in connection with the overhaul of legislation on the processing of personal data in the defence administration.

It is proposed that the act enter into force as soon as possible, taking issues related to the procedure for enactment into account.

LUONNOS HALLITUKSEN ESITYKSEKSI

Esityksen pääasiallinen sisältö

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

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

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

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

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

YLEISPERUSTELUT

1 Johdanto

Yleinen kansainvälistymis- ja teknistymiskehitys on tärkeää ja välttämätöntä. Sen seurauksena Suomen turvallisuusympäristö on viime vuosina merkittävästi muuttunut ja monimutkaistunut. Lisäksi sisäiseen ja ulkoiseen turvallisuuteen kohdistuvat uhat limittyvät toisiinsa entistä läheisemmin. Turvallisuuteen kohdistuvat vakavimmat uhat ovat lähes poikkeuksetta kansainvälistä alkuperää tai niillä on kytköksiä maamme ulkopuolelle. Myös Suomen etuihin ulkomailla - mukaan lukien sellaiset kriisinhallintaoperaatiot, joihin Suomi osallistuu - kohdistuu enemmän ja vakavampia uhkia kuin aiemmin. Uhkien taustalla olevien valtiollisten ja ei-valtiollisten tahojen tunnistaminen ja niiden toiminnan ennakoiminen on vaikeutunut, koska esimerkiksi tekniikan ja tietotekniikan kehitys on antanut pienillekin valtioille ja ei-valtiollisille toimijoille mahdollisuuden toimia tehokkaasti. Teknologian kehittyminen on mahdollistanut kansallista turvallisuutta vaarantavien tekojen toteuttamisen entistä lyhyemmällä valmisteluajalla ja vakavimmin seurauksin. Tietoverkossa toteutettavia hyökkäyksiä voidaan käyttää myös poliittisen ja taloudellisen painostuksen välineinä ja vakavassa kriisissä yhtenä vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella.

Uhkien kansainvälisestä luonteesta seuraa, että niiden taustalla olevat tahot ovat verkostoituneet eri maiden alueelle ja osalliset kommunikoivat yli valtiorajojen. Viestintäteknologian nopea kehitys on tehostanut ja helpottanut Suomelle uhan muodostavien tahojen välistä rajat ylittävää yhteydenpitoa ja verkostoitumista sekä nopeuttanut uhkien kansainvälistymistä. Kehityskulku on vaikuttanut siihen, että tietotekniikan nopean kehityksen ja alhaisempien kustannusten vuoksi asevoimat ottavat laajasti käyttöönsä sellaisia johtamis- ja viestintäjärjestelmiä, jotka on suunniteltu siviilitarpeita varten. Siviilipuolen toimijoiden ohella myös modernien asevoimien johtaminen tukeutuu entistä enemmän yleiseen teleinfrastruktuuriin. Teknologian kehityksen osalta on tärkeä huomioida, että myös asevoimien harjoittama viestiliikenne on siirtynyt merkittävissä määrin analogisesta kanavista digitaalisiin kanaviin kuten tietoliikennekaapeleihin.

Turvallisuuspoliittiseen toimintaympäristöön liittyvät haasteet sekä valtioiden rajat ylittävät uhat ovat yhä moniulotteisempia. Näihin haasteisiin ja uhkiin vastaaminen vaatii laajan keinovalikoiman hyödyntämistä ja kehittämistä viranomaisten puolelta. Turvallisuuden ylläpitäminen edellyttää aktiivista ulko-, turvallisuus- ja puolustuspolitiikkaa. Tarve sisäisen ja ulkoisen turvallisuuden politiikkanalojen yhteistyöhön korostuu. Uhkakuviin vastaaminen edellyttää monialaista ja tiivistä yhteistyötä sekä kansallisesti, EU:ssa että kansainvälisesti. Vuonna 2009 voimaan tullut Lissabonin sopimus (SopS 66 ja 67/2009) on vahvistanut EU:n roolia erilaisiin uhkiin vastaamisessa. EU:n yhteisvastuulauseke (Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 222 artikla) ja keskinäisen avunannon lauseke (Euroopan unionista tehdyn sopimuksen (SEU) 42 artiklan 7 kohta) edistävät unionin luonnetta turvallisuusyhteisönä ja vahvistavat EU:n jäsenvaltioiden mahdollisuuksia pyytää ja antaa apua erilaisissa kriisitilanteissa.

Kansallisesta turvallisuudesta vastaavien viranomaisten tehtävänä on ennakoida ja ennalta estää toimialallaan sellaisia vahingollisia tekoja ja toimenpiteitä, jotka voivat vaarantaa erityisen tärkeiksi miellettyjä kansallisia etuja. Suomeen voidaan kohdistaa vakavia turvallisuusuhkia Suomen rajojen ulkopuolelta. Tietoverkkojen kehitys on vähentänyt fyysisen etäisyyden merkitystä uhkien toteuttamisessa. Kansallisesta turvallisuudesta vastaavat viranomaiset harjoittavat lakisääteisten tehtäviensä hoitamisen edellyttämää tiedustelua. Tiedustelua varten ei kuitenkaan ole laissa säädettyjä toimivaltuuksia. Tiedustelu perustuu pitkälti julkisiin lähteisiin sekä kansainvälisen ja muun vapaaehtoisen yhteistyön puitteissa saataviin tietoihin.

Puolustusministeriön hallinnonalalle kuuluva Puolustusvoimat vastaa Suomen sotilaallisesta puolustamisesta sekä sotilaalliseen uhkaan varautumisesta. Hallinnonalan tiedonhankintatarpeet liitty-

vät sotilasstrategisen tilannekuvan muodostamiseen ja ylläpitämiseen sekä kansainvälisten tehtävien turvallisuuteen. Puolustusvoimille lakisääteisten tehtävien toteuttaminen edellyttää sotilastiedustelujärjestelmää, jolla kyetään seuraamaan turvallisuusympäristön kehitystä ja tuottamaan strateginen ja operatiivinen toimintaympäristötietoisuus ja sitä koskevat arviot valtion ja Puolustusvoimien johdon päätöksenteon tueksi. Järjestelmä antaa valtionjohdolle ennakkovaroituksen sotilaallisten uhkien kehittymisestä, mikä mahdollistaa valtionjohdon oikea-aikaisen päätöksenteon ja yhteiskunnan elintärkeiden toimintojen johtamisen. Sotilastiedustelun toiminnassa korostuu näin ennakkovaroituskyky, eli kyky varoittaa mahdollisista sotilaallisista uhista, jotta näihin uhkiin voidaan varautua.

Sotilastiedustelulla tarkoitetaan kohdennettua tietojen hankkimista ja hankittujen tietojen analysointia vallitsevasta turvallisuusympäristöstä sekä eri toimijoiden toimintakyvystä ja suunnitelmista, minkä tavoitteena on tuottaa tietoa Suomen ylimmän valtiojohdon ja Puolustusvoimien päätöksenteon tueksi.

Pääministeri Juha Sipilän hallituksen ohjelman (VNT 1/2015 vp.) mukaan kasvavat riskit ja uudet uhat edellyttävät koko yhteiskunnalta uudenlaista valmiutta ja varautumista. Hallitus vahvistaa kokonaisturvallisuusajattelua kansallisesti, EU:ssa ja kansainvälisessä yhteistyössä. Tämä koskee erityisesti uusien ja laaja-alaisten uhkien kuten hybridivaikuttamisen, kyberhyökkäysten ja terrorismin torjuntaa. Hallitus vahvistaa ulkoisen turvallisuuden sisäisiä edellytyksiä. Hallitus esittää säädösperustaa ulkomaantiedustelulle ja tietoliikennetiedustelulle. Niiden yhteydessä kiinnitetään huomioita perus- ja ihmisoikeuksien toteutumiseen.

Tiedustelulainsäädäntöhanketta käsiteltiin hallituksen strategiakokouksessa 20.8.2015. Kokouksessa päätettiin, että puolustusministeriö johtaa sotilastiedustelua koskevaa hanketta, sisäministeriö johtaa siviilitiedustelua koskevaa hanketta ja oikeusministeriö perustuslain mahdollista muuttamista koskevaa hanketta. Puolustusministeriö asetti 1.10.2015 hankkeen, jonka tehtävänä on valmistella ehdotus sotilastiedustelua koskevaksi lainsäädännöksi. Lainsäädäntöhanke valmisteltiin kiinteässä yhteistyössä sisäministeriön ja oikeusministeriön hankkeiden kanssa. Lisäksi oikeusministeriö asetti 17.10.2016 hankkeen turvallisuusviranomaisten tiedustelutoiminnan valvonnan järjestämisestä.

2 Nykytila

2.1 Muuttuva turvallisuusympäristö

Valtioneuvosto antoi 19.5.2016 eduskunnalle selonteon Suomen sisäisestä turvallisuudesta (VNS 5/2016 vp.) sekä 17.6.2016 selonteon Suomen ulko- ja turvallisuuspolitiikasta (VNS 6/2016 vp.). Molemmat selonteot perustuvat hallitusohjelman edellyttämällä tavalla kokonaisturvallisuuskäsitteeseen. Valtioneuvoston puolustuspoliittinen selonteko annettiin eduskunnalle 16.2.2017 (VNS 5/2017). Sisäisen turvallisuuden selonteko, ulko- ja turvallisuuspoliittinen selonteko sekä valtioneuvoston puolustusselonteko muodostavat kokonaisturvallisuuden keskeisen viitekehyksen ja niiden tarkastelujaksot ulottuvat 2020-luvun puoliväliin. Taustaa tälle työlle antoivat vuoden 2012 turvallisuus- ja puolustuspoliittinen selonteko sekä yhteiskunnan turvallisuusstrategia vuodelta 2010.

Puolustuspoliittisen selonteon mukaan Suomen lähialueen turvallisuustilanne on heikentynyt Krimin valtauksen ja Itä-Ukrainan konfliktin jälkeen. Sotilaalliset jännitteet Itämeren alueella ovat lisääntyneet ja epävarmuus on lisääntynyt laajemminkin.

Itämeren alueen sotilasstrateginen merkitys on kasvanut ja sotilaallinen toiminta alueella lisääntynyt. Venäjä on osoittanut kykenevänsä tekemään nopeasti strategisia päätöksiä ja käyttämään koordinoidusti sotilaallista voimaa ja muuta laajaa keinovalikoimaa tavoitteidensa saavuttamiseksi.

Venäjä kehittää asevoimiensa suorituskykyjä ja ylläpitää valmiuksia toimi myös laajamittaisessa sotilaallisessa kriisissä. Kaikkien puolustushaarojen korkeassa valmiudessa olevia joukkoja kyetään siirtämään valtakunnan eri osista haluttuun suuntaan nopeasti ja yllätyksellisesti muun muassa rajoitetun alueen valtaamiseksi ja kohdevaltion suvereniteetin kiistämiseksi. Kaikkien Venäjän turvallisuusviranomaisten suorituskykyjä voidaan käyttää sotilaallisiin tehtäviin. Sodan kuvan monipuolistuttua Suomeen kriisiaikana kohdistuva keinovalikoima olisi laaja. Se sisältäisi sotilaallisia ja ei-sotilaallisia keinoja. Sotilaallisten kriisien ennakkovaroitusaika on lyhentynyt ja kynnys voimankäyttöön on alentunut. Samanaikaisesti yhteiskunnan haavoittuvuus on lisääntynyt.

Puolustuspoliittisen selonteon mukaan kybertoimintaympäristön merkitys kasvaa. Kyberkeinojen käyttöä poliittisten päämäärien saavuttamiseksi ei voida sulkea pois. Yhteiskunnan digitalisaatio, teknisten järjestelmien riippuvaisuus rajat ylittävistä tietoverkoista sekä järjestelmien keskinäiset riippuvuussuhteet ja haavoittuvuudet altistavat yhteiskunnan elintärkeät toiminnot kybervaikuttamiselle. Kyber- ja informaatiovaikuttamista on kohdistettu lähialueillemme ja myös Suomeen muun muassa kriittistä infrastruktuuria, teollisuuslaitoksia sekä poliittista päätöksentekojärjestelmää ja kansalaisia vastaan. Tieteen ja teknologian kehitys aiheuttaa myös muunlaisia haasteita uhkiin varautumiselle. Monimuotoiset kemialliset, biologiset, radiologiset uhkat sekä ydinaseuhkat (CBRN) säilyvät.

Turvallisuuspoliittisen selonteon mukaan Suomen puolustaminen edellyttää kykyä toimia maa-, meri-, ilma- ja kybertoimintaympäristöissä. Toimintaympäristön asettamat vaatimukset korostavat muun muassa tiedustelukykyä, eri hallinnonalojen valmiutta toimia nopeasti kehittyvissä tilanteissa, kykyä suojautua kauaskantoisten asejärjestelmien vaikutuksilta ja kyberpuolustuskykyä.

Sisäisen turvallisuuden selonteon mukaan sisäisen ja ulkoisen turvallisuuden uhkat limittyvät yhä tiiviimmin toisiinsa. Uhkat monimutkaistuvat ja muuttuvat nopeasti. Tilanteen ennustettavuus on viimeaikoina heikentynyt merkittävästi eikä turvallisuustilanteessa ole nähtävissä muutosta parempaan. Uudessa tilanteessa sisäisen turvallisuuden merkitys on korostunut ja tästä syystä valtioneuvosto laatikin ensimmäistä kertaa erikseen sisäisen turvallisuuden selonteon.

Sisäisen turvallisuuden selonteon mukaan muun muassa Venäjän ja lännen suhteiden huononeminen sekä kyberuhat ovat eräitä merkittävimpiä viimeaikaisia muutoksia turvallisuusympäristössä. Selonteon mukaan hybridivaikuttamisen keinot valtiollisessa vaikuttamisessa ovat lisääntyneet ja sisäisen turvallisuuden viranomaisilla tulee olla sekä kyky havaita uhkat että riittävät voimavarat pitkäkestoisenkin tilanteen hallitsemiseksi. Myös valtiollisten ja muiden toimijoiden informaatiovaikuttaminen on tunnistettava ja siihen on pystyttävä vastaamaan. Muuttuneessa tilanteessa korostuvat valtiollisen päätöksenteon ja ulkorajojen koskemattomuuden turvaaminen. Uudet jännitteet valtioiden välillä ovat myös mahdollisia. Lisäksi ulkomaisten tiedustelupalveluiden toiminta Suomessa on palannut kylmän sodan tasolle. Henkilölähteisiin perustuvan tiedustelun rinnalle on tullut tietoverkoissa tapahtuva tiedustelu. Kriittiseen infrastruktuuriin kohdistuvat häiriöt voivat vaikuttaa suureen määrään ihmisiä. Selonteon mukaan keskeisiä sisäiseen turvallisuuteen vaikuttavia elementtejä ovat esimerkiksi huoltovarmuus, digitalisaatio, kyberturvallisuus ja perusinfrastruktuuri sekä niiden voimakas keskinäisriippuvuus.

Ulko- ja turvallisuuspoliittinen selonteko muodostaa perustan Suomen ulko- ja turvallisuuspolitiikalle. Selonteossa käsitellään kansainvälisessä toimintaympäristössä tapahtuvia nopeasti muuttuvia ja vaikeasti ennakoitavissa olevia kehityskulkuja sekä turvallisuuskysymysten globalisoitumisen merkitystä Suomen turvallisuudelle. Selonteon mukaan voimakas muutos ulko- ja turvallisuuspolitiikan toimintaympäristössä jatkuu niin Suomen lähialueilla kuin maailmanlaajuisesti. Valtiot ja muut toimijat ovat entistä tiiviimmin ja moninaisemmin sitein yhteydessä toisiinsa ja toisistaan riippuvaisia. Toimintaympäristön viimeaikainen muutos on luonut myös uusia uhkia ja epävakautta. Kansainvälinen turvallisuustilanne on eurooppalaisesta näkökulmasta heikentynyt viime vuosien aikana. Kansainvälisesti merkittävien toimijoiden määrä ja kirjo kasvaa ja niiden valtasuhteet ovat jat-

kuvassa muutoksessa. Yleismaailmallisten arvojen kunnioitus horjuu. Ulko- ja turvallisuuspoliittisen toimintaympäristön muutoksilla on monenlaisia vaikutuksia myös Suomen sisäiseen kehitykseen. Sisäiseen turvallisuuteen kohdistuu niiden myötä uusia epävarmuustekijöitä ja yhteiskunnan yleinen kriisinkestokyky joutuu koetukselle.

Ulko- ja turvallisuuspolitiikan selonteon mukaan ulko- ja turvallisuuspoliittinen tavoitteenasettelu, päätöksenteko ja vaikuttaminen perustuvat tietoon toimintaympäristöstä. Tietoa toimintaympäristön muuttujista ja niistä syntyvistä mahdollisuuksista ja uhista on hankittava ja analysoitava jatkuvasti. Tiedon ja analyysin pohjalta on oltava valmius mukauttaa toimintaa ja tarvittaessa ulko- ja turvallisuuspolitiikan painopisteitä. Keskeisimpiä ulkoisia muuttujia Suomen ulko- ja turvallisuuspoliittisessa toimintaympäristössä ovat maailmanlaajuiset kehityssuunnat, poliittinen ja turvallisuuskehitys Suomelle tärkeillä maantieteellisillä alueilla, ulko- ja turvallisuuspolitiikan toimijat sekä kansainväliset säännöt.

Yhteenvetona voidaan todet, että selonteot korostavat suomalaisten turvallisuutta ja hyvinvointia on parannettava. Rajat ylittävien uhkien torjuminen ja niihin varautuminen edellyttävät niin sotilaallisten voimavarojen kuin siviilivoimavarojen hyödyntämistä, laajan keinovalikoiman käyttämistä. Omien vahvuuksiensa pohjalta Suomen on pystyttävä ennakoimaan toimintaympäristön muutoksia ja vastaamaan muutosten asettamiin vaatimuksiin. Tilanne, jossa Suomen viranomaiset puutteellisesta kansallisesta sääntelystä johtuen ovat riippuvaisia ulkomaista saadakseen tietoa Suomen elintärkeisiin intresseihin kohdistuvista uhkista, on kestämätön. Jokaisella valtiolla - myös Suomella - on velvoite huolehtia omasta ja kansalaistensa turvallisuudesta ja perustaa siihen liittyvä päätöksenteko itse hankittuun tietoon.

Kansallinen turvallisuusympäristö

Yhteiskunnan turvallisuusstrategian 2010 mukaan yhteiskunnan tärkeimpänä suojattavana etuna voidaan pitää valtion itsemääräämisoikeutta, jolla tarkoitetaan valtion suvereenisuutta suhteissa ulkovaltioihin ja oikeutta muista riippumattomalla tavalla käyttää ylintä valtaa omien rajojensa sisällä. Muina keskeisinä suojattavina etuina voidaan pitää ainakin valtion johtamista, kansainvälistä toimintaa, puolustuskykyä, sisäistä turvallisuutta, talouden ja infrastruktuurin toimivuutta sekä väestön toimeentuloturvaa ja toimintakykyä. Edellä mainittuihin etuihin kohdistuvien uhkien voidaan katsoa vaarantavan kansallista turvallisuutta. Uhkien torjunnasta vastaavia viranomaisia kutsutaan tässä mietinnössä kansallisen turvallisuuden viranomaisiksi. Kansainvälistymisen myötä valtioiden ulkoisen ja sisäisen turvallisuuden välinen raja on muuttunut yhä häilyvämmäksi. Myös uhkien ja riskien rajaaminen alue- tai paikkasidonnaisiksi on entistä vaikeampaa taloudellisten, teknisten ja sosiaalisten järjestelmien valtiorajat ylittävästä luonteesta ja keskinäisriippuvuudesta johtuen. Suomen turvallisuutta uhkaavat vakavimmat tekijät liittyvät nykyisin usein Suomen ulkopuolisiin tapahtumiin. Siten myös ulkomaista alkuperää olevan ja siellä syntyvän uhan seuraukset saattavat realisoitua Suomessa aiempaa herkemmin. Kansalliseen turvallisuuteen kohdistuville ulkoisille uhille on yhteistä se, että taustalla olevien valtiollisten ja ei-valtiollisten tahojen tunnistaminen ja erottaminen toisistaan on yhä vaikeampaa. Tästä johtuen uhkien ennakoiminen on aiempaa haasteellisempaa.

Sotilaallisten uhkien luonne on muuttunut. Perinteisen sotilaallisen toiminnan lisäksi modernit sotilasoperaatiot sisältävät erilaisia epäsymmetrisiä keinoja. Modernit sotilasoperaatiot alkavat ajallisesti jo rauhan aikaisilla painostus- ja disinformaatio-operaatioilla sekä tietoverkkohyökkäyksillä. Näin voidaan pyrkiä tietoisesti vaikuttamaan toisen valtion päätöksentekoon, jotta saavutettaisiin sellaisia strategisia päämääriä, joihin painostuksen kohteena oleva valtio ei muutoin suostuisi. Nykyisin painostus- ja disinformaatio-operaatiot kuuluvat valtioiden ulko- ja turvallisuuspolitiikan jatkumoon. Sotilasoperaatioissa ei-valtiollisten toimijoiden vaikuttamismahdollisuudet ovat kasvaneet teknologian kehittymisen ja yhteiskuntien lisääntyneen haavoittuvuuden myötä.

Poliittisen vaikuttamisen ja sodankäynnin raja hämärtyy käytettäessä poliittisia ja taloudellisia painostuskeinoja sekä disinformaatio-operaatioita. Laaja-alainenkaan voimankäyttö ei tulevaisuudessa välttämättä tarkoita kattavien maa-alueiden haltuunottoa ja hallintaa. Tavoitteet voidaan pyrkiä saavuttamaan voimankäytön yllätyksellisyydellä ja rajattujen alueiden nopealla valtaamisella.

Tietoteknistyvä viestintä

Informaatio sekä henkilöiden välinen kanssakäyminen on suureksi osin siirtynyt tietoverkkoihin. Yhteiskunta on muuttunut ympäristöksi, jossa lähes kaikki perinteiset palvelut ja toiminnot ovat tietoteknisesti ohjattuja tai kokonaan muutettu tietoverkoissa toimiviksi. Tietoverkkojen toimintalogiikka eroaa vanhoista puhelinverkoista. Siinä missä puhelu varasi piirikytkentäisen puhelinverkon kokonaan soittajan ja vastaajan välille, internet-verkossa kulkee limittäin lukuisten yhteyksien liikennettä. Lähettävä laite jakaa viestin paketteihin, jotka vastaanottajalaite kokoaa jälleen kokonaiseksi viestiksi. Kaikki paketit eivät välttämättä kulje samaa reittiä vastaanottajalle, sillä verkko reitittää kunkin paketeista kulloisenakin hetkenä kustannustehokkainta reittiä. Kahden samassa maassa olevan osapuolen välinen tietoliikenne voi reitittyä ulkomaisen yhteyspisteen kautta.

Tietoverkkojen kehittyminen on mahdollistanut esimerkiksi pilvipalvelujen yleistymisen. Pilvipalvelussa on kyse tallennuspalvelusta, josta tieto on saatavilla miltä tahansa verkon laitteelta tiedon haltijan oikeuksin. Pilvipalveluun liittyvät palvelimet voivat sijaita yhden tai useamman valtion alueella. Käyttäjällä ei välttämättä ole mahdollisuutta selvittää, mihin tiedot fyysisesti tallentuvat.

Turvallisuusuhkiin liittyy globalisoitumisen seurauksena yhä useammin Suomessa ja ulkomailla olevien henkilöiden välisiä kytköksiä ja siitä seuraavaa tarvetta molemminpuoliseen kommunikointiin. Sähköisiä välineitä käytetään hyväksi turvallisuusuhkien taustalla olevien valtiollisten ja ei-valtiollisten tahojen viestinnässä, tehtäväksi annoissa tehtävien toteuttamista koskevassa raportoinnissa, tekojen suunnittelussa, kohteita koskevassa tiedonhankinnassa, osallisten motivoinnissa ja radikalisoinnissa sekä uusien jäsenten rekrytoinnissa. Turvallisuusuhkien menestyksekkään torjumisen edellytyksenä on se, että kansallisesta turvallisuudesta vastaavat viranomaiset mahdollisimman varhaisessa vaiheessa saavat tiedon tällaisista yhteyksistä ja niiden puitteissa käsiteltävistä kansallista turvallisuutta vaarantavista seikoista. Varhaisvaiheen tiedonsaanti parantaa suomalaisen yhteiskunnan vastekykyä ja laajentaa sitä keinovalikoimaa, jonka avulla uhkien toteutuminen voidaan estää tai siihen varautua. Tietoverkoissa tapahtuvaan viestintään kohdistettu kansallisesta turvallisuudesta vastaavien viranomaisten tiedonhankinta on maailmanlaajuisesti ollut keskeisessä asemassa tekojen estämisessä.

Tietoverkoissa tapahtuvan verkostoitumisen merkitys kansallista turvallisuutta uhkaavien toimijoiden keskuudessa tulee entisestään kasvamaan. Sosiaalisen median kehittyessä verkostoitumisen tavat monimuotoistuvat. Valtiolliset toimijat panostavat omien modernien mediaorganisaatioiden kehittämiseen niiden kautta propagandan levittämiseen. Ne käyttävät yhä laajemmin sosiaalista mediaa, kuten pika-viestipalveluita, sekä ylläpitävät avoimia ja suljettuja keskustelufoorumeita. Nämä mahdollistavat sekä helppokäyttöisen kahden- ja monenvälisen viestinnän että toiminnan suunnittelun ja reaaliaikaisen koordinoinnin. Turvallisuus- ja puolustuspoliittisen selonteon 2012 arvion mukaan valtiotoimijoiden korostuvia sotilaallisia kykyjä ovat muun muassa tiedustelu- ja valvontajärjestelmät. Valtiot kehittävät miehittämättömiä laitteita tiedusteluun, valvontaan ja täsmäasejärjestelmien laveteiksi. Sotilaallinen toimintaympäristö on muuttunut. Puolustusselonteon 2017 mukaan Suomi vahvistaa kansallista puolustuskykyä ja tiivistää kansainvälistä puolustusyhteistyötä rakentamalla myös kybertoimintaympäristöön uusia kykyjä.

Ulkovaltojen sotilaalliset kohdejärjestelmät ovat muuttuneet entistä monimutkaisemmiksi, signaalien määrä on kasvanut merkittävästi, ja yhä suurempi osa tietoliikenteestä kulkee radiotien sijaan tietoliikennekaapeleissa. Toimintaympäristön muutoksen vuoksi Suomen sotilastiedustelun mahdollisuudet kerätä tiedustelutietoa ovat heikentyneet. Tietotekniikan nopean kehityksen ja alhai-

sempien kustannusten vuoksi sotilastiedustelun kohteet ottavat käyttöön entistä enemmän siviilikäyttöön suunniteltuja kommunikaatiojärjestelmiä. Asevoimien johtaminen tukeutuu entistä enemmän yleiseen tietoverkkoinfrastruktuuriin. Tietoteknistymisen myötä tietojärjestelmissä käsiteltävän tiedon määrä on kasvanut merkittävästi ja suurin osa tiedosta on nykyisin digitaalisessa muodossa. Nykyisin tiedustelun tulisi kohdistua digitaaliseen tietoon ollakseen tehokasta tietoteknistyneessä toimintaympäristössä.

Suomen turvallisuuteen kohdistuvat tietoverkkouhat

Digitalisoitumisen vaikutus turvallisuusympäristön kehittymiseen ja kyberturvallisuutta käsitellään muun muassa Suomen kyberturvallisuusstrategiassa ja puolustusministeriön mietinnössä Suomalaisen tiedustelulainsäädännön suuntaviivoja.

Kyberturvallisuusstrategia toteaa Suomen olevan tietoyhteiskuntana riippuvainen tietoverkkojen ja -järjestelmien toiminnasta ja näin ollen myös erittäin haavoittuvainen niihin kohdistuville häiriöille. Kybertoimintaympäristöön kohdistuvat uhkat ovat muuttuneet vaikutuksiltaan aiempaa vaarallisemmiksi yksittäisten ihmisten, yritysten sekä koko yhteiskunnan kannalta. Uhkia muodostavat toimijat ovat ammattimaisempia kuin ennen ja nykyään niihin voidaan laskea kuuluviksi myös valtiolliset toimijat. Kybertoimintaympäristössä toteutettavia hyökkäyksiä voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä ja vakavassa kriisissä yhtenä vaikuttamiskeinoa perinteisten sotilaallisten voimakeinojen ohella.

Tiedonhankintalakityöryhmän mietintö käsittelee digitalisoitumisen vaikutusta sekä viestinnän että tietoverkkoihin kohdistuvien uhkien näkökulmasta. Viestinnällisestä näkökulmasta digitalisoituminen mahdollistaa kansallista turvallisuutta uhkaavien tahojen aiempaa merkittävästi laajemman ja monimuotoisemman verkostoitumisen. Tietoverkkoja hyödynnetään näiden tahojen keskuudessa välineenä viestiä sellaisista suunnitelmista ja aikeista, jotka koskevat reaalimaailmassa toteutettavia tekoja. Teot voivat olla luonteeltaan sotilaallisia (aseellinen hyökkäys) tai ne voivat kohdistua muihin kansallisiin etuihin kuin valtion alueelliseen koskemattomuuteen, kuten vakoilu. Toisaalta tietoverkkoja hyödynnetään varsinaisena tekovälineenä kohdistaa kohteeseen, esimerkiksi Suomen valtioon, tätä vakavasti vahingoittavia tekoja. Kyse voi olla Suomen kyberturvallisuusstrategian tarkoittamista kybervakoiluksi tai kyberhyökkäykseksi luonnehdittavista teoista.

Turvallisuusviranomaisten arvion mukaan useat ulkovallat pyrkivät kohdistamaan laajaa ja teknisesti edistynyttä kybervakoilua Suomen valtiohallintoon ja kansataloudellisesti merkityksellisiin yrityksiin.

Maanpuolustukselle ja kansalliselle turvallisuudelle uhan muodostavat tahot käyttävät tietoverkkoja paitsi viestinnän myös uhkien toteuttamisen välineenä. Turvallisuusviranomaisten arvion mukaan useat ulkovallat pyrkivät kohdistamaan laajaa ja teknisesti edistynyttä kybervakoilua Suomen valtionhallintoon ja kansantaloudellisesti merkityksellisiin yrityksiin.

Suomen kyberturvallisuusstrategiassa käsiteltyjä valtion elinkelpoisuutta tai valtion keskeisiä turvallisuusetuja vaarantavia uhkia ovat ennen kaikkea kybervakoilu, kyberterrorismi ja kyberoperaatiot. Viimeksi mainittu käsite pitää sisällään sekä painostuksen, kyberympäristössä toteutuvan sotaa alemman tason konfliktin että sotaan liittyvät kyberoperaatiot. Kybervakoilulla hankitaan valtio- tai yrityssalaisuuksien tapaista luokiteltua tai sensitiivistä tietoa tietojärjestelmistä. Kybertoimintaympäristössä tapahtuva vakoilu voi jatkua jopa vuosia huomaamatta. Turvallisuusviranomaisten arvion mukaan useat ulkovallat pyrkivät kohdistamaan laajaa ja teknisesti edistynyttä kybervakoilua Suomen valtionhallintoon ja kansantaloudellista merkitystä omaaviin yrityksiin. Kybervakoilussa tekovälineenä ei ole tavallinen kaupallisella virustorjuntaohjelmalla havaittava haittaohjelma, vaan teknisesti kehittynyt ja monipuolinen verkkohyökkäystyökalu. Työkalun ensimmäisenä tehtävänä on verkon tietyn osan haltuunotto ja seuraavana tehtävänä kehittyneimpien hyökkäyksellisten vakoilu-

ja haittaohjelmien asentaminen. Vakoiluoperaatio on ennakkoon tarkoin suunniteltu ja sillä on täsmällinen operatiivinen tavoite kerätä tietoa esimerkiksi kohdevaltion ulko- ja turvallisuuspolitiikkaan, talouteen ja teollisuuteen liittyvistä seikoista. Tiedusteluohjelmien lisäksi voidaan tietojärjestelmiin toimittaa haittaohjelmia, jotka aktivoituvat kriisin alkaessa. Uudet teknologiat luovat uusia mahdollisuuksia kyberoperaatioilla käytävään sodankäyntiin, jonka vaikutukset kohdistetaan koko yhteiskuntaan, ei ainoastaan asevoimiin.

Kybervakoilun ja -operaatioiden merkitys kasvaa tulevina vuosina entisestään. Syitä tälle ovat mahdollisuus toteuttaa kybertoimintaympäristössä tekoja alhaisin kustannuksin, suojautumisen vaikeus ja kalleus sekä vähäinen kiinnijäämisriski. Myös kaikki Suomen turvallisuusympäristön kehityksen kannalta olennaiset ulkovallat panostavat määrätietoisesti hyökkäyksellisen kyberkapasiteettinsa rakentamiseen. 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.

Valtioneuvoston kanslia julkaisi 17.2.2017 riippumattoman tutkimuksen Suomen kyberturvallisuuden tilasta (Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017). Tutkimuksen mukaan kansallisen 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.

2.2 Lainsäädäntö ja käytäntö

2.2.1 Puolustusvoimia ja tiedonhankintaa koskeva lainsäädäntö

2.2.1.1 Laki puolustusvoimista

Puolustusvoimista annetun lain 2 §:n mukaan Puolustusvoimien tehtäviin kuuluu Suomen sotilaallinen puolustaminen, muiden viranomaisten tukeminen sekä osallistuminen sotilaalliseen kriisinhallintaan. Lain 2 §:n 1 momentin 1 kohdan a alakohdan mukaan Suomen sotilaalliseen puolustamiseen kuuluu maa-alueen, vesialueen ja ilmatilan valvominen sekä alueellisen koskemattomuuden turvaaminen ja b alakohdan mukaan kansan elinmahdollisuuksien, perusoikeuksien ja valtionjohdon toimintavapauden turvaaminen ja laillisen yhteiskuntajärjestyksen puolustaminen.

Puolustusvoimista annetun lain 2 §:n yksityiskohtaisissa perusteluissa (HE 264/2006 vp.) todetaan, että sotilasstrategisen tilannekuvan muodostamiseksi ja ylläpitämiseksi tiedustelu- ja valvontajärjestelmä seuraa Suomen turvallisuusympäristön kehitystä, määrittää ympäristön muutokset ja tuottaa tietoa vallitsevasta tilanteesta. Järjestelmä antaa ennakkovaroituksen sotilaallisten uhkien kehittymisestä, jotta voidaan käynnistää tarvittavat vastatoimet.

Edellä mainittujen tehtävien lisäksi Puolustusvoimille ollaan esittämässä uutta lakisääteistä tehtävää. EU:n yhteisvastuulauseke (Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 222 artikla) ja keskinäisen avunannon lauseke (Euroopan unionista tehdyn sopimuksen (SEU) 42 artiklan 7 kohta) edistävät unionin luonnetta turvallisuusyhteisönä ja vahvistavat EU:n jäsenvaltioiden mahdollisuuksia pyytää ja antaa apua erilaisissa kriisitilanteissa. Ulkoasiainministeriö asetti 25 päivänä maaliskuuta 2015 työryhmän valmistelemaan kansainvälisen avun antamiseen ja vastaanottamiseen liittyvää lainsäädäntöä. Puolustusministeriössä käynnistettiin asiassa toimialakoh-

tainen valmistelu. Esityksen tavoitteena on tehdä tarvittavat muutokset puolustusministeriön toimialan lainsäädäntöön, jotta Suomi voi osallistua täysimääräisesti Suomen kansainvälisten velvoitteiden mukaiseen yhteistyöhön sekä avun antamisen ja vastaanottamisen tilanteisiin puolustusministeriön hallinnonalalla. Hallitus antoi 2.6.2016 eduskunnalle hallituksen esityksen laiksi puolustusvoimista annetun lain, aluevalvontalain ja asevelvollisuuslain muuttamisesta.

Puolustusvoimista annetun lain 31 §:n mukaan tasavallan presidentti päättää valtakunnan sotilaallisen puolustuksen keskeisistä perusteista, sotilaallisen puolustusvalmiuden merkittävistä muutoksista, sotilaallisen puolustuksen toteuttamisen periaatteista sekä muista Puolustusvoimien sotilaallista toimintaa ja sotilaallista järjestystä koskevista laajakantoisista tai periaatteellisesti merkittävistä sotilaskäskyasioista. Sotilaskäskymenettelyllä on merkitystä tiedustelutehtävien antamisessa.

Sotilastiedustelun toimivaltuuksista ei ole säädetty. Puolustusvoimien vastatiedustelutehtävästä eli maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyvästä rikosten ennalta estämisestä ja paljastamisesta Suomen alueella sen sijaan on säädetty sotilaskurinpidosta ja rikostorjunnasta Puolustusvoimissa annetussa laissa (255/2014).

Puolustusvoimista annetun lain 47 §:n 1 momentin mukaan eroamisikä sotilasvirassa on 1) Puolustusvoimain komentajan virassa 63 vuotta, 2) pääesikunnan päällikön, kenraalin, amiraalin, everstin ja kommodorin sekä sotilasprofessorin virassa tai valtioneuvoston asetuksella tarkemmin säädettävässä näihin rinnastuvassa muussa sotilasvirassa 60 vuotta, kuitenkin lentäjän koulutusta edellyttävässä tehtävässä kenraalinvirassa 55 vuotta ja everstin virassa 52 vuotta sekä 3) muissa sotilasviroissa 55 vuotta, lentäjän koulutusta edellyttävässä tehtävässä kuitenkin 45–50 vuotta henkilön koulutus ja kokemus huomioon ottaen.

Pykälän 2 momentin mukaan valtioneuvoston asetuksella säädetään tarkemmin koulutuksen ja kokemuksen huomioon ottamisesta eroamisiästä säädettäessä. Puolustusvoimain komentaja määrää puolustusministeriön vahvistamien perusteiden mukaisesti ne tehtävät, jotka edellyttävät lentäjän koulutusta. Pääesikunta päättää näissä tehtävissä palvelevien eroamisiästä.

2.2.1.2 Laki sotilaallisesta kriisinhallinnasta

Puolustusvoimista annetun lain 2 §:n 1 momentin 3 -kohdan mukaan Puolustusvoimien tehtävänä on osallistuminen kansainväliseen sotilaalliseen kriisinhallintaan. Saman lain 2 luvussa säädetään Puolustusvoimien toimivallasta. Lain 13 §:n mukaan Puolustusvoimat osallistuu kansainväliseen sotilaalliseen kriisinhallintaan siten kuin sotilaallisesta kriisinhallinnasta annetussa laissa (211/2006) säädetään.

Sotilaallisesta kriisinhallinnasta annetun lain 5 §:n mukaan puolustusministeriö antaa sotilaallisen kriisinhallinnan edellyttämät tehtävät Puolustusvoimille sekä ohjaa ja valvoo sotilaallista kriisinhallintaa. Suomalaiseen kriisinhallintaorganisaatioon voi kuulua kriisinhallintajoukkoja, erillisiä yksiköitä ja yksittäisiä henkilöitä. Kriisinhallintaorganisaatio kuuluu Puolustusvoimiin ja on pääesikunnan alainen siten kuin sotilaallisesta kriisinhallinnasta annetun lain 5 §:ssä säädetään. Toiminnallisesti kriisinhallintaorganisaatio on sotilaallisesta kriisinhallinnasta annetun lain 1 §:n 3 momentissa tarkoitetun toimeenpanijan alainen. Näitä ovat YK, Euroopan turvallisuus- ja yhteistyöjärjestö (Etyj), Euroopan unioni (EU), Pohjois-Atlantin liitto (Nato) taikka muu kansainvälinen järjestö tai maaryhmä. Sotilaallisesta kriisinhallinnasta annetussa laissa tai Puolustusvoimien toimintaa koskevissa laessa ei ole erityissääntelyä kriisinhallintaoperaatioiden sotilastiedustelusta.

Sotilaallisesta kriisinhallinnasta annetun lain 7 §:n 1 momentin mukaan kriisinhallintahenkilöstöllä tarkoitetaan lain 8 §:n 1 momentin mukaisen palvelussitoumuksen tehneitä henkilöitä, kriisinhallintaorganisaatioon kuuluvia henkilöitä, vaihtohenkilöstöä sekä valmistelu- ja varautumistehtäviin erikseen määrättyjä henkiöitä.

Pykälän 2 momentin mukaan palvelussuhteen alkamisen jälkeen kriisinhallintahenkilöstö on palvelussuhteessa valtioon, jota työnantajana edustavat puolustusministeriö ja Puolustusvoimat siten kuin puolustusministeriön asetuksella säädetään.

Pykälän 3 momentin mukaan kriisinhallintatehtäviin valittavien henkilöiden tulee olla Suomen kansalaisia. Heitä koskevista pätevyysvaatimuksista säädetään puolustusministeriön asetuksella.

Sotilaallisesta kriisinhallinnasta annetun lain 9 §:n 1 momentin mukaan kriisinhallintajoukon komentajan ja kriisinhallintaorganisaatiossa kenraalin sotilas- tai palvelusarvossa palvelevan määrää tehtävään tasavallan presidentti valtioneuvostossa valtioneuvoston ratkaisuehdotuksessa. Palvelussuhde alkaa nimetystä päivästä ja on voimassa toistaiseksi. Muun henkilöstön enintään vuodeksi kerrallaan määrää puolustusministeriö tai Puolustusvoimien tehtävään määräävä viranomainen ministeriön tehtävien osalta.

2.2.1.3 Aluevalvontalaki

Valtion täysivaltaisuuteen kuuluu sen alueellinen koskemattomuus. Aluevalvontalakiin (755/2000) sisältyvät säännökset Suomen alueellisen koskemattomuuden valvonnasta ja turvaamisesta. Aluevalvonnalla ehkäistään tai paljastetaan ja selvitetään aluerikkomukset ja alueloukkaukset. Lain nojalla on annettu tarkempia säännöksiä aluevalvonnasta annetussa valtioneuvoston asetuksessa (971/2000).

Vieraan valtion vihamielinen toiminta määritellään aluevalvontalain 34 §:ssä. Pykälän 2 momentin 4 kohdan mukaan vihamielistä toimintaa on vieraan valtion Suomen alueella oleviin, valtakunnan turvallisuuden kannalta tärkeisiin kohteisiin oikeudettomasti kohdistamaa tiedustelua ja elektronista häirintää. Lisäksi momentin 5 kohdan mukaan vihamielistä toimintaa on vieraan valtion aluevalvontatehtävässä olevaan suomalaiseen valtionilma-alukseen tai valtionalukseen oikeudettomasti kohdistamaa elektronista häirintää.

2.2.1.4 Laki sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa

Sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain tarkoittamassa sotilasvastatiedustelussa on kyse rikosten ennalta estämisestä ja paljastamisesta Suomen alueella. Lain tarkoittamalla sotilasvastatiedustelulla tarkoitetaan sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaa laittoman tiedustelutoiminnan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyvää rikosten ennalta ehkäisemistä ja paljastamista.

Rikoksen estäminen määritellään poliisilaissa. Poliisilain 5 luvun 1 §:n 2 momentin mukaan rikoksen estämisellä tarkoitetaan toimenpiteitä, joiden tavoitteena on estää rikos, sen yritys tai valmistelu, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan perustellusti olettaa hänen syyllistyvän rikokseen, taikka keskeyttää jo aloitetun rikoksen tekeminen tai rajoittaa siitä välittömästi aiheutuvaa vahinkoa tai vaaraa. Henkilön toiminnasta tehdyillä havainnoilla tai siitä muutoin saaduilla tiedoilla tarkoitetaan välittömästi henkilön omasta toiminnasta tehtyjä havaintoja ja vihjetietoja sekä muuta välillistä selvitystä. Havaintoihin ja muuten saatuihin tietoihin kuuluvat myös muun muassa rikostiedustelutiedot, tarkkailuhavainnot, muut vihjetiedot ja rikosanalyysilla tiedoista tehtävät johtopäätökset. Edellytyksenä rikoksen estämiseksi säädetyn tiedonhankintakeinon käytölle on, että tällaisten tietojen perusteella on muodostunut perusteltu oletus henkilön syyllistymisestä rikokseen (HE 224/2010 vp, s. 89).

Lisäksi poliisilain mukaan rikoksen estäminen on varhaisvaiheen ennakollista viranomaistoimintaa. Poliisilain 5 luvun 1 §:n 2 momentin mukaan rikoksen estäminen kattaa toimenpiteet, joiden tarkoituksena on estää rikoksen yritys ja valmistelu. Valmistelun estämisellä tarkoitetaan rangaistavan teon valmistelun estämistä myös silloin, kun itse valmistelua ei ole kriminalisoitu.

Poliisilain 5 luvun 1 §:n 3 momentin mukaan rikoksen paljastamisella tarkoitetaan toimenpiteitä, joiden tavoitteena on selvittää, onko esitutkinnan aloittamiselle esitutkintalain 3 luvun 3 §:n 1 momentissa tarkoitettua perustetta, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan olettaa, että rikos on tehty. Rikoksen paljastamisen käsite viittaa rikoksen estämisen ja selvittämisen väliin jäävään harmaaseen alueeseen.

Rikoksen paljastamisessa ei ole kyse rikoksen selvittämisestä, koska esitutkinnan käynnistämisen edellytykset puuttuvat, eikä myöskään rikoksen estämisestä, koska rikos oletetaan jo tehdyksi. Rikoksen paljastamisesta on kyse esimerkiksi tilanteessa jossa vihjetiedon mukaan rikos olisi jo tehty, mutta konkreettista perustetta epäilylle ei vielä ole eli esitutkintalain mukainen syytä epäillä -kynnys ei ole ylittynyt. (HE 224/2010 vp, s. 90).

Puolustusvoimien rikostorjunnalla estetään ulkovaltojen Suomeen kohdistama, Suomen rikoslaissa kriminalisoitu tiedonhankinta Suomessa esimerkiksi Puolustusvoimien suorituskyvyistä ja kokoonpanoista. Tyypillisiä rikosnimikkeitä, jotka ovat ennalta estämisen ja paljastamisen kohteina, ovat rikoslain 12 luvussa tarkoitetut maanpetosrikokset, kuten maanpetos, vakoilu ja luvaton tiedustelutoiminta, ja 13 luvun valtiopetosrikokset. Myös tavallisemmat rikokset, kuten omaisuusrikokset, voivat kuitenkin olla ennalta estämisen ja paljastamisen kohteina, mikäli ne liittyvät sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan. Esimerkkeinä tällaisista ovat Puolustusvoimien salassa pidettävään tietoon kohdistuva tietoturvallisuusrikos tai omaisuusrikos. Tyhjentävää luetteloa toimivaltaa koskevista rikoksista ei ole säädetty.

Puolustushallinnon alalla Puolustusvoimien sotilasvastatiedustelutehtävästä säädetään sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetussa laissa. Puolustusvoimat toimii vastatiedustelun osalta erityisviranomaisena, jonka tehtävänä on huolehtia suojelupoliisille laissa säädettyä toimivaltaa rajoittamatta sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyvien rikosten ennalta estämisestä ja paljastamisesta. Puolustusvoimien toimivalta rikosten ennalta estämisen ja paljastamisen osalta on suojelupoliisille poliisin hallinnosta annetun lain 10 §:ssä säädettyä yleistoimivaltaa rajatumpi ja koskee vain niitä rikoksia, jotka liittyvät sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan. Tällä alueella toimivalta on rinnakkainen suojelupoliisin rikosten ennalta estämistä ja paljastamista koskevan yleistoimivallan kanssa, mutta se ei rajoita suojelupoliisin yleistoimivaltaa. Lakiin on sisällytetty poliisille otto-oikeus, eli oikeus myös omaaloitteisesti ottaa Puolustusvoimissa ennalta estettävä ja paljastettava asia hoitaakseen.

Rikosten ennalta estämisessä ja paljastamisessa noudatetaan myös Puolustusvoimissa poliisilaissa säädettyjä periaatteita, ja niistä erityisesti perus- ja ihmisoikeuksien kunnioittamisen periaatetta, suhteellisuusperiaatetta, vähimmän haitan periaatetta ja tarkoitussidonnaisuuden periaatetta.

Suojelupoliisi vastaa Puolustusvoimien sotilasvastatiedustelussa esille tulleen rikoksen selvittämisestä.

Puolustusvoimissa rikosten ennalta estämistä ja paljastamista hoitavien virkamiesten toimivaltuuksista on sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain mukaan voimassa, mitä poliisilaissa säädetään toimivaltuuksista rikosten ennalta estämiseksi ja paljastamiseksi. Salaisten tiedonhankintakeinojen osalta Puolustusvoimien käytössä on kuitenkin vain seuraava rajattu osa poliisin toimivaltuuksista; 1) tukiasematietojen hankkiminen, 2) suunnitelmallinen tarkkailu, 3) peitelty tiedonhankinta, 4) tekninen kuuntelu, 5) tekninen katselu, 6) tekninen seuranta, 7) teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen. Yksittäisiä toimivaltuuksia käsitellään tarkemmin jäljempänä kappaleessa 2.2.2.

Lisäksi rikosten paljastamistehtävää koskevan lisärajauksen mukaisesti rikosten paljastamisessa näitä tiedonhankintatoimenpiteitä saadaan käyttää vain kun on kyse Suomen itsemääräämisoikeuden vaarantamista, sotaan yllyttämistä, maanpetosta tai törkeää maanpetosta, vakoilua tai törkeää vakoilua, turvallisuussalaisuuden paljastamista tai luvatonta tiedustelutoimintaa koskevan rikoksen paljastamisesta. Puolustusvoimien rikosten ennalta estämistä ja paljastamista hoitavan virkamiehen on ilmoitettava edellä mainittujen salaisten tiedonhankintakeinojen käyttämisestä suojelupoliisille.

Rikoksen paljastamiseen yllä mainittuja salaisia tiedonhankintakeinoja voidaan käyttää vain, jos kysymyksessä on laissa tarkemmin säädetty maanpetosrikos. Rikosten paljastamisen yhteydessä ei sovelleta salaisten tiedonhankintakeinojen keinokohtaisissa säännöksissä säädettyjä erityisiä edellytyksiä.

Salaisten tiedonhankintakeinojen valintaa ja käyttöä ohjaavat poliisilain 1 luvussa säädetyt yleiset periaatteet, kuten perus- ja ihmisoikeuksien kunnioittamisen periaate, suhteellisuusperiaate, vähimmän haitan periaate ja tarkoitussidonnaisuuden periaate.

Sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetussa laissa säädetään poliisin antamasta avusta silloin, kun Puolustusvoimien rikostorjuntaa hoitavilla ei ole toimivaltaa tehtävien hoitamiseksi tarpeellisen toimenpiteen suorittamiseen. Käytännössä kyse on tietojen hankkimisesta sellaisella poliisin käytössä olevalla toimivaltuudella, jonka käyttämiseen Puolustusvoimilla ei ole oikeutta. Rikosten ennalta estämistä ja paljastamista toteuttavat pääesikunnan ja sen alaisuudessa toimivaan Puolustusvoimien tiedustelulaitokseen sijoitetut virkamiehet.

Myös asevelvollisuuslain mukaisessa palveluksessa olevia reserviläisiä voidaan SKRTL:n 86 §:n mukaan käyttää Puolustusvoimien rikosten ennalta estämiseen ja paljastamiseen liittyvässä tehtävässä normaaliolojen vakavissa häiriötilanteissa ja poikkeusoloissa. SKRTL:n 86 §:n mukaiset reserviläisten toimivaltuudet häiriötilanteissa ja poikkeusoloissa on katsottu tarpeelliseksi, sillä oletettavaa, että sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaan ja sotilaalliseen maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyvien rikosten määrä tuolloin lisääntyy. Varusmiespalvelustaan suorittavia tähän toimintaan ei ole sallittua käyttää. Tämä johtuu siitä, että varusmiespalveluksen tarkoitus ei kata tehtävää, minkä lisäksi on huomattava, että varusmiespalveluksessa olevien koulutus on kesken.

Reserviläinen, joka on määrätty SKRTL:n mukaiseen Puolustusvoimien rikosten ennalta estämis- ja paljastamistehtävään, voi osallistua SKRTL:n 89 §:ssä tarkoitettujen tiedonhankintamenetelmien käyttöön Puolustusvoimien rikosten ennalta estämis- ja paljastamistehtävään määrätyn virkamiehen ohjauksessa ja valvonnassa. Näin ollen merkittävää julkisen vallan käyttöä ei poikkeusoloissakaan siirry muille kuin virkamiehille. Reserviläisiä koskevat samat salassapitovelvoitteet kuin heitä ohjaavia ja valvovia virkamiehiä.

SKRTL:n 10 luvussa säädetään normaaliolojen vakavista häiriötilanteista ja poikkeusoloista. SKRTL:n 102 §:n 1 momentin mukaan poliisimiehelle säädettyjä toimivaltuuksia voi 86 §:n 1 momentissa tarkoitetussa tehtävässä käyttää tehtävään riittävän koulutuksen saanut asevelvollisuuslain mukaisessa palveluksessa oleva reserviläinen.

Pykälän 2 momentin mukaan asevelvollisuuslain mukaisessa palveluksessa oleva reserviläinen, joka on määrätty tämän lain mukaiseen Puolustusvoimien rikosten ennalta estämis- ja paljastamistehtävään, saa osallistua 86 §:n 1 momentissa tarkoitetun tehtävän suorittamiseen ja 89 §:n 1 momentissa tarkoitettujen tiedonhankintamenetelmien käyttöön Puolustusvoimien rikosten ennalta estämis- ja paljastamistehtävään määrätyn virkamiehen ohjauksessa ja valvonnassa.

2.2.1.5 Poliisilaki

Poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen. Poliisi toimii turvallisuuden ylläpitämiseksi yhteistyössä muiden viranomaisten sekä yhteisöjen ja asukkaiden kanssa ja huolehtii tehtäviinsä kuuluvasta kansainvälisestä yhteistyöstä.

Poliisin organisaatiossa kansalliseen turvallisuuteen kohdistuvien uhkien torjunnasta vastaa valtakunnallisena yksikkönä toimiva suojelupoliisi. Suojelupoliisin tärkeimpänä tehtävänä on ennalta estää ja paljastaa terrorismiin, laittomaan tiedustelutoimintaan, joukkotuhoaseiden levittämiseen ja ääriliikkeisiin kytkeytyviä rikoksia ja hankkeita. Tehtävän suorittaminen edellyttää, että suojelupoliisi kykenee hankkimaan tällaisista rikoksista ja hankkeista tietoa. Poliisin hallinnosta annetun lain 10 §:n mukaan suojelupoliisin tehtävänä on sisäministeriön ohjauksen mukaisesti torjua sellaisia hankkeita ja rikoksia, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta sekä suorittaa tällaisten rikosten tutkintaa. Sen tulee myös ylläpitää ja kehittää yleistä valmiutta valtakunnan turvallisuutta vaarantavan toiminnan estämiseksi. Poliisin hallintolaki koskevan hallituksen esityksen (HE 155/1991 vp.) mukaan säännöksen kirjoittamistavassa on pyritty ottamaan huomioon ennalta estävän toiminnan korostunut merkitys suojelupoliisin tehtäväalueella. Esitöiden mukaan suojelupoliisin työssä on erityisen keskeisellä sijalla valtakunnan turvallisuutta vaarantavien tekojen estäminen ennakolta, kun taas tutkinnan kohdistaminen jo tapahtuneeseen turvallisuusetujen loukkaamiseen on yleensä osoitus ennalta estävän toiminnan jonkinasteisesta epäonnistumisesta.

Poliisin hallintolain 10 § määrittelee suojelupoliisin toimialan luettelemalla ne oikeushyvät - sisäinen turvallisuus, ulkoinen turvallisuus, valtiojärjestys, yhteiskuntajärjestys -, joiden suojeleminen kuuluu suojelupoliisille. Niitä konkreettisia ilmiöitä ja turvallisuusuhkia, joiden torjuminen kuuluu suojelupoliisille, ei mainita laissa.

Kuten Puolustusvoimien kohdalla, julkisiin lähteisiin kohdistuva tiedonhankinta ei vaadi erillistä sääntelyä. Koska suojelupoliisin torjuttavina olevat hankkeet ja rikokset pyritään valmistelemaan salassa, ei tiedonhankintaa voida käytännössä perustaa julkisesti saatavilla oleviin tietoihin. Suojelupoliisin on siten keskeisesti saatava tietoa toiminnasta, joka tehdään salassa. Ollakseen tehokasta on tiedonhankinta lisäksi suoritettava salassa sen kohteelta.

Suojelupoliisille ei ole säädetty erityisiä toimivaltuuksia valtion turvallisuuteen liittyvän uhkatiedon hankkimista varten. Suojelupoliisi on poliisiviranomainen, joka toiminnassaan käyttää poliisille säädettyjä tiedonhankinta- ja muita toimivaltuuksia.

Suojelupoliisin käytännön toiminnassa keskeisiä ovat poliisilaissa säädetyt salaiset tiedonhankintakeinot rikoksen estämiseksi ja paljastamiseksi. Rikosten selvittämistehtävät rajoittuvat suojelupoliisin osalta käytännössä lähinnä vakoilurikosten tutkintaan. Suojelupoliisi toimittaa esitutkinnan vain harvoin.

Poliisilain 5 luvun 1 §:n 2 momentin mukaan rikoksen estämisellä tarkoitetaan toimenpiteitä, joiden tavoitteena on estää rikos, sen yritys tai valmistelu, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan perustellusti olettaa hänen syyllistyvän rikokseen, taikka keskeyttää jo aloitetun rikoksen tekeminen tai rajoittaa siitä välittömästi aiheutuvaa vahinkoa tai vaaraa. Henkilön toiminnasta tehdyillä havainnoilla tai siitä muutoin saaduilla tiedoilla tarkoitetaan välittömästi henkilön omasta toiminnasta tehtyjä havaintoja ja ulkopuolisen henkilön antamia vihjetietoja ja muuta välillistä selvitystä. Havaintoihin ja muuten saatuihin tietoihin kuuluvat myös muun muassa rikostiedustelutiedot, tarkkailuhavainnot, muut vihjetiedot ja rikosanalyysilla tiedoista tehtävät johtopäätökset. Edellytyksenä rikoksen estämiseksi säädetyn tiedonhankintakeinon käy-

tölle on, että tällaisten tietojen perusteella on muodostunut perusteltu oletus henkilön syyllistymisestä rikokseen (HE 224/2010 vp, s. 89).

Poliisilain mukainen rikoksen estäminen on varhaisvaiheen ennakollista viranomaistoimintaa. Poliisilain 5 luvun 1 §:n 2 momentin mukaan rikoksen estäminen kattaa toimenpiteet, joiden tarkoituksena on estää rikoksen yritys ja valmistelu. Valmistelun estämisellä tarkoitetaan rangaistavan teon valmistelun estämistä myös silloin, kun itse valmistelua ei ole kriminalisoitu.

Poliisilain 5 luvun 1 §:n 3 momentin mukaan rikoksen paljastamisella tarkoitetaan toimenpiteitä, joiden tavoitteena on selvittää, onko esitutkinnan aloittamiselle esitutkintalain 3 luvun 3 §:n 1 momentissa tarkoitettua perustetta, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan olettaa, että rikos on tehty. Rikoksen paljastamisen käsite viittaa rikoksen estämisen ja selvittämisen väliin jäävään harmaaseen alueeseen. Kyse ei ole rikoksen selvittämisestä, koska esitutkinnan käynnistämisen edellytykset puuttuvat, eikä myöskään rikoksen estämisestä, koska rikos oletetaan jo tehdyksi. Rikoksen paljastamisesta on kyse esimerkiksi tilanteessa jossa vihjetiedon mukaan rikos olisi jo tehty, mutta konkreettista perustetta epäilylle ei vielä ole eli esitutkintalain mukainen syytä epäillä -kynnys ei ole ylittynyt. (HE 224/2010 vp, s. 90).

Poliisilain 5 luku sisältää säännökset salaisista tiedonhankintakeinoista, joita suojelupoliisi saa käyttää tietojen hankkimiseksi toimenpiteen kohteelta salassa. Salaisia tiedonhankintakeinoja ovat telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, televalvonta teleosoitteen tai telepäätelaitteen haltijan suostumuksella, tukiasematietojen hankkiminen, suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen laitetarkkailu, teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen, peitetoiminta, valeosto, tietolähdetoiminta ja tietolähteen ohjattu käyttö ja valvottu läpilasku.

Sisäministeriö määrää Poliisihallitusta kuultuaan tarkemmin ne asiaryhmät, jotka kuuluvat suojelupoliisin tutkittaviksi sekä päättää Poliisihallitusta kuultuaan tarvittaessa tarkemmin suojelupoliisin ja muiden poliisiyksiköiden välisestä yhteistoiminnasta ja yhteistyöstä sekä niiden välisistä tutkintajärjestelyistä.

Suojelupoliisille säädettyjen tehtävien hoitaminen pitää sisällään aktiivisen Suomen turvallisuusympäristön seurannan, turvallisuusuhkia koskevan ennakoivan tiedonhankinnan ja hankittujen tietojen analysoinnin. Analysoitua tietoa tuotetaan ensisijaisesti ylimmän valtiojohdon tarpeisiin. Poliisin hallinnosta annetun lain 4 a § säätää suojelupoliisille velvollisuuden ilmoittaa tehtäviinsä kuuluvista yhteiskunnallisesti merkittävistä asioista suoraan sisäministerille ja poliisiylijohtajalle. Säännöksen perusteluiden mukaan suojelupoliisilla on velvollisuus informoida myös tasavallan presidenttiä, pääministeriä ja ulkoasiainministeriä ottaen huomioon heille säädetyt ulko- ja turvallisuuspoliittiset tehtävät. Lisäksi suojelupoliisi informoi eduskunnan perustuslaki-, hallinto- ja ulkoasiainvaliokuntia Suomen turvallisuustilanteen kehittymisestä.

Suojelupoliisi siirtyi Poliisihallituksen alaisuudesta suoraan sisäministeriön alaiseksi poliisiyksiköksi 1.1.2016. Sisäministeriö vastaa suojelupoliisin toiminnan ohjauksesta, tulos- ja resurssiohjauksesta sekä laillisuusvalvonnasta. Suojelupoliisi säilyy edelleen poliisiyksikkönä. Suojelupoliisin ja muiden poliisiyksiköiden välistä yhteistyötä ja työnjakoa koskevat ohjaustehtävät siirtyvät Poliisihallitukselta sisäministeriölle. Siirron tavoitteena on ollut tehostaa suojelupoliisin erityistehtävien hoitamista ja vahvistaa toiminnan strategista ja poliittista ohjausta sekä selkeyttää viraston asemaa kansallisessa ja kansainvälisessä yhteistyössä.

Suojelupoliisin tärkeimpänä tehtävänä on ennalta estää ja paljastaa terrorismiin, laittomaan tiedustelutoimintaan, joukkotuhoaseiden levittämiseen ja ääriliikkeisiin sekä valtion turvallisuutta vaarantavaan järjestäytyneeseen rikollisuuteen kytkeytyviä hankkeita ja rikoksia sekä rajatussa määrin

myös suorittaa edellä mainittuihin ilmiöihin liittyvien rikosten tutkintaa. Tehtävän suorittaminen edellyttää, että suojelupoliisi kykenee hankkimaan tällaisista hankkeista ja rikoksista tietoa.

Salaisten tiedonhankintakeinojen käytön yleisenä edellytyksenä poliisilain 5 luvun 2 §:n 1 momentin mukaan on, että sillä voidaan olettaa saatavan rikoksen estämiseksi tai paljastamiseksi taikka vaaran torjumiseksi tarvittavia tietoja. Telekuuntelun, tietojen hankkimisen telekuuntelun sijasta, suunnitelmallisen tarkkailun, teknisen kuuntelun, henkilön teknisen seurannan, teknisen laitetarkkailun, peitetoiminnan, valeoston, tietolähteen ohjatun käytön ja valvotun läpilaskun yleisenä lisäedellytyksenä saman pykälän 2 momentin mukaan on, että niillä voidaan olettaa olevan erittäin tärkeä merkitys rikoksen estämiselle tai paljastamiselle. Peitetoiminnan ja valeoston käyttäminen edellyttää lisäksi, että käyttö on välttämätöntä rikoksen estämiseksi tai paljastamiseksi.

Eri tiedonhankintakeinojen käytölle on poliisilaissa asetettu niin sanottuja yleisiä edellytyksiä ja erityisiä edellytyksiä. Salaisten tiedonhankintakeinojen käytön erityisinä edellytyksinä ovat ennen kaikkea ne yksilöidyt rikokset, joiden estämiseksi kutakin keinoa voidaan käyttää. Eri tiedonhankintakeinoja koskevissa säännöksissä on myös voitu asettaa muita erityisiä edellytyksiä. Kokoavasti voidaan todeta, että suojelupoliisi voi likimain kattavasti käyttää poliisilain 5 luvussa säädettyjä salaisia tiedonhankintakeinoja rikoslain 34 a luvussa rangaistaviksi säädettyjen terrorismirikosten ja rikoslain 12 luvussa rangaistaviksi säädettyjen laittomaan tiedustelutoimintaan liittyvien rikosten estämiseksi. Joukkotuhoaseiden ja kaksikäyttötuotteiden levittämiseen tähtäävien rikosten samoin kuin järjestäytyneen rikollisryhmän toimintaan liittyvien valtion turvallisuutta vaarantavien rikosten estämisen kohdalla tilanne on moniulotteisempi ja tulkinnanvaraisempi.

Poliisilain 5 luvun mukaisia salaisia tiedonhankintakeinoja ovat telekuuntelu (PolL 5:5), televalvonta (PolL 5:8), tukiasematietojen hankkiminen (PolL 5:11), suunnitelmallinen tarkkailu (PolL 5:13), peitelty tiedonhankinta (PolL 5:15), tekninen kuuntelu (PolL 5:17), tekninen katselu (PolL 5:19), henkilön tekninen seuranta (PolL 5:21), tekninen laitetarkkailu (PolL 5:23), teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen (PolL 5:25), peitetoiminta (PolL 5:28) ja valeosto (PolL 5:35), tietolähteen ohjattu käyttö (PolL 5:40) sekä valvottu läpilasku (PolL 5:43). Yksittäisiä toimivaltuuksia käsitellään tarkemmin jäljempänä tässä kappaleessa 2.2.2.

Toimivaltuuksilla on käytännön merkitystä Puolustusvoimien rikostorjunnassa SKRTL:n 90 §:n kautta. Sen mukaan poliisi voi suorittaa toimivaltaansa kuuluvan yksittäisen toimenpiteen Puolustusvoimille, jos Puolustusvoimilla ei ole toimivaltaa toimenpiteen suorittamiseen, ja luovuttaa saadut tallenteet ja asiakirjat Puolustusvoimien rikosten ennalta estämistä ja paljastamista suorittaville virkamiehille.

2.2.1.6 Laki viestintähallinnosta ja tietoyhteiskuntakaari

Viestintähallinnosta annetun lain (625/2001) 1 §:n mukaan viestinnän hallintotehtäviä varten on liikenne- ja viestintäministeriön hallinnonalalla toimiva Viestintävirasto.

Lain 2 §:n 1 kohdan mukaan viestintäviraston tehtävänä on huolehtia muun muassa tietoyhteiskuntakaaressa sille säädetyistä tehtävistä. Pykälän 2 kohdan mukaan Viestintäviraston tehtävänä on hoitaa muut tehtävät, jotka sille säännösten tai liikenne- ja viestintäministeriön määräysten mukaan kuuluvat.

Tietoyhteiskuntakaaren 272 § antaa sähköisiä viestintäpalveluja hyödyntäville yrityksille, yhteisöille ja viranomaisille tietoturvastaan huolehtimisen tarkoituksessa oikeuden analysoida verkkoonsa tulevien ja siitä lähtevien viestien sisältöä muun muassa haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi.

Tietoyhteiskuntakaarta edeltäneen sähköisen viestinnän tietosuojalain (516/2004) 20 §:n alkuperäisten esitöiden (HE 125/2003 vp, s. 71) mukaan ilmaisulla ”haittaa aiheuttavat häiriöt” viitataan muun muassa haittaohjelmien tahalliseen laajaan levittämiseen ja käyttöön. Tietoyhteiskuntakaaren 272 §:n yksityiskohtaisissa perusteluissa todetaan, ettei tämän säännöksen osalta ole tarkoitus muuttaa vallitsevaa oikeustilaa (HE 221/2013 vp, s. 106).

2.2.1.7 Asevelvollisuuslaki

Asevelvollisuuslain 2 §:n 1 momentin mukaan jokainen miespuolinen Suomen kansalainen on asevelvollinen sen vuoden alusta, jona hän täyttää 18 vuotta, sen vuoden loppuun, jona hän täyttää 60 vuotta, jollei asevelvollisuuslaissa toisin säädetä.

Pykälän 2 momentin mukaan asevelvollisuuden suorittamiseen kuuluu varusmiespalvelus, kertausharjoitus, ylimääräinen palvelus ja liikekannallepanon aikainen palvelus sekä osallistuminen kutsuntaan ja palveluskelpoisuuden tarkastukseen.

Pykälän 3 momentin mukaan asevelvollinen on palveluksessa taikka kuuluu reserviin tai vara-reserviin.

Asevelvollisuuslain 32 §:ssä säädetään kertausharjoitukseen määräämisestä. Pykälän 1 momentin mukaan kertausharjoitukseen voidaan määrätä reserviin kuuluva asevelvollinen.

Pykälän 2 momentin mukaan määräys osallistua kertausharjoitukseen lähetetään asevelvolliselle vähintään kolme kuukautta ennen harjoituksen alkamista. Määräajasta voidaan asevelvollisen suostumuksella poiketa.

Pykälän 3 momentin mukaan Suomen turvallisuusympäristössä ilmenevän välttämättömän tarpeen sitä edellyttäessä voidaan reserviin kuuluvia asevelvollisia määrätä 48 §:n 4 kohdassa tarkoitettuun kertausharjoitukseen 2 momentissa säädetystä määräajasta poiketen. Määräys kertausharjoitukseen annetaan kunkin asevelvollisen osalta enintään 30 päiväksi kerrallaan.

Pykälän 4 momentin mukaan päätöksen 3 momentissa tarkoitetusta kertausharjoituksesta tekee tasavallan presidentti Puolustusvoimain komentajan esittelystä puolustusvoimista annetun lain 32 §:n 2 momentissa tarkoitetussa päätöksentekomenettelyssä siten, että puolustusministerin tulee olla läsnä ja lausua käsityksensä asiasta. Lisäksi pääministeri voi olla läsnä ja lausua käsityksensä asiasta. Tasavallan presidentin päätös ja sen nojalla annetut määräykset on peruutettava, kun kertausharjoitukseen johtanut tilanne sen sallii. Sotilaskäskyasian siirtämisestä presidentin valtioneuvostossa ratkaistavaksi säädetään puolustusvoimista annetun lain 32 §:n 3 momentissa.

Asevelvollisuuslain 48 §:ssä säädetään kertausharjoituksen tarkoituksesta. Pykälän 1 momentin mukaan reservin kertausharjoituksilla 1) pidetään yllä varusmiespalveluksen aikana saatuja sotilaallisia tietoja ja taitoja sekä koulutetaan vaativampiin tehtäviin, 2) perehdytetään asevelvolliset sotilaallisessa maanpuolustuksessa tapahtuneen kehityksen mukanaan tuomiin muutoksiin, 3) harjoitetaan joukkokokonaisuuksia niille suunnitelluissa kokoonpanoissa tai 4) mahdollistetaan sotilaallisen valmiuden joustava kohottaminen.

2.2.1.8 Laki viranomaisten toiminnan julkisuudesta

Viranomaisten toiminnan julkisuudesta annetun lain (jälj. julkisuuslaki) 31 § 2 momentin mukainen yleinen salassapitoaika on 25 vuotta. Yleinen salassapitoaika on jo aiemmin Puolustusvoimissa todettu liian lyhyeksi kysymyksen ollessa tietyistä Puolustusvoimien toimitiloista ja pitkäaikaiskäytössä olevista puolustusmateriaaleista, mikä on huomioitu vuoden 2005 julkisuuslain päivityksessä (495/2005). Salassapitoaikaa voidaan jatkaa julkisuuslain 31 §:n nojalla, mikäli asiakirjan julkiseksi

tulemisella olisi haittaa maanpuolustuksen tai väestönsuojelun kannalta. Tällaista tietoa sisältävä asiakirja voi koskea kiinteistöä, rakennusta, rakennelmaa, järjestelmää, laitetta tai menetelmää. Mahdollisuus salassapitoajan jatkamiseen ei koske henkilötietoja.

Julkisuuslain 31 § 3 momentin mukaan valtioneuvosto voi jatkaa laissa säädetyin edellytyksin salassapitoaikaa enintään 30 vuodella. Tämä on kuitenkin tarkoitettu poikkeukselliseksi toimenpiteeksi eikä siihen turvautumista voida pitää asianmukaisena silloin, kun kysymys on säännönmukaisesta ja ennakoitavissa olevasta salassapitotarpeesta.

2.2.2 Puolustusvoimien tiedonhankinnan nykytila

2.2.2.1 Sotilastiedustelu osana maanpuolustusta

Puolustusvoimien maanpuolustustehtävässä suoritettavan sotilastiedustelutoiminnan on katsottu perustuvan Puolustusvoimien lakisääteiseen tehtävään puolustaa valtakunnan itsenäisyyttä ja alueellista koskemattomuutta. Tällöin sotilastiedustelun on katsottu sisältyvän puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdan a ja b alakohtiin eikä sitä ole mainittu laissa erikseen.

Sotilastiedustelu kohdistuu Suomen ulkopuoliseen toimintaympäristöön. Sotilastiedustelun tehtävänä on muodostaa ja ylläpitää sotilaallisen päätöksenteon edellyttämää sotilasstrategista tilannekuvaa. Sen muodostamiseksi sotilastiedustelu seuraa Suomen turvallisuusympäristön kehitystä, määrittää ympäristön muutokset ja tuottaa tietoa vallitsevasta tilanteesta.

Sotilastiedustelulla Puolustusvoimat ylläpitää ja kehittää puolustusvalmiutta. Keskeistä on ennakkovaroituskyky sotilaallisten uhkien kehittymisestä, jotta Suomen turvallisuutta koskeva ylimmän valtionjohdon päätöksenteko Suomen valtion suvereniteettia vaarantavista uhista perustuu oikea-aikaiselle tilannetiedolle, ja mahdollistaa tarvittaessa oikea-aikaisiin varautumis- ja vastatoimiin ryhtymisen.

Suomen turvallisuusympäristö on voimakkaasti kansainvälistynyt ja siten ulkomaita koskevilla tiedoilla on yhä suurempi merkitys niiden turvallisuusetujen suojelemisessa, jotka kuuluvat Puolustusvoimille. Sotilastiedustelun tiedonhankintatoimivaltuuksista ei ole säädetty laissa. Puolustusvoimissa sotilastiedustelu on järjestetty Puolustusvoimien sisäisin määräyksin ja ohjein. Puolustusvoimat tekee toiminnan edellyttämää yhteistyötä ulkomaisten tiedusteluviranomaisten kanssa. Yhteistyöllä pyritään tarpeellisten ulkomaisten tiedustelutietojen saamiseen Puolustusvoimien käyttöön.

Sotilastiedustelun tarvitsemia tietoja hankitaan eri tiedustelulajien menetelmillä, aluevalvonnan valvontajärjestelmästä sekä yhteistyön avulla viranomaisilta ja kumppaneilta. Tietoja hankitaan myös kansainvälisen yhteistyön avulla. Seuraavassa osiossa kuvataan sotilastiedustelun käytössä olevia tiedustelulajeja. Sotilastiedustelun kokonaisuus muodostuu tiedustelusta ja vastatiedustelusta, joiden toteuttamiseen käytetään eri tiedustelulajeja. Tällä hetkellä lainsäädäntö mahdollistaa avointen lähteiden tiedustelun, radiosignaalitiedustelun, kuvaustiedustelun sekä henkilötiedustelun tietyissä tilanteissa Suomen sotilaalliseen puolustamiseen liittyvässä tiedonhankinnassa.

2.2.2.2 Puolustusvoimien salaiset tiedonhankintakeinot

Toimivaltuudet rikostorjunnassa

Puolustusvoimien rikostorjunnan tärkeimpänä tehtävänä on sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyvien rikosten ennalta estäminen ja paljastaminen. Tämä tehtävä ei kuitenkaan rajoita suojelupoliisin toimivaltaa.

Julkisesti saatavilla olevan tiedon hankkiminen ei edellytä perustakseen erikseen säädettyä viranomaistoimivaltuutta. Koska Puolustusvoimien torjuttavina olevat hankkeet ja rikokset pyritään valmistelemaan salassa, ei tiedonhankintaa voida käytännössä perustaa julkisesti saatavilla oleviin tietoihin. Puolustusvoimien on siten keskeisesti saatava tietoa toiminnasta, joka tehdään salassa. Ollakseen tehokasta on tiedonhankinta lisäksi suoritettava salassa sen kohteilta.

Puolustusvoimille ei ole säädetty erityisiä toimivaltuuksia valtion turvallisuuteen liittyvän uhkatiedon hankkimista varten, vaan sen on osittain katsottu perustuvan puolustusvoimista annetun lain 2 §:n mukaisiin Puolustusvoimien tehtäviin.

Puolustusvoimat voi käyttää rikostorjunnassa eräitä poliisille säädettyjä tiedonhankintatoimivaltuuksia. SKRTL:n 89 §:n 1 momentin mukaan Puolustusvoimien rikosten ennalta estämistä ja paljastamista hoitavien virkamiesten toimivaltuuksista on voimassa, mitä poliisilaissa säädetään toimivaltuuksista rikosten ennalta estämiseksi ja paljastamiseksi. Puolustusvoimien rikosten ennalta estämistä ja paljastamista hoitavien virkamiesten käytettävissä ovat kuitenkin poliisilain 5 luvun tarkoitetuista salaisista tiedonhankintakeinoista vain 1) tukiasematietojen hankkiminen, 2) suunnitelmallinen tarkkailu, 3) peitelty tiedonhankinta, 4) tekninen kuuntelu, 5) tekninen katselu, 6) tekninen seuranta, 7) teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen. Puolustusvoimilla ei ole käytössään poliisilain 5 luvun tarkoittamista salaisista tiedonhankintakeinoista telekuuntelua, tietojen hankkimista telekuuntelun sijasta, televalvontaa, televalvontaa teleosoitteen tai telepäätelaitteen haltijan suostumuksella, peiteltyä tiedonhankintaa, teknistä laitetarkkailua, peitetoimintaa, valeostoa, tietolähdetoimintaa ja tietolähteen ohjattua käyttöä ja valvottu läpilaskua.

Vaikka salaisista tiedonhankintakeinoista säädetään poliisilaissa, toimivaltuuksien käytöstä on säädetty erityisesti SKRTL:n 87 §:ssä. Sen mukaan päällystöön kuuluvalle poliisimiehelle tai pidättämiseen oikeutetulle poliisimiehelle säädettyjä toimivaltuuksia käyttävät pääesikunnan vastatiedustelusta vastaavan apulaisosastopäällikön tehtävään määrätty upseeri sekä sotilaslakimies. Lisäksi poliisimiehelle säädettyjä toimivaltuuksia käyttävät rikosten ennalta estämis- ja paljastamistehtävään määrätty upseeri, erikoisupseeri, opistoupseeri tai aliupseeri taikka muu tehtävään määrätty Puolustusvoimissa palveleva virkamies.

Yhteistoiminta poliisin kanssa salaisessa tiedonhankinnassa

SKRTL 90 §:n 1 momentin mukaan jos Puolustusvoimien rikosten ennalta estämistä ja paljastamista hoitavilla ei ole toimivaltaa tehtävän hoitamiseksi tarpeellisen toimenpiteen suorittamiseen, poliisi voi Puolustusvoimien rikostorjuntaa hoitavan virkamiehen kirjallisesta pyynnöstä suorittaa sellaisen toimivaltaansa kuuluvan yksittäisen toimenpiteen.

Pykälän 2 momentin mukaan poliisi luovuttaa 1 momentissa tarkoitetulla toimenpiteellä saadut tallenteet ja asiakirjat Puolustusvoimien rikosten ennalta estämistä ja paljastamista hoitaville. Poliisi saa luovuttaa tallenteet ja asiakirjat käsittelemättöminä. Tällöin tallenteiden ja asiakirjojen tarkastamisesta sekä muista tiedon käsittelyyn liittyvistä tehtävistä vastaavat Puolustusvoimien rikosten ennalta estämistä ja paljastamista hoitavat siten kuin poliisilain 5 luvussa säädetään.

Pykälän 3 momentin mukaan asian laadun niin vaatiessa Puolustusvoimien rikosten ennalta estämisen ja paljastamisen tehtävä suoritetaan yhteistoiminnassa poliisin kanssa. Puolustusvoimien rikosten ennalta estämistä ja paljastamista hoitava ja asianomainen poliisiviranomainen sopivat yhteistoiminnassa tehtävään liittyvistä kysymyksistä. Poliisilla on myös erityisestä syystä oikeus oma-aloitteisesti ottaa Puolustusvoimien rikosten ennalta estämistä ja paljastamista koskeva asia tutkittavakseen.

Kuten edellä on todettu, Puolustusvoimilla ei ole käytössään salaisista tiedonhankinta keinoista telekuuntelua, tietojen hankkimista telekuuntelun sijasta, televalvontaa, teknistä laitetarkkailua,

peitetoimintaa (mukaan lukien peitetoiminta tietoverkoissa), valeostoa, tietolähdetoimintaa tai valvottua läpilaskua.

2.2.2.3 Salaiset tiedonhankintakeinot

Kuten edeltä käy ilmi, perustuvat Puolustusvoimien salaiset tiedonhankintakeinot poliisilakiin. Salaisten tiedonhankintakeinojen yleisiä edellytyksiä ja salaisia tiedonhankintakeinoja ei voida tarkastella tarkastelematta poliisilain säännöksiä SKRTL:n säännösten rinnalla. Salaisten tiedonhankintakeinojen käytön edellytykset Puolustusvoimilla ja poliisilla eroavat toisistaan vaikka itse salainen tiedonhankintakeino olisikin toteuttamistavaltaan sama.

Salaisten tiedonhankintakeinojen käytön yleiset edellytykset

Poliisilain 5 luvun 1 §:n 2 momentin mukaan rikoksen estämisellä tarkoitetaan toimenpiteitä, joiden tavoitteena on estää rikos, sen yritys tai valmistelu, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan perustellusti olettaa hänen syyllistyvän rikokseen, taikka keskeyttää jo aloitetun rikoksen tekeminen tai rajoittaa siitä välittömästi aiheutuvaa vahinkoa tai vaaraa. Henkilön toiminnasta tehdyillä havainnoilla tai siitä muutoin saaduilla tiedoilla tarkoitetaan välittömästi henkilön omasta toiminnasta tehtyjä havaintoja ja ulkopuolisen henkilön antamia vihjetietoja ja muuta välillistä selvitystä. Havaintoihin ja muuten saatuihin tietoihin kuuluvat myös muun muassa rikostiedustelutiedot, tarkkailuhavainnot, muut vihjetiedot ja rikosanalyysilla tiedoista tehtävät johtopäätökset. Edellytyksenä rikoksen estämiseksi säädetyn tiedonhankintakeinon käytölle on, että tällaisten tietojen perusteella on muodostunut perusteltu oletus henkilön syyllistymisestä rikokseen (HE 224/2010 vp, s. 89).

Rikoksen estäminen on varhaisvaiheen ennakollista viranomaistoimintaa. Poliisilain 5 luvun 1 §:n 2 momentin mukaan rikoksen estäminen kattaa toimenpiteet, joiden tarkoituksena on estää rikoksen yritys ja valmistelu. Valmistelun estämisellä tarkoitetaan rangaistavan teon valmistelun estämistä myös silloin, kun itse valmistelua ei ole kriminalisoitu.

Poliisilain 5 luvun 1 §:n 3 momentin mukaan rikoksen paljastamisella tarkoitetaan toimenpiteitä, joiden tavoitteena on selvittää, onko esitutkinnan aloittamiselle esitutkintalain 3 luvun 3 §:n 1 momentissa tarkoitettua perustetta, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan olettaa, että rikos on tehty. Rikoksen paljastamisen käsite viittaa rikoksen estämisen ja selvittämisen väliin jäävään harmaaseen alueeseen. Kyse ei ole rikoksen selvittämisestä, koska esitutkinnan käynnistämisen edellytykset puuttuvat, eikä myöskään rikoksen estämisestä, koska rikos oletetaan jo tehdyksi. Rikoksen paljastamisesta on kyse esimerkiksi tilanteessa jossa vihjetiedon mukaan rikos olisi jo tehty, mutta konkreettista perustetta epäilylle ei vielä ole eli esitutkintalain mukainen syytä epäillä -kynnys ei ole ylittynyt. (HE 224/2010 vp, s. 90).

Viranomaisten käytössä olevia salaisia tiedonhankintakeinoja voidaan käyttötapansa ja -tarkoituksensa mukaan ryhmitellä eri tavoin. Kohdehenkilön viestintään kohdistuvia teknisiä tiedonhankintakeinoja ovat telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, televalvonta teleosoitteen tai telepäätelaitteen haltijan suostumuksella sekä tekninen kuuntelu. Perinteisenä henkilötiedonhankintakeinona pidetään tietolähdetoimintaa ja siihen liittyvää tietolähteen ohjattua käyttöä. Tietolähdetoiminnassa kohdehenkilöä koskevia tietoja hankitaan välikäden kautta. Tiedonhankintakeinon käyttäjän ja joko välikäden tai suoraan kohdehenkilön välisessä vuorovaikutuksessa käytettäviä harhautusta sisältäviä henkilötiedonhankintakeinoja ovat peitelty tiedonhankinta, peitetoiminta ja valeosto. Kohdehenkilön käyttäytymisen teknisen havainnoinnin keinoja ovat tekninen kuuntelu, tekninen katselu, tekninen seuranta ja tekninen laitetarkkailu. Suunnitelmallinen tarkkailu puolestaan perustuu kohdehenkilön käyttäytymisen aistinvaraiseen havainnointiin. Kuten edellä on todettu, Puolustusvoimien salaiset tiedonhankintakeinot rikostorjunnassa on rajoitettu.

Salaisten tiedonhankintakeinojen käytön yleisenä edellytyksenä poliisilain 5 luvun 2 §:n 1 momentin mukaan on, että sillä voidaan olettaa saatavan rikoksen estämiseksi tai paljastamiseksi taikka vaaran torjumiseksi tarvittavia tietoja. Telekuuntelun, tietojen hankkimisen telekuuntelun sijasta, suunnitelmallisen tarkkailun, teknisen kuuntelun, henkilön teknisen seurannan, teknisen laitetarkkailun, peitetoiminnan, valeoston, tietolähteen ohjatun käytön ja valvotun läpilaskun yleisenä lisäedellytyksenä saman pykälän 2 momentin mukaan on, että niillä voidaan olettaa olevan erittäin tärkeä merkitys rikoksen estämiselle tai paljastamiselle. Peitetoiminnan ja valeoston käyttäminen edellyttää lisäksi, että käyttö on välttämätöntä rikoksen estämiseksi tai paljastamiseksi.

Eri tiedonhankintakeinojen käytölle on SKRTL:n viittaussäännösten kautta poliisilaissa asetettu niin sanottuja yleisiä edellytyksiä ja erityisiä edellytyksiä. Salaisten tiedonhankintakeinojen käytön erityisinä edellytyksinä ovat ennen kaikkea ne yksilöidyt rikokset, joiden estämiseksi kutakin keinoa voidaan käyttää. Eri tiedonhankintakeinoja koskevissa säännöksissä on myös voitu asettaa muita erityisiä edellytyksiä. Kokoavasti voidaan todeta, että suojelupoliisi voi kattavasti käyttää poliisilain 5 luvussa säädettyjä salaisia tiedonhankintakeinoja rikoslain 34 a luvussa rangaistaviksi säädettyjen terrorismirikosten ja rikoslain 12 luvussa rangaistaviksi säädettyjen maanpetoksellisten rikosten estämiseksi.

Rikoksen paljastamiseen yllä mainittuja salaisia tiedonhankintakeinoja voidaan käyttää vain, jos kysymyksessä on maanpetos- tai terrorismirikos.

Salaisten tiedonhankintakeinojen valintaa ja käyttöä ohjaavat SKRTL:n viittaussäännösten kautta poliisilain 1 luvussa säädetyt yleiset periaatteet, kuten perus- ja ihmisoikeuksien kunnioittamisen periaate, suhteellisuusperiaate, vähimmän haitan periaate ja tarkoitussidonnaisuuden periaate.

Salaisten tiedonhankintakeinojen käyttöperusteille 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 vakavuusasteen rikokseen tai sellaisen valmisteluun. Jos tällaista tiettyyn henkilöön liittyvää rikostorjunnallista perustetta ei ole olemassa, ei poliisilain mukaisen salaisen tiedonhankintakeinon käyttö ole mahdollista. Muun tiedustelutiedon hankinnan on näin ollen perustuttava avointen lähteiden seurantaan, poliisin niin sanottuun yleisvalvontaan sekä tietoihin, jotka suojelupoliisi yhteistyöverkostonsa kautta saa muilta viranomaisilta ja yksityisiltä tahoilta.

Teletiedonhankintakeinot

Teletiedonhankintakeinoja ovat telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, suostumusperusteinen televalvonta sekä tukiasematietojen hankkiminen. Puolustusvoimilla on rikostorjunnassaan käytössä teletiedonhankintakeinoista tukiasematietojen hankkiminen.

Poliisilain 5 luvun 3 §:n 1 momentin mukaan telekuuntelulla tarkoitetaan viestintämarkkinalaissa (393/2003) tarkoitetun yleisen viestintäverkon tai siihen liitetyn viestintäverkon kautta teleosoitteeseen tai telepäätelaitteeseen vastaanotettavan taikka siitä lähetetyn viestin kuuntelua, tallentamista ja muuta käsittelyä viestin sisällön ja siihen liittyvien 8 §:ssä tarkoitettujen tunnistamistietojen selvittämiseksi. Telekuuntelua saadaan kohdistaa vain siltä henkilöltä lähtöisin olevaan tai sellaiselle henkilölle tarkoitettuun viestiin, jonka voidaan perustellusti olettaa syyllistyvän 2 momentissa mainittuun rikokseen. Koska mainittu henkilö on nimenomaisesti mainittava telekuuntelua koskevassa vaatimuksessa ja luvassa, voi telekuuntelu kohdistua vain tähän henkilöön. Pykälän 2 momentissa mainitaan rikokset, joiden estämiseksi telekuuntelua poliisi saa käyttää.

Poliisilain 5 luvun 3 §:n 1 momentissa säädetään nimenomaisesti, että telekuuntelua saa kohdistaa vain tietyltä henkilöltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin. Laki mahdollistaa myös tuntemattomien henkilöiden viestinnän, jos on perusteltua syytä olettaa hänen syyllistyvän edellä

mainittuun rikokseen. Pykälän 2 momentin mukaan poliisille voidaan rikoksen estämiseksi antaa lupa kohdistaa telekuuntelua henkilön hallussa olevaan tai hänen oletettavasti muuten käyttämäänsä teleosoitteeseen tai telepäätelaitteeseen. Teleosoitteen tai telepäätelaitteen ei tarvitse olla kyseisen henkilön omistama tai hallitsema, vaan riittävää on, että henkilön tai hänen käyttämänsä tai oletettavasti käyttämänsä teleosoitteen ja telepäätelaitteen välillä on yhteys. Näyttökynnys ei ole tältä osin korkea. Käytännössä jokaiseen uuteen henkilön käyttämään tai oletettavasti käyttämän teleosoitteen ja telepäätelaitteen telekuunteluun tulee hakea tuomioistuimelta uusi lupa. Pykälän 3 momentin mukaan poliisille voidaan lisäksi antaa lupa telekuunteluun, jos se on välttämätöntä henkeä tai terveyttä välittömästi uhkaavan vakavan vaaran torjumiseksi.

Tietojen hankkimisesta telekuuntelun sijasta säädetään poliisilain 5 luvun 6 §:ssä. Telekuuntelu säädettiin alun perin puhelinverkkoihin. Nykyisestä telekuuntelusta säädettäessä paikattiin eräitä teknologiasidonnaisuudesta aiheutuneita rajoitteita. Pykälän 1 momentin mukaan jos on todennäköistä, että 5 §:ssä tarkoitettua viestiä ja siihen liittyviä tunnistamistietoja ei ole enää saatavissa telekuuntelulla, poliisille voidaan antaa rikoksen estämiseksi lupa tietojen hankkimiseen teleyrityksen tai yhteisötilaajan hallusta 5 §:ssä säädetyillä edellytyksillä. Kysymys on telekuuntelun edellytyksillä suoritettavasta takavarikosta, jos se kohdistetaan teleyritykseen tai yhteistilaajaan. Tietojen hankkiminen telekuuntelun sijasta soveltuu esimerkiksi sellaisiin tapauksiin, joissa telekuuntelutoimivaltuudella saatava viesti on hävinnyt tai hävitetty, mutta se olisi vielä teknisesti saatavissa teleyritykseltä tai yhteisötilaajalta. Kyseisen säätelyn tarkoituksen on ollut estää telekuuntelun käyttöedellytysten kiertäminen takavarikoimalla data kuljetusreitin varrelta teleyrityksen tai yhteisötilaajan hallusta.

Poliisilain 5 luvun 6 §:n 2 momentin mukaan jos tietojen hankkiminen kohdistetaan viestin sisällön selvittämiseksi telepäätelaitteeseen välittömästi yhteydessä olevaan viestin lähettämiseen ja vastaanottamiseen soveltuvaan henkilökohtaiseen tekniseen laitteeseen tai tällaisen laitteen ja telepäätelaitteen väliseen yhteyteen, poliisille voidaan antaa rikoksen estämiseksi lupa tietojen hankkimiseen telekuuntelun sijasta, jos 5 §:ssä säädetyt edellytykset täyttyvät. Ilman kyseistä lainkohtaa tiedonhankinta voitaisiin toteuttaa esimerkiksi teknisenä kuunteluna, koska teleosoitteen rajapinnan ylittänyt viesti edelleen siirrettynä tällaiseen henkikohtaiseen laitteeseen ei kuuluisi enää telekuuntelutoimivaltuuden piiriin. Momentissa tarkoitettuja henkilökohtaisia laitteita ovat esimerkiksi bluetooth -kuulokkeet. Kaiutinpuhelun tai muuten kovaäänisen puhelun kuuntelu ei ole momentissa tarkoitettua tietojen hankkimista telekuuntelun sijasta.

Poliisilain 5 luvun 7 §:n 1 momentin mukaan tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta pakkokeinolain 2 luvun 9 §:n 1 momentin 1 kohdassa tarkoitetun poliisimiehen (pidättämiseen oikeutettu poliisimies) vaatimuksesta. Pykälän 2 momentin mukaan lupa telekuunteluun ja 6 §:n 2 momentissa tarkoitettuun tietojen hankkimiseen voidaan antaa enintään kuukaudeksi kerrallaan. Pykälän 3 momentin mukaan telekuuntelua ja telekuuntelun sijasta toimitettavaa tietojen hankkimista koskevassa vaatimuksessa ja päätöksessä on mainittava: 1) toimenpiteen perusteena oleva rikos ja sen oletettu tekoaika taikka toimenpiteen perusteena oleva vaara; 2) henkilö, jonka voidaan perustellusti olettaa syyllistyvän 1 kohdassa tarkoitettuun rikokseen; 3) tosiseikat, joihin henkilöön kohdistuva epäily ja telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen edellytykset perustuvat; 4) telekuuntelua tai 6 §:n 2 momentissa tarkoitettua tietojen hankkimista koskevan luvan voimassaoloaika kellonajan tarkkuudella; 5) toimenpiteen kohteena oleva teleosoite tai telepäätelaite; 6) telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen suorittamista johtava ja valvova pidättämiseen oikeutettu poliisimies; 7) mahdolliset telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen rajoitukset ja ehdot.

Vaatimuksessa ja päätöksessä on esitettävä huomattavan yksityiskohtaiset tiedot. Poliisi- ja pakkokeinolain uudistuksessa (HE 224/2010 vp. ja HE 222/2010 vp.) korostettiin velvollisuutta esittää ja perustella tosiseikkoja, joiden perusteella tuomioistuin voi tehdä salaisen tiedonhankintakeinon

käytön edellytysten täyttymisestä oman johtopäätöksensä. Edellytyksissä on kysymys ensinnäkin edellä kerrotuista yleisistä edellytyksistä ja varsinaisista poliisilain 5 luvun 5 ja 6 §:ssä säädetyistä edellytyksistä.

Poliisilain 5 luvun 8 §:n 1 momentin mukaan Televalvonnalla tarkoitetaan tunnistamistietojen hankkimista viestistä, joka on lähetetty 5 §:ssä tarkoitettuun viestintäverkkoon kytketystä teleosoitteesta tai telepäätelaitteesta taikka vastaanotettu tällaiseen osoitteeseen tai laitteeseen, sekä teleosoitteen tai telepäätelaitteen sijaintitiedon hankkimista taikka osoitteen tai laitteen käytön tilapäistä estämistä. Tunnistamistiedolla tarkoitetaan sähköisen viestinnän tietosuojalain (516/2004) 2 §:n 8 kohdassa tarkoitettua tilaajaan tai käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi. Voimassa olevassa sääntelyssä käytetään tunnistamistiedon määritelmää, joka periytyy sähköisen viestinnän tietosuojalain (516/2004) 2 §:n 8 kohdassa olevaan määritelmään. Tunnistamistiedon tyhjentävä ja yksiselitteinen määrittely ei ole mahdollista. Määritelmän rajoittuminen viestiä koskeviin tietoihin kuitenkin tarkoittaa sitä, että viestiin liittymätön tietokoneiden välinen ohjausliikenne ei ole luottamuksellisen viestinnän suojan piirissä. Pykälän 2 momentin mukaan poliisille voidaan rikoksen estämiseksi antaa lupa sellaisen henkilön hallussa olevan tai oletettavasti muuten käyttämän teleosoitteen tai telepäätelaitteen televalvontaan, jonka lausumien, uhkausten tai käyttäytymisen perusteella taikka muutoin voidaan perustellusti olettaa hänen syyllistyvän momentissa mainittuun rikokseen.

Poliisilain 5 luvun 9 §:ssä säädetään suostumusperusteisesta televalvonnasta. Pykälän nojalla poliisi voi telepäätelaitteen tai -osoitteen haltijan suostumuksella kohdistaa televalvontaa tämän hallinnassa olevaan teleosoitteeseen tai telepäätelaitteeseen rikoksen estämiseksi, kun jonkun voidaan lausumiensa tai muun käyttäytymisensä perusteella perustellusti olettaa syyllistyvän pykälässä mainittuun rikokseen. Televalvonnan koskeminen suostumuksen antajan hallinnassa olevaa teleosoitetta tai telepäätelaitetta tarkoittaa tosiasiallista hallintaa. Näin ollen esimerkiksi työnantaja ei voi antaa suostumusta työntekijän käytössä olevan matkapuhelimen televalvontaan.

Poliisilain 5 luvun 10 §:n mukaan tuomioistuin päättää rikoksen estämiseksi tai paljastamiseksi käytettävästä televalvonnasta sekä 9 §:ssä säädetystä suostumusperusteisesta televalvonnasta pidättämiseen oikeutetun virkamiehen vaatimuksesta. Lupa voidaan antaa enintään kuukaudeksi kerrallaan. Se voidaan myöntää koskemaan myös päätöstä edeltänyttä tiettyä aikaa, joka voi olla kuukautta pidempi.

Poliisilain 5 luvun 11 §:n 1 momentin mukaan tukiasematietojen hankkimisella tarkoitetaan tiedon hankkimista tietyn tukiaseman kautta telejärjestelmään kirjautuneista tai kirjautuvista telepäätelaitteista ja teleosoitteista. Tukiasematietojen hankkiminen voi siten koskea myös tulevaisuudessa kirjautuvia teleosoitteita ja telepäätelaitteita. Pykälän 2 momentissa säädetään tukiasematietojen hankkimisen edellytyksistä. Momentin mukaan poliisille voidaan antaa lupa tukiasematietojen hankkimiseen rikoksen estämiseksi oletettuna tapahtuma-aikana oletetun tekopaikan läheisyydessä sijaitsevasta tukiasemasta, kun henkilön lausumien, uhkausten tai käyttäytymisen perusteella taikka muutoin voidaan perustellusti olettaa hänen syyllistyvän rikokseen, josta säädetään televalvonnan edellytyksiä koskevassa 8 §:n 2 momentissa.

Poliisilain 5 luvun 12 §:ssä säädetään tukiasematietojen hankkimisen päätösmenettelystä. Pykälän 1 momentin mukaan tuomioistuin päättää tukiasematietojen hankkimisesta pidättämiseen oikeutetun poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies saa päättää tukiasematietojen hankkimisesta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta. Pykälän 2 momentin mukaan lupa annetaan tietyksi ajanjaksoksi. Lupa voi koskea myös päätöksentekohet-

keä edeltäviä tietoja, koska myös päätöksentekohetkeä edeltävillä tiedoilla voi olla merkitystä rikoksen estämisen kannalta. Olennaista on se, että tietojen merkitys pystytään perustelemaan.

Tarkkailutyyppiset keinot

Tarkkailutyyppisiin keinoihin kuuluvat suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, tekninen seuranta (henkilön tekninen seuranta), tekninen laitetarkkailu ja teleosoitteen ja telepäätelaitteen yksilöintitietojen hankkiminen sekä näitä keinoja tukeva laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen. Puolustusvoimat voi käyttää rikostorjunnassaan kaikkia tarkkailutyyppisiä keinoja.

Poliisilain 5 luvun 13 §:ssä säädetään suunnitelmallisesta tarkkailusta. Pykälän 1 momentissa säädetään yleismääritelmästä, jonka mukaan tarkkailulla tarkoitetaan tiettyyn henkilöön salaa kohdistettavaa havaintojen tekemistä tiedonhankintatarkoituksessa. Pykälän 2 momentin mukaan suunnitelmallisella tarkkailulla tarkoitetaan muun kuin lyhytaikaisen tarkkailun kohdistamista henkilöön, jonka voidaan perustellusti olettaa syyllistyvän rikokseen. Tarkkailun määritelmän mukaisesti myös suunnitelmallista tarkkailua käytettäisiin salaa, mikä pitäisi sisällään myös vuorovaikutuksen välttämisen. Pykälän 3 momentin mukaan poliisi saisi rikoksen estämiseksi kohdistaa 2 momentissa tarkoitettuun henkilöön suunnitelmallista tarkkailua, jos on perusteltua syytä olettaa hänen syyllistyvän rikokseen, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta, taikka varkauteen tai kätkemisrikokseen. Pykälän 4 momentin mukaan tässä pykälässä tarkoitettua tarkkailua ei saisi kohdistaa vakituiseen asumiseen käytettävään tilaan. Aistinvarainen tarkkailu rikoksen estämiseksi ja paljastamiseksi saisi kuitenkin kohdistua myös kotirauhan piirissä olevaan henkilöön.

Poliisilain 5 luvun 14 §:ssä säädetään suunnitelmallisen tarkkailun päätösmenettelystä. Pykälän 1 momentin mukaan pidättämiseen oikeutettu poliisimies päättäisi suunnitelmallisesta tarkkailusta, joka voitaisiin pykälän 2 momentin mukaan tehdä kerrallaan enintään kuudeksi kuukaudeksi. Pykälän 3 momentissa säädettäisiin suunnitelmallista tarkkailua koskevan päätöksen sisällöstä.

Poliisilain 5 luvun 15 §:n 1 momentin mukaan peitellyllä tiedonhankinnalla tarkoitetaan tiettyyn henkilöön kohdistuvaa lyhytkestoisessa vuorovaikutuksessa tapahtuvaa tiedonhankintaa, jossa poliisimiehen tehtävän salaamiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja. Erotuksena tarkkailusta ja suunnitelmallisesta tarkkailusta toimivaltuuden käytölle olisi luonteenomaista nimenomaan pyrkimys henkilökohtaiseen tapaamiseen tai vastaavaan vuorovaikutukseen tiedonhankinnan kohteen kanssa. Erotuksena peitetoiminnasta peitellyssä tiedonhankinnassa ei ole kyse soluttautumisesta, jossa pyritään luomaan pitkäaikainen luottamussuhde. Peitellyssä tiedonhankinnassa voitaisiin käyttää vääriä, harhauttavia tai peiteltyjä tietoja tiedonhankinnan paljastumisen estämiseksi. Pykälän 2 momentin mukaan poliisi saa käyttää peiteltyä tiedonhankintaa rikoksen estämiseksi, jos henkilön lausumien tai muun käyttäytymisen perusteella voitaisiin perustellusti olettaa hänen syyllistyvän momentissa mainittuun rikokseen. Peitelty tiedonhankinta voi kuitenkin kohdistua myös muuhun henkilöön, kuin henkilöön, jonka voidaan perustellusti olettaa syyllistyvän rikokseen.

Poliisilain 5 luvun 16 §:n 1 momentin mukaan peitellystä tiedonhankinnasta päättää keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu poliisimies. Pykälän 2 momentissa säädetään peitellyn tiedonhankinnan kirjallisesti tehtävän päätöksen sisällöstä. Toimivaltuuden käytön osalta edellytetään erikseen siitä vastaavan poliisimiehen nimeämistä, jonka tehtävänä on huolehtia muun muassa siitä, ettei toiminnassa ole tosiasiallisesti kysymys peitetoiminnasta. Pykälän 3 momentin mukaan päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava. Momentti velvoittaa toimenpiteestä vastaavan poliisimiehen seuraamaan peitellyn tiedonhankinnan edellytysten olemassaoloa. Peiteltyä tiedonhankintaa ei ole mahdollista toteuttaa asunnossa edes silloin, kun

asuntoon meneminen tapahtuu asunnonhaltijan myötävaikutuksella. Asunnossa tapahtuvana peiteltynä tiedonhankintana ei kuitenkaan pidetä vielä sitä, että lähetyksen vastaanottaja pyytää lähetystä kuitatessaan lähettinä esiintyvän poliisimiehen odottamaan esimerkiksi asuntonsa eteisessä.

Poliisilain 5 luvun 17 § 1 momentin mukaan teknisellä kuuntelulla tarkoitetaan tietyn henkilön sellaisen keskustelun tai viestin, joka ei ole ulkopuolisten tietoon tarkoitettu ja johon keskusteluun kuuntelija ei osallistu, kuuntelua, tallentamista ja muuta käsittelyä teknisellä laitteella, menetelmällä tai ohjelmistolla keskustelun tai viestin sisällön tai sen osapuolten taikka 4 momentissa tarkoitetun henkilön toiminnan selvittämiseksi. Tietojärjestelmässä ohjelmistolla tai laitteella toteutettu näppäimistökuuntelu kuuluisi myös momentin mukaisen teknisen kuuntelun määritelmän piiriin. Erona poliisilain 23 §:n mukaiseen tekniseen laitetarkkailuun on se, että teknisellä laitetarkkailulla voi hankkia tiedon laitteelle talletetuista tai laitteella prosessoitavana olevasta muusta kuin viestintää sisältävästä tiedosta. Pykälän 2 momentin mukaan teknistä kuuntelua ei saa kohdistaa vakituiseen asumiseen käytettävään tilaan. Pykälän 3 momentin mukaan poliisilla on oikeus tekniseen kuunteluun rikoksen estämiseksi vakituiseen asumiseen käytettävän tilan ulkopuolella sijaitsevassa tilassa tai muussa paikassa, jossa tiedonhankinnan kohteena olevan henkilön voidaan olettaa todennäköisesti oleskelevan tai käyvän. Teknistä kuuntelua voitaisiin momentin nojalla kohdistaa henkilöön hänen ollessaan rikoslain 24 luvun 11 §:n mukaisessa kotirauhan suojaamassa tilassa, kunhan se ei ole vakituiseen asumiseen käytetty tila. Poliisille voidaan antaa lupa myös viranomaisten tiloissa olevaan rikoksen johdosta vapautensa menettäneen henkilön tekniseen kuunteluun. Pykälän 4 momentin mukaan teknistä kuuntelua saa kohdentaa henkilöön, jonka lausumien, uhkausten tai käyttäytymisen perusteella taikka muutoin voidaan perustellusti olettaa hänen syyllistyvän momentissa mainittuun rikokseen. Teknisen kuuntelun edellytyksenä olisi 2 §:n 2 momentin mukaan lisäksi se, että tämän keinon käytöllä voidaan olettaa olevan erittäin tärkeä merkitys rikoksen estämiselle tai paljastamiselle. Pykälän 5 momentin mukaan poliisilla olisi aina 2 momentin estämättä oikeus tekniseen kuunteluun, jos se on välttämätöntä poliisitoimenpiteen turvalliseksi suorittamiseksi ja toimenpiteen suorittajan, kiinni otettavan tai suojattavan henkilön henkeä tai terveyttä uhkaavan välittömän vaaran torjumiseksi (rynnäkkökuuntelu). Teknisestä kuuntelusta syntyneiden tallenteiden tarkastamisesta ja tutkimisesta sekä teknisen kuuntelun keskeyttämisestä säädetään tarkemmin poliisilain 5 luvun 51, 52 ja 56 §:ssä. Myös näissä tapauksissa saattavat tulla sovellettaviksi poliisilain 5 luvun 53—55 §:n säännökset ylimääräisestä tiedosta. Teknisen kuuntelun osalta on syytä mainita, että telekuuntelu- sekä televalvonta on suunniteltu ajatellen puhelinverkkoja, kun taas tietoverkoissa tapahtuvaan salattuun viestintään kohdistuvaa tiedonhankintaa on toteutettava osin tarkkailutyyppisillä toimivaltuuksilla, nimenomaisesti teknisellä kuuntelulla.

Poliisilain 5 luvun 18 §:n 1 momentin mukaan tuomioistuin päättää rikoksen johdosta vapautensa menettäneen henkilön teknisestä kuuntelusta pidättämiseen oikeutetun poliisimiehen vaatimuksesta. Pykälän 2 momentin mukaan pidättämiseen oikeutettu poliisimies päättää muusta kuin 1 momentissa tarkoitetusta teknisestä kuuntelusta sekä aina 17 §:n 5 momentissa tarkoitetusta rynnäkkökuuntelusta. Pykälän 3 momentin mukaan teknistä kuuntelua koskeva lupa voidaan antaa ja päätös tehdä enintään kuukaudeksi kerrallaan. Pykälän 4 momentissa säädetään vaatimuksen ja päätöksen sisällöstä. Tekniselle kuuntelulle on asetettu erityinen tuloksellisuusodotus. Siksi vaatimuksessa ja päätöksessä tulee tuoda esille ne tosiseikat, joiden perusteella voidaan arvioida tietyn tilan tai muun paikan olevan sellainen, jossa tiedonhankinnan kohteena olevan henkilön voidaan todennäköisesti olettaa oleskelevan tai käyvän. Teknisen kuuntelun kohdistuessa tilaan, ei tilaa tarvitse kuitenkaan yksilöidä vastaavalla tarkkuudella kuin epäillyn henkilön asuntoa, jos ei tila ole päätöksentekohetkellä tarkasti tiedossa

Poliisilain 5 luvun 19 § 1 momentin mukaan teknisellä katselulla tarkoitetaan rikoslain 24 luvun 6 §:n estämättä tapahtuvaa tietyn henkilön taikka tilan tai muun paikan tarkkailua tai tallentamista kameralla tai muulla sellaisella paikkaan sijoitetulla teknisellä laitteella, menetelmällä tai ohjelmistolla. Kuten tekninen kuuntelu, myös tekninen katselu voi kohdistua tilan tai paikan lisäksi tiettyyn henkilöön. Tekninen katselu eroaa tarkkailusta ja suunnitelmallisesta tarkkailusta siinä, että tekni-

sessä katselussa käytetään paikkaan sijoitettuja teknisiä laitteita, menetelmiä tai ohjelmistoja. Pykälän 2 momentin mukaan teknistä kuuntelua ei saa kohdistaa vakituiseen asumiseen käytettävään tilaan. Asuntokatselukielto ei koske kuitenkaan vaaran estämiseksi tehtävää teknistä katselua eli niin sanottua rynnäkkökatselua. Pykälän 3 momentin mukaan poliisilla on rikoksen estämiseksi oikeus vakituiseen asumiseen käytettävän tilan ulkopuolella olevan henkilön tekniseen katseluun. Poliisille voidaan antaa lupa myös viranomaisen tiloissa olevan rikoksen johdosta vapautensa menettäneen henkilön tekniseen katseluun. Katselu voidaan toteuttaa kohdistamalla se tilaan tai muuhun paikkaan, jossa tiedonhankinnan kohteena olevan henkilön voidaan olettaa todennäköisesti oleskelevan tai käyvän. Pykälän 4 momentin mukaan rikoslain 24 luvun 11 §:ssä tarkoitetun kotirauhan suojaaman tilan tai muun paikan ja rikoksen johdosta vapautensa menettäneen henkilön teknisen katselun edellytyksenä on, että henkilön lausumien, uhkausten tai käyttäytymisen perusteella taikka muutoin voidaan perustellusti olettaa hänen syyllistyvän 17 §:n 4 momentissa tarkoitettuun rikokseen eli teknisen kuuntelun perusteena oleviin rikoksiin. Muun teknisen katselun edellytyksenä on, että henkilön voidaan perustellusti olettaa syyllistyvän rikokseen, josta säädetty ankarin rangaistus on vähintään vuosi vankeutta. Pykälän 5 momentin mukaan poliisilla on aina 2 momentin estämättä oikeus tekniseen katseluun, jos se on välttämätöntä poliisitoimenpiteen turvalliseksi suorittamiseksi ja toimenpiteen suorittajan, kiinni otettavan tai suojattavan henkilön henkeä tai terveyttä uhkaavan välittömän vaaran torjumiseksi.

Poliisilain 5 luvun 20 § 1 momentin mukaan tuomioistuin päättää teknisestä katselusta pidättämiseen oikeutetun poliisimiehen vaatimuksesta, kun katselu kohdistuu rikoslain 24 luvun 11 §:ssä tarkoitettuun kotirauhan suojaamaan tilaan tai muuhun paikkaan taikka rikoksen johdosta vapautensa menettäneeseen henkilöön. Pykälän 2 momentin mukaan pidättämiseen oikeutettu poliisimies päättää 19 §:n 5 momentissa tarkoitetusta rynnäkkökatselusta sekä muusta kuin 1 momentissa tarkoitetusta teknisestä katselusta. Pykälän 3 momentin mukaan lupa tekniseen katseluun voidaan antaa tai päätös tehdä enintään kuukaudeksi kerrallaan. Pykälän 4 momentissa säädetään teknistä katselua koskevan vaatimuksen ja päätöksen sisällöstä.

Poliisilain 5 luvun 21 § 1 momentissa määritellään tekninen seuranta, jolla tarkoitetaan esineen, aineen tai omaisuuden liikkumisen seurantaa siihen erikseen sijoitettavalla tai siinä jo olevalla radiolähettimellä tai muulla sellaisella teknisellä laitteella taikka menetelmällä tai ohjelmistolla. Pykälän 2 momentin mukaan poliisi saa rikoksen estämiseksi kohdistaa rikoksen kohteena olevaan tai sellaisen henkilön oletettavasti hallussa olevaan tai käyttämään esineeseen, aineeseen tai omaisuuteen teknistä seurantaa, jonka lausumien, uhkausten tai käyttäytymisen perusteella taikka muutoin voidaan perustellusti olettaa hänen syyllistyvän rikokseen, josta säädetty ankarin rangaistus on vähintään vuosi vankeutta. Pykälän 3 momentissa säädetään henkilön teknisestä seurannasta. Jos teknisen seurannan tarkoituksena on seurata henkilön liikkumista sijoittamalla seurantalaite hänen yllään oleviin vaatteisiin tai mukanaan olevaan esineeseen (henkilön tekninen seuranta), saadaan toimenpide suorittaa vain, jos hänen voidaan perustellusti olettaa syyllistyvän 17 §:n 4 momentissa tarkoitettuun rikokseen eli jos myös tekninen kuuntelu olisi mahdollista. Pykälän 4 momentin mukaan poliisilla on lisäksi oikeus tekniseen seurantaan, jos se on välttämätöntä poliisitoimenpiteen turvalliseksi suorittamiseksi ja toimenpiteen suorittajan, kiinni otettavan tai suojattavan henkilön henkeä tai terveyttä uhkaavan välittömän vaaran torjumiseksi (rynnäkköseuranta).

Poliisilain 5 luvun 22 § 1 momentin mukaan tuomioistuin päättää henkilön teknisestä seurannasta pidättämiseen oikeutetun poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies saa päättää seurannasta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta. Pykälän 2 momentin mukaan pidättämiseen oikeutettu poliisimies päättää 21 §:n 4 momentissa tarkoitetusta seurannasta (ns. rynnäkköseuranta) ja muusta kuin 1 momentissa tarkoitetusta teknisestä seurannasta. Pykälän 3 momentin mukaan lupa voidaan antaa tai päätös tehdä enintään kuudeksi kuu-

kaudeksi kerrallaan. Pykälän 4 momentissa säädetään teknistä seurantaa koskevassa vaatimuksessa ja päätöksessä mainittavista tiedoista.

Poliisilain 5 luvun 23 § 1 momentti sisältää teknisen laitetarkkailun määritelmän. Sillä tarkoitetaan tietokoneen tai muun vastaavan teknisen laitteen taikka sen ohjelmiston toiminnan, sisältämien tietojen tai yksilöintitietojen muuta kuin yksinomaan aistinvaraista tarkkailua, tallentamista tai muuta käsittelyä rikoksen estämiselle merkityksellisen seikan tutkimiseksi. Teknisellä laitetarkkailulla voidaan tarkkailla teknistä laitetta ja yleensä laitteen sisältämiä epäillyn henkilön tallentamia tietoja. Tällaiset tiedot voisivat olla laitteeseen tallennetussa asiakirjassa. Teknisellä laitetarkkailulla voidaan seurata henkilön ja teknisen laitteen välistä vuorovaikutusta. Pykälän 2 momentissa säädetään rajanvedosta telepakkokeinoihin. Sen mukaan teknisellä laitetarkkailulla ei saa hankkia tietoa viestin sisällöstä eikä 8 §:ssä tarkoitetuista tunnistamistiedoista. Poliisi saa kohdistaa teknistä laitetarkkailua mainitun henkilön todennäköisesti käyttämään tietokoneeseen tai muuhun vastaavaan tekniseen laitteeseen taikka sen ohjelmiston toimintaan. Teknisen laitetarkkailun edellytyksenä on 2 §:n 2 momentin mukaan lisäksi se, että laitetarkkailulla voidaan olettaa olevan erittäin tärkeä merkitys rikoksen estämiselle tai paljastamiselle. Teknistä laitetarkkailua voidaan käyttää niin sanotun näppäimistökuuntelun toteuttamiseen vain niiltä osin, kun laitteen käyttäjä ei kirjoita viestiä. Viestintää koskevan näppäimistökuuntelun toteuttamiseksi poliisin on käytettävä 17 § teknisen kuuntelun toimivaltuutta, jonka perusterikokset ovat samat kuin laitetarkkailulla. Pykälän 3 momentin mukaan poliisille voidaan antaa rikoksen estämiseksi lupa tekniseen laitetarkkailuun, jos henkilön lausumien, uhkausten tai käyttäytymisen perusteella taikka muutoin voidaan perustellusti olettaa hänen syyllistyvän 17 §:n 4 momentissa tarkoitettuun rikokseen.

Poliisilain 5 luvun 24 §:n 1 momentin mukaan tuomioistuin päättää teknisestä laitetarkkailusta pidättämiseen oikeutetun poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies saa päättää teknisestä laitetarkkailusta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua tiedonhankintakeinon käytön aloittamisesta. Pykälän 2 momentin mukaan lupa voidaan antaa enintään kuukaudeksi kerrallaan. Pykälän 3 momentissa säädetään teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä mainittavista tiedoista.

Poliisilain 5 luvun 25 §:n 1 momentin mukaan poliisi saa rikoksen estämiseksi hankkia teknisellä laitteella teleosoitteen tai telepäätelaitteen yksilöintitiedot, jos estettävänä on rikos, josta säädetty ankarin rangaistus on vähintään vuosi vankeutta. Pykälän 2 momentin mukaan poliisi saa käyttää 1 momentissa tarkoitettujen tietojen hankkimiseksi ainoastaan sellaista teknistä laitetta, jota voidaan käyttää vain teleosoitteen ja telepäätelaitteen yksilöimiseen. Viestintävirasto tarkastaa teknisen laitteen tässä momentissa tarkoitetun vaatimustenmukaisuuden sekä sen, ettei laite ominaisuuksiensa vuoksi aiheuta haitallista häiriötä yleisen viestintäverkon laitteille tai palveluille. Pykälän 3 momentin mukaan teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisesta päättää pidättämiseen oikeutettu poliisimies.

Poliisilain 5 luvun 26 §:n 1 momentin mukaan poliisimiehellä on oikeus sijoittaa tekniseen tarkkailuun käytettävä laite, menetelmä tai ohjelmisto toimenpiteen kohteena olevaan esineeseen, aineeseen, omaisuuteen, tilaan tai muuhun paikkaan taikka tietojärjestelmään, jos tarkkailun toteuttaminen sitä edellyttää. Poliisimiehellä on tällöin oikeus laitteen, menetelmän tai ohjelmiston asentamiseksi, käyttöön ottamiseksi ja poistamiseksi salaa mennä edellä mainittuihin kohteisiin tai tietojärjestelmään sekä kiertää, purkaa tai muulla vastaavalla tavalla tilapäisesti ohittaa kohteiden tai tietojärjestelmän suojaus tai haitata sitä. Kotietsinnästä säädetään erikseen. Pykälän 2 momentissa säädettäisiin, että tekniseen tarkkailuun käytettävän laitteen, menetelmän tai ohjelmiston saa asentaa vakituiseen asumiseen käytettävään tilaan vain, jos tuomioistuin on antanut siihen luvan pidättämiseen oikeutetun poliisimiehen vaatimuksesta taikka jos asentaminen on välttämätöntä 17 §:n 5 momentissa, 19 §:n 5 momentissa tai 21 §:n 4 momentissa tarkoitetuissa tapauksissa. Laitteen,

menetelmän tai ohjelmiston saisi ilman tuomioistuimen lupaa asentaa vakituiseen asumiseen käytettävään tilaan momentissa tarkoitetuissa vaaran estämiseksi tehtävissä tapauksissa eli niin sanotuissa rynnäkkötarkkailutilanteissa.

Peitetoiminta ja valeosto

Peitetoimintaa ja valeostoa pidetään kovimpina salaisina tiedonhankintakeinoina, sillä näiden keinojen käytön edellytykset ovat erittäin tiukkoja. Puolustusvoimille ei ole säädetty toimivaltaa käyttää peitetoimintaa tai valeostoa rikostorjuntatehtävissään.

Poliisilain 5 luvun 27 §:n 1 momentin mukaan Peitetoiminnalla tarkoitetaan tiettyyn henkilöön tai hänen toimintaansa kohdistuvaa suunnitelmallista tiedonhankintaa käyttämällä soluttautumista, jossa tiedonhankinnan edellyttämän luottamuksen hankkimiseksi tai tiedonhankinnan paljastumisen estämiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka valmistetaan tai käytetään vääriä asiakirjoja. Poliisi saa 2 momentin mukaan kohdistaa rikoksesta epäiltyyn peitetoimintaa, jos tätä on syytä epäillä 3 §:ssä tarkoitetusta muusta rikoksesta kuin törkeästä laittoman maahantulon järjestämisestä tai törkeästä tulliselvitysrikoksesta taikka jos tätä on syytä epäillä rikoslain 17 luvun 18 §:n 1 momentin 1 kohdassa tarkoitetusta rikoksesta. Edellytyksenä on lisäksi, että tiedonhankintaa on rikollisen toiminnan suunnitelmallisuuden, järjestäytyneisyyden tai ammattimaisuuden taikka ennakoitavissa olevan jatkuvuuden tai toistuvuuden vuoksi pidettävä tarpeellisena. Pykälän 3 momentissa säädetään niin sanotusta nettipeitetoiminnasta. Momentin mukaan poliisi saa kohdistaa epäiltyyn peitetoimintaa tietoverkossa, jos tätä on syytä epäillä rikoksesta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta tai jos kysymyksessä on rikoslain 17 luvun 19 §:ssä tarkoitettu rikos.

Peitetoiminnalla ei saa kiertää kotietsintää koskevia säännöksiä. Siksi peitetoiminta asunnossa on sallittua vain, jos sisäänkäynti tai oleskelu tapahtuu asuntoa käyttävän aktiivisella myötävaikutuksella. Kotietsinnästä säädetään erikseen.

Poliisilain 5 luvun 28 §:ssä säädetään rikoksentekokiellosta ja 29 §:ssä järjestäytyneen rikollisryhmän toimintaan ja valvottuun läpilaskuun osallistumisesta. Peitetoimintaa koskevasta esityksestä ja suunnitelmasta sekä peitetoiminnasta päättämisestä säädetään 5 luvun 30 ja 31 §:ssä. Peitetoiminnan laajentamisesta ja ratkaisusta peitetoiminnan edellytyksistä säädetään 33 ja 32 §:ssä.

Poliisilain 5 luvun 34 §:n 1 momentin mukaan valeostolla tarkoitetaan poliisin tekemää esineen, aineen, omaisuuden tai palvelun ostotarjousta tai ostoa, jonka tavoitteena on saada poliisin haltuun tai löytää todiste rikosasiassa, rikoksella saatu hyöty taikka esine, aine tai omaisuus, joka on rikoksella joltakulta viety tai jonka tuomioistuin voi julistaa menetetyksi taikka jonka avulla voidaan muuten saada selvitystä rikosasiassa. Muun kuin näyte-erän ostaminen edellyttää, että ostaminen on välttämätöntä valeoston toteuttamiseksi. Pykälän 2 momentin mukaan valeosto saadaan tehdä, jos on syytä epäillä rikosta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta, taikka varkautta tai kätkemisrikosta ja on todennäköistä, että valeostolla saavutetaan jokin 1 momentissa mainittu tavoite. Valeoston toteuttaja saa 3 momentin mukaan tehdä vain sellaista tiedonhankintaa, joka on välttämätöntä valeoston toteuttamiseksi. Valeosto on toteutettava siten, ettei se saa kohteena olevaa tai muuta henkilöä tekemään rikosta, jota hän ei muuten tekisi. Valeostolla ei myöskään saa kiertää kotietsintää koskevia säännöksiä. Siksi 4 momentin mukaan kotietsintä asunnossa on sallittua vain, jos sisäänkäynti tai oleskelu tapahtuu asuntoa käyttävän aktiivisella myötävaikutuksella. Kotietsinnästä säädetään erikseen.

Valeostosta päättämisestä ja valeoston toteuttamista koskevasta suunnitelmasta ja sen toteuttamista koskevasta päätöksestä säädetään 5 luvun 35–37 §:ssä.

Poliisimiehen turvaamisesta peitellyssä tiedonhankinnassa, peitetoiminnassa ja valeostossa säädetään 5 luvun 38 §:ssä. Pidättämiseen oikeutettu virkamies saa päättää, että peiteltyä tiedonhankintaa, peitetoimintaa tai valeostoa toteuttava poliisimies varustetaan kuuntelun ja katselun mahdollistavalla teknisellä laitteella, jos varustaminen on perusteltua hänen turvallisuutensa varmistamiseksi (1 momentti). Kuuntelu ja katselu saadaan tallentaa. Tallenteet on hävitettävä heti sen jälkeen, kun niitä ei tarvita poliisimiehen turvaamiseen. Jos niitä on kuitenkin tarpeen säilyttää asiaan osallisen oikeusturvaan liittyvistä syistä, tallenteet saadaan säilyttää ja niitä saadaan käyttää tässä tarkoituksessa. Tällöin tallenteet on hävitettävä, kun asia on lainvoimaisesti ratkaistu tai jätetty sillensä (2 momentti).

Tietolähteen ohjattu käyttö ja valvottu läpilasku

Tietolähdetoiminnasta ja valvotusta läpilaskusta säädetään 5 luvun 39–42 §:ssä. Puolustusvoimille ei ole säädetty toimivaltaa käyttää tietolähdettä ohjatusti tai valvottua läpilaskua rikoksentorjuntatehtävässä.

Luvun 39 §:n 1 momentin mukaan tietolähdetoiminnalla tarkoitetaan muuta kuin satunnaista luottamuksellista, rikoksen selvittämiselle merkityksellisten tietojen vastaanottamista poliisin ja muun esitutkintaviranomaisen ulkopuoliselta henkilöltä (tietolähde). Pykälän 2 momentin mukaan poliisi tai Tulli saa pyytää tähän tarkoitukseen hyväksyttyä, henkilökohtaisilta ominaisuuksilta sopivaa, rekisteröityä ja tiedonhankintaan suostunutta tietolähdettä hankkimaan 1 momentissa tarkoitettuja tietoja (tietolähteen ohjattu käyttö). Pykälän 3 momentin mukaan tietolähteen ohjatussa käytössä tietoja ei saa pyytää hankittavaksi sellaisella tavalla, joka edellyttäisi viranomaiselle kuuluvien toimivaltuuksien käyttöä tai joka vaarantaisi tietolähteen tai muun henkilön hengen tai terveyden. Ennen tietolähteen ohjattua käyttöä tietolähteelle on tehtävä selkoa hänen oikeuksistaan ja velvollisuuksistaan sekä erityisesti hänelle lain mukaan sallitusta ja kielletystä toiminnasta. Tietolähteen turvallisuudesta on tarpeen mukaan huolehdittava tiedonhankinnan aikana ja sen jälkeen. Pykälän 4 momentin mukaan tietolähdettä koskevien tietojen tallettamisesta henkilörekisteriin ja palkkion maksamisesta säädetään poliisilaissa ja rikostorjunnasta Tullissa annetussa laissa. Tietolähteen ohjatusta käytöstä päättämisestä säädetään 5 luvun 40 §:ssä.

Valvotusta läpilaskusta ja sen edellytyksistä säädetään 5 luvun 41 §:ssä. Pykälän 1 momentin mukaan esitutkintaviranomainen saa olla puuttumatta esineen, aineen tai omaisuuden kuljetukseen tai muuhun toimitukseen tai siirtää tällaista puuttumista, jos tämä on tarpeen tekeillä olevaan rikokseen osallisten henkilöiden tunnistamiseksi taikka tekeillä olevaa rikosta vakavamman rikoksen tai laajemman rikoskokonaisuuden selvittämiseksi (valvottu läpilasku). Pykälän 2 momentin mukaan esitutkintaviranomainen saa käyttää valvottua läpilaskua, jos on syytä epäillä rikosta, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta. Edellytyksenä on lisäksi, että läpilaskua voidaan valvoa ja siihen voidaan tarvittaessa puuttua. Toimenpiteestä ei saa myöskään aiheutua merkittävää vaaraa kenenkään hengelle, terveydelle tai vapaudelle eikä merkittävää huomattavan ympäristö-, omaisuus- tai varallisuusvahingon vaaraa. Pykälän 3 momentin mukaan Suomea sitovaan kansainväliseen sopimukseen tai muuhun Suomea sitovaan velvoitteeseen liittyvästä kansainvälisestä valvotusta läpilaskusta on lisäksi voimassa, mitä siitä erikseen laissa säädetään. Valvotusta läpilaskusta päättämisestä säädetään 5 luvun 42 §:ssä.

2.2.2.4 Muut tiedonhankintakeinot

Puolustusvoimat voi lakisääteisten tehtäviensä toteuttamiseksi käyttää myös muita kuin säädettyjä toimivaltuuksia. Tällaisia ovat avointen lähteiden tiedustelu, henkilötiedustelu kansainvälisessä toiminnassa, kuvaustiedustelu, geotiedustelu ja radiosignaalitiedustelu.

Avointen lähteiden tiedustelu

Avointen lähteiden tiedustelutieto (OPEN SOURCE INTELLIGENCE, OSINT) on avoimista lähteistä hankittuun informaatioon perustuvaa tietämystä, joka on yhdenmukaisesti jaoteltu, arvioitu ja suodatettu.

Avoimista lähteistä saatava informaatio koostuu tiedoista, jotka ovat jokaisen kansalaisen laillisesti saatavilla pyytämällä tai itse havainnoimalla. Tyypillisiä tiedonlähteitä ovat kirjallisuus, tilastot, kartat, lehdet, julkaisut, yleisölle suunnatut televisio- ja radiolähetykset sekä sosiaalisen median sisällöt. Avointen lähteiden tiedonhankinta voidaan jakaa rajattuun tiedustelukysymykseen perustuvaan tiedonhankintaan ja media-seurantaan, jonka tarkoituksena on tiedustelutilannekuvan muodostamisen tukeminen.

Avointen lähteiden tiedustelussa tiedonhankinta kohdistuu pääasiassa laajempiin ilmiöihin tai tapahtumiin. Pitkäkestoisessa tiedonhankinnassa esimerkiksi yksittäisten sosiaalisen median käyttäjätilien seuranta on kuitenkin tärkeää tapahtuman ymmärtämiseksi tai tiedon luotettavuutta arvioidessa.

Avointen lähteiden tiedusteluun ei katsota sisältyvän aktiivista osallistuminen esimerkiksi internetverkossa käytävään keskusteluun tiedon hankkimiseksi. Tietoa voidaan hankkia muiden viranomaisten tavoin myös ostamalla tai kolmansien osapuolien (esim. asiantuntijat, mediaseurantayritykset) avulla.

Avointen lähteiden tiedustelua käytetään muiden tiedustelulajien tukena tai itsenäisenä tiedustelulajina tilanteissa, joissa muiden tiedustelulajien käyttö ei ole mahdollista tai tehokasta. Tiedustelulajille on ominaista tiedon suuri määrä ja disinformaation mahdollisuus. Viime vuosina erityisesti sosiaalisen median kautta saatavien havaintojen määrä on kasvanut suhteessa muihin lähteisiin.

Avointen lähteiden tiedustelun vahvuuksiin kuuluvat sen nopeus, edullisuus, maantieteellinen rajoittamattomuus ja mahdollisuus kerätä tietoja tulevista tapahtumista. Pelkästään avoimiin lähteisiin perustuva tiedustelutuote on tavallisesti suojaustasoltaan muita tiedustelutuotteita julkisempi, jolloin tuotteen käytettävyys on parempi.

Kuvaustiedustelu

Kuvaustiedustelulla (IMAGERY INTELLIGENCE, IMINT) tuotetaan elektro-optisen ja tutkakuvauksen keinoin analysoitua tietoa ja uhkakuvaa sotilaallisista ja sotilaalliseen toimintaan liittyvistä kohteista ja niiden toiminnasta.

Geotiedustelu

Geotiedustelulla tarkoitetaan tiedonhankkimista vieraan valtion maantieteellisistä ja alueen toimintaympäristön olosuhteista. Geotiedustelun tarkoituksena on kuvata, arvioida ja esittää tietyt kohteet, alueet, luonnonilmiöt ja olosuhteet. Geotiedustelussa käytetään hyväksi muun muassa kansallista ja kansainvälistä paikkatieto- ja kuva-aineistoa, olosuhdetietoja sekä tilastollisia aineistoja. Sotilastiedusteluviranomainen voi myös tilata ulkopuolisilta toimijoilta tällaista tietoa oman tiedustelunsa tueksi.

Henkilötiedustelu kansainvälisessä toiminnassa

Henkilötiedustelu (HUMAN INTELLIGENCE, HUMINT) yleisesti on tiedustelulaji, jonka päämääränä on tehtävään koulutetulla henkilöstöllä hankkia tietoa tiedonhankinnan kohdistuessa ihmisiin ja heidän hallussaan oleviin asiakirjoihin ja sähköisiin tallenteisiin.

Nykytilassa henkilötiedustelua voidaan käyttää rajoitetusti Puolustusvoimien rikostorjunnassa, mutta henkilötiedustelua voidaan toteuttaa myös Puolustusvoimien kansainvälisessä toiminnassa.

Puolustusvoimien tiedonhankinnassa on käytettävänä Suomen ulkomaan edustustoissa toimiva sotilasasiamiesverkosto. Diplomaattisia suhteita koskevan Wienin yleissopimuksen 3 artiklan mukaan diplomaattisen edustuston tehtäviin sisältyy muun muassa tutustuminen kaikin laillisin keinoin vastaanottajavaltion oloihin ja tapahtumiin sekä niistä tiedottaminen lähettäjävaltion hallitukselle. Yleissopimuksen 7 artiklassa mainitaan edustuston henkilöistä erikseen sotilas-, laivasto- ja ilmailuasiamiehet.

Henkilötiedustelun alaan voidaan lukea Suomen puolustusasiamiesverkoston tuottamat tiedot. Puolustusasiamiesten tehtäviin kuuluu muun muassa yhteyshenkilönä toimiminen kohdemaan ja lähettävän maan (asemamaa) puolustusministeriöiden kesken, kohdemaan puolustuspolitiikan ja asevoimien yleinen seuraaminen sekä puolustusteknologian vientikysymyksissä yhteyshenkilönä toimiminen kohde- ja asemamaiden välillä. Puolustusvoimia koskevissa laeissa ei ole säännöksiä edustustoissa toimivien Puolustusvoimien virkamiesten toimivaltuuksista.

Henkilötiedustelua voidaan käyttää myös tietyissä tilanteissa kriisinhallintaoperaatioissa. Kriisinhallintaoperaatiossa sotilasjoukko toimii toisen valtion alueella. Sotilasjoukkojen asema toisen suvereenin valtion alueella (operaation isäntävaltio) järjestetään valtioiden välisin sopimuksin, joissa määrätään joukkojen oikeudellisesta asemasta ja immuniteetista isäntävaltion alueella. Näitä sopimuksia kutsutaan joukkojen oikeudellista asemaa säänteleviksi sopimuksiksi (Status of Forces Agreement, SOFA-sopimus). Lähtökohtaisesti SOFA-sopimusten neuvottelusta vastaa operaation valtuuttaja tai toimeenpanija suhteessa operaation isäntävaltioon. Pääsääntöisesti kyseisten sopimusjärjestelyistä johtuvat velvollisuudet, käytännössä erivapauksien ja –oikeuksien myöntäminen kriisinhallintajoukolle, kohdentuvat yksipuolisesti operaation isäntävaltioon. SOFA-sopimukset eivät luo toimivaltuuksia operaatioissa palveleville joukoille. Toimivaltuudet seuraavat operaation kansainvälisoikeudellisesta mandaatista, joukkoja lähettävien maiden kansallisesta lainsäädännöstä sekä operaatiossa annetuista sotilaskäskyistä.

Kriisinhallintaoperaatioissa tiedusteluyksiköt tai tiedustelu-upseerit toimivat pääsääntöisesti osana kansallista tai monikansallista joukkoa. Kriisinhallinnan tiedustelu tapahtuu pääasiassa operaatiota johtavan organisaation määräysten ja ohjeistuksen mukaisesti. Toimintaympäristö ja operaatiokohtaiset määräykset aiheuttavat hyvin erilaisia vaatimuksia tiedustelulle. Kriisinhallinnassa sotilastiedustelu tuottaa suomalaisten kriisinhallintajoukkojen toiminta-alueen toimintaympäristötietoisuutta kansallisen päätöksenteon sekä kriisinhallintajoukkojen omasuojan ja toiminnan suunnittelun tueksi. Tavoitteena on varmistaa kriisinhallintajoukon omasuoja sekä toisaalta kehittää kansallisen puolustuksen suorituskykyä.

Radiosignaalitiedustelu

Radiosignaalitiedustelun tavoitteena on osana sotilastiedustelua ylläpitää tilannekuvaa ja tuottaa ennakkovaroitus. Lyhyellä aikavälillä radiosignaalitiedustelu muodostaa tilannekuvaa seurattavana olevien sotilasorganisaatioiden ryhmityksestä, valmiudesta ja toiminnasta. Pitkällä aikavälillä radiosignaalitiedustelun keinoin voidaan seurata kohdeorganisaatioiden teknisen ja operatiivisen kyvyn kehittymistä. Puolustushaarat ja Puolustusvoimien tiedustelulaitos suorittavat signaalitiedustelua taktisen tason tiedusteluna.

Radiosignaalitiedustelua suoritetaan normaalioloissa kotimaan alueella, Suomen hallinnassa olevalla alueella tai kansainvälisellä alueella olevilla tiedustelujärjestelmillä. Puolustusvoimien harjoitustoimintaan tai virka-aputehtäviin liittyvää tiedustelutoimintaa voidaan lisäksi suorittaa vieraan valtion alueella. Kriisinhallintatehtäviin liittyvää tiedustelua suoritetaan joko kotimaan, kohdemaan tai kolmannen valtion alueelta.

Radiosignaalitiedustelu suunnataan tiedonhankintasuunnitelman mukaisesti ulkomaisiin kohteisiin, jotka sijaitsevat kohdevaltion alueella, kansainvälisellä alueella tai kolmannen valtion alueella. Poikkeustilanteissa, kuten alueloukkaustapauksissa sekä normaaliolojen häiriötilanteessa, ulkomainen kohde voi olla ja siten myös tiedustelu kohdistua myös Suomen valtion alueelle.

Virka-aputehtävissä radiotiedustelua suunnataan kaikkiin tarvittaviin kohteisiin myös Suomen alueella. Sotilastiedustelun tunnistustietokantojen ja kohdejärjestelmien ominaispiirteiden tunnistamisen näkökulmasta tiedustelua suunnataan kaikkiin kotimaisiin ja ulkomaisiin kohteisiin.

Suomessa radiosignaalitiedustelu on jaettu seuraavasti:

Radioaalloilla tapahtuva viestitiedustelu (Communications Intelligence, COMINT) on erityyppisten radioaalloilla tapahtuvien tiedonsiirtosignaalien tiedustelua. Tiedustelun kohteena voi olla signaalin informaatiosisältö, tekniset parametrit, signaalilähteen sijainti tai mikä tahansa muu signaaliin liittyvä informaatio, joka tuottaa tiedustelutietoa signaalin käyttäjästä tai käytetystä järjestelmästä.

Elektroninen mittaustiedustelu (Electronic Intelligence, ELINT) on muiden radiolähetteiden kuin viestintään käytettävien radioaaltojen tiedustelua, tyypillisimmin tutkalähetteiden ja muiden navigointisignaalien tiedustelua. Tutkasignaaleita tiedustelemalla pystytään selvittämä esimerkiksi tutkan sijainti, tekniset parametrit, tyyppi ja tietoa tutkan suorituskyvystä. Näiden tietojen perusteella voidaan tuottaa esimerkiksi uhkatietoja hävittäjien ja alusten omasuojajärjestelmille. sekä syvällistä tietoa järjestelmien suorituskyvyistä. Elektroninen mittaustiedustelu ei kohdistu henkilöiden väliseen viestintään.

Vieraiden laitteiden teknisten instrumentointisignaalien tiedustelussa (Foreign Instrumentation Signals Intelligence, FISINT) hyödynnetään tyypillisimmin avaruus-, maanpäällisten- ja vedenalaistenjärjestelmissä käytettävät elektromagneettiset lähetteet eli telemetrialähetteet. Tiedustelun kohteena ovat teknisten järjestelmien väliset tekniset signaalit, jotka eivät sisällä luottamuksellista viestintää. . Tällaisia lähetteitä ovat erilaisten laitteiden, esimerkiksi ohjusten ja lentokoneiden, ohjaussignaalit. Kohdesignaaleista pyritään yleensä tuottamaan tiedustelutietoa kohdejärjestelmän toiminnasta ja suorituskyvystä.

2.2.3 Puolustusvoimien tiedonhankinta ulkomailla

Puolustusvoimista annetun lain 2 §:n 1 kohdassa säädetysti Puolustusvoimien tehtävänä on Suomen sotilaallinen puolustaminen, johon kuuluu a) maa-alueen, vesialueen ja ilmatilan valvominen sekä alueellisen koskemattomuuden turvaamine sekä b) kansan elinmahdollisuuksien, perusoikeuksien ja valtiojohdon toimintavapauden turvaaminen ja laillisen yhteiskuntajärjestyksen puolustaminen. Ulkomaista alkuperää olevia kohteita ovat muun muassa sotilaallinen toiminta, ulkovaltojen Suomeen ja sen etuihin kohdistama vakoilu sekä sotatarvikkeiden valmistus ja levittäminen. Puolustusvoimien tehtävänä on myös analysoida Suomen turvallisuusympäristöä ja ylläpitää toimialansa kansainvälistä tilannekuvaa. Puolustusvoimat raportoi kansainvälisen turvallisuusympäristön kehittymisestä muille turvallisuusviranomaisille ja Suomen ylimmälle valtionjohdolle.

Suomen turvallisuusympäristö on voimakkaasti kansainvälistynyt, kuten aiemmin tässä esityksessä viitatuista selonteoista käy ilmi. Ulkomaita koskevilla tiedoilla on yhä suurempi merkitys niiden turvallisuusetujen suojelemisessa, jotka kuuluvat Puolustusvoimien vastuulle.

Puolustusvoimien tiedonhankinnasta ulkomailla ei ole säädetty erikseen. Tietyissä määrin tiedonhankinta on katsottu perustuvan Puolustusvoimien lakisääteisiin tehtäviin. Puolustusvoimat ovat voineet ilman nimenomaista sääntelyä käyttää ulkomaan tiedonhankinnassaan avointen lähteiden tiedustelua, kuvaustiedustelua, geotiedustelua, henkilötiedustelua kansainvälisessä toiminnassa sekä radiosignaalitiedustelua.

Puolustusvoimien salainen tiedonhankinta perustuu SKRTL:n mukaisten rikosten estämistä ja paljastamista koskevien toimivaltuuksien käyttöön sekä SKRTL:ssä tarkoitettuun poliisin antamaan apuun. Näitä toimivaltuuksia voi käyttää vain Suomen alueella.

Puolustusvoimien ulkomaita koskeva tiedonsaanti nojaa käytännössä kuitenkin suurimmalta osin sen harjoittamaan kansainvälisen tiedusteluyhteistyön, avointen lähteiden seurannan sekä puolustusasiamiestoiminnan varaan.

Puolustusvoimat on tehnyt laajaa kahden- ja monenvälistä yhteistyötä ulkomaisten tiedustelu- ja turvallisuuspalveluiden kanssa. Yhteistyön avulla varmistetaan valtion turvallisuuden ylläpitämiseksi tarpeellisten ulkomaisten tiedustelutietojen saaminen. Turvallisuuskysymysten yleisestä globalisoitusmiskehityksestä ja siitä seuranneesta ulkomaisten tiedustelutietojen merkityksen korostumisesta johtuen Puolustusvoimat on viime vuosina suunnitelamallisesti laajentanut kansainvälistä yhteistyöverkostoaan siten, että sen tällä on katsottava kattavan kaikkien Suomen turvallisuuden kannalta olennaisten maiden tiedustelu- ja turvallisuusviranomaiset.

Kansainvälisestä tiedusteluyhteistyöstä on pidettävä erillään rikostorjuntaa palvelevat kansainväliset yhteistyömenettelyt. Puolustusvoimien toimialalla niiden merkitys on vähäinen.

Puolustusvoimien ulkomaita koskeva avointen lähteiden seuranta kattaa koko Puolustusvoimien toimialan. Avoimista lähteistä hankitut tiedot yhdistetään muista lähteistä saataviin tietoihin analysoidun turvallisuustilannekuvan muodostamiseksi Suomen kansainvälisestä turvallisuusympäristöstä.

Lisäksi Puolustusvoimien ulkomaita koskevaksi tiedonhankinnaksi voidaan katsoa Wienin yleissopimuksen nojalla tapahtuva toiminta, jota on kuvattu aiemmin tässä esityksessä kohdassa henkilötiedustelu kansainvälisessä toiminnassa.

2.2.4 Puolustusvoimien ohjaus

Puolustusministeriö vastaa perustuslain 68 §:n 1 momentin, valtioneuvostosta annetun lain (175/2003) ja valtioneuvoston ohjesäännön (262/2003) mukaisesti Puolustusvoimia koskevista ministeriötehtävistä.

Toiminnallisen ohjauksen lisäksi puolustusministeriö vastaa Puolustusvoimien tulosohjauksesta ja resursoinnista. Puolustusvoimien tiedonhankintaa ei ole eriytetty omalle momentilleen Puolustusvoimien toimintamenomomentista eikä tiedonhankinnalle ole asetettu erillistä tulosmittaristoa tai resurssijakomallia.

Puolustusministeriö antaa puolustusministeriöstä annetun valtioneuvoston asetuksen (375/2003) 4 §:n mukaan ministeriön työjärjestyksessä säädetään ministeriön tehtävien ja ratkaisuvallan käytön lisäksi ministeriön hallinnonalana ohjauksesta.

Puolustusvoimista annetun lain 24 §:ssä todetaan Puolustusvoimien toimivan puolustusministeriön ohjauksessa. Puolustusvoimien ohjausta voidaan käsitellä myös valmistelevasti ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteisessä kokouksessa. Kyse on kokonaisuutena arvioituna valtioneuvostotason ohjaus- ja yhteensovittamismekanismista. Tästä mekanismista ei ole annettu laintasoisia säännöksiä.

Puolustusministeri kantaa poliittista vastuuta Puolustusvoimien toiminnasta ja siksi hänen tulee olla tietoinen viraston toimialaan kuuluvista keskeisistä asioista. Tämän vuoksi Puolustusvoimien rikostorjunnassa SKRTL:n 128 §:n mukaan Puolustusvoimien on toimitettava puolustusministeriölle

tiedot yhteiskunnallisesti, taloudellisesti tai vakavuudeltaan merkittävistä Puolustusvoimien rikostorjuntaan liittyvistä asioista.

Puolustusvoimat informoi tasavallan presidenttiä, ulko- ja turvallisuuspoliittista ministerivaliokuntaa sekä eduskunnan puolustus- ja ulkoasiainvaliokuntia pitääkseen heidät ajan tasalla ulko- ja turvallisuuspolitiikkaan liittyvistä asioista ja turvallisuustilanteesta.

2.2.5 Sotilastiedustelun järjestäminen

Sotilastiedustelun tasot jaetaan strategiseen, operatiiviseen ja taktiseen tasoon. Strategisella johtamistasolla tarkoitetaan ylintä valtionjohtoa eli eduskuntaa, tasavallan presidenttiä ja valtioneuvostoa.

Strategisella sotilasjohdolla tarkoitetaan Puolustusvoimien ylipäällikköä ja Puolustusvoimain komentajaa, joiden tehtäväkenttä käsittää sotilaspoliittiset ja erityisesti puolustusjärjestelmän käyttöä ja johtamista koskevat asiat.

Strateginen tiedustelu tuottaa poliittisille ja sotilaallisille päätöksentekijöille pitkän aikavälin laaja-alaisen toimintaympäristötietoisuuden ja tarvittaessa ennakkovaroituksen. Strategisen tiedustelun tehtävänä on antaa jo normaalioloissa ennakkovaroitus valtioiden ja sotilasliittojen politiikan huomattavista muutoksista, sotilaallisista toimista tai teknologian merkittävästä kehittymisestä. Strateginen tiedustelu on kansallisella ja kansainvälisellä tasolla tapahtuvan politiikan valmistelussa ja toteuttamisessa ja sotilaallisessa suunnittelussa tarvittavan tiedon keräämistä, käsittelyä, analysointia, tuotteistamista ja jakelua sekä kyseisen tiedusteluprosessin johtamista. Strategisen tiedustelun tärkeimmät kerääjät ovat sotilastiedustelu ja siviilitiedustelu. Myös ulkoministeriö tuottaa strategisen tasan tietoja.

Sotilastiedustelu vastaa osaltaan strategisen sotilasjohdon toimintaympäristötietoisuuden ylläpitämisestä laajan turvallisuuskäsitteen mukaisella tavalla ja sotilaallisilla tiedoilla painotettuna. Jaettavan tiedustelutiedon tulee olla sisällöltään ja muodoltaan tätä palvelevaa.

Sotilastiedustelun operatiivinen johtamistaso käsittää kokonaisuutena Puolustusvoimat eli Puolustusvoimain komentajan, Pääesikunnan päällikön ja apulaisesikuntapäälliköt, Pääesikunnan ja sen alaiset laitokset, Maanpuolustuskorkeakoulun sekä puolustushaarat. Pääesikunnan tiedusteluosaston päällikkö (jäljempänä tiedustelupäällikkö) on sotilastiedustelutoimialan toimialapäällikkö ja Puolustusvoimien tiedustelulaitoksen johtajan suoranainen esimies. Tiedustelupäällikkö johtaa sotilastiedustelutoimialaa Puolustusvoimien operaatiopäällikön alaisuudessa apunaan Pääesikunnan tiedusteluosasto. Tiedustelupäällikkö antaa sotilastiedustelun tuotteiden laatimisesta ohjeet Puolustusvoimien tiedustelulaitokselle, puolustushaaroille ja muille Pääesikunnan alaisille laitoksille. Tiedustelupäällikkö vastaa sotilastiedustelutoimialan kokonaisuudesta sekä sen johtamisesta ja suorituskyvyn käytöstä. Sotilastiedustelutoimialan kokonaisuuteen kuuluvat sotilastiedustelun sekä sotilasvastatiedustelun asiat sisältäen tiedonhankinnan, tiedon käsittelyn ja raportoinnin.

Tiedusteluosaston vastatiedustelusta vastaava apulaisosastopäällikkö käyttää itsenäistä toimivaltaa rikosten ennalta estämisen ja paljastamisen osalta, käyttäen päällystöön kuuluvalle poliisimiehelle ja pidättämiseen oikeutetulle poliisimiehelle säädettyjä toimivaltuuksia, sotilaskurinpidosta ja rikostorjunnasta Puolustusvoimissa annetun lain 87 §:n mukaisesti. Vastatiedustelupäällikkö vastaa laissa sotilaskurinpidosta ja rikostorjunnasta Puolustusvoimissa säädetyistä turvallisuustietorekisteristä ja tilapäisistä henkilörekistereistä.

Puolustusvoimien tiedustelulaitos on Pääesikunnan alainen sotilaslaitos, joka tuottaa valtionjohdon ja Puolustusvoimien tarvitsemia tiedustelupalveluja. Laitos on puolustusvoimallinen ja valtakunnallinen toimija, ja se vastaa myös Puolustusvoimien paikka- ja olosuhdetiedosta. Laitokseen sisälty-

vä Tiedustelukoulu antaa sotilastiedustelu- ja turvallisuustoimialan täydennyskoulutusta Puolustusvoimien ja tärkeimpien yhteistyöviranomaisten henkilöstölle. Puolustusvoimien Tiedustelulaitoksen toimintoihin kuuluvat tiedon hankinta eri tiedustelulajeilla ja hankitun tiedon analysointi ja raportointi.

Puolustusvoimien tiedustelulaitoksella on sotilastiedustelutoiminnassa keskeinen rooli. Jaettava tieto muokataan ja sen jakaminen ajoitetaan asiakkaan toimintaympäristötietoisuuden ylläpitämiseksi tehtävien edellyttämällä ja tarkoituksenmukaisella tavalla.

Puolustushaarat, eli maa-, meri- ja ilmavoimat vastaavat valvontajärjestelmän ylläpidosta ja käytöstä sekä tuottavat ja perustavat poikkeusoloissa toimivat taktisen tason sotilastiedustelujoukot ja -yksiköt. Normaalioloissa puolustushaarojen tiedustelun päätehtävänä on suorituskykyjen rakentaminen ja valmiuden ylläpito. Puolustushaarat osallistuvat sekä normaali- että poikkeusoloissa sotilastiedustelun operatiiviseen toimintaan Pääesikunnan tiedustelupäällikön ohjauksessa. Ne vastaavat poikkeusoloissa tarvittavien tiedustelujoukkojen joukkotuotannosta ja perustamisesta. Puolustushaarojen valvontajärjestelmän tehtävänä on tuottaa ja ylläpitää reaaliaikaista alueellisen koskemattomuuden valvonnan ja turvaamisen vaatimaa tilannekuvaa maa- ja merialueelta sekä ilmatilasta. Maanpuolustuskorkeakoulu ja Pääesikunnan alaiset laitokset tukevat sotilastiedustelutoimialaa erikoisosaamisellaan ja -kyvyillään.

2.2.6 Asevelvollisten osallistuminen Puolustusvoimien tehtäviin

Asevelvollisuuslain mukaan asevelvollisuuden suorittamiseen kuuluu varusmiespalvelus, kertausharjoitus, ylimääräinen palvelus ja liikekannallepanon aikainen palvelus. Asevelvollinen voi olla palveluksessa taikka kuulua reserviin tai varareserviin. Reserviin kuuluvat myös sotilasvirasta eroamaan joutuneet henkilöt sen vuoden loppuun, jona hän täyttää 60 vuotta.

Kertausharjoitukseen voidaan määrätä reserviin kuuluva asevelvollinen. Asevelvollisuuslain mukaan kertausharjoituksilla voidaan pitää yllä varusmiespalveluksen aikana saatuja sotilaallisia tietoja ja taitoja sekä koulutetaan vaativampiin tehtäviin, perehdyttää asevelvolliset sotilaallisessa maanpuolustuksessa tapahtuneen kehityksen mukanaan tuomiin muutoksiin ja mahdollistaa sotilaallisen valmiuden joustava kohottaminen.

Lisäksi reserviin kuuluvia riittävän koulutuksen saaneita voidaan käyttää SKRTL:n 102 §:n mukaan Puolustusvoimien rikosten ennalta estämisessä ja paljastamisessa, kun tasavallan presidentti on päättänyt asevelvollisuuslain 83 §:n mukaisesti ylimääräisestä palveluksesta.

Oikeuskanslerin vastauksen (OKV/50/20/2015) mukaan varusmiespalveluksessa olevia asevelvollisia voidaan käyttää ja muita palveluksessa olevia asevelvollisia voidaan käyttää sotilaallista valmiutta kohotettaessa. Tällöin on kuitenkin otettavan huomioon näiden tiedolliset ja taidolliset valmiudet erilaisten tehtävien hoitamiseen. Tällöin on muun muassa arvioitava sitä, miten pitkälle varusmies on ehtinyt päästä koulutuksessaan tai kuinka pitkä aika on ehtinyt kulua reserviläisen saamasta koulutuksesta.

Sotilaallisesta kriisinhallinnasta annetun lain mukaiseen palvelussuhteeseen voidaan ottaa asevelvollisuuslain mukaisen koulutuksen saanut ja erityisen sitoumuksen antanut henkilö. Sotilaallisesta kriisinhallinnasta annetun lain mukaisessa palveluksessa oleva henkilö on kriisinhallintaoperaatiosta tehdyn sopimuksen mukaisesti kriisinhallintaorganisaation alainen ja hänen oikeudet ja velvollisuudet määräytyvät sen mukaan.

2.2.7 Puolustusvoimien oikeudellinen valvonta

2.2.7.1 Yleistä

Puolustusvoimien toiminnan laillisuutta pyritään turvaamaan sekä sisäisen että ulkoisen valvonnan keinoin. Valvontaa toteuttava taho voi vaihdella valvottavan toiminnon tai asian mukaan. Myös valvontaa toteuttavien tahojen toimivalta ja käytettävissä olevat valvontakeinot vaihtelevat.

Sisäisen ja ulkoisen laillisuusvalvonnan suhdetta on käsitelty esimerkiksi Jaakko Jonkan selvityksessä Poliisin johtamisjärjestelmä ja sisäinen laillisuusvalvonta (Sisäasiainministeriön julkaisuja 48/2004). Selvityksessä on todettu sisäisen ja ulkoisen valvonnan täydentävän toisiaan. Ulkopuolinen valvonta on uskottavuuden kannalta tärkeää. Lisäksi se voi paljastaa ehkä paremmin joitakin organisaation systeemivirheitä tai oikeudellisesti kestämättömiä käytäntöjä. Toisaalta se voi tehokkaanakin paljastaa ja selvittää vain osan virheistä. Mitä lähempänä itse toimintaa valvonta on, sitä paremmin se toimii virheitä ennalta ehkäisevästi ja kykenee havaitsemaan vähäisetkin ongelmat. Selvityksen mukaan sisäinen laillisuusvalvonta tulisikin nähdä osana johtamiseen kuuluvaa laadunvalvontaa.

Laillisuuden merkitys korostuu Puolustusvoimien toiminnassa moneen muuhun julkisen sektorin toimintaan verrattuna. Puolustusvoimat voi lain perusteella niin normaaliaikana kuin poikkeusoloissakin puuttua ihmisten perusoikeuksina suojattuihin oikeushyviin. Ulkopuolisten tarkkailijoiden mahdollisuudet tehdä havaintoja Puolustusvoimien toiminnasta ovat usein rajalliset. Kaikissa tapauksissa toimenpiteiden kohteellakaan ei toiminnan erityisolosuhteiden vuoksi ole välttämättä aitoa mahdollisuutta tehdä toiminnasta havaintoja. Edelleen sotilasviranomaisten toiminnasta ei aina ole valitusmahdollisuutta (esim. sotilaskäskyasiat). Uskottava laillisuusvalvonta on tärkeää virkatoimintaa kohtaan tunnettavan luottamuksen kannalta. Puolustusvoimien toimintaan kohdistuva laillisuusvalvonta jaetaan ulkoiseen laillisuusvalvontaan ja sisäiseen laillisuusvalvontaan.

Viranomaisten sisäinen valvonta ja esimiestyö ovat keskeisiä toiminnan lainmukaisuuden takaamisessa. Mitä lähempänä toimintaa valvonta on, sitä paremmin se voi havaita ja välittömästi puuttua vähäisiinkin ongelmiin. Myös hallintovaliokunta on lausunnossaan (HaVL 40/2014) todennut, ettei mikään järjestelmä tai valvonta voi korvata sitä, että asiat tehdään jo ensi vaiheessa oikein. Tähän seikkaan on panostettava kaikkein eniten.

2.2.7.2 Puolustusvoimien sisäinen laillisuusvalvonta

Sisäinen laillisuusvalvonta kohdistetaan ulkoista valvontaa kattavammin Puolustusvoimien toiminnan eri osa-alueisiin. Sisäinen laillisuusvalvonta toimii lähellä konkreettista käytännön toimintaa ja yhteistyössä oikeudellisen asiantuntijatuen tehtäviä hoitavien kanssa. Näin pyritään saavuttamaan riittävä kyky laillisuusvalvonnan toimenpiteitä edellyttävien kohteiden havaitsemiseksi.

Puolustusvoimien sisäinen laillisuusvalvonta voidaan jakaa kahteen eri kokonaisuuteen. Laillisuusvalvontaa suoritetaan kunkin hallintoyksikön johtamiseen liittyen yleisenä toiminnan laillisuuden seurantana. Kunkin esimiehen virkavelvollisuutena on puuttua lainvastaisiin toimintatapoihin osana päivittäistä johtamistyötä. Sisäiseen valvontaan kuuluu lisäksi henkilökunnan koulutukseen liittyvä eettinen koulutus, toiminnan päivittäisen toiminnan yhteydessä tapahtuva esimiesten toteuttama valvonta sekä vertaisvalvonta, työjärjestykset, operatiiviset ohjeet ja muu dokumentaatio.

Toisena kokonaisuutena on Puolustusvoimien johdon suorittama erityinen laillisuusvalvonta, joka on puolustusvoimista annetussa valtioneuvoston asetuksessa (1319/2007) säädetty Puolustusvoimien asessorin toteutettavaksi. Puolustusvoimien asessori ohjaa ja valvoo Puolustusvoimien toiminnan lainmukaisuutta ja sotilasoikeudenhoitoa. Sisäisen laillisuusvalvonnan keskeiset toimenpiteet valmistelee ja esittelee asessorille pääesikunnan oikeudellisen osaston apulaisosastopäällik-

kö, laillisuusvalvontasektorin sektorijohtaja tai laillisuusvalvontatehtäviä hoitava sotilaslakimies. Laillisuusvalvonnan käytännön toimeenpanosta huolehtivat keskeisinä toimijoina pääesikunnan oikeudellisen osaston laillisuusvalvontasektori. Oikeudellisen toimialan sotilaslakimiehet ja joukko-osastojen oikeusupseerit raportoivat laillisuusvalvontaan liittyvistä tapahtumista pääesikunnan oikeudelliselle osastolle.

Pääesikunnan oikeudellinen osasto voi suorittaa laillisuusvalvontaan liittyviä kyselyjä ja tehdä omasta aloitteestaan itse tai yhteistyössä sidosryhmiensä kanssa tarpeellisia tutkimuksia ja muistioita laillisuusvalvonnan piiriin kuuluvista asiakokonaisuuksista. Pääesikunnan oikeudellinen osasto voi käsitellä asevelvollisten, Puolustusvoimien henkilökunnan tai muiden tahojen tekemiä laillisuuskysymyksiin liittyviä aloitteita ja kysymyksiä. Pääesikunnan oikeudellinen osasto voi tehdä havaintojensa perusteella aloitteita lainsäädännön ja hallinnollisten määräysten ja ohjeiden muuttamiseksi tai laatimiseksi.

Lähinnä nyt hallituksen esityksessä esitettäviin toimivaltuuksiin verrattavissa olevat toimivaltuudet liittyvät salaisten tiedonhankintakeinojen ja salaisten pakkokeinojen käyttöön, sekä niiden valvontamekanismeihin. Sotilastiedustelun valvonnasta on säädetty erikseen siltä osin, kuin se koskee sotilasvastatiedustelun tekemää rikostorjuntaa.

Sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain (SKRTL 255/2014) 129 § mukaan puolustusministeriö antaa eduskunnan oikeusasiamiehelle vuosittain kertomuksen lain 37 §:ssä mainittujen salaisten pakkokeinojen ja 89 §:n 1 momentissa mainittujen salaisten tiedonhankintakeinojen ja niiden suojaamisen käytöstä ja valvonnasta. Kertomus toimitetaan lisäksi tiedoksi suojelupoliisille.

Puolustusvoimien johto valvoo SKRTL:n 127 § mukaan Puolustusvoimien rikostorjuntaa. Tämän lisäksi Puolustusvoimien asessori valvoo pääesikunnan SKRTL:n 35 §:n nojalla suorittamaa rikosten selvittämistä ja tiedusteluosaston osastopäällikkö valvoo 86 §:n mukaista rikosten ennalta estämistä ja paljastamista.

SKRTL 128 §:n mukaan SKRTL 37 §:ssä mainittujen salaisten pakkokeinojen ja 89 §:n 1 momentissa mainittujen salaisten tiedonhankintakeinojen käytöstä laadittu pöytäkirja on toimitettava puolustusministeriölle. Puolustusministeriölle on lisäksi toimitettava tiedot yhteiskunnallisesti, taloudellisesti tai vakavuudeltaan merkittävistä Puolustusvoimien rikostorjuntaan liittyvistä asioista.

Erikseen on huomattava, että kukin sotilasesimies vastaa hänelle sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain mukaan kuuluvista kurinpitomenettelyn valvontaan liittyvistä tehtävistä. Näissä tehtävissä kurinpitoesimiehiä avustavat sotilaslakimiehet ja oikeusupseerit. Sisäinen laillisuusvalvonta tulee niin ikään erottaa sisäisestä tarkastuksesta, jonka tehtävänä on mm. riskienhallinta-, valvonta- sekä johtamis- ja hallintoprosessien tehokkuuden arviointi ja kehittäminen.

2.2.7.3 Puolustusvoimien ulkoinen laillisuusvalvonta

Puolustusministeriön suorittama laillisuusvalvonta

Edellä määritellyn laillisuusvalvonnan mukaan puolustusministeriön Puolustusvoimiin kohdistama valvonta voidaan lukea ulkoiseksi valvonnaksi. Perustuslain (731/1999) 68 § mukaan kukin ministeriö vastaa toimialallaan valtioneuvostolle kuuluvien asioiden valmistelusta ja hallinnon asianmukaisesta toiminnasta. Puolustusvoimista annetun lain 24 §:n 1 momentin mukaan Puolustusvoimat on hallinnollisesti puolustusministeriön alainen. Puolustusministeriön työjärjestyksestä annetun puolustusministeriön asetuksen (585/2003) mukaan lainvalmistelu- ja oikeusyksikön yhtenä tehtävänä on ministeriön ja hallinnonalan laillisuusvalvonta sekä sen kehittäminen ja yhteensovittami-

nen. Lainvalmistelu- ja oikeusyksikön johtaja ratkaisee laillisuusvalvontaa koskevat asiat. Merkittävät laillisuusvalvonta-asiat ratkaisee kuitenkin kansliapäällikkö, jos ne eivät yhteiskunnallisen tai taloudellisen merkittävyytensä vuoksi vaadi ministerin ratkaisua.

Sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain (SKRTL 255/2014) 128 §:ssä säädetään puolustusministeriön valvonnasta. Saman lain 129 § mukaan puolustusministeriö antaa eduskunnan oikeusasiamiehelle vuosittain kertomuksen lain 37 §:ssä mainittujen salaisten pakkokeinojen ja 89 §:n 1 momentissa mainittujen salaisten tiedonhankintakeinojen ja niiden suojaamisen käytöstä ja valvonnasta. Kertomus toimitetaan lisäksi tiedoksi suojelupoliisille.

Ylimmät laillisuusvalvojat

Ylimpien laillisuusvalvojien, eduskunnan oikeusasiamiehen ja valtioneuvoston oikeuskanslerin tehtävänä on muun ohessa Puolustusvoimiin kohdistuva laillisuusvalvonta.

Suomen perustuslain 108 §:ssä säädetään valtioneuvoston oikeuskanslerin tehtävistä. Perustuslain mukaan oikeuskanslerin tulee muun muassa valvoa, että tuomioistuimet ja muut viranomaiset sekä virkamiehet, julkisyhteisön työntekijät ja muutkin julkista tehtävää hoitaessaan noudattavat lakia ja täyttävät velvollisuutensa. Eduskunnan oikeusasiamiehen tehtävistä säädetään tältä osin vastaavalla tavalla perustuslain 109 §:ssä. Ylimmillä laillisuusvalvojilla on perustuslain 110 §:n mukaisesti syyteoikeus. Valvojat voivat ajaa syytettä tai määrätä syytteen nostettavaksi. Lisäksi ylimmillä laillisuusvalvojilla on laaja tietojensaantioikeus, josta säädetään perustuslain 111 §:ssä.

Eduskunnan oikeusasiamiehen tehtävistä säädetään tarkemmin eduskunnan oikeusasiamiehestä annetussa laissa (197/2002). Oikeusasiamiehen suorittaman valvonnan erityiseksi kohteeksi on määritelty varusmiesten, muiden asepalvelusta suorittavien ja kriisinhallintahenkilöstön kohtelu. Lain 5 § mukaan oikeusasiamies toimittaa tarpeen mukaan tarkastuksia perehtyäkseen laillisuusvalvontaansa kuuluviin asioihin. Tarkastuksen yhteydessä oikeusasiamiehellä on oikeus päästä valvottavan kaikkiin tiloihin ja tietojärjestelmiin sekä oikeus keskustella luottamuksellisesti tarkastuskohteen henkilökunnan sekä siellä palvelevien tai sinne sijoitettujen henkilöiden kanssa.

Valtioneuvoston oikeuskaslerista säädetään valtioneuvoston oikeuskanslerista annetussa laissa (193/2000). Kuten eduskunnan oikeusasiamiehenkin kohdalla, oikeuskanslerin keskeisimpiä toimintamuotoja on kantelujen tutkiminen, omat aloitteet ja tarkastustoiminta.

Ylimpien laillisuusvalvojien toiminnassa korostuu erityisesti perus- ja ihmisoikeuksien toteutumisen valvonta. Laillisuusvalvonnassa kiinnitetään huomiota yhä enenevässä määrin muodollisen lainmukaisuuden valvonnan lisäksi lain soveltamisen tosiasiallisiin vaikutuksiin. Lisäksi eduskunnan oikeusasiamiehen valvonnassa korostuu Puolustusvoimien osalta salaisten pakkokeinojen ja salaisen tiedonhankinnan valvonta. Ylimmillä laillisuusvalvojilla on rajoittamaton oikeus saada valvontaansa varten tarvitsemansa tiedot viranomaiselta.

Ylimmät laillisuusvalvojat ovat suosittaneet Euroopan ihmisoikeussopimuksen, Euroopan ihmisoikeustuomioistuimen, Suomen perustuslain ja korkeimman oikeuden ratkaisukäytännön perusteella maksettavaksi hyvityksiä virheellisestä viranomaistoiminnasta.

Ylimpien laillisuusvalvojien toiminta luo osaltaan uskottavuutta Puolustusvoimien toiminnan lainmukaisuuteen. Ulkoinen laillisuusvalvonta puuttuu mm. selkeisiin virheisiin ja kestämättömiin käytäntöihin. Ulkopuolinen laillisuusvalvoja arvioi tutkittavakseen saatettuja ja tutkittavakseen ottamiaan asioita yleisestä näkökulmasta.

Kansalliset tuomioistuimet

Puolustusvoimat tekee hallintopäätöksiä useissa eri asiaryhmissä. Puolustusvoimien tekemään päätökseen voidaan pääsääntöisesti hakea muutosta siten kuin hallintolainkäyttölaissa (586/1996) säädetään. Näin hallintotuomioistuimetkin omalta osaltaan osallistuvat tosiasiallisesti Puolustusvoimien valvontaan. Kun hallintotuomioistuin varmistaa yksilön oikeusturvaa suhteessa hallintoviranomaisiin, se toimii samalla hallinnon lainmukaisuuden valvojana yksittäisessä tapauksessa. Puolustusvoimien osalta hallintolainkäytön piiriin kuuluvana asiaryhminä voidaan mainita asiakirjajulkisuuskysymykset.

Yleisillä tuomioistuimilla on myös päätöksentekovaltaa eräissä sotilaskurinpidosta ja rikostentorjunnasta puolustusvoimista annetun lain 89 §:n 1 momentissa tarkoitettujen toimivaltuuksien osalta. Näin yleiset tuomioistuimet osallistuvat yksittäistapauksissa Puolustusvoimien toimenpiteiden laillisuuden valvontaan.

Eurooppa-tuomioistuimet

Euroopan ihmisoikeustuomioistuin valvoo Euroopan ihmisoikeussopimuksen noudattamista. Euroopan ihmisoikeustuomioistuimen voidaan katsoa myös osallistuvan viranomaisten toiminnan laillisuuden valvontaan valituksia ratkaistessaan. Poliisiin kohdistuneet valitukset ovat olleet varsin suuri asiaryhmä tuomioistuimessa. Euroopan ihmisoikeustuomioistuin on antanut viime vuosikymmeninä myös lukuisia turvallisuuspoliisia, turvallisuuspalveluja ja tiedustelupalveluja koskevia ratkaisuja sekä myös salaisia pakkokeinoja ja salaista tiedonhankintaa koskevia ratkaisuja. Ratkaisuissa on tulkittu erityisesti Euroopan ihmisoikeussopimuksen yksityiselämän suojaa koskevaa 8 artiklaa ja tehokkaita oikeussuojakeinoja koskevaa 13 artiklaa. Euroopan ihmisoikeussopimuksen tulkinnalla on tärkeä merkitys tiedustelutoiminnan laillisuuden ja riittävien oikeussuojatakeiden arvioinnin kannalta. Kysymys on myös Euroopan ihmisoikeustuomioistuimen asettamista vähimmäisvaatimuksista kansalliselle lainsäädännölle.

Euroopan unionin tuomioistuin tulkitsee EU-lainsäädäntöä ja varmistaa, että sitä sovelletaan samalla tavalla kaikissa EU-maissa. Se myös ratkaisee EU-maiden ja EU-toimielinten välisiä riitaasioita. Euroopan unionin tuomioistuimen rooli tiedustelutoiminnan valvonnassa on ollut Euroopan unionista tehdyn sopimuksen (SEUT) 4 (2) artiklasta johtuen vielä etäisempi tai välillisempi kuin Euroopan ihmisoikeustuomioistuimen, mutta eräillä Euroopan unionin tuomioistuimen ennakkoratkaisuilla ja EU-lainsäädännön kumoamiskanteilla on merkitystä myös tiedustelutoiminnalle ja erityisesti tiedustelua koskevan lainsäädännön kehittämiselle.

Tietosuojavaltuutetun suorittama valvonta

Tietosuojavaltuutetun tehtävistä säädetään tietosuojalautakunnasta ja tietosuojavaltuutetusta annetussa laissa (389/1994). Lain 5 §:n mukaan tietosuojavaltuutetun tehtävänä on käsitellä ja ratkaista henkilötietojen ja luottotietojen käsittelyä koskevat asiat siten kuin henkilötietolaissa (523/1999) ja luottotietolaissa (527/2007) säädetään sekä hoitaa muut mainituista laeista johtuvat tehtävät. Valtuutetun kuuluu myös seurata näiden tietojen käsittelyn yleistä kehitystä ja tehdä tarpeelliseksi katsomiaan aloitteita. Lisäksi valtuutetun tulee huolehtia toimialaansa kuuluvasta tiedotustoiminnasta sekä henkilötietojen käsittelyyn liittyvästä kansainvälisestä yhteistyöstä. Käytännössä tietosuojavaltuutettu antaa yleistä ohjausta ja neuvontaa sekä toimii yhteistyössä eri sidosryhmien kanssa, antaa ratkaisuja, valvoo ja tekee tarkastuksia, on kuultavana ja antaa lausuntoja, tiedottaa sekä tekee kansainvälistä yhteistyötä. Puolustusvoimien tietojärjestelmät ovat suurelta osin niin sanotun välillisen tarkastusoikeuden piirissä (Laki henkilötietojen käsittelystä poliisitoimessa 761/2003 45 §:n 2 momentti). Tietosuojavaltuutettu on tehnyt Puolustusvoimien vuosittain yhdestä kymmeneen tarkastusta pääasiassa tarkastuspyyntöjen perusteella. Yhdellä käynnillä on tarkastettu useita tarkastuspyynnön tehneiden henkilöiden henkilötietojen käsittelyä.

2.2.8 Tietoturvauhkien torjunta

Viestintäviraston Kyberturvallisuuskeskus on kansallinen tietoturvaviranomainen, joka muun muassa ennaltaehkäisee, kerää ja selvittää yleisiin viestintäverkkoihin liittyviä ja niiden kautta suomalaisiin tahoihin suuntautuvia tietoturvaloukkauksia sekä tiedottaa merkittävistä tietoturvauhkista. Kyberturvallisuusstrategian mukaan kyberturvallisuuskeskuksen tehtävänä on myös yhdistetyt kyberturvallisuuden tilannekuvan tuottaminen ja ylläpitäminen. Kyberturvallisuuskeskus kerää tietoja tietoverkkotapahtumista ja välittää sitä eri toimijoille sekä muodostaa ja jakaa kyberturvallisuuden yhdistettyä tilannekuvaa. Kyberturvallisuuskeskuksen asiakkaat voivat hyödyntää tilannekuvatietoa oman varautumisensa järjestämisessä ja priorisoinnissa.

Tilannekuvan muodostamisessa hyödynnetään kansallisten lähteiden lisäksi kyberturvallisuuskeskuksen vapaaehtoisuuteen ja molemminpuoliseen luottamukseen perustuvaa kansainvälistä yhteistyöverkostoa. Yhteistyöverkostoon kuuluvien GovCERT-ryhmien emo-organisaatiot ovat sijoittuneet omissa maissaan valtionhallinnon eri toiminteisiin. Esimerkiksi Ruotsin CERT-SE on osa siviilivalmiusvirastoa, kun taas Saksan CERT-BUND toimii sisäministeriön hallinnonalalla. Joissain valtioissa CERT-ryhmät on sijoitettu puolustusministeriön hallinnonalalle ja joissain CERT-ryhmät toimivat puolestaan osana tiedusteluviranomaista (Government Communications Headquarters, GCHQ).

Toimintaoikeuksista tietoturvasta huolehtimiseksi säädetään tietoyhteiskuntakaaren 272 §:ssä. Säännös antaa yrityksille, yhteisöille ja viranomaisille työkaluja niihin kohdistuvien kybertekojen havaitsemiseksi ja torjumiseksi. Havainnointitoimenpiteet suoritetaan hajautetusti, jolloin niiden laatu ja taso vaihtelevat organisaatiokohtaisesti. Tietoyhteiskuntakaaren 272 § sekä sen edeltäjä SVTSL 20 § ovat mahdollistaneet myös tietoturvauhkien keskitetyn havainnointijärjestelmän (HAVARO) kehittämisen yhteiskunnan kokonaisturvallisuuden kannalta merkittävimpien tahojen suojaksi.

HAVARO on viestintäviraston kyberturvallisuuskeskuksen huoltovarmuuskriittisille yrityksille ja valtionhallinnon toimijoille tarjoama tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä. Toiminta perustuu tietoyhteiskuntakaaren 272 §:ään. HAVAROn tarkoituksena on tunnistaa erilaisten tunnisteiden avulla haitallista verkkoliikennettä ja tietoturvaa vaarantavia kehittyneitä verkkohyökkäyksiä (Advanced Persisten Threat, yleisesti APT). Järjestelmän toisena tarkoituksena on tukea paremman tilannekuvan muodostamista suomalaisiin tietoverkkoihin kohdistuvista tietoturvauhkista. Järjestelmässä hyödynnettävät tekniset haittaohjelmatunnisteet perustuvat pääosin kyberturvallisuuskeskuksen kotimaisilta ja ulkomaisilta yhteistyökumppaneilta saamiin tietoihin.

Viestinnän sisällön automaattinen analysointi kohdistuu kaikkien niiden viestien sisältöön, jotka tulevat sisään tai lähtevät ulos automaattista analysointia käyttävän tahon tietoverkosta tai -järjestelmästä. Analysoinnin pääasiallisena tarkoituksena on havaita haittaohjelmien yrityksiä tunkeutua tietojärjestelmään sekä järjestelmään mahdollisesti jo tunkeutuneiden haittaohjelmien viestintää isäntiensä kanssa.

Haitalliset ohjelmat ja käskyt tunnistetaan ensi vaiheessa automaattisessa sisällöllisessä analysoinnissa ennalta tehtyjen määrittelyiden perusteella, eikä viestin sisältö tällöin tule luonnollisen henkilön tietoon. Jos on ilmeistä, että automaattisessa suodatuksessa esiin noussut viesti sisältää haittaohjelman eikä tietoturvaa voida varmistaa automaattisin keinoin, sallii tietoyhteiskuntakaaren 272 § sen, että yritys, yhteisö tai viranomainen ottaa viestin sisällön manuaaliseen käsittelyyn.

Suomi on tietoyhteiskuntana ja kansainvälisiin markkinoihin nojaavana taloutena riippuvainen tietoinfrastruktuurin häiriöttömästä toiminnasta. Viestintäverkkojen ja -palvelujen toimivuus ja luotettavuus ovat tärkeitä edellytyksiä Suomen talouden kasvulle, kilpailukyvylle, innovaatioille ja hyvinvoinnille kaikilla yhteiskunnan toimialoilla.

Tietoinfrastruktuurin toimintavarmuus on tärkeää myös yhteiskunnan kokonaisturvallisuuden kannalta. Yhteiskunnan tietoteknistyminen, tietoliikenneinfrastruktuurin ulkomaisen omistuksen kasvu sekä valtionhallinnon tietoteknisten toimintojen ulkoistaminen asettavat uudenlaisia vaatimuksia yhteiskunnan elintärkeiden toimintojen turvaamiseksi. Yhteiskunnan elintärkeillä toiminnoilla tarkoitetaan poikkihallinnollisia, yhteiskunnalle välttämättömiä toimintokokonaisuuksia, joiden on oltava turvattuina kaikissa tilanteissa. Tietoteknisten järjestelmien toimimattomuus, informaatioinfrastruktuurin luhistuminen ja erilaiset tietoturvauhat vaikuttavat kielteisesti julkisiin palveluihin, liikeelämään sekä hallintoon ja siten koko yhteiskunnan toimintaan. Valtaosa Suomen kriittisestä tietoliikenneinfrastruktuurista ja sen palveluista on yksityisen sektorin omistamaa ja tuottamaa, mistä johtuen sen merkitys yhteiskunnan elintärkeiden toimintojen turvaamisessa on tärkeä.

Sähköisen viestinnän sekä tietoverkkojen ja -järjestelmien toimintaa ja häiriöttömyyttä suojataan tietoturvan avulla. Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla (luottamuksellisuus), ettei tietoja voida muuttaa muiden kuin siihen oikeutettujen toimesta (eheys) ja että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä (käytettävyys).

Sähköisten viestintäverkkojen ja -palveluiden käyttäjinä olevat tahot huolehtivat tietoturvastaan eri menetelmillä. Tietoturvaa voidaan ylläpitää esimerkiksi tietohallinnollisin keinoin ja asettamalla viestintäverkon tai palvelun käytölle teknisiä rajoituksia. Valtionhallinnon yhtenäinen luonne mahdollistaa sen, että hallinnon tietoturvaa voidaan ohjata keskitetysti ja yhdenmukaisten periaatteiden nojalla. Valtiovarainministeriö ohjaa ja johtaa julkisen hallinnon tietoturvallisuuden yleistä kehittämistä ja valtionhallinnon tietoturvallisuutta sekä ICT-varautumista. Valtiovarainministeriön ohjaava tehtävä perustuu muun muassa julkisen hallinnon tietohallinnon ohjauksesta annettuun lakiin (634/2011) ja valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä annettuun lakiin (1226/2013).

Julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain (10/2015) tarkoituksena on normaalioloissa ja niiden häiriötilanteissa sekä poikkeusoloissa varmistaa valtion ylimmän johdon ja yhteiskunnan turvallisuuden kannalta tärkeiden viranomaisten ja muiden toimijoiden yhteistoiminnan edellyttämän viestinnän häiriöttömyys ja jatkuvuus sekä turvata päätöksenteossa ja johtamisessa tarvittava tiedon käytettävyys, eheys ja luottamuksellisuus. Laissa säädetään turvallisuusverkosta (TUVE), joka yhdistää samaan tietoliikenneverkkoon valtion johdon, ministeriöt, Puolustusvoimat, rajavartioston, poliisin ja pelastustoimien.

Julkisen hallinnon turvallisuusverkon tarjoaa kaikille sen käyttäjille ja heidän keskeisille palvelun-tuottajilleen vakaa tieto- ja viestintäteknisen palveluympäristö. Turvallisuusverkon tietoliikenne- ja tietoturvaratkaisut mahdollistavat eri suojaustasojen sekä käyttäjien yhteisten tai erillisten tietojenkäsittely-ympäristöjen toteuttamisen. Näin tavoitteena on saavuttaa kustannustehokkaasti viranomaisille yhteinen ja yhteen toimiva koko maan kattava tietoverkko, joka toimii luotettavasti myös poikkeusoloissa ja muun muassa luonnonilmiöiden, sähkökatkosten tai jatkuvasti lisääntyvien tietoverkkohyökkäysten sattuessa. Valtiovarainministeriö päättää normaalioloissa ja niihin liittyvissä häiriötilanteissa turvallisuusverkon palvelutuotannon ja käytön ensisijaisuus-, kiireellisyys- ja muusta tärkeysmäärittelystä.

Valtiovarainministeriö käynnisti vuonna 2013 myös valtion ympärivuorokautisen tietoturvatoiminnan kehittämishankkeen (SecICT). Hankkeen tehtävänä on suunnitella ja perustaa viranomaistoiminto laajojen sekä vakavien tietoturvahäiriötilanteiden ennaltaehkäisyyn ja koordinointiin. Hankkeessa laajennetaan ja kehitetään valtionhallinnon tietoturvallisuutta parantavia palveluita. Lisäksi hankkeessa käynnistetään häiriönratkaisuryhmien toiminta (VIRT-toiminta) sekä operatiivisten ja häiriönhallintaa tukevien palveluiden kehittäminen (GovSOC-palvelut). Kehittäminen tapahtui yhteistyössä valtion ja yksityisen sektorin tieto- ja kyberturvallisuuden toimijoiden sekä pilottiorganisaati-

oiden kanssa. Hankkeen oli määrä päättyä vuoden 2016 ja tulokset on tarkoitus siirtää tämän jälkeen vaiheittain jatkuvaksi toiminnaksi.

Yksityisellä sektorilla keskitetty tietoturvaohjaus ei ole mahdollista, vaan tietoturvan taso ja tietoturvan ylläpitämiseksi valitut ratkaisut vaihtelevat jokaisen organisaation omien tarpeiden ja painotusten mukaan. Tietoturvauhkien havaitseminen ja niiltä suojautuminen perustuu niin hallinnossa kuin yksityiselläkin sektorilla käytännössä kaupallisiin tietoturvaohjelmiin ja -palveluihin. Osa valtionhallintoa ja huoltovarmuus-kriittisistä yrityksistä hyödyntää suojautumisessaan myös HAVARO:a.

2.3 Kansainvälinen kehitys ja ulkomaiden lainsäädäntö

2.3.1 Kansainväliset ihmisoikeussopimukset

2.3.1.1 Kansalaisoikeuksia ja poliittisia oikeuksia koskeva Yhdistyneiden Kansakuntien yleissopimus

YK:n yleiskokouksen vuonna 1966 hyväksymä kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus (ns. KP-sopimus; SopS 8/1976) tuli Suomessa voimaan vuonna 1976.

Yksityisyyden ja luottamuksellisen viestinnän suojan kannalta keskeinen on sopimuksen 17 artikla, jonka mukaan kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon ei saa mielivaltaisesti tai laittomasti puuttua eikä suorittaa hänen kunniaansa ja mainettaan loukkaavia hyökkäyksiä. Lisäksi jokaisella on oikeus lain suojaan tällaista puuttumista tai tällaisia hyökkäyksiä vastaan. Artiklan mukaisesta velvoitteesta voidaan poiketa ainoastaan yleisen hätätilan aikana, joka uhkaa kansallista olemassaoloa ja joka on virallisesti sellaiseksi julistettu.

KP-sopimuksen 17 artiklan määräämä kielto puuttua yksityiselämään ja kirjeenvaihtoon ei ole ehdoton, vaan kielto koskee ”mielivaltaista” ja ”laitonta” oikeuksiin puuttumista. Sopimusvaltiot voivat kansallisessa lainsäädännössään säätää puuttumisen oikeuttavista tilanteista ja puuttumisessa käytettävistä keinoista. Kaikki sopimusvaltiot ovatkin säätäneet rikostorjuntatarkoituksessa tapahtuvasta oikeuksiin puuttumisesta ja monet myös kansallisen turvallisuuden ylläpitämisen tarkoituksessa tapahtuvasta oikeuksiin puuttumisesta.

KP-sopimuksen täytäntöönpanoa valvoo YK:n ihmisoikeuskomitea, joka jatkuvasti kehittää sopimusmääräysten tulkintaa. Ihmisoikeuskomitean yleiskommentissa nro 16 vuodelta 1988 (A/43/20) tulkitaan 17 artiklan sisältöä muun muassa sähköisen viestinnän näkökulmasta. Kommentin mukaan riittävää ei ole, että yksityiselämän suojaan puuttumisesta on säädetty lailla. Puuttumisen oikeuttava lainsäädäntö ei saa olla sisällöltään mielivaltainen eikä sen soveltaminen mielivaltaista. Lainsäädännön on oltava KP-sopimuksen määräysten ja tavoitteiden mukainen, ja siinä on tarkoin yksilöitävä olosuhteet, joissa puuttuminen on sallittu. Yksityisyyden suojaan puuttuvaa toimenpidettä koskeva päätös tulee voida tehdä ainoastaan tapauskohtaisesti ja laissa määrätyn viranomaisen toimesta, ja niiden tietojen, joita puuttumisen avulla kerätään, on oltava yhteiskunnan etujen kannalta välttämättömiä (”essential in the interests of society”). Henkilön yksityiselämään liittyviä tietoja ei saa käyttää KP-sopimuksen kanssa ristiriidassa oleviin tarkoituksiin.

Yksityisyyden suojaa koskevan 17 artiklan loukkauksista on tehty useita valituksia KP-sopimuksen valinnaisen pöytäkirjan nojalla, mutta komitea ei toistaiseksi ole käsitellyt tietoverkkoturvallisuuteen ja sähköiseen viestintään liittyviä asioita. Todennäköisenä voidaan pitää, että sähköisen viestinnän luottamuksellisuuteen liittyvät kysymykset nousevat näkyvämmin esille ihmisoikeuskomitean työssä.

2.3.1.2 Euroopan ihmisoikeussopimus

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

Yksityiselämän suoja (EIS 8 artikla)

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

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

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

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

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

erikseen lueteltujen etujen turvaksi ja 3) puuttumisen on oltava demokraattisessa yhteiskunnassa välttämätön. Yksi yksityiselämän ja siten myös luottamuksellisen viestinnän suojaan puuttumisen mahdollistavista eduista on kansallinen turvallisuus.

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

EIT on ratkaisuissaan toistuvasti korostanut sitä, että yksityiselämän suojaan puuttuvan, salaiset viranomaistoimenpiteet mahdollistavan lain on oltava oikeusvaltioperiaatteiden mukainen, kansalaisten saatavilla sekä laadultaan sellainen, että kansalaiset kykenevät ennakoimaan sen soveltamisen seuraukset omalta osaltaan (mm. Kruslin v. Ranska, Huvig v. Ranska, Lambert v. Ranska). Sen on oltava tarpeeksi selkeä [”sufficiently clear in its term”] antaakseen riittävän osoituksen [”an adequate indication”] siitä, missä olosuhteissa ja millä edellytyksillä kansalaiset voivat joutua salaisten viranomaistoimenpiteiden kohteeksi (Kopp v. Saksa, Kruslin v. Ranska, Huvig v. Ranska). Laki ei voi olla sellainen, että se mahdollistaa salaisen tarkkailun kohdistamisen sattumanvaraisesti keneen tahansa (Amann v. Sveitsi).

Arvioitaessa sitä, täyttyykö ennakoitavuusvaatimus, on huomioon otettava kansanedustuslaitoksen säätämän varsinaisen lain ohella myös asetukset ja viranomaismääräykset. Varsinaisen lain hyvinkin yleistasoisia säännöksiä voidaan täsmentää alemmantasoisin instrumentein. Näiden tulee kuitenkin olla julkistettuja - sellaiset sisäiset viranomaismääräykset, jotka eivät ole kansalaisten saatavilla, eivät täytä ennakoitavuusvaatimusta (mm. Silver ja muut v. Yhdistynyt Kuningaskunta, Malone v. Yhdistynyt Kuningaskunta). Yleisesti saatavilla olevan lain tulee määritellä ainakin salaisesti käytettävien tarkkailuvaltuuksien laatu ja laajuus; niiden henkilöiden kategoriat, joita vastaan valtuuksia voidaan käyttää; sen toiminnan luonne, joka antaa aiheen valtuuksien käyttöön; valtuuksien avulla hankittuja tietoja tutkittaessa, hyödynnettäessä, tallennettaessa, edelleen jaettaessa ja poistettaessa noudatettavat menettelyt; säännökset valtuuksien valvonnasta ja niitä koskevista oikeussuojakeinoista (Amann v. Sveitsi, Valenzuela Contreras v. Espanja, Prado Bugallo v. Espanja, Shimovolos v. Venäjä). Lainsäädännön ennakoitavuudelle asetettavat vaatimukset ovat siitä riippumattomia, onko kyse yksittäisten henkilöiden viestiyhteyksiä koskevasta rikosperusteisesta tarkkailusta vai laajamittaisesta viestiyhteyksien uhkaperusteisesta yleisvalvonnasta (Weber ja Saravia v. Saksa, Liberty ja muut v. Yhdistynyt Kuningaskunta).

EIT on arvioinut kansainvälisten viestiyhteyksien laajamittaisen yleisvalvonnan ihmisoikeussopimuksen mukaisuutta kahdessa tärkeässä ratkaisussaan. Tapauksessa Liberty ja muut v. Yhdistynyt Kuningaskunta se katsoi yleisvalvonnan mahdollistavan kansallisen lainsäädännön olevan laadultaan sellainen, ettei se täyttänyt EIS 8(2) artiklassa asetettua vaatimusta salaisen tarkkailun perustumisesta lakiin. Tapauksessa Weber ja Saravia v. Saksa se päätyi päinvastaiseen tulokseen - kansallinen lainsäädäntö täytti lain laadulle asetettavat vaatimukset ja oli siten ihmisoikeussopimuksen mukainen.

Tapauksessa Liberty ja muut v. Yhdistynyt Kuningaskunta kyse oli Iso-Britannian puolustusministeriön alaisen signaalitiedustelulaitoksen suorittamasta laajamittaisesta ulkomaan puhelinliikenteen valvonnasta, jonka puitteissa pystyttiin kuuntelemaan samanaikaisesti jopa 10 000 puhelinlinjaa. Asiassa oli sinänsä riidatonta, että toiminta perustui kansalliseen lakiin. Kyseisen lain mukaan sisäministeri saattoi antaa eri turvallisuusviranomaisille luvan [”warrant”] kohdistaa tiedonhankintaa Iso-Britannian ja ulkomaiden välisiin viestiyhteyksiin. Luvissa ne viestiyhteydet, joihin tiedonhankintaa voitiin kohdistaa, määriteltiin hyvin yleisellä tasolla (esimerkiksi ”kaikki Iso-Britannian ja muun Euroopan välisten merikaapelien kautta välittyvät viestit”). Luvan myöntämisen yhteydessä sisämi-

nisterin oli määriteltävä se aineisto, jota tiedonhankinta koski. Lain mukaan määrittelyksi kuitenkin riitti se, että hankittavat tiedot sisäministerin käsityksen mukaan olivat tarpeen joko kansallisen turvallisuuden ylläpitämisen, vakavan rikollisuuden ennalta estämisen tai paljastamisen taikka maan taloudellisten etujen turvaamisen kannalta. Luvan myöntäessään sisäministerin tuli myös antaa tarpeellisina pitämänsä salassa pidettävät määräykset sen varmistamiseksi, että luvan alaan kuulumattomia viestejä ei tarkastettu ja että tarkastettavia viestejä paljastettiin tai jäljennettiin vain tarpeellisessa laajuudessa. Laissa ei ollut tarkempia säännöksiä näiden määräysten sisällöstä tai alasta. Luvan sisäministeriltä saatuaan turvallisuusviranomaiset muotoilivat itsenäisesti ne automaattiset hakuehdot, joiden avulla kansallista turvallisuutta tai muita laissa mainittuja intressejä koskevat tiedot suodatettiin viestinnän kokonaismassasta. Turvallisuusviranomaisilla oli omat sisäiset määräyksensä siitä, millä perusteilla suodatuksen tuloksena saatuja tietoja käsiteltiin, tallennettiin, jaettiin ja poistettiin, mutta nämä määräykset eivät olleet julkisia tai yleisesti saatavilla.

Asiassa antamassaan ratkaisussa EIT totesi, että sisäministerin lupapäätöksen alaan voitiin lain mukaan sisällyttää millainen viesti tahansa, minkä johdosta kenen tahansa henkilön maan ulkopuolelle lähettämä tai sieltä saama mikä tahansa viesti oli voitu siepata. Niin ollen toimeenpanovallalle oli ulkomaisten viestien sieppaamisen osalta myönnetty tosiasiassa rajoittamatonta harkintavaltaa. Laki myös jätti väljän harkintamarginaalin sen suhteen, mitkä viestit tosiasiassa tarkastettiin. Riittävää tässä suhteessa oli, että sisäministeri piti tarkastamista tarpeellisena kansallisen turvallisuuden tai muiden laissa mainittujen yleisesti muotoiltujen etujen kannalta. Laissa ei ollut tarkempia säännöksiä luvan alaan kuulumattomien viestien käsittelystä eivätkä sisäministerin asiasta antamat määräykset olleet julkisia. Yhteenvetona EIT totesi, että kansallisella lailla ei ollut osoitettu riittävän selkeästi toimeenpanovallalle viestien sieppaamista ja tarkastamista varten myönnetyn hyvin väljän harkintavallan rajoja. Varsinkaan ei ollut osoitettu julkisesti, miten siepatun aineiston seulonta, käyttö, säilytys ja hävittäminen oli toimitettava. Näin ollen Iso-Britannian signaalitiedustelulainsäädäntö ei vastannut EIS 8(2) artiklan asettamia laatuvaatimuksia ja ihmisoikeussopimusta oli rikottu.

Tapauksessa Weber ja Saravia v. Saksa kyse oli Saksan tiedustelupalvelu BND:n harjoittamasta Saksan ja ulkomaiden välisen matkapuhelinliikenteen laajamittaisesta niin sanotusta strategisesta valvonnasta, josta oli säädetty kansallisessa laissa. Kyseisen lain mukaan matkapuhelinliikenteen strategista valvontaa saatiin harjoittaa eräiden kansalliseen turvallisuuteen kohdistuvien erikseen mainittujen uhkien torjumiseksi. Tällaisia laissa määriteltyjä uhkia olivat Saksaan kohdistuva sotilaallinen hyökkäys, Saksassa toteutettavat luonteeltaan kansainväliset terroriteot, kansainvälinen aseiden salakuljetus, huumeiden laajamittainen maahantuonti, ulkomailla tapahtuva rahan väärentäminen ja edellä mainittuihin ilmiöihin liittyvä rahanpesu. Luvan kunkin strategisen valvontatehtävän suorittamiseen myönsi liittovaltion ministeri kuultuaan lupahakemuksen johdosta ensin parlamentaarista valvontaelintä. Niiden automaattisten hakuehtojen, joiden avulla matkapuhelinliikennettä oli tarkoitus suodattaa, oli käytävä ilmi sekä BND:n lupahakemuksesta että ministerin myöntämästä luvasta. Laki sisälsi säännökset siitä, kuinka suodatettua aineistoa oli käsiteltävä ja missä tapauksissa suodatuksen myötä esiinnousseita henkilöitä koskevia tietoja saatiin käyttää rikosten ennalta estämistä, paljastamista ja selvittämistä varten. Laki sisälsi samoin säännökset siitä, milloin suodatettua tietoa oli pidettävä asiaankuulumattomana ja miten asiaankuulumattoman tiedon suhteen oli meneteltävä. Edelleen laissa säädettiin valvontalupien voimassaoloajoista, suodatettujen tietojen säilyttämisajoista, tietojen hävittämisestä sekä niistä perusteista ja edellytyksistä, joilla tietoja voitiin luovuttaa muille viranomaisille.

EIT katsoi, että Saksan lainsäädäntö täytti EIS 8 artiklan nojalla laille asetettavat laatu- ja ennakoitavuusvaatimukset. Keskeistä tässä suhteessa oli muun muassa se, että laki määritteli ne uhat, joiden torjumiseksi valvontaa voitiin harjoittaa. Lain katsottiin myös tarjoavan riittävän osoituksen siitä, mihin henkilöluokkiin valvonta voitiin lainmukaisesti kohdistaa. Valvonnan kohdentamiseksi käytettävien automaattisten hakuehtojen tuli suoraan lain nojalla ilmetä valvontaa varten myönnettävistä luvista, jolloin valvontaa harjoittavalla viranomaisella ei ollut rajoittamatonta harkintavaltaa

niiden määrittelemisessä. Ennakoitavuusvaatimuksen täyttymisen kannalta merkityksellistä oli myös se, että laki määritteli lupien maksimaaliset voimassaoloajat ja sisälsi säännökset niistä menettelyistä, joita oli noudatettava tietoja tarkastettaessa ja hyödynnettäessä. Samoin merkitystä EIT:n mukaan oli sillä, että laki sääti niistä rajoituksista ja ehdoista, joita tietojen edelleen luovuttamisessa oli noudatettava, sekä niistä olosuhteista, joissa tiedot oli hävitettävä. Weber ja Saravia -tapauksen johdosta antamassaan ratkaisussa EIT totesi erikseen myös sen, ettei Saksan maaperällä harjoitettava viestiyhteyksien yleisvalvonta lähtökohtaisesti voi loukata muiden maiden valtiosuvereniteettia vaikka viestiyhteyksien toinen osapuoli jossain tällaisessa muussa maassa oleskelisikin.

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

Kolmas ehto sille, että viranomaiset saavat puuttua EIS 8 artiklan takaamien oikeuksien käyttöön on se, että puuttuminen on välttämätöntä demokraattisessa yhteiskunnassa demokraattisten instituutioiden suojaamiseksi ja saatavan elintärkeän tiedon ehdottoman välttämätöntä tiedusteluoperaation kannalta. Salaiseen tiedonhankintaan pitää olla aina korkea kynnys. Järjestelmät pitää rakentaa siten, että niitä käytetään säästeliäästi ja ainoastaan erittäin perustelluissa tapauksissa. Mallit, joissa viranomaisille jätetään liikaa harkintavaltaa, ovat Euroopan ihmisoikeustuomioistuimen mielestä aina alttiita väärinkäytöksille eivätkä ole siten yhteensopivia Euroopan ihmisoikeussopimuksen asettamien vaatimusten kanssa *(Szabó ja Vissy v. Unkari).*

Välttämätön demokraattisessa yhteiskunnassa -edellytys pitää sisällään sen, että oikeuksiin puuttumisen tulee vastata pakottavaan yhteiskunnalliseen tarpeeseen [”correspond to a pressing social need”]. Edellytyksestä seuraa myös, että puuttumisen on oltava suhteellisuusperiaatteen mukaista: Puuttumisen on oltava järkevässä suhteessa siihen EIS 8(2) artiklan sallimaan tavoitteeseen, johon vedotaan oikeuttamisperusteena (mm. Gillow v. Yhdistynyt Kuningaskunta, Silver ja muut v. Yhdistynyt Kuningaskunta, Handyside v. Yhdistynyt Kuningaskunta).

Puuttumisen välttämättömyyden arviointi niin yhteiskunnallisen tarpeen pakottavuuden kuin suhteellisuudenkin näkökulmasta kuuluu ensisijaisesti tai ainakin ensi vaiheessa kansalliselle lainsäätäjälle ja kansallisille viranomaisille (Silver ja muut v. Yhdistynyt Kuningaskunta, Handyside v. Yhdistynyt Kuningaskunta). Tätä arviointia suorittaessaan kansallisilla tahoilla on tiettyä harkintamarginaalia, jonka laajuutta määrittää muun muassa se, mitä EIS:n takaamaa oikeutta puuttuminen koskee, se, kuinka syvällekäyvästä puuttumisesta on kyse, sekä se, mikä EIS 8(2) artiklan sallima tavoite on puuttumisen oikeuttamisperusteena. Harkintamarginaali on tavanomaista väljempi silloin, kun oikeuttamisperusteena on kansallinen turvallisuus (Klass ja muut v. Saksa, Leander v. Ruotsi). Kansallisen turvallisuuden kysymyksissä valtion melko laaja harkintavalta koskee myös niitä konkreettisia keinoja ja menetelmiä, joiden avulla se kyseistä etua suojaa. Ratkaisussaan Weber ja Saravia v. Saksa EIT katsoi, että valtio sille kuuluvan harkintavallan puitteissa oli voinut

säätää laajamittaisesta viestintäyhteyksien valvonnasta menetelmänä suojata kansallista turvallisuuttaan. Kyse oli demokraattisessa yhteiskunnassa välttämättömästä puuttumisesta EIS 8 artiklan yksityisille oikeussubjekteille takaamiin oikeuksiin.

EIT on lisäksi kiinnittänyt huomiota salaisiin tiedonhankintakeinoihin kohdistuviin valvontajärjestelmiin. Erityisesti valvonnan tehokkuus ja valvontaelimen riippumattomuus ovat nousseet tärkeiksi vaatimuksiksi. Valvonnan tehokkuuteen kytkeytyvät kysymykset valvontaviranomaisen tiedonsaantioikeudesta ja toimivaltuuksien käytöstä niiden kohteelle ilmoittamisesta jälkikäteen. EIT:n asettamia riippumattomuutta koskevia vaatimuksia ei ole täyttänyt esimerkiksi järjestelmä, jossa valvojalla on läheinen suhde toimeenpanovaltaan. Myös liian läheiset poliittiset kytkökset ovat merkkinä siitä, että valvontajärjestelmä ei ole riittävän riippumaton. Vaikka EIT korostaa, ettei valvonnan tarvitse tapahtua tuomioistuinten toimesta, toimielinten jäsenten ammatilliseen pätevyyteen on kiinnitetty huomiota ja toisaalta argumentoinnissa on huomioitu tehtävään valittujen ammatillinen tausta. EIT on suhtautunut myönteisesti valvontamalleihin, joissa tehtävään valituilta edellytetään toimimista korkeissa tuomarin tehtävissä. *(Szabó ja Vissy, Dumitru Popescu v. Romania nro 2).*

Laillisuusvalvontaa suorittavien tahojen ratkaisuilla tulisi olla oikeudellisesti sitova vaikutus suhteessa valvottuihin tahoihin. Demokratian suojelemisen kannalta riittävää ei ole, että laillisuusvalvojat voivat ohjata valvomiaan tahoja suositusten avulla (Segerstedt-Wiberg ja muut v. Ruotsi). Salaisia valtuuksia koskevan oikeudellisen sääntelyn tulee olla julkista ja siinä määrin täsmällistä, että laillisuusvalvontaa voidaan uskottavasti suorittaa (Liberty ja muut v. Yhdistynyt Kuningaskunta), kuitenkaan salaisen tiedonhankinnan tarkoitusta vaarantamatta (Segerstedt-Wiberg ja muut v. Ruotsi). Demokratian suojelemisen kannalta merkitystä on myös sillä, että kansanedustuslaitos osaltaan osallistuu salaisten tarkkailuvaltuuksien valvontaan (Campbell v. Yhdistynyt Kuningaskunta, Leander v. Ruotsi).

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

Oikeus tehokkaaseen oikeussuojakeinoon (EIS 13 artikla)

EIS 13 artiklan mukaan jokaisella, jonka EIS:n yleissopimuksessa tunnustettuja oikeuksia ja vapauksia on loukattu, on oltava käytettävissään tehokas oikeussuojakeino (”effective remedy”) kansallisen viranomaisen edessä siinäkin tapauksessa, että oikeuksien ja vapauksien loukkauksen ovat tehneet virantoimituksessa olevat henkilöt.

EIS:n 13 artikla eroaa luonteeltaan edellä kuvatusta 8 artiklasta, sillä artiklalla 13 tulee aina olla kytkentä EIS:n muihin oikeuksiin ja vapauksiin. 8 artikla koskee itsenäistä oikeutta, kun taas 13 artiklaa tarkastellaan vain suhteessa jonkin toisen oikeuden määrittelevään sopimusmääräykseen. 13 artikla täydentää sopimuksessa turvattuja materiaalisia ihmisoikeuksia määritteleviä sopimusartikloita edellyttämällä tehokkaita valtionsisäisiä oikeussuojakeinoja näitä oikeuksia koskevien louk-

kausten varalta. Näin ollen, jos valittajan väite menee ihmisoikeussopimuksen soveltamisalan ulkopuolelle, 13 artiklaakaan ei ole voitu loukata.

Sopimusmääräystä voidaan pitää yhtenä ilmauksena siitä, että myös kansainvälisellä sopimuksella suojatut ihmisoikeudet tulisi prosessuaalisellakin tasolla ensisijaisesti turvata kansallisen oikeusjärjestyksen puitteissa. Jäsenvaltioilla on valta päättää, millä tavoin ne saattavat 13 artiklan vaatimukset voimaan. Artikla 13 ei edellytä sellaisen oikeussuojakeinon olemassaoloa, jolla voitaisiin kansallisesti tutkia kansallisen lainsäädännön yhdenmukaisuus EIS:n kanssa. EIT on soveltanut tätä periaatetta tapauksiin, joissa on haluttu riitauttaa joko tietty lainsäädännön normi tai yleisemmin kansallisen lainsäädännön tila.

Oikeussuojakeinoa koskevan 13 artiklan pääsääntöinen soveltumattomuus oikeudenkäyntimenettelyä koskevien artikloiden osalta liittyy siihen, että toisin kuin artikla 5 (oikeus vapauteen ja turvallisuuteen) ja 6 artikla (oikeus oikeudenmukaiseen oikeudenkäyntiin), 13 artikla ei välttämättä vaadi tarkoittamansa tehokkaan oikeussuojakeinon olevan tuomioistuin. Pikemminkin kysymyksessä olevan oikeuden luonteesta ja kulloisenkin tapauksen olosuhteesta riippuu, millaista kansallista oikeussuojaa 13 artiklan voidaan katsoa edellyttävän. 13 artiklan mukainen määräys edellyttää oikeussuojakeinoa, mutta ei takaa valittajalle myönteistä lopputulosta itse asiakysymyksessä. Tehokkuutta arvioidaankin lähinnä siltä osin, onko kyseessä oleva toimielin toimivaltainen ratkaisemaan asian ja millaiset prosessuaaliset oikeusturvatakeet se pystyy prosessille antamaan. Valtioilla on laaja harkintavalta, miten ne toteuttavat tehokkaan oikeussuojakeinon vaatimukset. Valtioilta vaaditaan ainoastaan, että ne turvaavat ihmisoikeussopimuksen oikeuksien sisällöt oikeusjärjestyksessään.

EIT on korostanut, että 13 artiklan tulkinnassa on jätettävä tiettyä tapauskohtaista joustovaraa ja vältettävä liiallista muodollisuutta. Kunkin yksittäisen tapauksen olosuhteilla on merkitystä EIT:n kokonaisharkinnassa, jossa otetaan huomioon kansallisen sääntelyn muodolliset edellytykset ja asianomaisen valtion oikeudellisen ja poliittisen järjestelmän realiteetit sekä valittajan yksilölliset olosuhteet. Artiklasta 13 ei myöskään seuraa, että valtionsisäisen muutoksenhakuelimen tulisi voida tutkia nimenomaisesti väite jonkin ihmisoikeussopimuksen muun määräyksen rikkomisesta. Riittävää on sellaisen oikeussuojakeinon olemassaolo, johon turvautumalla kysymys sopimusrikkomuksesta on asiallisesti ottaen ollut mahdollista saattaa tutkittavaksi.

Euroopan ihmisoikeussopimuksen 13 artiklan soveltamisalue rajoittuu vain tapauksiin, joissa valittajalla on todellista oikeussuojan tarvetta ihmisoikeussopimuksen turvaamien oikeuksien osalta. EIT ratkaisukäytännön mukaan perusteltavissa oleva väite (”arguable claim”) ihmisoikeussopimuksessa turvatun oikeuden loukkauksesta velvoittaa takaamaan väitetyn loukkauksen kohteelle 13 artiklan mukaisen oikeuskeinon. Jos henkilö esimerkiksi katsoo yksityisyyttään loukatun 8 artiklan vastaisesti, tulee valtionsisäisen oikeuden tarjota tehokas oikeuskeino tällaista väitettyä loukkausta vastaan, paitsi milloin väite ei ole perusteltavissa. Vaikka väitteen perusteltavuudesta huolimatta valvontaelimet eivät lopulta katsoisikaan 8 artiklaa loukatun, saattaa kansallisen oikeussuojakeinon puuttuminen merkitä 13 artiklan loukkausta. Väitteen perusteltavuus on puolestaan ratkaistava kunkin tapauksen omien erityispiirteiden valossa. Ratkaisussa Powell ja Rayner v. Yhdistynyt kuningaskunta (1990) EIT ilmaisi nyt vakiintuneena pidettävän kannan, että ilmeisen perusteettomana tutkittavaksi ottamatta jätetyn valituksen taustalla ei voida ajatella olevan sillä tavoin perusteltavissa olevaa väitettä, että valtiolla olisi velvollisuus taata 13 artiklan mukainen oikeussuojakeino.

Edellytys asian tutkimiselle EIT:ssä on, että kansalliset oikeussuojakeinot on käytetty loppuun saakka. Jos tehokas oikeussuojakeino puuttuu kokonaan, valittajalla ei ole velvoitetta oikeussuojakeinon käyttämiseen kansallisesti. On siis selvää, että kansallisen oikeussuojakeinon puuttuminen kokonaan johtaa 13 artiklan loukkaukseen. Näin oli esimerkiksi silloin, kun kansallinen järjestelmä ei taannut mitään oikeussuojakeinoa työpaikan puhelimen kuuntelun osalta (Halford v. the United Kingdom 1997).

Ihmisoikeussopimuksen 8 artiklan kohdalla EIT on todennut, että oikeussuojakeinojen tulee olla niin tehokkaita, kuin mahdollista. Puhelinkuuntelua koskeneessa Klass ym. v. Saksan liittotasavalta (1978) ratkaisussa EIT totesi, että tällaisessa tapauksessa ”effective remedy” tarkoittaa mahdollisimman tehokasta oikeussuojakeinoa salaisessa valvonnassa luonnostaan aiheutuvat rajoitukset huomioon ottaen. Näissä olosuhteissa itsensä valvotuksi tuntevan henkilön käytännössä merkitykseltään rajallinen mahdollisuus vedota erityiseen lain täytäntöönpanoa valvovaan komissioon sekä valtiosääntötuomioistuimeen on katsottu 13 artiklan valossa riittäväksi. Myöhemmässä oikeuskäytännössään EIT on katsonut, että niin kauan kuin pakkokeinot pysyvät salaisina, pelkkä objektiivisen kontrollimekanismin, kuten kansallisen valitusmahdollisuuden, olemassaolo on 13 artiklan kannalta riittävä, mutta heti kun tällainen pakkokeino tulee ilmi konkreettisessa tapauksessa, sen kohteeksi joutuneella tulee olla käytettävissään riittävät oikeussuojakeinot.

Oikeussuojakeino on tehoton silloin, kun asiaa ratkaisevalla taholla ei ole toimivaltaa tehdä sitovia päätöksiä. Tapauksessa Leander v. Ruotsi (1987) taustalla oli Ruotsin suojelupoliisin pitämä kortisto, jossa olevien tietojen nojalla turvallisuusriskiksi luokitellulta henkilöltä voitiin evätä pääsy tiettyihin valtion virkoihin tai toimiin. Ruotsin hallituksen mukaan henkilöllä oli neljä oikeussuojakeinoa: 1) mahdollisuus hakea virkaa ja valittaa päätöksestä hallitukselle; 2) mahdollisuus pyytää poliisihallitukselta lupa perehtyä itseään koskeviin tietoihin sekä saada tässä suhteessa annettu kielteinen päätös viime kädessä Regeringsrättenin tutkittavaksi; 3) mahdollisuus kannella oikeusasiamiehelle; 4) mahdollisuus kannella oikeuskanslerille. EIT katsoi äänin 4-3, että yksinään mikään näistä ei ollut 13 artiklan mukainen tehokas oikeussuojakeino, mutta asian luonne huomioon ottaen niitä sekä valittajan käyttämää mahdollisuutta kannella hallitukselle poliisihallituksen toimista oli yhdessä tarkasteltuna pidettävä riittävinä. Tähän lopputulokseen päätyessään EIT korosti myös Ruotsin asianomaiseen järjestelmään liittyvää parlamentaarista valvontaa. Edellä kuvattu oikeussuojakeinojen yhteisvaikutus voi olla riittävä eritoten valtion turvallisuutta koskevissa tilanteissa.

Sitä vastoin 13 loukkaus vahvistettiin tapauksessa Segerstedt-Wiberg v. Ruotsi (2006). Vaikka tuomio ei kumoa Leander-ratkaisussa kehiteltyjä periaatteita, se osoittaa kriittisempää suhtautumista sitä näkemystä kohtaan, että oikeussuojakeinojen kokonaisuus voisi olla yhdessä tarkasteltuna riittävän tehokas tilanteessa, jossa yksikään oikeussuojakeino ei yksin tai itsessään tarjoa tehokasta oikeussuojaa, ja itse oikeussuojakeinolla halutaan päästä konkreettisempaan lopputulokseen. Oikeussuoja saattaakin olla tehoton, jos asiaa ratkaisevalla taholla ei ole toimivaltaa tuomita valittajalle vahingonkorvausta.

Valtio ei voi vedota kansalliseen turvallisuuteen 13 artiklan oikeussuojakeinon puuttumisen perusteena muissa kuin poikkeustapauksissa. Tapauksessa Smith ja Grady v. Yhdistynyt kuningaskunta EIT ei hyväksynyt valtion väitettä, että homoseksuaalien kielto palvella armeijassa palveli kansallisen turvallisuuden vaatimuksia. EIT totesi 13 artiklan loukkauksen, koska olemassa olevat oikeuskeinot olivat liian heikkoja ja estivät 8 artiklan näkökohtien tehokkaan tutkinnan.

Tapaus Al-Nashif v. Bulgaria (2002) koski ulkomaalaisen karkottamista valtion turvallisuuteen liittyvistä syistä. Valittaja vetosi syihin, joiden johdosta 13 artikla tuli sovellettavaksi 8 artiklan perheelämän suojan valossa tarkasteltuna. Vaikka valtion turvallisuusintressien johdosta asianosaisen oikeutta saada tietoonsa kaikkea tapauksensa tausta-aineistoa voidaan rajoittaa, täytyy riippumattoman tahon tällöin arvioida menettelyn perusteiden asianmukaisuus ja varmistaa kontradiktorisen menettelyn riittävä toteutuminen. Koska tapauksessa toimivaltainen tuomioistuin ei voinut lainkaan tutkia viranomaisen päätöksen perusteita, katsottiin 13 artiklaa loukatun. Vastaava asetelma tuli niin ikään esille tapauksessa C.G. ym. v. Bulgaria (2008). Siinä maastakarkoitus perustui sisäministeriön salaiseen raporttiin, jonka mukaan valittaja tiedustelutietojen perusteella osallistunut huumausainerikoksiin. Asiaa myöhemmin käsitelleet tuomioistuimet olivat kylläkin saaneet salaisen raportin tietoonsa, mutta ne tyytyivät raportin sisältämiin tietoihin tekemättä muita toimenpiteitä asian faktojen selvittämiseksi ja tarjoamatta valittajalle tehokasta mahdollisuutta riitauttaa salaisen

raportin sisällön paikkansapitävyyttä tai mahdollisuutta argumentoida perhe-elämän suojaan liittyvillä perusteilla. Tässäkin tapauksessa oikeussuojakeinoa pidettiin 13 artiklan vastaisena.

Suomen korkein hallinto-oikeus viittasi mm. Al-Nashif -tuomioon useassa kesällä 2007 antamassaan päätöksessä, joissa oli kyse suojelupoliisin turvallisuusriskiarvion sisältävien lausuntojen asianosaisjulkisuudesta ulkomaalaislain mukaisia perheenyhdistämisiä ja kansalaisuushakemuksia koskevissa asioissa. Korkein hallinto-oikeus katsoi, että lausunnot voitiin pitää asianosaisilta salassa, mutta oikeudenmukaisen menettelyn takaaminen edellytti, että tuomioistuin sai tiedon asianosaiselle negatiivisen lausunnon perusteista ja että tuomioistuin otti kantaa näiden perusteiden asianmukaisuuteen.

Tehokkaan oikeussuojakeinon 13 artiklan mukaisuus ei riipu siitä, onko oikeuskeinoon turvautuminen ollut menestyksekästä. Tapauksessa Vereinigung Demokratischer Soldaten Österreichs ja Gubi v. Itävalta (1994) oli kysymys 10 artiklaan liittyvästä kiellosta levittää sanomalehteä kasarmialueella. Tässä tapauksessa valtiolla katsottiin olevan todistustaakka siitä, että olemassa olevat oikeussuojakeinot ovat tehokkaita. Hallitus ei osoittanut valittajayhdistyksellä olleen käytettävissään tehokasta oikeuskeinoa, minkä johdosta 13 artiklaa katsottiin loukatun. Sen sijaan toisena valittajana ollut varusmies saattoi valittaa sananvapautensa loukkauksesta valtiosääntötuomioistuimeen, kuten hän tekikin. Sillä, että valitus oli tulokseton, ei ollut merkitystä 13 artiklan kannalta, joten tältä osin ei ollut tapahtunut loukkausta.

EIT on uudemmassa oikeuskäytännössä edellyttänyt tehokkaita oikeussuojakeinoja myös kotirauhaan puuttuvien pakkokeinojen laillisuuskontrolliin. Tapauksessa Stefanov v. Bulgaria (2008) kotietsintään liittyviä oikeussuojatakeita arvioitiin 13 artiklan vaatimusten kannalta. Tapauksessa kansallinen lainsäädäntö ei mahdollistanut kotietsinnän perusteiden tai suorittamistavan tuomioistuinkontrollia. Ihmisoikeussopimuksen 13 artikla ei edellytä, että oikeussuojakeinon tulisi olla käytettävissä ennen kotietsintää. Artiklan 13 loukkaus aiheutui kuitenkin siitä, että kansallinen oikeusjärjestelmä ei tuntenut mitään muuta oikeudellista menettelyä, jossa etsinnän kohteena ollut henkilö olisi voinut riitauttaa etsinnän ja takavarikon laillisuuden ja saada asianmukaisen hyvityksen siinä tilanteessa, että etsintä ja takavarikko oli määrätty tai toimeenpantu laittomasti.

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

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

EIT on useissa aiemmissa ratkaisuissaan ottanut kantaa kysymykseen siitä, tuleeko ja missä tilanteissa tiedonhankinnan kohdehenkilöllä olla oikeus saada viranomaiselta tieto häneen kohdistetusta tiedonhankintatoimenpiteestä. Tapauksissa Klass v. Saksa ja Weber & Saravia v. Saksa EIT piti ihmisoikeussopimuksen kannalta hyväksyttävänä sääntelyä, jonka mukaan tiedonhankinnan koh-

teelle oli ilmoitettava heti, kun ilmoittaminen ei enää vaarantanut tiedonhankinnan tarkoitusta. EIT kiinnitti huomiota myös siihen, että Saksan järjestelmässä ilmoittamisen ja toiselta puolen ilmoittamatta jättämisen edellytysten käsillä olon arviointi kuului riippumattomalle elimelle (G10-komissio), ei turvallisuusviranomaiselle.

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

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

Valitus- tai kantelumahdollisuuden käytön edellytyksenä yleensä on, että henkilö saa viranomaiselta tiedon häneen kohdistetusta tiedonhankinnasta sen jälkeen kun tiedonhankintakeinon käyttö on päättynyt (ks. yllä Zakharov v. Venäjä). Tästä ei kuitenkaan seuraa, että ilmoitus on tehtävä välittömästi tiedonhankinnan päätyttyä. Uhka, josta tiedonhankintamenetelmän avulla on hankittu tietoja, voi jatkua vuosia tai jopa vuosikymmeniä, jolloin ilmoituksen tekemistä on turvallisuusviranomaisten toiminnan suojaamiseksi välttämätöntä lykätä vastaavasti. Oikeussuojakeinon käytön mahdollistamiseksi ilmoitus olisi kuitenkin tehtävä sen jälkeen, kun ilmoittamatta jättämiselle ei enää ole yksilöllistä perustetta (Klass v. Saksa, Zakharov v. Venäjä). Kuitenkin myös järjestelmä, joka ei lainkaan edellytä kohdehenkilölle ilmoittamista, voi olla sopusoinnussa ihmisoikeussopimuksen kanssa. Tällöin kanteluoikeus on tullut kansallisessa lainsäädännössä säätää niin yleiseksi, että kuka hyvänsä saa kannella pelkästään sen perusteella, että epäilee viranomaisten puuttuneen luottamuksellisen viestintänsä nauttimaan suojaan (Kennedy v. Yhdistynyt Kuningaskunta).

2.3.1.3 Euroopan unionin perusoikeuskirja

Vuonna 2009 voimaantullut Euroopan unionin perusoikeuskirja määrittelee unionin tasolla pätevät perusoikeudet. Jäsenvaltiot ovat velvollisia noudattamaan perusoikeuskirjaa aina, kun ne soveltavat unionin oikeutta. Perusoikeuskirjan 7 artiklan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa sekä viesteihinsä kohdistuvaa kunnioitusta. Perusoikeuskirjan 8 artiklan mukaan puolestaan jokaisella on oikeus henkilötietojensa suojaan. Henkilötietojen suojaan kuuluvien tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava laissa määritettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty ja saada ne oikaistuiksi. Riippumattoman viranomaisen on valvottava näiden sääntöjen noudattamista.

Perusoikeuskirjan 52 artikla määrää perusoikeuskirjalla turvattujen oikeuksien kattavuudesta. Artiklan 1 kappaleen mukaan perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla, ja kyseisten oikeuksien ja vapauksien olennaista sisältöä nou-

dattaen. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan tehdä ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia. Saman artiklan 3 kappaleen mukaan, siltä osin kuin perusoikeuskirjan oikeudet vastaavat ihmisoikeuksien ja perusvapauksien suojaamista koskevassa eurooppalaisessa yleissopimuksessa taattuja oikeuksia, niiden merkitys ja kattavuus ovat samat kuin mainitussa yleissopimuksessa. Tämä ei kuitenkaan estä unionia määräämästä tätä laajemmasta suojasta.

Perusoikeuskirjan 52 artiklan 3 kohdasta seuraa, että perusoikeuskirjan 7 artiklan sisältö vastaa EIS 8 artiklan sisältöä. Perusoikeuskirjan johdannossa todetaan erikseen, että vahvistettavat oikeudet perustuvat paitsi Euroopan ihmisoikeussopimukseen, myös Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöön. EIT:n laajalla ihmisoikeussopimuksen 8 artiklaa koskevalla ratkaisukäytännöllä on näin ollen katsottava olevan relevanssia myös perusoikeuskirjan 7 artiklan tulkinnalle.

Perusoikeuskirjan mukaisten perusoikeuksien kunnioittamisen valvonta ei edellä sanotusta huolimatta kuulu EIT:lle vaan Euroopan unionin tuomioistuimelle (EUT) ja kansallisille tuomioistuimille. Tietoliikennetiedustelun kannalta merkitystä on EUT:n huhtikuussa 2014 antamalla tuomiolla, jolla EUT julisti pätemättömäksi vuonna 2006 säädetyn Data Retention -direktiivin. Direktiivi oli asettanut unionin jäsenvaltioille velvoitteen säätää teletunnistamistietojen kattavasta säilyttämisestä vakavien rikosten torjunnan ja tutkinnan tarpeita varten.

EUT katsoi edellä mainitussa tuomiossaan, että Data Retention -direktiivi oli perusoikeuskirjan 52 artiklan 1 kappaleessa tarkoitetun suhteellisuusperiaatteen vastainen. Suhteellisuusperiaate pitää sisällään sen, että perusoikeuden rajoitus on välttämätön. Arvioidessaan Data Retention -direktiivillä tapahtuneen oikeuksien rajoittamisen välttämättömyyttä EUT kiinnitti huomiota siihen, että direktiivin säätämä teletunnistamistietojen säilyttämisvelvoite kattoi kaikki henkilöt, kaikki sähköisen viestinnän tavat ja lähes kaikki tunnistamistiedot ilman minkäänlaista vakavan rikollisuuden ehkäisemisen tavoitteeseen perustuvaa erottelua, rajaamista tai poikkeusta. Säilyttämisvelvollisuuden piirissä olivat myös kaikkien sellaisten henkilöiden teletunnistamistiedot, joiden osalta ei ole mitään näyttöä edes etäisestä tai epäsuorasta kytkennästä rikollisuuteen. Näin ollen direktiivin oli katsottava puuttuvan käytännössä jokaisen EU:n alueella oleskelevan henkilön oikeuksiin.

EUT:n mukaan direktiivin olisi tullut sisältää ainakin osa seuraavista elementeistä ollakseen suhteellisuusperiaatteen mukainen:

- Jonkinlaiset direktiivin tavoitteeseen liittyvät objektiiviset rajat sille, keiden henkilöiden teletunnistamistiedot saadaan säilyttää
- Tarkemman määrittelyn niistä rikoksista, joiden torjumiseksi tai tutkimiseksi kansalliset viranomaiset saavat säilytettyihin tunnistamistietoihin tutustua ja niitä käyttää. Direktiivi viittaa tältä osin ainoastaan ”vakaviin rikoksiin”, joiden sisältö määräytyy kunkin jäsenvaltion kansallisen lainsäädännön mukaan
- Aineelliset ja menettelylliset edellytykset tietoihin tutustumiselle ja niiden käytölle. Tietoihin tutustumisen edellytykseksi ei ole direktiivissä asetettu esimerkiksi tuomioistuimen tai muun riippumattoman elimen lupaa, vaan menettelystä päättäminen on siinä jätetty kansallisten säädösten varaan
- Tarkemmat säännökset tunnistamistietojen säilyttämisajoista. Direktiivissä säädetään vähimmäissäilytysajaksi kuusi kuukautta tekemättä mitään eroa sen suhteen, voivatko tiedot olla rikostorjunnassa hyödyllisiä
- Tehokkaan tietosuojan varmistamiseksi riittävät takeet siitä, että säilytettäviä tietoja ei väärinkäytetä. Direktiivi sallii sen, että teleyritykset huomioivat taloudelliset näkökohdat määrittäessään soveltamansa turvan tason
- Määräykset siitä, että tiedot on säilytettävä unionin alueella

Eduskunnan perustuslakivaliokunta on lausunnossaan PeVL 18/2014 vp esittänyt EUT:n tuomiota koskevia huomioita. Valiokunnan mukaan tuomiosta ei voida suoraan johtaa vastausta siihen, millainen kansallinen lainsäädäntö täyttäisi yksityiselämän ja henkilötietojen suojaan liittyvät oikeasuhtaisuusvaatimukset. Lähtökohtana on valiokunnan mukaan kuitenkin pidettävä sitä, että oikeasuhtaisuusvaatimuksen vastaisena voidaan pitää ainakin sellaista sääntelyä, joka merkitsee laajamittaista, erittelemätöntä, pitkäaikaista ja rajoittamatonta tietojen säilyttämistä yhdistettynä viranomaisten erittelemättömään ja rajoittamattomaan pääsyyn näihin tietoihin. Perustuslakivaliokunta totesi myös, että tuomion perusteella jää avoimeksi, merkitseekö viranomaistarpeita varten säädetyn säilyttämisvelvollisuuden ulottuminen käytännössä kaikkien sähköisiä viestimiä käyttävien ihmisten tietoihin jo yksinään oikeasuhtaisuusvaatimuksen loukkausta.

Tuomiossaan EUT totesi, että direktiivin olisi tullut asettaa tavoitteeseensa liittyvät objektiiviset rajat sille, keiden henkilöiden tunnistamistiedot saadaan säilyttää. Lisäksi direktiivin olisi tullut tarkemmin määritellä ne rikokset, joiden torjumiseksi säilyttämisvelvollisuus asetettiin. Tärkeää on tältä osin tiedostaa, ettei EUT:n tuomio varsinaisesti luo uutta oikeutta. Se vastaa Euroopan ihmisoikeustuomioistuimen vakiintunutta ratkaisukäytäntöä. Ihmisoikeustuomioistuin on antanut suurehkon määrän ratkaisuja, joissa se EUT:n tuomiota vastaavalla tavalla mutta yksityiskohtaisemmin on käsitellyt niitä elementtejä, jotka yksityiselämän suojaan puuttuvan lain on sisällettävä ollakseen suhteellisuusperiaatteen mukainen ja ennakoitava. Merkittävimpiä tässä suhteessa ovat ihmisoikeustuomioistuimen tietoliikennetiedustelua tai sen lähi-ilmiöitä suoraan koskeneet ratkaisut Klass vastaan Saksa (1978), Weber ja Saravia vastaan Saksa (2006) ja Liberty ja muut vastaan Yhdistynyt Kuningaskunta (2008).

EUT on pohtinut perusoikeuskirjan 7, 8 ja 47 artikloiden vaikutusta asiaan, jossa oli kyse henkilötietojen siirrosta kolmanteen maahan, jonka tietosuojan riittävästä tasosta oli esitetty väitteitä (Schrems v. Data Protection Commissioner). Asian taustalla oli huoli Yhdysvaltain tiedustelusta, minkä johdosta Schrems teki 25.6.2013 Irlannin tietosuojavaltuutetulle kantelun, jossa hän vetosi siihen, että Yhdysvaltojen oikeus ja käytänteet eivät tarjonneet mitään tosiasiallista suojaa valtion harjoittamaa tarkkailua vastaan tiedoille, joita säilytettiin Yhdysvaltojen alueella. Kyseisen tuomion perusteella kumottiin komission päätös 2000/520/EY, jossa komissio oli mm. todennut, että Yhdysvalloissa taataan siirrettyjen henkilötietojen tietosuojan riittävä taso, joka nojautuu safe harbor –järjestelmään ja joka estää käytännössä kansallisia valvontaviranomaisia tutkimasta kyseisestä riittävää tasoa ja keskeyttämään tarvittaessa tiedonsiirron. Safe harbor -järjestelmä sisältää joukon henkilötietojen suojaa koskevia periaatteita, joihin yhdysvaltalaiset yritykset voivat sitoutua vapaaehtoisesti.

EUT katsoi antamassaan tuomiossa että komission kyseinen päätös ei voi tehdä tyhjäksi toimivaltaa, joka kansallisilla valvontaviranomaisilla on perusoikeuskirjan ja tietosuojadirektiivin 95/46/EY nojalla. EUT korosti tässä yhteydessä perusoikeuskirjassa taattua oikeutta henkilötietojen suojaan sekä perusoikeuskirjassa annettuun valvontaviranomaisten tehtävään.

Unionissa taattuja vapauksia ja perusoikeuksia pääosiltaan vastaavasta suojan tasosta EUT totesi, että unionin oikeuden mukaan säännöstö ei rajoitu siihen, mikä on ehdottomasti tarpeen, silloin, kun siinä sallitaan yleisesti kaikkien henkilöiden, joiden henkilötiedot siirretään unionista Yhdysvaltoihin, kaikkien henkilötietojen säilyttäminen tekemättä mitään erottelua, rajoitusta tai poikkeusta tavoiteltavan päämäärän mukaan ja säätämättä objektiivisista perusteista, jotta voitaisiin rajoittaa viranomaisten pääsyä tietoihin ja niiden myöhempää käyttöä. Säännöstöä, jonka nojalla viranomaiset pääsevät yleisesti sähköisen viestinnän sisältöön, on katsottava loukkaavan yksityiselämän kunnioittamista koskevan perusoikeuden keskeistä sisältöä. EUT katsoi samoin viitaten perusoikeuskirjan 47 artiklaan, että säännöstöllä, jossa yksityisille ei anneta mitään mahdollisuutta käyttää oikeussuojakeinoja, jotta he saisivat tutustua itseään koskeviin henkilötietoihin tai saada tällaiset tiedot oikaistuiksi tai poistetuiksi, loukataan tehokasta oikeussuojaa koskevan perusoikeuden keskeistä sisältöä, koska kyseinen mahdollisuus on erottamaton osa oikeusvaltiota. Lopuksi

EUT totesi, että 26.7.2000 tehty komission päätös estää kansallisia valvontaviranomaisia käyttämästä toimivaltaansa, mikäli henkilö kyseenalaistaa päätöksen yhteensopivuuden henkilöiden yksityiselämän, vapauksien ja perusoikeuksien suojan kanssa. Komissiolla ei ole näin ollut toimivaltaa rajoittaa kansallisten valvontaviranomaisten toimivaltaa.

Edellä mainituista syistä EUT julisti 26.7.2000 tehdyn komission päätöksen pätemättömäksi. Tuomion seurauksena Irlannin valvontaviranomainen on velvollinen tutkimaan Schremsin kantelun kaikkea asianmukaista huolellisuutta noudattaen. Tästä syystä tietosuojadirektiivin artikla 29 mukainen työryhmä (jälj. tietosuojatyöryhmä) antoi lausunnon 16.10.2015 Schrems -tuomion vaikutuksista. Tietosuojatyöryhmä piti tärkeänä, että tuomion soveltamiseen on olemassa valvontaviranomaisten yhteinen kanta. Tietosuojatyöryhmä kehotti jäsenvaltioita ja EU:n toimielimiä avaamaan keskustelun Yhdysvaltojen viranomaisten kanssa, jotta löydettäisiin kattava ja perusoikeuksia kunnioittava ratkaisu mahdollistamaan tietojen siirto Yhdysvaltoihin. Tietosuojatyöryhmä jatkaa EUT:n tuomion vaikutusten arviointia muihin tiedonsiirtotapoihin ja toteaa toistaiseksi voitavan käyttää mallisopimuslausekkeita henkilötietojen siirtoa varten sekä sisäisiä tietosuojasääntöjä (Binding Corporate Rules). Tietosuojatyöryhmä huomauttaa kuitenkin, että tämä ei estä tietosuojaviranomaisia tutkimasta yksittäisiä tapauksia esimerkiksi kanteluita ja käyttää toimivaltaansa yksilöiden suojaamiseksi.

Tuomion antamisen jälkeisten neuvottelujen tuloksena EU ja Yhdysvallat sopivat Safe Harborin korvaavasta Privacy Shield -järjestelmästä, joka tuli käyttöön 1. elokuuta 2016.

Jo aikaisempi Safe Harbor -järjestelmä sisälsi seitsemän pääperiaatetta, jotka on sisällytetty myös Privacy Shieldiin. Näitä periaatteita ovat yksityishenkilöiden informointi, valinnanvapaus, tietojen edelleen siirtämisen rajoittaminen, tietoturvallisuus, käyttötarkoitussidonnaisuus, tietojen oikeellisuuden vaatimus ja oikeussuojakeinot. Privacy Shield kuitenkin parantaa yksilöiden mahdollisuuksia turvautua oikeussuojakeinoihin ja saada korvauksia tietosuojaloukkauksista. Lisäksi se rajoittaa Yhdysvalloissa toimivien organisaatioiden oikeutta luovuttaa tietoja edelleen kolmansille tahoille. Privacy Shield -järjestelmän piirissä olevat organisaatiot eivät esimerkiksi voi laajamittaisesti luovuttaa käsittelemiään tietoja Yhdysvaltojen viranomaisille.

Kuten aiemminkin, henkilötietojen siirtäminen EU:sta Yhdysvaltoihin on edelleen mahdollista myös muun muassa tietoja koskevan henkilön nimenomaisella suostumuksella, erityisillä tietosuojan tason takaavilla sopimuksilla tai yritystä koskevilla sitovilla BCR-säännöillä. Privacy Shield -järjestelmän käyttöönoton myötä organisaatioiden tulisi kuitenkin arvioida, onko niillä käytössään tarjolla olevista vaihtoehdoista kaikkein tarkoituksenmukaisin tapa siirtää henkilötietoja EU:sta Yhdysvaltoihin.

EUT on tuomiossaan yhdistetyissä asioissa Tele2 Sverige ja Watson (C-203/15 ja C-697/15) katsonut, että sähköisten viestintävälineiden kaikkien liikenne- ja paikkatietojen yleinen ja erotuksetta tapahtuva säilyttäminen ei ole EU-oikeuden mukaista (kohta 103 ja 105). Pääasiasiassa kyseessä olevilla kansallisilla säännöstöillä oli ollut tarkoitus panna täytäntöön teletunnistetietojen tallentamista koskeva direktiivi, jonka EU-tuomioistuin katsoi kuitenkin pätemättömäksi edellä kuvatussa Digital Rights Ireland -tuomiossa.

Vaikka kaikkien tietojen yleinen ja erittelemätön säilyttäminen ei ole EUT:n mukaan suhteellisuusperiaatteen mukaista, jäsenvaltiot voivat kuitenkin säätää sekä näiden tietojen kohdennetusta säilyttämisestä että toimivaltaisten kansallisten viranomaisten oikeudesta saada kyseisiä tietoja jonkin sähköisen viestinnän tietosuojadirektiivissä mainitun oikeutetun tavoitteen toteuttamiseksi ja sillä edellytyksellä, että kyseiset säännöt ovat selviä ja täsmällisiä ja tietojen säilyttäminen ja pääsy niihin on suhteellisuusperiaatteen mukaisesti rajoitettu täysin välttämättömään (kohdat 94–96, 103, 108, 109, 116).

Sähköisen viestinnän tietosuojadirektiivissä suljetaan nimenomaisesti direktiivin soveltamisalan ulkopuolelle muun muassa valtion toimet rikosoikeuden alalla ja yleistä turvallisuutta ja puolustusta koskevat toimet, mutta siinä mahdollisestaan näiden tavoitteiden toteuttamiseen liittyvät tai niitä palvelevat lainsäädännölliset toimenpiteet. Kyseisten toimenpiteiden katsotaan siten kuuluvan direktiivin soveltamisalaan (kohdat 69-76). EUT kiinnitti tätä koskevassa arvioinnissaan ensisijaisesti huomiota direktiivin kohteena olevien palveluntarjoajien toimiin ja velvollisuuksiin, joilla turvataan direktiivin tehokas vaikutus.

Vaikka tietojen säilyttämistä ja käyttöä koskevat edellytykset voivat vaihdella eri kansallisissa säännöstöissä, tuomioistuin luetteli kuitenkin useita aineellisia ja menettelyllisiä seikkoja, jotka tulisi huomioida tällaisten sääntöjen yhteydessä. Sääntöjen tulee ensinnäkin mahdollistaa asianmukaiset oikeussuojakeinot. Säilytettäväksi säädettyjen tietojen tulee olla objektiivisten perusteiden mukaisia ja niillä tulee olla kiinteä yhteys asetettuun tavoitteeseen. Säännöksen laajuutta ja soveltamista voidaan rajoittaa ehdottoman välttämättömään myös edellytyksillä, jotka koskevat muun muassa aiotun säilytyksen kestoa, maantieteellisesti määriteltyä aluetta, henkilöpiiriä, tietoluokkia, viestintävälineitä ja kohdennettua yleisöä (kohdat 106–111, 117–119).

Tuomioistuin katsoi lisäksi, että etukäteisvalvontaa, tietojen säilyttämistä unionin alueella, tietosuojan ja -turvan korkeaa tasoa, tietojen lopullista hävittämistä säilytysajan päätyttyä ja tietojen kohteena olevien henkilöiden tiedottamista on pidettävä edellytyksinä sille, että toimivaltaiset viranomaiset voivat saada kyseisiä tietoja (kohdat 120–122).

Perusoikeuskirjan 54 artiklan mukaan perusoikeuskirjan määräysten ei saa tulkita antavan oikeutta ryhtyä sellaiseen toimintaan tai tehdä sellaista tekoa, jonka tarkoituksena on tehdä tyhjäksi jokin perusoikeuskirjassa tunnustettu oikeus tai vapaus tai rajoittaa sitä laajemmalti kuin perusoikeuskirjassa on sallittu. Perusoikeuskirjan 54 artiklan muotoilu on monessa suhteessa samanlainen Euroopan ihmisoikeussopimuksen 17 artiklan kanssa.

2.3.2 Ulkomaiden lainsäädäntö

2.3.2.1 Ruotsi

Sotilastiedustelua harjoittavat puolustusvoimien tiedustelu- ja turvallisuuspalvelu (Militära Underrättelse- och Säkerhetstjänsten, MUST), puolustusvoimien radiolaitos (Försvarets radioanstalt, FRA), puolustusvoimien materiaalilaitos (Försvaretsmaterielverk, FMV) ja kokonaismaanpuolustuksen tutkimusinstituutti (Totalförsvarets forskningsinstitut, FOI).

Puolustushallinnon tiedustelutoiminnasta säädetään puolustustiedustelusta annetulla yleislailla (Lag om försvarsunderrättelseverksamhet) ja sitä täydentävällä asetuksella (Förordning om underrättelseverksamhet). Yleislakia täydentävät lait, kuten laki henkilötietojen käsittelystä puolustustiedustelutoiminnassa (Lag om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst), laki pätevästä peitehenkilöllisyydestä (Lag om kvalificerade skyddsidentiteter) ja laki sähköisestä viestinnästä (Lag om elektronisk kommunikation).

Ohjaus

Tiedustelutoiminnan kohdentamisen linjaa puolustustiedustelusta annetun lain mukaan Ruotsin hallitus. Hallituksen erikseen nimeämät viranomaiset voivat hallituksen päättämän yleisen kohdentamisen puitteissa antaa tiedustelutoiminnan tarkempaa kohdentamista koskevia määräyksiä. Lisäksi lainsäädännössä on annettu hallitukselle mahdollisuus antaa tarkentavia asetuksia.

Puolustusministeriössä toimii puolustustiedustelukysymyksiä yhteen sovittava yksikkö SUND, joka vastaa valtioneuvostotasolla puolustustiedusteluun liittyvien kysymysten valmistelusta ja yhteenso-

vittamisesta. Myös puolustustiedusteluviranomaiset tekevät yhteistyötä koordinoidakseen siviili- ja sotilastiedustelun kiinnostuksen kohteisiin liittyvää tiedustelua.

Tiedustelupalvelun tehtävä

Tiedustelun toimiala on puolustustiedustelulain 1 §:ssä rajattu siten, että tiedustelutoimintaa harjoitetaan Ruotsin ulko-, turvallisuus- ja puolustuspolitiikan tueksi ja Ruotsiin kohdistuvien ulkoisten uhkien kartoittamiseksi. Toiminnalla tuetaan myös Ruotsin osallistumista kansainväliseen turvallisuusyhteistyöhön. Tiedustelu saa koskea vain ulkomaisia olosuhteita. Teknistä tiedustelua koskevat säännökset on annettu signaalitiedustelusta puolustustiedustelutoiminnassa annetussa laissa.

Tiedonhankintakeinot ja niiden käytöstä päättäminen

Tiedusteluviranomaiset saavat käyttää toiminnassaan teknistä tiedustelua ja henkilötiedustelua (lag om förvarsunderrättelseverksamhet 2 §). Keskeinen teknisen tiedustelun toimivaltuus on signaalitiedustelu, jonka sääntely muodostuu usean lain kokonaisuudesta. Yleislakina on laki signaalitiedustelusta (Lag om signalspaning, signaalitiedustelulaki), jota tarkennetaan asetuksella (Förordning om signalspaning i försvarsunderrättelseverksamhet, signaalitiedusteluasetus). Kokonaisuus täydentyy lailla puolustustiedustelutuomioistuimesta ja lailla henkilötietojen käsittelystä signaalitiedustelutoiminnassa. (Lag om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet).

Ruotsissa tiedustelu toteutetaan hankkimalla, käsittelemällä ja analysoimalla tietoja. Tiedot raportoidaan niille viranomaisille, joita asia koskee.

Signaalitiedustelusta säädetään sitä koskevassa erityislaeissa ja -asetuksessa. FRA:n tehtävänä on hankkia tiedustelutietoja saamiensa toimeksiantojen mukaisesti ja toimittaa hankkimansa tiedot toimeksiantajien käyttöön. Signaalitiedusteluun ryhtyminen edellyttää aina toimeksiantoa, jonka FRA:lle voi antaa signaali-tiedustelulain 4 §:n mukaan valtioneuvosto, valtioneuvoston kanslia, puolustusvoimat, poliisiviranomainen tai suojelupoliisi.

Signaalitiedustelulain mukaan signaalitiedustelulla tarkoitetaan elektronisessa muodossa olevien signaalien hakemista (inhämta signaler i elektronisk form). Määritelmä on tekniikkaneutraali ja kattaa kaikki signaalitiedustelun menetelmät, kuten esimerkiksi kaapeli- ja radiosignaalitiedustelun sekä manuaalisen ja automaattisen tiedonkeräämisen. Signaalitiedustelu jakautuu neljään vaiheeseen, jotka ovat signaalitiedustelun kohdentaminen, tietojen kerääminen, tietojen työstäminen ja analysointi, sekä tietojen raportointi.

Signaalitiedustelun käytön edellytyksenä on, että sekä puolustustiedustelulaissa että signaalitiedustelua koskevassa erityislaissa määritellyt ehdot täyttyvät. Puolustustiedustelulain mukaan kyse tulee olla Ruotsin ulko-, turvallisuus- ja puolustuspolitiikan tueksi harjoitettavasta, ulkomaisia olosuhteita koskevasta tiedustelutehtävästä, jossa kartoitetaan Ruotsiin kohdistuvia ulkoisia uhkia. Signaalia ei saa kerätä, jos vastaanottaja ja lähettäjä ovat Ruotsissa. Kaapelitietoliikennettä saadaan tiedustella vain silloin, kun se ylittää Ruotsin rajan.

Signaalitiedustelua koskeva erityislain 1 § määrittelee tyhjentävästi ne kohteet, joita signaalitiedustelulla voidaan kartoittaa:

- Ruotsiin kohdistuvat sotilaalliset uhat,
- Ruotsin etuihin tai toimintaedellytysten turvaamiseen kohdistuvat uhat kansainvälisten rauhanturvaamis- ja humanitaaristen operaatioiden toteutuksessa,
- Olennaisia kansallisia etuja mahdollisesti uhkaavat kansainvälistä terrorismia ja muuta törkeää rajat ylittävää rikollisuutta koskevat strategisia olosuhteet;

- Joukkotuhoaseiden, sotatarvikkeiden ja kaksikäyttötuotteiden valvonnasta ja teknisestä tuesta annetussa laissa (lag om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd, 2000:1064) tarkoitettujen tuotteiden kehittäminen ja levittäminen,
- Yhteiskunnan infrastruktuureihin kohdistuvat vakavat ulkoiset uhat,
- Kansainväliseen turvallisuuteen vaikuttavat konfliktit ulkomailla,
- Ruotsin etuihin kohdistuva ulkomaalainen tiedustelutoiminta ja
- Ruotsin ulko-, turvallisuus- ja puolustuspolitiikan kannalta merkittävä vieraan vallan toiminta

Jos toiminnan kannalta on välttämätöntä, voidaan tietoja hankkia myös signaaliympäristössä, teknisessä kehityksessä ja signaalisuojassa tapahtuvien muutosten seuraamiseksi sekä tiedonhankinnassa käytettävän puolustustiedustelulain mukaisen toimialan tekniikan ja menetelmien kehittämiseksi.

Signaalitiedustelu edellyttää aina erityistuomioistuimena toimivan puolustustiedustelutuomioistuimen lupaa. Kaapelitiedustelua koskevan lupahakemuksen tulee sisältää kuvaus tiedonkeräystehtävästä, tieto siitä, mihin kaapelin kuituihin tiedonhankinta halutaan kohdistaa, käytettävät hakuehdot, luvan kesto ja muut seikat, joihin signaalitiedusteluviranomainen haluaa vedota. Laissa on myös annettu tarkat edellytykset sille, milloin tuomioistuin voi myöntää luvan, ja mitä luvasta tulee käydä ilmi. Myöntämisedellytykset liittyvät erityisesti toiminnan ja tehtävän lainmukaisuuteen ja suhteellisuuteen. Lupa voi olla voimassa korkeintaan kuusi kuukautta ja se voidaan uusia korkeintaan kuudeksi kuukaudeksi kerrallaan. Tuomioistuimessa kansalaisten yksityisyyttä edustavat erityiset yksityisyydensuojaa valvovat valtuutetut (integritetsskyddsombud), jotka ovat tai ovat olleet tuomareita tai asianajajia.

Luvasta tulee käydä ilmi tiedonhakutehtävä, mitä kaapeleiden kuituja lupa koskee, mitä hakuehtoja tai hakuehtokategorioita saa käyttää, luvan kesto ja muut ehdot, joita tarvitaan yksittäisen henkilön yksityisyyden suojaan puuttumisen rajoittamiseksi. Hakuehdoilla tarkoitetaan lain esitöiden mukaan sellaisia käsitteitä, joiden avulla tietomäärästä (informationsmängd) voidaan löytää sellaiset tietueet tai tietoryhmät (uppgiftskonstellationer), joissa kyseinen käsite esiintyy. Hakuehto voi myös sisältää sellaisia muuttujia, joilla kyetään erottelemaan suurempia tietomääriä. Mahdollisuutta käyttää yksittäiseen luonnolliseen henkilöön viittaavaa hakuehtoa on rajattu yksityisyyden suojan varmistamiseksi. Tällaista hakuehtoa voidaan käyttää vain, jos se on erityisen tärkeää tiedustelutoiminnalle.

Tietoliikennekaapelissa tapahtuva tietojenkeruu edellyttää tietoliikenneoperaattorin kanssa tehtävää yhteistyötä. Laki sähköisestä kommunikaatiosta edellyttää, että kaapelin omistavat tietoliikenneoperaattorit vievät Ruotsin rajat ylittävä tietoliikenteen määritettyyn liityntäpisteeseen tai -pisteisiin. Lisäksi operaattoreilla on velvollisuus luovuttaa viranomaiselle sellaiset tiedot, jotka helpottavat signaalien haltuunottoa ja tietoliikenteen käsittelyä. Operaattoreiden tulee suorittaa edellä mainitut toimenpiteet siten, etteivät niiden salassapitoon liittyvät velvoitteet vaarannu.

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

Signaalitiedustelulain 11 a § edellyttää, että luonnolliselle henkilölle tulee ilmoittaa niin pian kuin mahdollista ja viimeistään kuukausi puolustustiedustelutehtävän päättymisestä, milloin ja missä tarkoituksessa tiedustelu on toteutettu, ellei salassapitomääräyksistä muuta johdu. Ilmoituksen antamisesta päättää FRA.

Raportointi

Tiedustelua harjoittavilla viranomaisilla on velvollisuus raportoida puolustusministeriölle toiminnan yleisestä suuntautumisesta, kansainvälisestä yhteistyöstä sekä erityisillä tiedonhankintakeinoilla eli henkilö- ja signaalitiedustelulla tehtävästä tiedustelusta. Tiedusteluviranomaisten tulee myös tehdä vuosittain menneen vuoden tiedustelutoiminnasta julkinen yleiskatsaus.

Viranomaiset jättävät kalenterivuoden loputtua hallitukselle vuosikertomuksensa, joka sisältää muun muassa tiedot toiminnan tuloksista ja ehdotuksen ensi vuoden tiedustelutoiminnan talousarvioksi.

Yhteistyö rikostorjuntaviranomaisten kanssa

Tiedusteluviranomaisilla ei ole rikoksentorjunta- tai estämistoimivaltuuksia. Tiedustelu ei voi ottaa hoitaakseen sellaisia tehtäviä, jotka lain tai muiden säännösten mukaan kuuluvat poliisin, turvallisuuspoliisin tai muiden lainvalvontaviranomaisten rikostorjunta- tai estämistoimivaltaan.

Puolustelutiedustelutoiminnasta vastaavat viranomaiset saavat kuitenkin antaa tukea muille lainvalvontaviranomaisille rikosten torjunta- tai ehkäisytoiminnassa. Tältä osin lain esitöissä todetaan, että turvallisuuspoliisi on nykyisin monilta osin tiedustelupalvelunomaista ja suuntautuu myös ulkomailla harjoitettavaa Ruotsin turvallisuutta vaarantavaa toimintaa koskevien tietojen hankintaan. Tämän tehtävänsä puitteissa turvallisuuspoliisin on voitava hyödyntää myös tiedustelusta vastaavien viranomaisten tiedonhankintakapasiteettia.

Kansallinen operatiivinen poliisiviranomainen ja suojelupoliisi voivat suunnata signaalitiedusteluviranomaisen toimintaa. Henkilötietojen käsittelyä FRA:ssa tarkentavan asetuksen nojalla tietyille turvallisuusviranomaisille on säädetty mahdollisuudesta päästä suoraan FRA:n tietokannan tiedusteluraportteja sisältäviin osiin.

Kansainvälinen yhteistyö

Puolustustiedustelutoimintaa harjoittavat viranomaiset voivat hallituksen tarkempien määräysten mukaan, laissa annetuin edellytyksin, tehdä yhteistyötä tiedustelutoiminnan alalla muiden maiden ja kansainvälisten organisaatioiden kanssa.

FRA saa signaalitiedustelulain 1 §:n 2 momentin 3 kohdan mukaisen terrorismiin ja rajat ylittävän törkeään rikollisuuteen liittyen tehdä signaalitiedusteluun liittyvää kansainvälistä yhteistyötä muiden maiden ja kansainvälisten organisaatioiden kanssa. Yhteistyön edellytys on, että sen tavoitteena on palvella Ruotsin valtiojohtoa ja kansallista turvallisuutta. Tiedot, joita viranomainen antaa muille maille ja kansainvälisille organisaatioille, eivät saa vahingoittaa Ruotsin etua.

Puolustusvoimien radiolaitos ilmoittaa yhteistyön aloittamista ja jatkamista koskevista kysymyksistä puolustusministeriölle (Försvarsdepartementet). Toiminnan aikana on myös ilmoitettava puolustusministeriölle yhteistyössä esiin tulevista tärkeistä kysymyksistä.

Valtion tiedustelutarkastus (SIUN) vastaa tiedustelutoiminnan tarkastamisesta ja valvonnasta. SIUN valvoo lainsäädännön noudattamista, puolustustiedustelun kohdentamista ja tiedonhankinnassa käytettyjä menetelmiä.

Vain valvontaviranomaisena toimivalla valtion tiedustelutarkastuksella on pääsy operaattoreiden yhteyspisteisiin viemään tietoliikenteeseen. Sen tehtävänä on erotella ja luovuttaa FRA:lle pääsy vain tuomioistuimen luvassa yksilöityihin kaapelin kuituihin. FRA:n suorittamat haut kohdistuvat

näihin kuituihin. FRA raportoi signaalitiedustelulla hankitut tiedot toimeksiantajalle sekä laissa määritellyin edellytyksin muillekin viranomaisille.

SIUN:n suorittama valvonta koskee signaalitiedustelulain 10 §:n mukaan etenkin signaalitiedustelun hakuehtojen käyttöä, tietojen hävittämistä ja raportointia. Se voi myös määrätä tiedustelutoimenpiteen lopetettavaksi ja tiedot tuhottaviksi, mikäli toiminta ei ole ollut luvan mukaista. Valtion tiedustelutarkastus voi luonnollisen henkilön pyynnöstä tarkastaa, onko tämän viestejä seurattu ja onko mahdollinen seuranta ollut lain mukaista.

FRA:ssa toimii tietosuojaneuvosto (Integritetsskyddsråd), jonka tehtävänä on valvoa yksityisyyden suojan toteutumista. Neuvosto raportoi FRA:n johdolle ja tarvittaessa valtion tiedustelutarkastukselle. Tietosuojavaltuutettu (Datainspektion) valvoo yksityisyydensuojan toteutumista myös FRA:n toiminnassa. Signaalitiedustelulla hankittujen henkilötietojen käsittelystä säädetään erillisessä laissa. Lisäksi signaalitiedustelua valvovat eduskunnan oikeusasiamies ja oikeuskansleri.

Parlamentaarinen edustus tiedustelun valvonnassa toteutuu SIUN:n kautta, jonka jäsenet nimittää hallitus. Puolueiden eduskuntaryhmät voivat vaikuttaa SIUN:in kokoonpanoon, joka muodostuu puheenjohtajasta, varapuheenjohtajasta ja viidestä jäsenestä. Hallitus nimittää jäsenet puolueiden eduskuntaryhmien asettamien ehdokkaiden joukosta. Nykyisin SIUN:ssa on jäseniä sosiaalidemokraattisesta työväenpuolueesta (Socialdemokratiska arbetarepartiet), maltillisesta kokoomuksesta (Moderata samlingspartiet) ja liberaaleista (Liberalerna). Hallitus jättää vuosittain kirjelmän eduskunnalle. Kirjelmässä annetaan selostus seurannan ja tarkastusten tuloksista puolustustiedustelun signaalitiedustelutoiminnassa edellisenä vuotena.

2.3.2.2 Norja

Norjan ulkomaan tiedustelupalveluna toimii Etterretningstjenesten (E-tjenesten), jonka tehtävistä ja toimivaltuuksista säädetään laissa ja asetuksessa tiedustelupalvelusta (Lag om Etterreningstjenesten, Instruks om Etterretningstjenesten). Norjassa ei ole kotimaan turvallisuuspalvelua, vaan maan sisäisestä kansallisen turvallisuuden ylläpitämisestä vastaa turvallisuuspoliisi Politiets sikkerhetstjeneste (PST). E-tjenestenin ja PST:n välisestä yhteistyöstä on säädetty oma asetuksensa (Instruks om samarbejdet mellom Etteretningstjenesten og Politiets sikkerhets).

Ohjaus

Tiedustelupalvelu on osa Norjan puolustusvoimia. Puolustusvoimien komentaja on tiedustelupalvelun päällikön suora esimies. Tiedustelupalvelun päällikkö toimii puolustusvoimien komentajan neuvonantajana tiedustelua koskevissa asioissa.

Tiedustelupalvelun poliittisesta ohjauksesta ja toiminnan valvonnasta vastaa puolustusministeriö. Tiedustelupalvelu pitää ministeriön tietoisena toiminnastaan ja saa siltä toimeksiantoja. Ohjaus, valvonta ja raportointi tapahtuvat puolustusvoimien komentajan kautta.

Tiedustelupalvelu on velvoitettu esittelemään eräät tärkeät asiat puolustusministeriön päätöksentekoa varten. Ministeriön päätettäviä asioita ovat yhteistyön aloittaminen uusien kansainvälisten kumppanien kanssa, miehitysvalmiuden järjestäminen, poliittisesti arkaluontoisiin niin sanottuihin erityisiin tiedusteluoperaatioihin ryhtyminen sekä muut erityisen tärkeät tai periaatteellisesti merkittävät asiat.

Muut ministeriöt ja viranomaiset voivat puolustusministeriön luvalla antaa toimeksiantoja tiedustelupalvelulle.

Tiedustelupalvelun tehtävä

Tiedustelupalvelun yleisenä tehtävänä on hankkia, työstää ja analysoida tietoa, joka koskee Norjan etuja suhteessa vieraisiin valtioihin, organisaatioihin ja yksilöihin, sekä laatia uhka- ja tiedusteluarvioita tärkeiden kansallisten etujen turvaamiseksi. Laki sisältää luettelon turvattavista kansallisista eduista. Sellaisia ovat muun muassa Norjan ulko-, puolustus- ja puolustuspolitiikan muotoilu, valmiussuunnittelu ja puolustusvoimien rakenteiden kehittäminen sekä tiedonsaanti kansainvälisestä terrorismista, rajat ylittävistä ympäristöongelmista ja joukkotuhoaseista. Luettelo ei ole tyhjentävä, ja tiedustelupalvelun kunakin ajankohtana turvaamat kansalliset edut riippuvat Norjan turvallisuustoimintaympäristössä tapahtuvista muutoksista. Päätehtäväksi tiedustelupalveluasetus kuitenkin säätää tiedonhankinnan sellaisista muiden valtioiden poliittisista ja yhteiskunnallisista kehityksistä, aikeista ja sotilaallisista kyvyistä, jotka voivat muodostaa uhkan Norjan turvallisuudelle. Priorisoiduksi tehtäväksi asetus säätää tiedustelutuen antamisen kansainvälisiin sotilasoperaatioihin osallistuville norjalaisille joukko-osastoille. Siviiliaiheisiin kohdistuvien tiedustelutehtävien keskinäisestä priorisoinnista päättää puolustusministeriö neuvoteltuaan asiasta tiedustelupalvelun sekä tiedustelutietoa tarvitsevien muiden viranomaisten kanssa.

Tiedonhankintakeinot ja niiden käytöstä päättäminen

Tiedustelupalvelun tiedonhankintakeinoista tai sen käyttämistä henkilötiedustelun ja teknisen tiedustelun menetelmistä ei ole lainkaan sääntelyä. Se seikka, että tiedustelupalvelu ylipäätään voi käyttää salaisia tiedonhankintakeinoja, on vain epäsuorasti pääteltävissä lainsäädännöstä. Tiedustelupalveluasetusta täydennettiin vuonna 2013 säännöksillä ulkomailla oleskeleviin norjalaisiin henkilöihin kohdistuvan tiedonkeruun edellytyksistä. Säännökset eivät sinänsä täsmennä tiedonkeruun keinoja, vaan ne asettavat rajoituksia sille, missä tarkoituksessa ja missä olosuhteissa tietoja ulkomailla oleskelevista Norjan kansalaisista voidaan kerätä. Täydentäviin säännöksiin sisältyvän tiedonkeruun määritelmän mukaan tiedonkeruulla kuitenkin tarkoitetaan "valvontaa ja muuta salaista tiedonhankintaa." Salaisen tiedonhankinnan olemassa olo on myös pääteltävissä tiedustelupalvelun ja poliisin turvallisuuspalvelun yhteistyötä koskevan asetuksen säännöksistä, joiden mukaan osapuolten tulee vaihtaa tietoa teknologioiden ja menetelmien kehityksestä sekä antaa toisilleen varusteisiin ja tekniikkaan liittyvää tukea konkreettisissa tiedonhankintaoperaatioissa. Salaisten tiedonhankintakeinojen käyttöön viittaa myös tiedustelupalvelulle asetettu velvoite alistaa poliittisesti arkaluontoisista erityisistä tiedusteluoperaatioista päättäminen ministeriölle.

Raportointi

Tiedustelupalvelulla on velvollisuus pitää puolustusministeriön sekä sen päättämät muut ministeriöt tietoisina Norjan ulkoisen turvallisuustoimintaympäristön muutoksista. Tietojen raportointi suoraan puolustushallinnon ulkopuolisille toimeksiantajille edellyttää puolustusministeriön lupaa.

Yhteistyö rikostorjuntaviranomaisten kanssa

Tiedustelupalvelun hankkimien tietojen luovuttamisesta rikosten estämiseen, paljastamiseen tai selvittämiseen ei ole konkreettista sääntelyä. Tiedustelupalvelun ja poliisin turvallisuuspalvelun välisestä yhteistyöstä on kuitenkin annettu oma asetuksensa. Poliisin turvallisuuspalvelun tehtävänä on estää, paljastaa ja selvittää eräitä kansalliseen turvallisuuteen kohdistuvat rikokset.

Asetus määrää osapuolten välisen tietojenvaihdon ja muun yhteistyön priorisoiduiksi aloiksi terrorismin, joukkotuhoaseiden levittämisen ja laittoman tiedustelutoiminnan torjunnan sekä Norjan tärkeitä etuja koskevat muut olosuhteet. Osapuolten tulee avustaa toisiaan niin konkreettisten tiedonhankintaoperaatioiden toteuttamisessa ja operatiivisten tietojen vaihtamisessa kuin strategisten tietojen analysoinnissa ja uhka-arvioinnissa. Yhteistyön muotoja ovat myös osapuolten toisilleen antama tekninen tuki ja koulutustuki, virkamiesvaihto ja kansainvälinen yhteyshenkilötoiminta. Yh-

teistyön edellytyksenä on, että osapuolet noudattavat omista toimivaltuuksistaan annettuja säännöksiä. Tiedonhankintaoperaatioiden toteuttamiseen liittyvän tuen pyytämisestä ja sen antamisesta päättävät normaalisti palveluiden päälliköt, erityisen tärkeissä asioissa kuitenkin palveluiden toimintaa ohjaavat ministeriöt.

Yhteistyöasetus velvoittaa osapuolet vaihtamaan niin sanottua ylimääräistä tietoa. Ylimääräisellä tiedolla tarkoitetaan tietoa, jonka palvelu on saanut haltuunsa tiedonhankintansa yhteydessä mutta joka ei kuulu sen toimialaan. Ylimääräinen tieto voi olla henkilötietoa, joka esimerkiksi koskee ulkomailla oleskelevia Norjan etuja vaarantavia henkilöitä. Ylimääräisen tiedon luovuttanut osapuoli voi edellyttää, ettei tiedon vastaanottaja luovuta sitä edelleen ilman luovuttajan suostumusta. Tiedustelupalveluasetuksen mukaan tiedustelupalvelu saa luovuttaa tiedonhankintansa yhteydessä saamiaan ylimääräisiä henkilötietoja myös muille norjalaisille viranomaisille kuin poliisin turvallisuuspalvelulle.

Tiedustelupalvelu ei saa Norjan maaperällä kohdistaa salaista tiedonhankintaa Norjan kansalaisiin tai norjalaisiin oikeushenkilöihin. Poikkeuksena tästä tiedustelupalvelu voi kuitenkin kohdistaa salaista tiedonhankintaa sellaisiin Norjassa oleskeleviin norjalaisiin henkilöihin, jotka osallistuvat laittomaan tiedustelutoimintaan vieraan valtion puolesta. Tiedustelupalvelun tiedonhankinnan on tällöin tapahduttava poliisin turvallisuuspalvelun välityksellä tai sen hyväksynnällä.

Tiedustelupalvelun ja avoimen poliisin yhteistyöstä ei ole säännöksiä. Yhteistyöasetuksesta kuitenkin välillisesti ilmenee, että tällaista yhteistyötä on, sillä asetuksen soveltamisalamääräyksen mukaan asetusta ei sovelleta tiedustelupalvelun tulliviranomaisille tai avoimelle poliisille antamaan tukeen tai tiedonluovutuksiin. Asetuksen mukaan tällaiset tiedonluovutukset voidaan kuitenkin kanavoida poliisin turvallisuuspalvelun kautta. Tiedustelupalvelu voi poliisin turvallisuuspalvelun välityksellä asettaa ehtoja sille, kuinka tietojen lopullisena vastaanottajana oleva poliisiyksikkö voi tietoja käyttää, sekä edellyttää, ettei poliisin turvallisuuspalvelu paljasta tietojen olevan peräisin tiedustelupalvelulta.

Kansainvälinen yhteistyö

Tiedustelupalvelulain mukaan tiedustelupalvelu saa ryhtyä tiedusteluyhteistyöhön ja harjoittaa sellaista ulkovaltojen kanssa. Yhteistyösuhteiden avaamisesta uusiin tahoihin päättää puolustusministeriö tiedustelupalvelun esittelystä. Tiedustelupalvelulla ja poliisin turvallisuuspalvelulla on velvoite koordinoida kansainväliset yhteistyösuhteensa.

Tiedustelupalveluasetukseen otettiin vuonna 2013 täydentäviä säännöksiä siitä, millä edellytyksillä tiedustelupalvelu saa luovuttaa Norjan kansalaisia koskevia henkilötietoja ulkomaisille tiedustelupalveluille. Tiedot voidaan luovuttaa, jos tämä on tiedustelupalvelulle säädettyjen tehtävien mukaista ja tiedustelupalvelulla on oikeus tallettaa ne henkilörekisteriinsä. Lisäksi edellytetään, että luovuttaminen tapahtuu Norjan intressissä, että se arvioidaan välttämättömäksi punnittaessa keskenään tärkeiden kansallisten etujen turvaamista ja niitä seurauksia, jotka tiedon kohteena olevalle henkilölle aiheutuu, ja että luovuttaminen on puolustettavaa huomioon ottaen tiedon luonne, tiedon kohdehenkilö sekä tiedon vastaanottajana oleva taho. Tietoihin on luovutuksen yhteydessä liitettävä ehto, että niitä ei saa käyttää perusteena salaiselle tiedonhankinnalle, joka kohdistuu Norjan maaperällä oleskeleviin henkilöihin. Edellä mainitut edellytykset soveltuvat vain silloin, kun luovutetaan Norjan kansalaisten henkilötietoja. Ulkomaalaisia henkilöitä koskevien tietojen luovutukselle ei ole asetettu ehtoja.

Tietoliikennetiedustelua koskeva lainsäädäntöhanke

Norjan puolustusministeri asetti helmikuussa 2016 komitean arvioimaan tarvetta säätää tietoliikennetiedustelusta. Komitea luovutti mietintönsä (Digitalt grenseforsvar (DGF). Lysne II-utvaget. 26 August 2016) puolustusministerille saman vuoden syyskuussa.

Komitea ehdotti mietinnössään tietoliikennetiedustelusta säätämistä, koska kyse sen mukaan on demokraattisen yhteiskunnan ja kansallisen turvallisuuden suojaamiseksi välttämättömästä toimivaltuudesta. Komitean mukaan toimivaltuus tulisi osoittaa E-tjenestenille, ja sitä tulisi voida käyttää tietojen hankkimiseksi muun muassa vakavista kyberuhkista, terrorismista ja Norjaan kohdistetusta vakoilusta. Käyttötarkoitukset tulisi sitoa E-tjenestenin tehtäviin, ja niiden tulisi myös vastata hallituksen vuosittain palvelulle osoittamia tiedusteluprioriteetteja. Tiedusteluprioriteetit eivät ole julkisia, eikä siten ole tiedossa, olisiko esitetty tiedonhankinta luonteeltaan puhtaan uhkaperusteista vai tätä laajempaa.

Komitean ehdottamassa tietoliikennetiedustelussa olisi kyse Norjan rajan ylittävissä tietoliikennekaapeleissa liikkuvan tietoliikenteen suodattamisesta hakuehtojen avulla. Sekä sisältöä kuvaavien että muiden hakuehtojen käyttö olisi toiminnassa sallittua, mutta edellyttäisi tuomioistuimen ennakkohyväksyntää. Komitean kannan mukaan toiminnassa saatava mahdollinen niin sanottu ylimääräinen tieto tulisi kaikissa tapauksissa hävittää. Säilyttää voitaisiin näin ollen ainoastaan sellainen tieto, joka välittömästi liittyy E-tjenestenin tehtäviin ja hallituksen sille osoittamiin tiedusteluprioriteetteihin. Komitea ei ottanut kantaa tällaisten tietojen poliisiviranomaisille luovuttamiseen, mutta totesi, että tietoliikennetiedustelutietojen käyttöä oikeudenkäynnissä todisteena ei tulisi missään olosuhteissa sallia.

Komitean mukaan sellainen tietoliikennetiedustelu, josta säädetään lain tasolla riittävän täsmällisesti, olisi omiaan parantamaan elinkeinoelämän toimintaedellytyksiä Norjassa. Komitea torjui näkemykset, joiden mukaan Norjan pysyminen "tiedusteluvapaana vyöhykkeenä" olisi vetotekijä mitä tulee kansainvälisiin investointeihin. Riittävän tarkkarajainen ja läpinäkyvä lainsäädäntö yhdistettynä tiedusteluviranomaisten tehostuvaan kykyyn torjua Norjaan kohdistuvia kyberuhkia päinvastoin vahvistaisi Norjan kansainvälistä kilpailukykyä ja houkuttelevuutta investointikohteena.

Komitea myös arvioi, että tietoliikennetiedustelusta voidaan säätää tavalla, joka on sopusoinnussa Euroopan ihmisoikeussopimuksesta (EIS) aiheutuvien Norjan kansainvälisten ihmisoikeusvelvoitteiden ja EU-oikeuden tulkintakäytännön kanssa. Tämä edellyttää, että tietoliikennetiedustelua koskevassa mahdollisessa laissa riittävän selkeästi säädetään tietoliikennetiedustelun käyttöperusteista ja sillä saatujen tietojen käsittelystä sekä oikeusturvamekanismeista. Komitea esitti, että tietoliikennetiedusteluun liitettävien oikeusturvajärjestelyjen tulisi olla sekä ennakollisia että jälkikäteisiä. Ennakollinen oikeusturva toteutuisi säätämällä tuomioistuin tietoliikennetiedustelun käytön päätöksentekijäksi. Tuomioistuimen edellytettäisiin hyväksyvän suodatuksessa käytettävien viestin sisältöä kuvaavien hakuehdon käytön. Tietoliikennetiedustelun yhteydessä kertyvä metadataa tallennettaisiin tarkoitusta varten luotavaan tietovarantoon, johon kohdistuvat haut tuomioistuin myös hyväksyisi. Komitean mukaan tuomioistuimen olisi suotavaa olla perehtynyt tiedustelun toimintaympäristöön, E-tjenestenin toimintaan ja teknisiin kysymyksiin, ja sen jäsenten lukumäärän olisi salassapitosyistä tarpeen olla rajattu. Tämä saattaisi perustella erityistuomioistuimen perustamisen.

Jälkikäteisen oikeusturvan varmistamiseksi komitea arvioi tarpeelliseksi sekä laillisuusvalvonnan että osittain myös parlamentaarisen valvonnan vahvistamisen. Komitean mukaan tietoliikennetiedustelun laillisuusvalvontaa varten tulisi perustaa uusi elin ("DGF-tilsynet"), jonka tulisi saada tieto muun muassa kaikista metadatavarastoon tehdyistä hauista, tuomioistuimen tietoliikennetiedustelua varten myöntämistä luvista ja niiden täytäntöönpanosta sekä tietoliikennetiedustelussa käytettävien suodattimien konfiguroinneista. EOS-valtuuskunta, jota edellä todetun mukaisesti ei

voida pitää puhdaspiirteisenä parlamentaarisena valvontaelimenä, valvoisi tietoliikennetiedustelua samalla tavalla kuin muutakin E-tjenestenin toimintaa. DGF-tilsynet olisi velvoitettu toimittamaan sille raporttinsa, ja sillä olisi rajattu pääsy tietoliikennetiedustelua koskeviin tietojärjestelmiin. EOS-valtuuskunta raportoisi Norjan suurkäräjille tietoliikennetiedustelun käytöstä samoin kuin puolustusministeriön siihen kohdistamasta ohjauksesta.

Mietintö sisältää seikkaperäisen EU-tuomioistuimen viimeaikaisten oikeustapausten analyysin. Edellä kuvattujen suuntaviivojen mukaan järjestetyn tietoliikennetiedustelun arvioidaan olevan sopusoinnussa niiden oikeusohjeiden kanssa, jotka sisältyvät tässäkin mietinnössä käsiteltävien tapausten Digital Rights Ireland ym. (C-293/12) ja Schrems (C-362/14) johdosta annettuihin ratkaisuihin. Ratkaisujen nähdään muutenkin soveltuvan vain osaksi tietoliikennetiedusteluun.

Mietintö sisältää myös kansainvälisen vertailun, joka on laajempi joskin yleispiirteisempi kuin se, joka sisältyy tähän hallituksen esitykseen. Vertailuvaltiona ovat Ruotsi, Ranska, Yhdistynyt Kuningaskunta, Kanada, Saksa, Alankomaat, Sveitsi ja Suomi. Komitea toteaa suorasanaisesti lähtevänsä siitä, että monet sellaisetkin maat, jotka eivät ole säätäneet tietoliikennetiedustelusta, käyttävät sitä säädöspohjan puutteellisuudesta huolimatta. Komitean mukaan avointa ja täsmällistä asiasta säätämistä perustelevat niin ihmisoikeuksien huomioiminen kuin taloudellisen toimintaympäristön ennalta-arvattavuuteen liittyvät seikat.

Mietinnöstä ilmenee, että Norjan kansallinen turvallisuusviranomainen hallinnoi suodatukseen perustuvaa tietoturvaloukkausten kansallista havainnointijärjestelmää. Mietintöön sisältyvästä havainnointijärjestelmän kuvauksesta voidaan päätellä, että se toimintaperiaatteiltaan vastaa jäljempänä tässä mietinnössä käsiteltävää Viestintäviraston niin sanottua HAVARO-järjestelmää. Mietinnön mukaan havainnointijärjestelmän mahdollisuudet tunnistaa vakavimpia Norjaan kohdistuvia kyberuhkia on riittämätön, mistä johtuen tietoliikennetiedustelusta säätäminen on välttämätöntä niiltä suojautumiseksi.

2.3.2.3 Tanska

Tanskassa ulkomaantiedustelusta vastaa puolustusvoimien tiedustelupalvelu FE (Forsvarets Efterretningstjeneste), jonka tehtävistä, toimivaltuuksista ja toiminnan valvonnasta säädetään laissa puolustusvoimien tiedustelupalvelusta (Lov om Forsvarets Efterretningstjeneste). Tanskassa ei ole kotimaan turvallisuuspalvelua, vaan maan sisäisestä kansallisen turvallisuuden ylläpitämisestä vastaa rikostorjuntatoimivaltuuksin toimiva turvallisuuspoliisi PET (Politiets Efterretningstjeneste).

Ohjaus

Puolustusvoimien tiedustelupalvelu ei nimestään huolimatta ole puolustusvoimien osa vaan siviiliviranomainen, joka toimii Tanskan puolustusministeriön alaisuudessa ja ohjauksessa. Puolustusministeri voi osoittaa tiedustelupalvelulle tehtäviä, joilla on yhteys sen laissa säädettyyn toimialaan.

Tiedustelupalvelun tehtävä

FE:n laissa säädettyinä tehtävinä on luoda tiedustelullinen perusta Tanskan ulko-, turvallisuus- ja puolustuspolitiikalle, auttaa ehkäisemään ja torjumaan Tanskaan ja Tanskan etuihin kohdistuvia uhkia, ja näissä tarkoituksissa kerätä, analysoida ja raportoida sellaisia ulkomaiden olosuhteita koskevia tietoja, joilla on merkitystä Tanskalle sekä Tanskan eduille ulkomailla. FE toimii myös Tanskan niin sanottuna kansallisena turvallisuusviranomaisena ja kansallisena tietoturvaviranomaisena.

Tiedonhankintakeinot ja niiden käytöstä päättäminen

Tiedustelupalvelun käyttämistä konkreettisista tiedonhankintakeinoista tai niiden käyttöedellytyksistä ei ole varsinaista sääntelyä. Puolustusvoimien tiedustelupalvelusta annetun lain mukaan FE voi kerätä ja hankkia tietoja, joilla voi olla merkitystä sen tiedustelutoiminnalle. Lain esitöiden mukaan tiedonhankinnan kynnys on tietoisesti asetettu varsin matalalle. Esitöiden mukaan tiedustelupalvelun erityisen tärkeänä tehtävänä on havaita uusia tuntemattomia turvallisuusuhkia. Tällaisissa tapauksissa tiedonhankinnan kohde ei ole yksilöitävissä siinä vaiheessa kun tiedonhankintaan ryhdytään. Tiedonhankintaa koskeva säännös on esitöiden mukaan pyritty kirjoittamaan siten, että se mahdollistaa erittäin suurten tietomassojen hankinnan.

Laki ei erottele tiedustelupalvelun tiedustelumenetelmiä. Julkisten lähteiden mukaan tietojen hankinta tapahtuu niin henkilötiedonhankintana, signaalitiedustelun avulla elektronisesti satelliiteista ja tietoliikennekaapeleista kuin myös avoimista lähteistä.

Norjan tavoin myös Tanskassa on hiljattain erikseen säädetty edellytyksistä, joiden nojalla ulkomailla oleskeleviin oman maan kansalaisiin saadaan kohdistaa tiedonhankintaa. Ulkomailla oleviin tanskalaisiin luonnollisiin henkilöihin ja oikeushenkilöihin saadaan kohdistaa tiedonhankintaa, jos on perusteltu syy olettaa, että tiedonhankinnan kohde osallistuu Tanskalle tai sen eduille terrorismin uhan aiheuttavaan toimintaan. Jos tiedonhankinta edellyttää luottamuksellisen viestin suojaan puuttumista, on siihen haettava lupa tuomioistuimelta. Lupahakemuksen on sisällettävä tieto henkilöstä tai henkilöistä, joita tiedonhankinta koskee, sekä olosuhteista, joiden nojalla kohteen voidaan perustellusti olettaa osallistuvan Tanskalle tai sen eduille terrorismin uhan aiheuttavaan toimintaan.

Lupamenettelyä sovelletaan vain tapauksiin, joissa tiedonhankintaa on tarve kohdistaa Tanskan kansalaiseen. Ulkomaalaisten luonnollisten tai oikeushenkilöiden luottamukselliseen viestintään puuttuminen ei edellytä tuomioistuimen lupaa.

Raportointi

Tiedustelupalvelulla on velvollisuus pitää puolustusministeriö jatkuvasti tietoisena toimialansa tapahtumista ja kehityksistä, jotka vaikuttavat Tanskaan ja sen etuihin, sekä seikoista, jotka merkittävästi vaikuttavat tiedustelupalvelun omaan toimintaan. Lisäksi sen on informoitava ministeriötä käsittelemistään merkittävämmistä yksittäisistä asioista. Muusta raportoinnista ei ole säädetty.

Yhteistyö rikostorjuntaviranomaisten kanssa

Poliisin turvallisuuspalvelu PET vastaa kansallista turvallisuutta vaarantavien rikosten, muun muassa terrorismirikosten sekä valtiopetos- ja maanpetosrikosten, estämisestä, paljastamisesta ja selvittämisestä.

Tiedustelupalvelu ja poliisin turvallisuuspalvelu saavat luovuttaa toisilleen henkilö- ja muita tietoja, jos luovuttamisella voi olla merkitystä jommankumman osapuolen tehtävien suorittamiselle. Tarkoituksena on, ettei osapuolten tarvitsisi jokaisen yksittäisen tiedonluovutustapahtuman yhteydessä arvioida erikseen sitä, onko tiedonluovutus välttämätön. FE:tä ja PET:iä koskevien lakien säätämistä esittäneen valtiollisen mietinnön mukaan palveluiden tehtävät ovat niin läheisesti sidoksissa toisiinsa, että tietojen luovuttaminen niiden välillä on pitkälti rinnastettavissa viranomaisen sisäiseen tietojen luovuttamiseen.

Tiedustelupalvelu saa luovuttaa Tanskan kansalaisia koskevia tietoja muille poliisiyksiköille kuin poliisin turvallisuuspalvelulle, jos tietojen luovuttamisella voi olla merkitystä tiedustelupalvelulle itselleen säädettyjen tehtävien hoitamisen kannalta. Samoin edellytyksin se voi luovuttaa tällaisia tietoja muillekin kotimaan viranomaisille.

Kansainvälinen yhteistyö

Laki ei sisällä tiedustelupalvelun kansainvälistä yhteistyötä koskevaa sääntelyä. Lain esityöt toteavat Tanskan pienenä maana olevan täysin riippuvainen ulkomaisten kumppanien tiedoista, minkä johdosta tiedustelupalvelun on tehtävä tiivistä operatiivista yhteistyötä muiden valtioiden turvallisuus- ja tiedustelupalveluiden kanssa. Tiedustelupalvelun oikeutta luovuttaa Tanskan kansalaisia koskevia tietoja muille valtioille ja kansainvälisille järjestöille on rajattu siten, että tietojen luovuttamisella tulee voida olla merkitystä tiedustelupalvelulle säädettyjen tehtävien hoitamisen kannalta. Tietoja voidaan näin ollen luovuttaa ulkomaille samoin edellytyksin kuin kotimaan viranomaisille.

2.3.2.4 Saksa

Saksan ulkomaan tiedustelupalveluna toimii Bundesnachrichtendienst (BND), joka vastaa sekä siviili- että sotilaallisia uhkia koskevasta ulkoisesta tiedonhankinnasta. Kotimaan turvallisuuspalvelun tehtävät on jaettu siten, että liittovaltion siviiliturvallisuuspalveluna toimii Bundesverfassungsschutz (BfV) ja sotilaallisena turvallisuuspalveluna Militärischer Abschirmsdienst (MAD). Kaikkien edellä mainittujen toimijoiden tehtävistä ja toimivaltuuksista säädetään omissa laeissaan, joskin BND:n ja MAD:n toimintaa koskevat lait toimivaltuuksien osalta laajasti viittaavat BfV:n toimintaa koskevaan lakiin. Toimivaltuussääntelyn kannalta suurta merkitystä on myös posti- ja telesalaisuuden rajoittamisesta annetulla lailla (G10-laki; Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses), joka sisältää kaikkia sellaisia tiedustelumenetelmiä koskevan sääntelyn, joilla turvallisuus- ja tiedustelupalvelujen tiedonhankinta puuttuu luottamuksellisen viestin sisältöön.

Saksa on liittovaltio, jossa liitolla ja osavaltioilla on jaettu toimivalta sisäasioihin liittyvissä kysymyksissä. Tästä seuraa, että Saksassa on liittovaltion siviiliturvallisuuspalvelu BfV:n ohella jokaisessa osavaltiossa oma siviiliturvallisuuspalvelunsa (Landesverfassungsschutz). Ulko- ja puolustusasiain kuuluessa liittovaltion yksinomaiseen toimivaltaan, ei osavaltioilla ole omia ulkomaan tiedustelupalveluita tai sotilaallisia turvallisuuspalveluita.

Ohjaus

Ulkomaan tiedustelupalvelu BND toimii liittokanslerinviraston alaisuudessa ja ohjauksessa. Ohjauksesta vastaa liittokanslerinviraston esikunnassa toimiva tiedustelukoordinaattori. Liittovaltion siviiliturvallisuuspalvelu BfV vastaavasti toimii liittovaltion sisäministeriön ja sotilaallinen turvallisuuspalvelu MAD liittovaltion puolustusministeriön alaisuudessa ja ohjauksessa. Osavaltioiden turvallisuuspalvelut eivät ole alisteisia liittovaltion turvallisuuspalvelulle, vaan kukin toimii oman osavaltionsa sisäministeriön alla. Toimivallan jaon vuoksi liittovaltion turvallisuuspalvelun ja osavaltioiden turvallisuuspalveluiden yhteistyöstä on säädetty erikseen.

Ministeriöiden ohjaustoimivallan käytöstä ei ole laeissa tarkempia säännöksiä. Muiden kuin luottamuksellisen viestin suojaan puuttuvien salaisten tiedonhankintakeinojen käytön edellytyksistä ja päätöksentekomenettelyistä ei säädetä laissa vaan tiedustelu- ja turvallisuuspalveluiden ohjesäännöissä, joiden antajina ovat toiminnasta vastaavat ministeriöt. Ohjesääntöjen, jotka ovat salassa pidettäviä, antamista voidaan jo sinänsä pitää tärkeänä ohjaustoimivallan muotona. Voitaneen lisäksi olettaa, että ohjesäännöt sisältävät tarkempia määräyksiä siitä, kuinka turvallisuus- ja tiedustelupalveluita konkreettisesti ohjataan.

Huomionarvoinen ohjauksen muoto on se, että turvallisuus- ja tiedustelupalveluiden toiminnasta vastaavat ministeriöt osallistuvat luottamuksellisen viestin suojaan puuttuvien salaisten tiedonhankintakeinojen käyttöä koskevaan päätöksentekoon. Ohjaava ministeriö hyväksyy ennakkoon esimerkiksi telekuuntelua ja tietoliikennetiedustelua koskevat hakemukset ennen kuin ne - tiedonhankintakeinosta riippuen - ohjataan laillisuusvalvontaviranomaisen tai parlamentaarisen valvontaviranomaisen lupamenettelyyn.

Tiedustelupalvelun tehtävä

BND:n laissa säädettynä tehtävänä on hankkia ja analysoida tiedustelutietoa, jolla on merkitystä Saksan ulko- ja turvallisuuspolitiikan kannalta. Ulkomaiden tapahtumia koskevien ulko- ja turvallisuuspoliittisesti merkityksellisten tietojen hankkimisen yleisenä edellytyksenä on, ettei niitä voida hankkia muilla tavoilla ja ettei mikään muu viranomainen ole vastuussa niiden hankkimisesta.

BfV:n ja osavaltioiden turvallisuuspalveluiden lakisääteisenä tehtävänä on hankkia ja analysoida tiedustelutietoa demokraattisen yhteiskuntajärjestyksen ja perustuslaillisen järjestyksen vastaisesta toiminnasta samoin kuin liittovaltion ja osavaltioiden olemassaoloa ja turvallisuutta vaarantavasta toiminnasta. Lisäksi niiden tulee hankkia ja analysoida tietoja vieraiden valtioiden puolesta harjoitettavasta tiedustelu- ja muusta Saksan turvallisuutta horjuttavasta toiminnasta, Saksan ulkoisia turvallisuusetuja vaarantavista väkivaltaisista pyrkimyksistä sekä kansainvälisen yhteisymmärryksen tai kansojen rauhanomaisen rinnakkaiselon vastaisista hankkeista. Tällaisia hankkeita edistävät yhteenliittymät on kielletty toisen maailmansodan päättymisen jälkeen säädetyssä Saksan perustuslaissa.

Sotilaallinen turvallisuuspalvelu MAD hankkii ja analysoi tiedustelutietoja samankaltaisista uhkista kuin BfV edellyttäen kuitenkin, että kyseiset uhkat kohdistuvat puolustusministeriön hallinnonalan henkilöstöön, yksiköihin tai laitoksiin ja että uhkan takana on puolustusministeriön hallinnonalan työntekijä. Lisäksi MAD:in tehtävänä on hankkia ja analysoida tietoja puolustusministeriön hallinnonalan henkilöstön mahdollisesta osallistumisesta kansainvälisen yhteisymmärryksen tai kansojen rauhanomaisen rinnakkaiselon vastaisiin hankkeisiin. MAD:in ensisijaisena tehtävänä on näin ollen havaita ja torjua sellaisia uhkia, jotka kumpuavat Saksan puolustushallinnon sisältä. Lisäksi sen tehtävänä on arvioida puolustushallinnon alaisten yksiköiden ja tukikohtien samoin kuin Saksaan sijoitettujen NATO:n tukikohtien turvallisuutta siihen katsomatta, minkä tahon toiminta sitä mahdollisesti vaarantaa. Viimeksi mainittuun tehtävään ei liity omia tiedonhankintatoimivaltuuksia, vaan kyse on muilta tahoilta saatujen tietojen analysoimisesta.

Tiedonhankintakeinot ja niiden käytöstä päättäminen

Saksan lainsäädäntö jakaa tiedustelu- ja turvallisuuspalveluiden salaiset tiedustelumenetelmät sellaisiin, joilla ei puututa Saksan perustuslain erityisesti suojaamaan luottamuksellisen viestin sisältöön, ja sellaisiin, joilla siihen puututaan. Ensin mainittuun ryhmään kuuluvista niin sanotuista yleisistä tiedustelumenetelmistä säädetään tiedustelu- ja turvallisuuspalveluiden toimintaa koskevissa erityslaeissa sekä niissä ohjesäännöissä, jotka ohjaavat ministeriöt ovat alaisilleen palveluille antaneet. Jälkimmäiseen ryhmään kuuluvista eli luottamuksellisen viestin sisältöön puuttuvista tiedustelumenetelmistä säädetään yhteisesti kaikkien palveluiden osalta niin sanotussa G10-laissa.

BfV-lain 8 § on yleisten tiedustelumenetelmien käyttöä koskeva perussäännös. Sen mukaan turvallisuuspalvelu voi hyödyntää sellaisia salaisia tiedonhankintamenetelmiä kuin avustajien käyttö ja ohjaaminen, soluttautuminen, tekninen katselu ja kuuntelu sekä väärien asiakirjojen ja rekisterikilpien käyttö, jos tarvittavat tiedot eivät ole saatavissa yksityisyyteen vähemmän puuttuvin keinoin. Säännöksen sisältämä luettelo salaisista tiedonhankintamenetelmistä on esimerkinomainen. Konkreettisemmin tiedonhankintamenetelmistä sekä niiden käyttöedellytyksistä ja käyttöä koskevasta päätöksenteosta määrätään BfV:n ohjesäännössä, jonka liittovaltion sisäministeri hyväksyy ja toimittaa tiedoksi parlamentaariselle valvontaelimelle. BfV:n ohjesääntö ei ole julkinen asiakirja.

BfV-lain 8a § ja 9 § sisältävät joitain erityissäännöksiä turvallisuuspalvelun tiedonsaantioikeuksista ja teknisistä tiedonhankintamenetelmistä. Ensin mainittu säännös koskee BfV:n oikeutta saada asiakastietoja lentoyhtiöiltä, pankeilta ja muilta rahoituslaitoksilta, postipalveluita tarjoavilta yrityksiltä sekä telepalveluntarjoajilta näitä sitovien salassapitosäännösten estämättä. Myös niin sanotut takautuvat televalvontatiedot kuuluvat tiedonsaantioikeuden piiriin. Tietojen pyytäminen posti- ja

teleyrityksiltä edellyttää BfV:n päällikön tai hänen sijaisensa päätöstä, matkustaja- sekä pankkitietojen pyytämistä koskeva päätöksenteko tapahtuu alemmalla tasolla. BfV-lain 9 §:n mukaan turvallisuuspalvelu saa kohdistaa salaista kuuntelua ja katselua asumiseen käytettävään tilaan vain silloin, kun tämä on välttämätöntä välittömän vaaran torjumiseksi ja kun poliisi ei voi ajoissa toimenpiteeseen ryhtyä. Päätöksen asuntokuuntelusta tai -katselusta tekee turvallisuuspalvelun päällikkö tai hänen sijaisensa ja sen vahvistaa käräjäoikeus. Myös matkapuhelimen paikantamista koskeva sääntely sisältyy BfV-lain 9 §:ään.

BND:n ja MAD:n toiminnasta annettujen lakien säännökset yleisistä tiedustelumenetelmistä viittaavat edellä selostettuun BfV-lain sääntelyyn. BND:llä on oikeus omalla toimialallaan käyttää BfV-lain 8, 8a ja 9 §:ssä sekä tarkemmin omassa ohjesäännössään säädeltyjä tiedustelumenetelmiä. MAD:lla on omalla toimialallaan samankaltainen oikeus, joskin olennaisesti suppeampana.

Saksan perustuslain 10 §:n mukaan luottamuksellisen viestin suoja on loukkaamaton, ja siihen voidaan säätää rajoituksia ainoastaan lailla. Tämän johdosta luottamuksellisen viestinnän sisältöön kohdistuvia tiedustelumenetelmiä koskeva sääntely on koottu omaan erillislakiinsa, G10-lakiin, josta kaikki palvelut ammentavat toimivaltuutensa.

G10-laki säätää edellytyksistä, joilla turvallisuus- ja tiedustelupalvelut saavat tarkastaa postin välittämiä luottamuksellisia viestejä ja kuunnella sekä nauhoittaa luottamuksellista televiestintää. Näiden toimivaltuuksien käyttö edellyttää toiminnasta vastaavan ministeriön kirjallista lupaa ja laillisuusvalvontaelimen (niin sanottu G10-komissio) kirjallista ennakkohyväksyntää. Kotimaan turvallisuuspalvelut saavat tarkastaa postilähetyksiä ja suorittaa telekuuntelua vain, jos on perusteltua aihetta olettaa jonkun henkilön suunnittelevan tietyn rikoksen tekemistä tai tehneen sellaisen rikoksen. Laki sisältää erittäin mittavan luettelon rikoksia, joita koskevien tietojen hankkimiseksi toimivaltuuksia voidaan käyttää. Rikosten yhteisenä piirteenä on se, että niiden voidaan katsoa kohdistuvan kansalliseen turvallisuuteen. Kotimaan turvallisuuspalvelut voivat käyttää kyseisiä toimivaltuuksia myös, jos henkilön voidaan perustellusti olettaa olevan sellaisen yhteenliittymän jäsen, jonka tarkoituksena on tehdä kansallisen turvallisuuden vastaisia rikoksia. Toimivaltuuksien käytön kohteena voi olla paitsi oletettu rikoksentekijä, myös henkilö, jonka voidaan kohtuudella olettaa olevan tähän viestintäyhteydessä. Toimivaltuuksia voidaan käyttää vain silloin kun tietojen hankkiminen muiden menetelmien avulla olisi mahdotonta tai huomattavasti vaikeampaa. Postilähetysten avaamisen tai telekuuntelun avulla ei saa hankkia tietoja sellaisista seikoista, joista henkilö rikosprosessilain nojalla saa kieltäytyä todistamasta. Myös niin sanotun yksityiselämän ydinalue nauttii korostettua suojaa viranomaisten tiedonhankinnalta. Jos toimenpiteen on syytä olettaa tuottavan ainoastaan yksityiselämän ydinalueeseen liittyvää tietoa, ei siihen saa ryhtyä. Yksityiselämän ydinalue muodostuu henkilön intiimistä yksityiselämästä. Esimerkiksi henkilön perhe-elämä ei vielä sinänsä kuulu hänen yksityiselämänsä ydinalueeseen.

Ulkomaan tiedustelupalvelu BND saa avata postilähetyksiä ja suorittaa telekuuntelua paitsi tiettyjen kansalliseen turvallisuuteen kohdistuvien rikosten ja rikoksentekosuunnitelmien havaitsemiseksi, myös silloin, kun se on välttämätöntä tiedustelupalvelulle BND-laissa säädettyjen tehtävien hoitamiseksi tai tiedon hankkimiseksi ulkomailla olevan henkilön henkeen tai terveyteen kohdistuvasta uhkasta.

G10-lain 5 § koskee viestintäsalaisuuden niin sanotusta strategista rajoittamista (strategische Beschränkungen) eli tietoliikennetiedustelua. Säännöksen mukaan ulkomaan tiedustelupalvelu BND saa liittokanslerinviraston ja liittovaltiopäivien yhteydessä toimivan parlamentaarisen valvontavaliokunnan luvalla suorittaa tietoliikennetiedustelua, jos tämä on välttämätöntä eräiden uhkien havaitsemiseksi ja estämiseksi hyvissä ajoin ennen niiden toteutumista. Tietoliikennetiedustelun käyttöön oikeuttavia uhkia ovat muun muassa Saksaan kohdistuva aseellinen hyökkäys, kansainvälinen terrorismi, sotilas- ja joukkotuhoaseiden kansainvälinen levittäminen, huumausaineiden ammattimainen maahantuonti, euroalueen vakautta horjuttava ulkomailla tapahtuva rahan väären-

täminen, laajamittainen organisoitu ihmissalakuljetus ja ulkomailla olevaan henkilön henkeen tai terveyteen kohdistuva uhka. Tietoliikennetiedustelu perustuu automaattisiin hakuehtoihin, jotka voivat koskea joko viestinnän sisältöä tai sen tunnistamistietoja. Hakuehtoperusteinen seulonta saa kullakin hetkellä kohdistua enimmillään 20 %:iin Saksan kansainvälisestä tietoliikenteestä. Hakuehdot on määriteltävä sekä BND:n kirjallisessa lupahakemuksessa että liittokanslerinviraston ja valvontavaliokunnan myöntämässä kirjallisessa luvassa, jonka enimmäisvoimassaoloaika on kolme kuukautta. Hakuehdot eivät saa yksilöidä yksittäistä teleliittymää eivätkä ne saa koskea yksityiselämän ydinaluetta. Yksityiselämän ydinaluetta koskevat tiedot, jotka tietoliikennetiedustelun yhteydessä mahdollisesti kuitenkin paljastuvat, on hävitettävä. Kaikkien tietoliikennetiedustelulla hankittujen tietojen välttämättömyys on arvioitava kuuden kuukauden välein. Jos tiedot eivät ole välttämättömiä niiden keräämistarkoitusta varten eikä ole perustetta niiden luovuttamiselle muulle viranomaiselle, ne on hävitettävä. Tietoja saadaan luovuttaa kotimaan turvallisuuspalveluille, jos on konkreettista aihetta olettaa, että ne ovat välttämättömiä näille säädettyjen tehtävien hoitamiseksi. Lisäksi tietoja saadaan tietyin edellytyksin luovuttaa vientivalvontaviranomaiselle. Tietojen luovuttamista poliisi- ja syyttäjäviranomaisille sekä ulkomaiden viranomaisille käsitellään erillisten otsikoiden alla tuonnempana.

Telekuuntelusta ja tietoliikennetiedustelusta on ilmoitettava niiden kohteelle sen jälkeen kun tiedonhankintakeinon käyttö on päättynyt. Turvallisuus- ja tiedustelupalvelut voivat kuitenkin lykätä ilmoittamista, jos se vaarantaisi tiedonhankinnan tarkoituksen tai jos ilmoittamisen voidaan arvioida haittaavan liittovaltion tai sen osavaltion yleisiä etuja. Jos ilmoitusta ei ole tehty 12 kuukauden kuluttua siitä, kun tiedonhankintakeinon käyttö päättyi, on ilmoittamisen edellytykset saatettava laillisuusvalvontaviranomaisen (G10-komissio) arvioitavaksi. Komissio päättää tämän jälkeen ilmoituksen lykkäämisen kestosta. Jos ilmoitusta ei ole tehty viiden vuoden kuluttua siitä, kun tiedonhankintakeinon käyttö päättyi, ja perusteet ilmoittamatta jättämiselle yhä sillä hetkellä ja suurella todennäköisyydellä tulevaisuudessakin ovat olemassa, voi G10-komissio yksimielisesti päättää pysyvästä ilmoittamatta jättämisestä.

Raportointi

Kukin turvallisuus- tai tiedustelupalvelu raportoi toimintaansa ohjaavalle ministeriölle. Raportointivelvoitteiden täyttämistä koskeva tarkempi sääntely sisältyy turvallisuus- ja tiedustelupalveluiden salassa pidettäviin ohjesääntöihin. Raportoinnin osalta on tosin myös syytä huomata, että niin ohjaavat ministeriöt kuin parlamentaarinen valvontaelin ja laillisuusvalvontaelin ovat osallisina salaisten tiedustelumenetelmien käyttöä koskevassa päätöksenteossa. Ne saavat näin ollen myös tätä väylää pitkin jo ennakkoon tiedon eräistä turvallisuus- ja tiedustelupalveluiden yksittäisistä operaatioista.

Yhteistyö rikostorjuntaviranomaisten kanssa

Eri tiedustelu- ja turvallisuuspalveluiden toiminnasta annetut lait toteavat nimenomaisesti, että palveluilla ei ole poliisivaltuuksia ja että niillä ei ole oikeutta pyytää poliisia suorittamaan puolestaan sellaisia toimia, joiden suorittamiseen niillä ei itse ole oikeutta. Turvallisuus- ja tiedustelupalveluiden sekä rikostorjuntaviranomaisten välinen tiedonkulku on toisaalta säännelty yksityiskohtaisesti.

Turvallisuus- ja tiedustelupalveluiden velvoite ilmoittaa rikoksista syyttäjä- ja poliisiviranomaisille määrittyy BfV-lain 20 §:n mukaan, johon säännökseen myös sotilasturvallisuuspalvelu MAD:n ja ulkomaan tiedustelupalvelu BND:n toiminnasta annetut lait suoraan viittaavat. Säännöksen mukaan turvallisuus- ja tiedustelupalveluilla on oma-aloitteinen velvollisuus luovuttaa syyttäjälle ja poliisiviranomaisille kaikki sellaiset tiedot, joita voidaan perustellusti olettaa tarvittavan valtioon kohdistuvien rikosten estämisessä, selvittämisessä ja syyttämisessä. Valtioon kohdistuvia rikoksia ovat eräiden laissa erikseen mainittujen rikosten ohella kaikki sellaiset rangaistavat teot, joiden voidaan olettaa kohdistuvan liittovaltion tai sen osavaltion perustuslailliseen yhteiskuntajärjestyk-

seen, olemassaoloon tai turvallisuuteen taikka Saksan ulkoiseen turvallisuuteen. Ilmoitusvelvollisuus koskee näin ollen sellaisia rikoksia, joiden laajasti voidaan katsoa liittyvän turvallisuus- ja tiedustelupalveluiden omiin lakisääteisiin toimialoihin. Poliisiviranomaisilla on toisaalta oikeus pyytää ja saada tällaisten rikosten estämiseksi tarvittavia tietoja turvallisuus- ja tiedustelupalveluilta. Näiden ei kuitenkaan tarvitse oma-aloitteisesti eikä pyynnöstäkään luovuttaa rikoksen estämiseksi, selvittämiseksi tai syyttämiseksi tarvittavia tietoja, jos esimerkiksi huomattavat turvallisuusedut perustelevat niiden luovuttamatta jättämisen.

Velvoite luovuttaa tietoja ei ole yksipuolinen, sillä syyttäjä-, poliisi- ja tulliviranomaisilla samoin kuin liittovaltion viranomaisilla yleisesti on velvollisuus omasta aloitteestaan informoida turvallisuus- ja tiedustelupalveluita uhkista, jotka kuuluvat niiden toimialaan. Turvallisuus- ja tiedustelupalveluilla on toisaalta oikeus pyytää ja saada uhkatietoa rikostorjuntaviranomaisilta ja liittovaltion viranomaisilta.

Molemminpuolisen tietojen luovuttamisen lisäksi turvallisuusviranomaiset ja rikostorjuntaviranomaiset voivat perustaa yhteisiä projektikohtaisia henkilörekistereitä silloin kun niihin talletettavat tiedot liittyvät molempien osapuolten tehtäviin. Projektikohtaisia henkilörekistereitä voidaan perustaa vain määräajaksi.

Luottamuksellisen viestin sisältöön kohdistuvien tiedustelumenetelmien avulla saadun tiedon luovuttaminen rikostorjuntaviranomaisille on säännelty erikseen G10-laissa. Telekuuntelun tai tietoliikennetiedustelun avulla saatu tieto saadaan luovuttaa syyttäjä- tai poliisiviranomaiselle vain laissa tyhjentävästi luetteloitujen rikosten estämistä, selvittämistä tai syyttämistä varten. G10-lain sisältämät luettelot niistä rikoksista, jotka perustelevat tiedon luovuttamisen, ovat sinänsä erittäin laajat. Tietoliikennetiedustelusäännöksen yhteydessä esiintyvä rikosnimikeluettelo on jossain määrin suppeampi kuin telekuuntelusäännöksen yhteydessä esiintyvä luettelo. Molempiin luetteloihin sisältyvien rikosten voidaan katsoa kohdistuvan kansalliseen turvallisuuteen.

Kansainvälinen yhteistyö

Turvallisuus- ja tiedustelupalveluiden toiminnasta annetut lait eivät sisällä kansainvälisen yhteistyön yleistä sääntelyä. Sen sijaan ne sääntelevät edellytykset, joilla palvelut voivat luovuttaa henkilötietoja ulkomaisille yhteistyöviranomaisille.

BfV-lain 19 §:n ja siihen viittaavien MAD- ja BND-lakien asiaankuuluvien säännösten mukaan turvallisuus- ja tiedustelupalvelut saavat luovuttaa henkilötietoja ulkomaan viranomaiselle tai kansainvälisille organisaatioille jos henkilötietojen luovuttaminen on välttämätöntä tiedon luovuttajalle säädettyjen tehtävien täyttämiseksi tai tiedon vastaanottajan merkittävien turvallisuusetujen suojaamiseksi. Tietoja ei kuitenkaan saa luovuttaa, jos tämä olisi ristiriidassa Saksan ulkopoliittisten etujen tai tiedonluovutuksen kohdehenkilön erittäin merkittävien etujen kanssa. Tiedonluovutustapahtuma on dokumentoitava ja tiedon vastaanottajalle on ilmoitettava, että tietoja saadaan käyttää ainoastaan luovutustarkoitusta varten.

Ulkomaan signaalitiedustelua koskeva uusi lainsäädäntö

BND:n ulkomaan signaalitiedustelutoimivaltuudet kodifioidaan ensi kertaa laissa (Gesetz zur Ausland-Ausland-Fernmedeaufklärung des Bundesnachrichtendienstes), joka tuli voimaan vuoden 2017 alussa.

Uusi laki asettaa ulkomaan signaalitiedustelun edellytykseksi, että se on välttämätöntä liittotasavallan sisäiseen tai ulkoiseen turvallisuuteen kohdistuvien uhkien varhaisvaiheen havaitsemiseksi, liittotasavallan toimintakyvyn turvaamiseksi tai asianomaisten ministeriöiden ulko- ja turvallisuuspoliittisesti merkityksellisiksi luokittelemien tietojen hankkimiseksi. Ulkomaan signaalitiedustelun on

perustuttava hakuehtojen käyttöön. Hakuehdot voivat kuvata niin henkilöitä ja organisaatioita kuin asioitakin. Laki sallii tietyin erityisedellytyksin Euroopan unionin toimielimiin ja unionin jäsenvaltioihin kohdistuvan tiedustelun. Tiedustelulla ei saa loukata yksityiselämän ydinaluetta. Yksityiselämän ydinalueella ei tarkoiteta henkilön perhe-elämää tai sosiaalisia suhteita, vaan tämän nauttiman intimiteetin ytimeen kuuluvia asioita, kuten seksuaalista käyttäytymistä. Laki sisältää nimenomaisen kiellon koskien taloudellista tiedustelua Saksan elinkeinoelämän etujen edistämiseksi (Wirtschaftsspionage), mutta sallii toisaalta talouspoliittisesti merkityksellisten tietojen hankinnan.

Ulkomaan signaalitiedustelun käyttöä koskevaa päätöstä ei aiemmasta poiketen tee tiedustelupalvelu itse, vaan liittokanslerinvirasto. Lisäksi ulkomaan signaalitiedustelun käyttöä koskeva päätös on ennakkoon hyväksyttävä lain myötä perustetun riippumattoman valvontaelimen (Unabhängiges Kontrollgremium) toimesta. Riippumaton valvontaelin koostuu puheenjohtajasta ja kahdesta jäsenestä. Puheenjohtajan ja yhden jäsenen on oltava Saksan liittotasavallan korkeimman oikeuden (Bundesgerichthof) tuomareita ja yhden jäsenen korkeimman oikeuden syyttäjä. Signaalitiedustelua koskevien päätösten hyväksymisen lisäksi elin suorittaa toiminnan jälkikäteistä valvontaa muun muassa laillisuustarkastusten muodossa. Se myös tutkii ulkomaan signaalitiedustelua koskevat kantelut. Riippumaton valvontaelin informoi liittovaltiopäivien valvontavaliokuntaa toiminnastaan vähintään kuuden kuukauden välein.

Laki sisältää ulkomaan signaalitiedustelun puitteissa tehtävää kansainvälistä yhteistyötä koskevan sääntelyn. BND:n on sallittua tehdä yhteistyötä ulkomaalaisten tiedusteluviranomaisten kanssa edellyttäen, että se on välttämätöntä ulkomaan signaalitiedustelun tarkoituksen toteutumiseksi eikä tietoja voida hankkia muulla tavalla. Yhteistyön yksityiskohdat on kirjattava osapuolten väliseen yhteisymmärryspöytäkirjaan. Yhteisymmärryspöytäkirja voivat koskea ainoastaan tiedonhankintaa kansainvälisestä terrorismista, joukkotuho- tai sota-aseiden levittämisestä, ulkomaisten kriisien kehittymisestä, sellaisista ulkomaisista poliittisista, taloudellisista tai sotilaallisista kehityskuluista, joilla voi olla vaikutusta Saksan ulko- tai turvallisuuspolitiikkaan, tai muista edellä mainittuihin asioihin rinnastettavista aiheista. Lisäksi yhteisymmärryspöytäkirja voi koskea Saksan puolustusvoimien tai liittolaisvaltioiden tukemiseksi taikka ulkomailla olevien Saksan tai liittolaisvaltioiden kansalaisten turvallisuustilanteen arvioimiseksi tarpeellista signaalitiedustelua.

2.3.2.5 Alankomaat

Alankomaissa tiedustelutoiminnasta vastaavat yleinen tiedustelu- ja turvallisuuspalvelu (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) ja sotilaallinen tiedustelu- ja turvallisuuspalvelu (Militaire Inlichtingen- en Veiligheidsdienst, MIVD). Palveluiden toiminnasta säädetään vuoden 2002 laissa tiedustelu- ja turvallisuuspalveluista (Wet op de inlichtingen- en veiligheidsdiensten, 2002, jäljempänä WIV-laki).

Ohjaus

Palvelut toimivat ministeriöiden alaisuudessa; yleinen tiedustelupalvelu sisäministeriön ja sotilastiedustelupalvelu puolustusministeriön. Ministerillä itsenäistä on toimivaltaa oman palvelunsa toimintaan liittyen (esim. lupahakemuksiin liittyvä päätöksenteko). Ministereillä on valtuus antaa yksityiskohtaisia sääntöjä organisaatiosta, työskentelytavoista ja hallinnosta.

Siviili- ja sotilastiedustelupalvelujen keskinäisestä yhteistyöstä on laissa velvoittavat säädökset. Lisäksi sisä- ja puolustusministerit neuvottelevat keskenään palveluidensa toiminnan yhteensovittamisesta. Palveluille on yhteinen koordinaattori, jonka tehtävänä on valmistella ministereiden keskinäisiä neuvotteluja ja koordinoida palveluiden tehtävien toteutusta. Koordinaattori vastaa toiminnastaan suoraan Alankomaiden pääministerille.

Tiedustelupalvelujen tehtävät

Palveluiden yleistehtävänä on toimia kansallisen turvallisuuden edistämiseksi. Käytännössä yleinen tiedustelupalvelu keskittyy ei-sotilaallisiin uhkiin ja tilannearvioihin kuten ääriryhmin ja terrorismiin, sotilastiedustelun keskittyessä sotilaallisiin uhkiin ja tilannearvioihin. Palveluilla on valtuudet harjoittaa tiedustelua ja vastatiedustelua. Molemmat palvelut voivat toimia sinänsä kotimaassa ja ulkomailla, mutta sotilastiedustelupalvelu saa käyttää salaisia tiedonhankintakeinoja kotimaassa puolustusministeriön tilojen ulkopuolella vain sisäministerin luvalla. Tehtävänjaosta ja toimivalta-alueista vieraissa valtioissa määrätään hallituksen ohjeistuksella.

Yleisen tiedustelupalvelun tehtävänä on suorittaa tutkimuksia organisaatiosta tai henkilöistä, jotka voidaan epäillä vaaran aiheuttamisesta demokraattiselle oikeusjärjestykselle tai valtion turvallisuudelle, laatia turvallisuusselvityksiä, toimia valtion elintärkeiden etujen turvaamiseksi (esimerkiksi suojella salassa pidettävää tietoa), laatia muita maita koskevia tutkimuksia hallituksen toimeksiannosta, ja laatia uhka- ja riskiarvioita

Sotilastiedustelun tehtävänä on hankkia tietoa muiden valtioiden asevoimien operatiivisen suorituskyvyn arvioimiseksi, suorittaa tutkimuksia seikoista, jotka vaikuttavat tai voivat vaikuttaa kansainvälisen oikeusjärjestyksen ylläpitämiseen tai edistämiseen, laatia turvallisuusselvityksiä, suorittaa tutkimuksia puolustusvoimien operatiivisen suorituskyvyn parantamiseksi (esimerkiksi vahingoittavan toiminnan estämiseksi, liikekannallepanon edistämiseksi), salassa pidettävän tiedon suojeleminen, suorittaa tutkimuksia hallituksen toimeksiannosta sotilaallisesti merkittävistä aiheista ja laatia uhka- ja riskiarvioita.

Tiedonhankintakeinot

Palveluiden erityisistä toimivaltuuksista eli salaisista tiedonhankintakeinoista on säädelty yksityiskohtaisesti. Laissa on lueteltu palveluiden käytettävissä olevat salaiset tiedonhankintakeinot, joita ovat tarkkailu, tekninen tarkkailu, televalvonta, peitetoiminta, salaiset etsinnät, postilähetysten salainen avaaminen, tietoteknisiin ympäristöihin tunkeutuminen ja tietoliikenteeseen kohdistuva tiedustelu. Tietoliikenteeseen kohdistuvan tiedustelun suhteen huomionarvoista on, että laki erottelee kaapelissa kulkevan ja kaapelin ulkopuolella kulkevan tietoliikenteen.

Tietojen käsittelylle asetetut vaatimukset määrittävät erityisten toimivaltuuksien käyttöä ja yhteistyötä rikostorjuntaviranomaisten tai vieraiden valtioiden tiedusteluviranomaisten kanssa. Vaatimukset koskevat tietojen käsittelyn käyttötarkoitussidonnaisuutta, välttämättömyyttä, huolellisuutta, asianmukaisuutta sekä luotettavuutta. Henkilötietojen käsittely saa liittyä vain demokraattisen oikeusjärjestyksen tai valtion turvallisuuden vaarantamiseen liittyvään epäilyyn, henkilön antamaan lupaan, tutkintaan liittyvän välttämättömään syyhyn, tietojen saamiseen vieraan valtion tiedustelu- tai turvallisuuspalvelusta tai moitteettoman tehtävänhoitoon.

Erityisten toimivaltuuksien käyttöä rajoittaa lain 6 artiklan 2 momentti, jonka mukaan yleinen tiedustelupalvelu saa käyttää laissa määriteltyjä erityisiä valtuuksia vain demokraattisen oikeusjärjestyksen vaarantamiseen, valtion turvallisuuteen tai vieraisiin valtioihin liittyviin tutkimuksiin. Vastaavasti sotilastiedustelun toimivaltuudet on sidottu tiedon hankkimiseen vieraiden valtioiden suorituskyvystä, suorituskyvyn parantamiseen ja salassa pidettävän tiedon suojelemiseen lain 7 artiklan 2 momentin mukaisesti.

Erityisten toimivaltuuksien käyttö on sidottu artiklan 31 mukaisiin periaatteisiin. Artiklan mukaan julkisia lähteitä tai muussa virastossa olevaa tietoa on käytettävä ensisijaisesti (toissijaisuusperiaate), palveluiden on käytettävä vähiten haittaa aiheuttavaa tiedonhankintakeinoa (vähimmän haitan periaate), erityisiä valtuuksia ei saa käyttää kohtuutonta haittaa aiheuttaen (kohtuullisuusperiaate) ja käytön oltava oikeassa suhteessa tavoiteltavaan päämäärään nähden (suhteellisuusperiaate).

Artikla 32 edellyttää, että valtuuden käyttö on lopettava välittömästi kun käytön päämäärä on saavutettu tai jos päämäärä voidaan saavuttaa vähemmän haittaa aiheuttavalla keinolla.

Televiestintälain (Telecommunicatiewet) 13.1 artikla asettaa teleoperaattoreille velvoitteen tehdä viestintään liittyvät tekninen toteutus siten, että televalvontaa on mahdollista tehdä. Teleoperaattorit ovat niin ikään velvollisia auttamaan televalvonnan teknisessä toteuttamisessa. Televiestintälain artikla 13.2 a asettaa teleoperaattoreille velvollisuuden säilyttää puhelinliikennedataa 12 kuukautta ja internetliikennedataa 6 kuukautta.

Televiestintälain artiklan 13.6 mukaan teleoperaattorit vastaavat omalla kustannuksellakaan teknisten toimien toteutuksesta, toiminnasta ja ylläpidosta ilman erillistä korvausta. Sitä vastoin teleoperaattorit voivat hakea korvausta niistä henkilö- ja hallintokuluista, jotka aiheutuvat televalvonnan toteutuksesta tai tietopyyntöön vastaamisesta. Tiedustelulain 28 ja 29 artiklat antavat palveluille mahdollisuuden saada tietoja käyttäjästä ja käyttäjän teleliikenteestä teleoperaattoreilta. Tiedot voivat sisältää tietoa käyttäjän perustiedoista, kontakteista, tietoliikenteestä kontaktien kanssa ja käyttäjän tietoliikennesopimuksesta sekä maksuliikenteestä.

Wiv-lakiin ei ole sisällytetty yleistä määräaikaa kerätyn tiedon säilyttämiselle. Poistamista ohjaa yleisluonteisesti 43 artikla, jonka mukaan tutkinnan kannalta merkityksettömät tiedot on poistettava. Artiklan 27 mukaisessa kohdentamattomassa tietoliikennevalvonnassa tallennettua tietoa voidaan säilyttää vuoden ajan valikointia varten. Postilähetysten avaamisesta, tietoliikennevalvonnasta ja tiloihin tunkeutumisesta ilmoitetaan kohdehenkilöille viiden vuoden kuluttua näiden valtuuksien käytön lopettamisesta. Ilmoitusvelvollisuus raukeaa, jos kohdehenkilöä ei voida selvittää tai jos ilmoittaminen voi vaarantaa palvelun menetelmiin, lähteisiin tai kansainvälisiin suhteisiin liittyviä intressejä.

Raportointi

Tiedustelutoiminnasta vastaavat ministerit antavat vuosittain kertomuksen parlamentin (Staten-Generaal) molemmille kamareille palveluiden toiminnasta. Kertomuksessa on mainittava ainakin edeltävän ja tulevan vuoden painopistealueet. Teknisiä tietoja tai tosiasiallista tiedon tasoa ei tarvitse kertoa.

Lisäksi ministereille on asetettu velvoite raportoida parlamentille oma-aloitteisesti tarpeen mukaan. Ainakin hakusanoihin perustuvasta valikoinnista on ilmoitettava luottamuksellisesti parlamentin kummallekin kamarille sekä valvontakomissiolle.

Tiedustelutoimintaa valvoo ulkoinen valvontakomissio (CTIVD), joka valvoo toiminnan lainmukaisuutta, suorittaen tarkastuksia ja raportoiden, sekä käsittelee kanteluita neuvoa antavassa roolissa. Parlamentaarista valvontaa suorittaa parlamentin alahuoneen turvallisuus- ja tiedusteluvaliokunta ja siltä osin, kuin se on julkisissa asiakirjoissa mahdollista edustajainhuoneen sisäasiainvaliokunta.

Yhteistyö rikostorjuntaviranomaisten kanssa

Tiedustelupalveluilla ei ole valtuuksia tutkia rikoksia, vaan palveluiden toiminta keskittyy tiedon keräämiseen ja uhkien analysointiin. Palvelut toimivat yhteistyössä muiden organisaatioiden kanssa.

Yhteistyö rikostorjuntaviranomaisten kanssa on vastavuoroista perustuen tietojen vaihtoon ja tekniseen tukeen. Palvelut voivat antaa syyttäjäviranomaisille sellaisia tietoja, joilla voi olla vaikutusta rikosten selvittämiseen tai syytteen nostamiseen. Tiedon antamisesta päättää ministeri tai tämän nimissä toimiva palvelun päällikkö. Tietojen antamisen on oltava välttämätöntä syyttäjäviranomaisen lakisääteisen tehtävän täyttämiseksi. Esitöiden mukaan palveluiden on punnittava rikoksen

selvittämisintressiä kansallisen turvallisuuden intressiä vastaan. Palveluiden ei tarvitse antaa tietoja, jos tietojen antaminen vakavasti vahingoittaisi palveluiden intressejä. Rikostorjuntaviranomaiset voivat pyytää palveluilta teknistä tukea.

Kansainvälinen yhteistyö

Palvelut toimivat aktiivisessa kansainvälisessä yhteistyössä joko yhteistyösuhteiden ylläpitämisen vuoksi tai palvelun omien lakisääteisten tehtävien suorittamiseksi. Palveluille saavat antaa ja vastaanottaa tietoja (ml. henkilöitä koskevat tiedot) sekä teknistä tukea. Lain esitöiden mukaan palveluiden tulee arvioida yhteistyötä Alankomaiden ulkopolitiikan ja vieraan valtion ihmisoikeustilanteen näkökulmasta. Yhteistyö ei saa olla ristiriidassa palveluiden suojaamien etujen kanssa, eikä yhteistyö saa estää palveluiden lakisääteisten tehtävien moitteetonta hoitamista. Palveluiden päälliköt ylläpitävät yhteisesti suhteita muiden valtioiden tiedustelu- ja turvallisuusviranomaisiin.

Palveluiden on noudatettava samoja sääntöjä antaessaan teknistä apua kuin muutoinkin, koskien myös erityisien valtuuksien käyttämistä. Tuen antamisesta päättää ministeri. Laissa ei nimenomaan säädellä avun pyytämistä muilta tiedustelupalveluilta, mutta palvelut voivat pyytää vieraan valtion tiedustelupalvelua esimerkiksi seuraamaan tiettyä kohdetta vieraassa valtiossa.

Alankomaiden palvelut saavat antaa tietoja ulkomaalaiselle tiedustelupalvelulle sillä ehdolla, että vastaanottava palvelu ei luovuta tietoja kolmannelle osapuolelle. Tämä koskee palveluita myös niiden vastaanottaessa tietoja vieraasta valtiosta. Tästä voidaan poiketa ministerin antamalla luvalla.

Vireillä olevat lainsäädäntöhankkeet Alankomaissa

Vuoden 2002 lain korvaavan lain valmistelu on ollut vireillä vuodesta 2013, jolloin lainsäädäntöä arvioimaan asetettu Dessensin komissio antoi raporttinsa. Vireillä olevan lakiesityksen tarkoitus on antaa palveluille uusia toimivaltuuksia, pidentää kerätyn tiedon säilytysaikaa koskevia säännöksiä, parantaa oikeudellista valvontaa sekä yleisemmin päivittää lainsäädäntöä vastaamaan teknologista kehitystä. Lakiesitys sisältää tietoliikennetiedustelun kehittämisehdotuksia, esimerkiksi erottelu kaapelissa liikkuvan ja kaapelin ulkopuolisen liikenteen välillä lopetettaisiin. Lakiuudistuksessa esitetään myös yhteistyövelvoitetta teleoperaattoreille. Lakiesityksessä erityisien valtuuksien käyttö on sidottu luvan saamiseen uudelta oikeudelliselta toimielimeltä.

Laista äänestettiin parlamentin alahuoneessa 9.2.2017 ja se etenee seuraavaksi äänestykseen parlamentin ylähuoneeseen.

2.3.2.6 Sveitsi

Sveitsin parlamentti hyväksyi syyskuussa 2015 esityksen uudesta tiedustelulaista, joka määrittäisi kansallisen tiedustelupalvelun (Nachrichtendienst des Bundes; NDB) toimenkuvaa ja muuttaisi tiedustelun toimivaltuuksia. Suurimmat muutokset koskevat yksityisissä tiloissa tapahtuvan valvonnan sallimista, sekä maan rajat ylittävän tietoliikenteen valvomista. Sotilastiedustelun toimivaltuuksia muutokset laajentaisivat eräiden viittaussäännösten kautta. Laista järjestettiin kansanäänestys 26.9.2016, jossa laki hyväksyttiin. Uusi tiedustelulaki tulee voimaan 1.9.2017.

Uusi tiedustelulaki korvaa yleislakina voimassa olevat lait sisäisen turvallisuuden turvaamisen keinoista (loi fédérale instituant des mesures visant au maintien de la sûreté intérieure; LIMS) ja siviilitiedustelusta (loi fédérale sur le renseignement civil; LFRC).

Ohjaus

Sveitsin liittoneuvosto ohjaa uuden lain mukaan tiedustelupalvelua poliittisesti. Liittoneuvoston tehtäviin kuuluu muun muassa salassa pidettävän, vähintään neljän vuoden välein uusittavan perustehtävän antaminen, sekä vuosittaisen tarkkailtavien organisaatioiden ja ryhmittymien listan hyväksyminen. Lisäksi liittoneuvosto määrää tarpeelliset toimenpiteet erityisissä uhkatilanteissa.

Tiedustelunpalvelun tehtävä

Uuden lain mukaan tiedustelupalvelun tehtävänä on tunnistaa ja estää ajoissa sisäiseen ja ulkoiseen turvallisuuteen kohdistuvat uhkat, jotka liittyvät terrorismiin, väkivaltaisiin ääriliikkeisiin, vakoiluun, laittomaan sotatarvike- ja asekauppaan ja kriittisen infrastruktuurin suojaamiseen. Tiedustelupalvelun tulee turvata maan etu ja toimintakyky. Tehtäviin kuuluu ulkomaantoimivaltuudet ja tiedustelupalvelun tulee arvioida turvallisuuspoliittisesti merkittäviä tapahtumia ulkomailla. Laki sisältää poikkeuspykälän, joka mahdollistaisi vakavan ja välittömän uhan vallitessa hallituksen päätöksellä lain soveltamisen myös Sveitsin ulkopolitiikan tukemiseksi, perustuslaillisen järjestyksen sekä teollisuuden, talouden ja finanssisektorin suojelemiseksi.

Tiedustelupalvelun päätehtävä on tuottaa ennakkovaroituksia kansallista turvallisuutta uhkaavista tekijöistä poliittista päätöksentekoa varten. NDB palvelee ensisijaisesti hallitusta, ministeriöitä sekä puolustusvoimien johtoa turvallisuuspoliittisena instrumenttina. Lisäksi NDB tukee kantoneja sisäisen turvallisuuden säilyttämisessä, sekä syyttäjäviranomaisia. Valtion tiedustelupalvelun NDB:n lisäksi myös Sveitsin puolustusvoimilla on oma tiedustelupalvelu (Militärischer Nachrichtendienst; MND), jonka kanssa NDB tekee yhteistyötä.

Tiedonhankintakeinot ja niiden käytöstä päättäminen

Puolustusvoimien tiedustelupalvelun tiedustelutehtävästä säädetään laissa puolustusvoimista (Loi Fédérale sur l’armée et administration militaire) ja sitä täsmennetään asetuksessa sähköisestä sodankäynnistä ja radiosignaalitiedustelusta (Ordonnance sur la guerre électronique et l'exploration radio). Sotilastiedusteluviranomainen voi suorittaa signaalitiedustelua edellä mainittujen säännösten nojalla ja siviilitiedusteluviranomaisten radiotiedustelun toimivaltuuksien perusteella. Puolustusvoimien sähköisten operaatioiden keskus (COE) suorittaa signaalitiedustelun Sveitsissä.

Tietoliikennetiedustelua olisi uuden lain mukaan lupa toteuttaa vain, mikäli joko vastaanottaja tai lähettäjä sijaitsee ulkomailla. Tiedustelupalvelu pääsisi käsiksi signaaleista saatuihin tietoihin vain, mikäli ne vastaisivat annettuja hakusanoja. Hakusanat tulisi lain mukaan rajata mahdollisimman vähän yksityisyyden suojaa loukkaaviksi, eivätkä ne saisi sisältää sveitsiläisten luonnollisten tai oikeudellisten henkilöiden nimiä. Mikäli lupa tietoliikennetiedustelulle olisi olemassa, olisivat kaapeli- ja verkko-operaattorit uuden lain mukaan velvoitettuja luovuttamaan signaalit asevoimien alaisuudessa toimivalle COE:lle. Lisäsi COE hankkii tarvittavat tekniset asennukset, jotka ovat tarpeen tehtäviensä suorittamisessa, sekä tekee tarvittavat vaiheet ja testit. Se voi myös ehdottaa toimeksiantonsa puitteissa tiedustelun uudelleen kohdistamista. COE voi tiedustella elektronista säteilyä, joka on peräisin ulkomaisista tietoliikennejärjestelmistä.

Tiedustelupalvelu voi uuden lain mukaan hakea lupaa tiettyihin toimenpiteisiin, mikäli olemassa on konkreettinen, esimerkiksi terrorismista johtuva sisäinen tai ulkoinen uhka. Luvanvaraista olisi posti- ja teleliikenteen valvonta, paikantamislaitteiden asentaminen henkilöihin ja esineisiin ja esineiden paikallistamiseksi, autojen ja tilojen kotietsintä, valvontalaitteiden asentaminen yksityisiin tiloihin sekä tietokonejärjestelmiin ja tietoverkkoihin tunkeutuminen tiedon saamiseksi tai tietoihin käsiksi pääsyn estämiseksi. Ulkomailla sijaitsevaan tietokoneeseen tai tietoverkkoon voitaisiin vaikuttaa siinä tapauksessa, jos niitä käytettäisiin Sveitsin kriittiseen infrastruktuuriin kohdistuviin hyökkäyksiin. Sveitsin maantieteelliset rajat ylittävän tietoliikenteen valvonta tarkkaan määriteltyjen

hakusanojen perusteella. Luvan myöntämisen edellytyksenä näiden keinojen käyttöön muun muassa on, että muut tiedustelutoimet ovat olleet tuloksettomia. Kaapeli- ja verkko-operaattorit ovat oikeutettuja valtion myöntämään rahalliseen korvaukseen, jonka suuruudesta hallitus päättäisi sen mukaan, kuinka paljon kuluja tietojen luovuttaminen elektronisten operaatioiden keskukselle on aiheuttanut.

Uuden lain mukaan lupaa toimenpiteisiin haetaan hallinto-oikeudesta, jonka jälkeen puolustusministeri antaa luvan aloittaa toiminnan konsultoituaan ensin kirjallisesti sekä ulko- että oikeusministeriä. Erityisen merkittävät tapaukset voitaisiin viedä liittoneuvoston käsiteltäväksi. Laki mahdollistaisi myös tiedustelupalvelun johtajan hätätapauksessa hyväksyä kiireellisesti luvanvaraisen valvonnan. Lupaa täytyy kuitenkin välittömästi anoa myös normaalin menettelyn mukaan ja toimenpiteet voitaisiin myös tarvittaessa keskeyttää. Ulkomaan toimivaltuuksien käyttöön luvan antaa aina liittoneuvosto. Kaikkiin liittovaltion viranomaisten tiedustelulain nojalla tekemiin päätöksiin voi hakea muutosta liittovaltion hallintotuomioistuimesta.

NBD voi kirjallisella tai suullisella kyselyllä hankkia valikoiden tietoja, joita se tarvitsee tehtäviensä hoitoon. Se voi lähettää henkilöille kirjallisen kutsun kuulusteluihin, mutta tietojen antamisen vapaaehtoisuudesta tulee kertoa henkilölle, jolta tietoja pyydetään. Tästä poikkeuksena on tiedonhankinta peitetoimintaa käyttäen. Mikäli konkreettisen uhkan havaitsemisen, estämisen tai torjumisen kannalta on välttämätöntä, voi NBD myös vaatia tietoja ja tallenteita a) sellaiselta luonnolliselta henkilöltä tai oikeushenkilöltä, joka hoitaa ammattimaisesti kuljetuksia tai antaa käytettäväksi kuljetusvälineitä tai välittää niitä ja b) turvallisuusinfrastruktuurin, kuten kuvansiirto- ja kuvantallennuslaitteiden, yksityisiltä tarjoajilta.

Lain mukaan lennokkien ja satelliittien käyttö on sallittua. Tiedustelupalvelu voi käyttää ilman erillistä lupaa lisäksi julkisia tietolähteitä (media, yksityisten julkiseksi asettamat tiedot, valtion ja kantonien viranomaisten julkiset rekisterit sekä julkisuudessa esitetyt lausumat), käyttää henkilöitä tietolähteinä, ilmoittaa henkilöitä ja ajoneuvoja poliisin etsintäkuulutusjärjestelmissä ja tarkkailla ja nauhoittaa kuvaa ja ääntä julkisissa tiloissa.

Uusi laki mahdollistaa myös tarvittaessa tiedustelupalvelun johtajan luvalla peitteen luomisen tiedustelupalvelun työntekijän suojelemiseksi. Puolustusministerin myöntämällä luvalla puolestaan voitaisiin työntekijälle luoda peitehenkilöllisyys.

Terroristiorganisaatioita sekä väkivaltaisia organisaatioita voidaan Sveitsissä kieltää harjoittamasta toimintaansa. Uusi tiedustelulaki sisältäisi pykälän, joka mahdollistaisi organisaatioiden kieltämisen kokonaan viideksi vuodeksi kerrallaan. Lain mukaan tiedustelupalvelulla ei ole oikeutta puuttua esimerkiksi poliittiseen aktiivisuuteen tai sananvapauden harjoittamiseen. Poikkeuksen tähän tekee konkreettinen terrorismi- tai radikalisoitumisepäily.

Laissa säädetään myös velvollisuudesta henkilötietojen poistamiseen viimeistään siinä vaiheessa, kun toimenpiteen perusteena olleet epäilyt on voitu sulkea pois. Mikäli terrorismia tai radikalistista toimintaa ei voitaisi todistaa, olisi henkilötiedot poistettava viimeistään vuoden kuluttua tutkinnan aloittamisesta. Puolustusvoimien signaalitiedustelusta on poikkeava säännös tietojen hävittämisen osalta. Viestit on tuhottava 18 kuukauden ja viestien välitystiedot 5 vuoden kuluttua niiden haltuun saamisesta.

Tiedustelupalvelulla on velvollisuus informoida tiedustelutoimenpiteiden kohteena ollutta henkilöä valvonnasta viimeistään kuukauden sisällä valvonnan päättymisestä. Painavasta syystä tiedoksiantoa voitaisiin kuitenkin luvanvaraisesti siirtää tai luopua siitä kokonaan.

Raportointi

Puolustus-, väestönsuoja- ja urheiluministeriö laatii vuosittain suunnitelman tiedusteluviranomaisen toiminnan laillisuuden, tarkoituksenmukaisuuden ja tehokkuuden valvonnasta ja asettaa sisäisen valvontaelimen harjoittamaan sen yleistä valvontaa. Tämä elin informoi ministeriön johtajaa jatkuvasti valvontatoimintansa tuloksista. Sen raportit eivät ole julkisia. Liittoneuvosto edellyttää lain mukaan ministeriön raportoivan sille tiedustelutoiminnasta säännöllisesti.

Tiedustelupalvelun päällikön on lain mukaan erityisesti raportoitava vuosittain peitteiden käytöstä puolustusministeriöön.

Yhteistyö rikostorjuntaviranomaisten kanssa

Lain mukaan tiedustelupalvelun on toimitettava sveitsiläisviranomaisille henkilötietoja, kun sisäisen tai ulkoisen turvallisuuden ylläpitäminen sitä vaatii. Kun NBD:n tiedoista on hyötyä muille viranomaisille rikosoikeudellisessa menettelyssä, rikoksen estämisessä tai yleisen järjestyksen ylläpitämisessä, sen tulee antaa tiedot kyseisten viranomaisten käyttöön huolehtien lähteiden suojelusta. NBD toimittaa rikostorjuntaviranomaisille luvanvaraisin menetelmin hankittuja tietoja vain, jos niissä on konkreettisia viitteitä rikoksesta, jonka syytetoimet voivat antaa aihetta rikosoikeudelliseen toimenpiteeseen. Jatkomenettely tapahtuu rikosprosessilain tai sotarikosprosessilain mukaisesti.

Kansainvälinen yhteistyö

Uusi tiedustelulaki mahdollistaa myös yhteistyön ulkomaalaisten tiedustelupalveluiden ja turvallisuusviranomaisten kanssa muun muassa yhteistyö informaation hankkimiseksi sekä uhkakuvan muodostamiseksi. Yhteistyötä tehdään poliittisen ohjauksen asettamissa rajoissa. Liittovaltion muut viranomaiset sekä kantonien viranomaiset saavat ylläpitää yhteyksiä ulkomaisiin tiedustelupalveluihin tai muihin ulkomaisiin viranomaisiin tässä laissa tarkoitettujen tiedustelutehtävien täyttämiseksi ainoastaan NBD:n suostumuksella tai sen kautta. NBD voi sotilasalan kansainvälisissä yhteyksissä tehdä yhteistyötä armeijan vastuullisten yksiköiden kanssa, pyytää viranomaisilta tietoja ja antaa niille kansainväliseen yhteistyöhön liittyviä toimeksiantoja.

Tiedustelupalvelu voi vastaanottaa ja välittää eteenpäin tarkoituksenmukaisia tietoja, järjestää yhteisiä neuvotteluja ja kokouksia, suorittaa yhteisiä toimia tietojen hankkimiseksi ja arvioimiseksi sekä uhka-arvion laadintaa varten, osallistua kansainvälisiin automatisoituihin tietojärjestelmiin ja hankkii ja toimittaa pyynnön esittäneelle valtiolle tietoja, jotta pystytään arvioimaan, voiko yksittäinen henkilö olla mukana ulkomaan turvaluokitelluissa projekteissa sisäisen tai ulkoisen turvallisuuden alalla tai voiko hän päästä käsiksi ulkomaan turvaluokiteltuihin tietoihin, materiaaleihin tai laitteisiin.

Uuden lain mukaan NBD voi yhteisymmärryksessä Sveitsin ulkoministeriön kanssa lähettää työntekijöitään Sveitsin ulkomaisiin edustustoihin kansainvälisten yhteyksien parantamiseksi. NBD:n työntekijät työskentelevät tämän lain täytäntöönpanoa varten suoraan vastaanottavan valtion ja kolmansien valtioiden toimivaltaisten viranomaisten kanssa.

2.4 Nykytilan arviointi

2.4.1 Yleistä

Kuten nykytilan kuvauksessa on todettu, Suomen turvallisuusympäristö on muuttunut. Tästä johtuen on entistä tärkeämpää, että ylimmällä valtiojohdolla on mahdollisuus saada oikea-aikaista, luotettavaa ja riippumatonta tietoa päätöksenteon tueksi.

Puolustusvoimien tiedustelullisesta tiedonhankinnasta eli sotilastiedustelusta ei ole nimenomaisia säännöksiä laissa. Sotilastiedustelua on käsitelty ainoastaan lain esitöiden tasolla hallituksen esityksessä puolustusvoimalaiksi ja eräiksi siihen liittyviksi laeiksi (HE 264/2006 vp.). Hallituksen esityksen mukaan tiedonhankinta on osa Puolustusvoimien tehtäviä, mutta varsinaisista toimivaltuuksista ei ole erikseen säädetty. Suomessa ei ole myöskään säädetty siitä, mihin tiedustelutoiminnalla pyritään tai millaista tiedustelutoimintaa voidaan harjoittaa. Puolustusvoimien, kuten suojelupoliisin, tiedonhankintatoimivaltuudet ovat puutteellisia toiminnan yhteiskunnalliseen merkittävyyteen nähden sekä muihin maihin verrattuna.

Nykytilassa toimivaltuudet rajoittuvat rikosten estämiseen ja paljastamiseen. Rikoksen estämisellä tarkoitetaan poliisilaissa toimenpiteitä, joiden tavoitteena on estää rikos, sen yritys tai valmistelu, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan perustellusti olettaa hänen syyllistyvän rikokseen, taikka keskeyttää jo aloitetun rikoksen tekeminen tai rajoittaa siitä välittömästi aiheutuvaa vahinkoa tai vaaraa. Salaisia tiedonhankintakeinoja voidaan käyttää valmistelun estämiseksi siinäkin tapauksessa, että asianomaisen rikoksen valmistelua ei ole erikseen kriminalisoitu. Voimassa oleva lainsäädäntö ei siis mahdollista turvallisuusviranomaisille tiedonhankkimista muuten kuin rikosperusteisesti, jossa tiedonhankinnan kohteena on aina tietty henkilö ja tämän toiminta.

Puolustusvoimien käytännön toiminnassa keskeisiä ovat poliisilaissa säädetyt eräät salaiset tiedonhankintakeinot rikoksen estämiseksi ja paljastamiseksi. Rikostorjuntatehtävät rajoittuvat maanpuolustuksen alalla tapahtuvaan laittomaan tiedustelutoimintaan sekä sotilaallista maanpuolustusta vaarantavaan toimintaan, josta Puolustusvoimat ei toimita esitutkintaa, vaan sen tekee suojelupoliisi.

Sotilasvastatiedustelutoiminnassa on kyse suojautumisesta vieraan valtion tiedustelupalveluiden, yksittäisten henkilöiden tai organisaatioiden Puolustusvoimiin tai sen hankkeissa, sekä kehitys- ja tutkimustoiminnassa mukana oleviin sidosryhmäyrityksiin kohdistamasta tiedonhankinnasta. Tavoitteena on kerätä tietoa vieraan valtion tiedustelupalveluiden, asevoimien tai muiden organisaatioiden Suomeen kohdistamasta tiedustelutoiminnasta, sen kehittymisestä ja suunnitelmista. Sotilasvastatiedustelu on osa laajempaa tiedustelukokonaisuutta, ja sen tehtävänä toimivaltuuksiensa mukaisesti hankkia myös sellaista merkityksellistä tiedustelutietoa, jossa ei ole kyse rikosten ennalta ehkäisemisestä tai paljastamisesta.

Muuttuvassa turvallisuusympäristössä sotilastiedustelu ei voi tukea riittävästi ylintä valtiojohtoa ulko-, turvallisuus- ja puolustuspoliittisessa päätöksenteossa sekä varautua torjumaan Suomeen kohdistuvia vakavia turvallisuusuhkia.

Vaikka salaisia tiedonhankintakeinoja voidaan käyttää myös rikoksen valmistelun estämiseksi ja keinojen käyttöala on siten laaja, on selvää, ettei salaisia tiedonhankintakeinoja voida nykyisin käyttää pelkän tiedustelutiedon hankkimiseen sellaisesta sotilaallisesta tai kansallista turvallisuutta uhkaavasta toiminnasta, joka ei ole edennyt rikoksen valmistelun asteelle tai ei ole säädetty rangaistavaksi. Niin ikään tulee huomioida sotilastiedustelun kolmas ulottuvuus eli Suomen rajojen ulkopuolella tapahtuva tiedonhankinta Suomen kansallisen turvallisuuden kannalta merkittävistä kohteista.

Yhteiskunnan tärkeimpänä suojattavana etuna voidaan pitää valtion itsemääräämisoikeutta, jolla tarkoitetaan valtion suvereenisuutta, jolla tarkoitetaan täysivaltaisuutta suhteissa ulkovaltioihin ja oikeutta muista riippumattomalla tavalla käyttää ylintä valtaa omien rajojensa sisällä. Muina keskeisinä suojattavina etuina voidaan pitää ainakin valtion johtamista, kansainvälistä toimintaa, puolustuskykyä, sisäistä turvallisuutta, talouden ja infrastruktuurin toimivuutta sekä väestön toimeentuloturvaa ja toimintakykyä.

Uhkien ja riskien rajaaminen alue- tai paikkasidonnaisiksi on entistä vaikeampaa taloudellisten, teknisten ja sosiaalisten järjestelmien valtiorajat ylittävästä luonteesta ja keskinäisriippuvuudesta johtuen. Suomen turvallisuutta uhkaavat vakavimmat tekijät liittyvät nykyisin usein Suomen ulkopuolisiin tapahtumiin. Siten myös ulkomaista alkuperää olevan ja siellä syntyvän uhan seuraukset saattavat realisoitua Suomessa aiempaa herkemmin. Tästä johtuen uhkien ennakoiminen on aiempaa haasteellisempaa.

Sotilaallisten uhkien luonne on muuttunut merkittävästi viime vuosien aikana. Perinteisen sotilaallisen toiminnan lisäksi modernit sotilasoperaatiot sisältävät erilaisia epäsymmetrisiä keinoja. Modernit sotilasoperaatiot saattavat alkaa ajallisesti jo rauhan aikaisilla painostus- ja disinformaatiooperaatioilla sekä tietoverkkohyökkäyksillä. Näin voidaan pyrkiä tietoisesti vaikuttamaan toisen valtion päätöksentekoon, jotta saavutettaisiin sellaisia strategisia päämääriä, joihin painostuksen kohteena oleva valtio ei muutoin suostuisi. Myös sotilasoperaatioissa ei-valtiollisten toimijoiden vaikuttamismahdollisuudet ovat kasvaneet teknologian kehittymisen ja yhteiskuntien lisääntyneen haavoittuvuuden myötä.

Turvallisuus- ja toimintaympäristön muutosten myötä merkittävät uhat siirtyvät yhä enemmän verkkoon. Poliittisen vaikuttamisen ja sodankäynnin raja hämärtyy käytettäessä poliittisia ja taloudellisia painostuskeinoja sekä disinformaatio-operaatioita. Laaja-alainenkaan voimankäyttö ei tulevaisuudessa välttämättä tarkoita kattavien maa-alueiden haltuunottoa ja hallintaa. Tavoitteet voidaan pyrkiä saavuttamaan voimankäytön yllätyksellisyydellä ja rajattujen alueiden nopealla valtaamisella tai välttämällä laaja-alaista voimakäyttöä ja kattavien maa-alueiden haltuun ottamista.

Sotilaallinen toimintaympäristö on muuttunut. Valtiot kehittävät miehittämättömiä laitteita tiedusteluun, valvontaan ja täsmäasejärjestelmien laveteiksi. ja ulkovaltojen sotilaalliset kohdejärjestelmät ovat muuttuneet entistä monimutkaisemmiksi, tiedon välittämiseen liittyvien signaalien määrä on kasvanut merkittävästi, ja yhä suurempi osa tietoliikenteestä kulkee radiotien sijaan tietoliikennekaapeleissa. Toimintaympäristön muutoksen vuoksi Suomen sotilastiedustelun mahdollisuudet kerätä tiedustelutietoa ovat heikentyneet. Uudentyyppiset uhat asettavat valtionjohdolle ja Puolustusvoimille vaatimukset entistä nopeampaan reagointiin. Asianmukainen reagointikyky edellyttää puolestaan luotettavaa ja reaaliaikaista tietoa päätöksenteon tueksi. Tämän tiedon tuottamisessa sotilastiedustelulla on keskeinen rooli.

Tieto- ja viestintäteknologian kehityksellä on kahtalainen merkitys kansalliseen turvallisuuteen kohdistuvien uhkien muotoutumisen kannalta. Tietoverkkoja hyödynnetään välineenä viestiä sellaisista suunnitelmista ja aikeista, jotka koskevat reaalimaailmassa toteutettavia tekoja. Tietoverkkoja ei tässä tapauksessa hyödynnetä tekovälineenä vaan suunnittelun ja valmistelun välineenä. Teot voivat olla luonteeltaan sotilaallisia (aseellinen hyökkäys) tai ne voivat kohdistua muihin kansallisiin etuihin kuin valtion alueelliseen koskemattomuuteen. Toisaalta tietoverkkoja hyödynnetään varsinaisena tekovälineenä kohdistaa kohteeseen, esimerkiksi Suomen valtioon, tätä vakavasti vahingoittavia tekoja. Kyse voi olla esimerkiksi Suomen kyberturvallisuusstrategian tarkoittamista sotilaallisista kyberoperaatioista.

Tietoverkkouhkien ja uhkia koskevan viestinnän havaitseminen, niiden taustalla olevien tahojen tunnistaminen ja uhan luonteen selvittäminen muodostaa edellytyksen sille, että kansallista turvallisuutta vaarantavien tekojen toteutuminen voidaan estää tai niiden toteutumiseen voidaan varautua. Torjunnasta vastaavan tahon on mahdollisimman varhaisessa vaiheessa saatava tieto uhista tai niitä koskevasta viestinnästä.

Yhteiskunta on muuttunut ympäristöksi, jossa lähes kaikki perinteiset palvelut ja toiminnot ovat tietoteknisesti ohjattuja tai kokonaan muutettu tietoverkoissa toimiviksi. Myös sotilasorganisaatioiden viestintä on digitalisoitumisen myötä siirtynyt enenevissä määrin tietoliikenneverkkoihin.

Sotilaallisiin uhkiin liittyy globalisoitumisen seurauksena yhä useammin Suomessa ja ulkomailla olevien henkilöiden välisiä kytköksiä ja siitä seuraavaa tarvetta molemminpuoliseen kommunikointiin. Sähköisiä välineitä käytetään hyväksi uhkien taustalla olevien valtiollisten ja ei-valtiollisten tahojen viestinnässä, toimeksiannoissa, tehtävien toteuttamista koskevassa raportoinnissa, tekojen suunnittelussa, kohteita koskevassa tiedonhankinnassa sekä osallisten motivoinnissa.

Tietoverkoissa tapahtuvan verkostoitumisen merkityksen sotilaallisten uhkien muodostumisessa voidaan katsoa entisestään kasvavan. Sosiaalisen median kehittyessä verkostoitumisen tavat ovat monimuotoistuneet. Myös eräät valtiot panostavat omien modernien mediaorganisaatioiden kehittämiseen ja propagandan levittämiseen ja ne käyttävät yhä laajemmin sosiaalista mediaa, kuten pikaviestipalveluita, sekä ylläpitävät avoimia ja suljettuja keskustelufoorumeita. Nämä mahdollistavat sekä helppokäyttöisen kahden- ja monenvälisen viestinnän että toiminnan suunnittelun ja reaaliaikaisen koordinoinnin.

Nykyisin tiedustelun tulisi kohdistua digitaaliseen tietoon ollakseen tehokasta tietoteknistyneessä toimintaympäristössä. Tämä edellyttäisi sotilastiedustelulle uusia laintasoisia toimivaltuuksia.

Tietoverkkoympäristössä tapahtuvien turvallisuusuhkien havainnoimiseksi Suomessa on luotu HAVARO-järjestelmä. Tietoverkkojen käyttäjinä olevat yritykset, yhteisöt ja viranomaiset suojautuvat tietoverkkouhilta tietoturvan avulla. HAVARO on huoltovarmuuskriittisille yrityksille ja toimijoille suunnattu tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä. Sen tuottaman tiedon avulla pyritään havaitsemaan tietoturvaan vaikuttavat ilmiöt mahdollisimman varhaisessa vaiheessa, jotta tarvittavat suojaustoimenpiteet voidaan aloittaa ajoissa ja suunnata oikein. Valtionhallinnolle vastaavaa tietoverkkojen tarkkailupalvelua erilaisten tietouhkien löytämiseksi ja torjumiseksi tarjotaan GovHAVAROn tuella.

Sotilaallisen ja kansalliselle turvallisuudelle uhan muodostavat tahot käyttävät tietoverkkoja paitsi viestinnän myös uhkien toteuttamisen välineenä. Suomen kyberturvallisuusstrategiassa käsiteltyjä valtion elinkelpoisuutta tai valtion keskeisiä turvallisuusetuja vaarantavia uhkia ovat ennen kaikkea kybervakoilu, kyberterrorismi ja kyberoperaatiot. Viimeksi mainittu käsite pitää sisällään sekä painostuksen, kyberympäristössä toteutuvan sotaa alemman tason konfliktin että sotaan liittyvät kyberoperaatiot.

Tietoverkkovakoilulla hankitaan valtio- tai yrityssalaisuuksien tapaista luokiteltua tai sensitiivistä tietoa tietojärjestelmistä. Kybertoimintaympäristössä tapahtuva vakoilu voi tällä hetkellä jatkua jopa vuosia huomaamatta. Turvallisuusviranomaisten arvion mukaan useat ulkovallat pyrkivät kohdistamaan laajaa ja teknisesti edistynyttä kybervakoilua Suomen valtionhallintoon ja kansantaloudellista merkitystä omaaviin yrityksiin. Kybervakoilussa tekovälineenä ei ole tavallinen kaupallisella virustorjuntaohjelmalla havaittava haittaohjelma, vaan teknisesti kehittynyt ja monipuolinen verkkohyökkäystyökalu. Työkalun ensimmäisenä tehtävänä on verkon tietyn osan haltuunotto ja seuraavana tehtävänä kehittyneimpien hyökkäyksellisten vakoilu- ja haittaohjelmien asentaminen. Vakoiluoperaatio on ennakkoon tarkoin suunniteltu ja sillä on täsmällinen operatiivinen tavoite kerätä tietoa esimerkiksi kohdevaltion ulko- ja turvallisuuspolitiikkaan, talouteen ja teollisuuteen liittyvistä seikoista. Tiedusteluohjelmien lisäksi voidaan tietojärjestelmiin toimittaa haittaohjelmia, jotka aktivoituvat kriisin alkaessa. Uudet teknologiat luovat uusia mahdollisuuksia kyberoperaatioilla käytävään sodankäyntiin, jonka vaikutukset kohdistetaan koko yhteiskuntaan, ei ainoastaan asevoimiin.

Marraskuussa 2013 Suomen ulkoasiainministeriö vahvisti tiedon, että Suomen ulkoasiainhallinto on ollut vakavan tietoturvaloukkauksen kohteena. Asiaa selvitettiin yhteistyössä esitutkinnasta vastaavan suojelupoliisin kanssa. Suojelupoliisin mukaan kaksi eri valtiota vakoili ulkoministeriötä kahden erillisen hyökkäyksen avulla. Suomen viranomaiset saivat alkuperäisen tiedon vakoilusta kolmannelta valtiolta alkuvuodesta 2013. Epäilty vakoilu oli ehtinyt jatkua siinä vaiheessa jo useita vuosia. Kun suojelupoliisi tutki ensimmäistä tapausta, sen yhteydessä havaittiin toinen, vielä vaka-

vampi tapaus. Suojelupoliisi tutki toista tietomurtoa vakoiluna ja toista törkeänä vakoiluna. Tilanne on kestämätön, mikäli viranomaiset joutuvat toimimaan kolmannen valtion avun varassa. Asianmukaiset tietoliikennetiedustelun toimivaltuudet antaisivat paremmat mahdollisuudet vakoilutapausten havainnointiin sekä niihin reagoimiseen.

2.4.2 Tiedonhankinnan kohteet

Suomen turvallisuusympäristön muuttumisesta johtuen on entistä tärkeämpää, että ylimmällä valtiojohdolla on mahdollisuus saada oikea-aikaista, luotettavaa ja riippumatonta tietoa päätöksenteon tueksi.

Puolustusvoimien tiedustelullisesta tiedonhankinnasta eli sotilastiedustelusta ei ole nimenomaisia säännöksiä laissa. Puolustusvoimista annetun lain esitöiden mukaan tiedonhankinta on osa Puolustusvoimien tehtäviä, mutta varsinaisista toimivaltuuksista ei ole erikseen säädetty. Suomessa ei ole myöskään säädetty siitä, mihin tiedustelutoiminnalla pyritään tai millaista tiedustelutoimintaa voidaan harjoittaa. Puolustusvoimien, kuten suojelupoliisin, tiedonhankintatoimivaltuudet ovat puutteellisia toiminnan yhteiskunnalliseen merkittävyyteen nähden sekä muihin maihin verrattuna.

Rikosperusteisella tiedonhankinnalla ei voida hankkia tietoja Puolustusvoimien tarpeisiin, jotka liittyvät tiedonhankkimiseen muusta kuin rikolliseksi katsottavasta toiminnasta. Puolustusvoimien rikosperusteisilla toimivaltuuksilla ei voida hankkia tietoa ulkomailta ja kotimaasta Puolustusvoimien lakisääteisien tehtävien hoitamiseksi. Tietoja ei voida hankkia riittävissä määrin sotilasstrategisen tilannekuvan muodostamiseksi ja ylläpitämiseksi Suomen turvallisuusympäristöstä ja ennakkovaroituksen antamiseksi sotilaallisten uhkien kehittymisestä, jotta tarvittaviin sotilaallisiin tai rikosperusteisiin vastatoimiin voitaisiin ryhtyä riittävän ajoissa. Tietoa ei voida hankkia ilman rikosperustetta esimerkiksi 1) sotilaallisesta toiminnasta, 2) ulkomaisten tiedustelupalveluiden toiminnasta, 3) valtio- ja yhteiskuntajärjestystä uhkaavasta toiminnasta, 4) joukkotuhoaseista, 5) sotatarvikkeiden kehittämisestä ja levittämisestä, 6) valtioon tai yhteiskunnan elintärkeisiin toimintoihin kohdistuvista vakavista aseelliseen hyökkäykseen verrattavista uhkista, 7) vieraan valtion suunnitelmista tai toiminnasta, joka voi aiheuttaa vakavaa vahinkoa Suomen kansainvälisille suhteille, 8) kansainvälistä rauhaa ja turvallisuutta vaarantavista kriiseistä, 9) kansainvälisiin kriisinhallintaoperaatioihin kohdistuvista uhkista ja 10) Puolustusvoimien kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuuteen kohdistuvista uhkista.

Muuttuvassa turvallisuusympäristössä sotilastiedustelu ei voi tukea riittävästi ylintä valtiojohtoa ulko-, turvallisuus- ja puolustuspoliittisessa päätöksenteossa sekä varautua torjumaan Suomeen kohdistuvia vakavia turvallisuusuhkia.

Vaikka salaisia tiedonhankintakeinoja voidaan käyttää myös rikoksen valmistelun estämiseksi ja keinojen käyttöala on siten laaja, on selvää, ettei salaisia tiedonhankintakeinoja voida nykyisin käyttää pelkän tiedustelutiedon hankkimiseen sellaisesta sotilaallisesta tai vakavasti kansallista turvallisuutta uhkaavasta toiminnasta, joka ei ole edennyt rikoksen valmistelun asteelle tai ei ole säädetty rangaistavaksi.

2.4.3 Puolustusvoimien tiedonhankintatoimivaltuudet

SKRTL:n 87 §:n mukaan Puolustusvoimien rikosten ennalta estämisessä ja paljastamisessa huolehditaan sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyvien rikosten ennalta estämisestä ja paljastamisesta.

SKRTL:n 89 §:ssä Puolustusvoimien rikosten ennalta estämistä ja paljastamista hoitavilla virkamiehillä on oikeus käyttää poliisilain 5 luvussa säädetyistä toimivaltuuksista tukiasematietojen

hankkimista, suunnitelmallista tarkkailua, peiteltyä tiedonhankintaa, teknistä kuuntelua, teknistä katselua, teknistä seurantaa ja teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimista. Muiden poliisilain salaisten tiedonhankintakeinojen osalta voi pyytää suojelupoliisia hankkimaan tarvittavat tiedot.

Poliisilain 5 luvun 1 §:n 2 momentin mukaan rikoksen estämisellä tarkoitetaan toimenpiteitä, joiden tavoitteena on estää rikos, sen yritys tai valmistelu, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan perustellusti olettaa hänen syyllistyvän rikokseen, taikka keskeyttää jo aloitetun rikoksen tekeminen tai rajoittaa siitä välittömästi aiheutuvaa vahinkoa tai vaaraa.

Henkilön toiminnasta tehdyillä havainnoilla tai siitä muutoin saaduilla tiedoilla tarkoitetaan välittömästi henkilön omasta toiminnasta tehtyjä havaintoja ja ulkopuolisen henkilön, esimerkiksi tietolähteen antamia vihjetietoja ja muuta välillistä selvitystä. Havaintoihin ja muuten saatuihin tietoihin kuuluvat myös muun muassa rikostiedustelutiedot, tarkkailuhavainnot, muut vihjetiedot ja analyysillä tiedoista tehtävät johtopäätökset. Edellytyksenä rikoksen estämiseksi säädetyn tiedonhankintakeinon käytölle on, että tällaisten tietojen perusteella on muodostunut perusteltu oletus henkilön syyllistymisestä rikokseen (HE 224/2010 vp. s. 89). Rikoksen paljastamisella tarkoitetaan toimenpiteitä, joiden tavoitteena on selvittää, onko esitutkinnan aloittamiselle esitutkintalain 3 luvun 3 §:n 1 momentissa tarkoitettua perustetta, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan olettaa, että rikos on tehty.

Poliisilain 5 luvun 1 §:n 3 momentin mukaan rikoksen paljastamisella tarkoitetaan toimenpiteitä, joiden tavoitteena on selvittää, onko esitutkinnan aloittamiselle esitutkintalain 3 luvun 3 §:n 1 momentissa tarkoitettua perustetta, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan olettaa, että rikos on tehty. Rikoksen paljastamisen käsite viittaa rikoksen estämisen ja selvittämisen väliin jäävään harmaaseen alueeseen. Kyse ei ole rikoksen selvittämisestä, koska esitutkinnan käynnistämisen edellytykset puuttuvat, eikä myöskään rikoksen estämisestä, koska rikos oletetaan jo tehdyksi. Rikoksen paljastamisesta on kyse esimerkiksi tilanteessa jossa vihjetiedon mukaan rikos olisi jo tehty, mutta konkreettista perustetta epäilylle ei vielä ole eli esitutkintalain mukainen syytä epäillä -kynnys ei ole ylittynyt (HE 224/2010 vp, s. 90).

Rikosten ennalta estäminen ja paljastaminen tapahtuvat nykytilassa Puolustusvoimissa erityisesti viranomaisyhteistoiminnan ja tapahtumaselvittelyjen keinoin. Kohteina ovat yksilöt tai tapahtumat, joiden epäillään liittyvän vihamielisten turvallisuus- ja tiedustelupalvelujen toimintaan. Ennalta estämisessä puututaan toimintaan ennen sen tekemistä tai tapahtumista. Paljastamisessa kerätään tehtyyn tai tekeillä olevaan toimintaan liittyviä relevantteja seikkoja, kuten tekijä, tekoaika ja tekopaikka.

Tällä hetkellä Puolustusvoimilla ei ole käytössään kaikkia niitä tarpeellisia toimivaltuuksia, joilla voitaisiin hankkia tietoja Puolustusvoimien lakisääteisen tehtävän suorittamiseksi. Vaikka Puolustusvoimat saavatkin tarvittaessa ´poliisilta apua tiedonhankinnan suorittamisessa, ei toisen viranomaisen resurssien käyttöä voida pitää tarkoituksen mukaisena Puolustusvoimien omassa toiminnassa. Tämä korostuu etenkin tilanteissa, joissa valmiutta olisi tehostettava, jolloin toisen viranomaisen resurssit saattavat olla sidottuina viranomaisen tehtävien mukaiseen toimintaan (HE 187/2016, PuVM 1/2017 vp. ja PuVL 8/2016 vp.).

Salaisilla tiedonhankintakeinoilla ei voida riittävän tehokkaasti ja varhaisessa vaiheessa havaita sotilaallista toimintaa, muita sotilastiedustelun kohteita eikä ryhtyä niistä saatujen tietojen edellyttämiin toimenpiteisiin, koska salaisten tiedonhankintakeinojen käyttö on lainsäädännössä sidottu rikoksen käsitteeseen (estäminen tai paljastaminen). Kohteina ovat yksilöt tai tapahtumat, joiden epäillään liittyvän vihamielisten turvallisuus- ja tiedustelupalveluiden toimintaa. Paljastamisessa

kerätään tehtyyn tai tekeillä olevaan toimintaan liittyviä relevantteja seikkoja, kuten tekijä, tekoaika ja tekopaikka.

Suomeen ja sen väestöön mahdollisesti kohdistuvien sotilaallisten, muiden ulkoisten uhkien tunnistamiseksi sekä niihin varautumiseksi ja niiden torjumiseksi olisi Puolustusvoimien voitava omin toimivaltuuksin hankkia tietoa sotilastiedustelun kohteista sekä suojata Suomea, sen turvallisuutta ja ylläpitää turvallisuutta. Tiedonhankinnan kohteena oleva toiminta ei monesti ole rangaistavaksi säädettyä tai edennyt niin pitkälle, että siihen voitaisiin kohdistaa konkreettinen ja yksilöity rikosepäily. Tiedontarpeet kohdistuvat esimerkiksi turvallisuusympäristön kehitykseen ja valtiota tai yhteiskunnan perustoimintoja vakaasti uhkaavaan toimintaan, kuten sotilaalliseen toimintaan taikka ulkomaisten tiedustelupalvelujen toimintaan. SKRTL on osoittautunut rikosten ennalta estämisen ja paljastamisen tehtävien osalta käyttökelpoiseksi, joskaan ei kaikilta osin edelleenkään riittäväksi tehtävien tarkoituksenmukaisen hoidon kannalta.

Poikkeuksen rikosperusteisesta tiedonhankinnasta muodostava sotilaalliset kriisinhallintaoperaatiot, joissa saattaa olla operaation mandaatin myötä mahdollista toteuttaa osana monikansallista kriisinhallintaoperaatiota myös henkilötiedusteluoperaatioita. Tämän lisäksi tiedustelutoimintaa voidaan tehdä joukkojen omasuojaksi.

Lisäksi Puolustusvoimilla on käytössä tiedonhankintakeinoja, joilla voidaan hankkia tiedustelutiedoksi katsottavaa tietoa, mutta jotka eivät vaadi erityistä säädösperustaa. Tällaisia ovat avointen lähteiden tiedustelu ja kuvaustiedustelu, jotka eivät loukkaa kohteiden yksityisyyden suojaa tai luottamuksellisen viestin salaisuutta. Myös radiosignaalitiedustelu on edelleen merkittävä osa sotilastiedustelua. Radiosignaalitiedustelun osalta ei sen menetelmien ja kohteiden vuoksi ole vaadittu nimenomaisia toimivaltuussäännöksiä; radiosignaalitiedustelulla ei loukata luottamuksellisen viestin suojaa ja kohteet ovat ulkomaan asevoimat.

Kansallinen turvallisuus on yksi niistä perusteista, joka Euroopan ihmisoikeussopimuksen 8 artiklan mukaan voi oikeuttaa puuttumisen yksityiselämän suojaan. Valtioilla on varsin laaja harkintamarginaali sen suhteen, millaisen toiminnan ne katsovat vaarantavan kansallista turvallisuutta. EIT:n ratkaisukäytännön perusteella ainakin sotilaallinen maanpuolustus ja laittoman tiedustelutoiminnan torjunta kuuluvat kansallisen turvallisuuden piiriin. Kansalliseen turvallisuuteen saattaa kuitenkin kohdistua monenlaisia uhkia, joita on vaikea ennakoida tai määritellä etukäteen. Tuomioistuimen mukaan tästä seuraa, että käsitteen selventäminen on ensisijaisesti jätettävä kansallisen käytännön varaan (Kennedy v. Yhdistynyt Kuningaskunta, 18.5.2010).

Tiedustelulainsäädännön suuntaviivoja arvioineen tiedonhankintalakityöryhmän mukaan tiedustelutoimintaa varten olisi välttämätöntä säätää ulkomaan henkilötiedustelusta, ulkomaan tietojärjestelmätiedustelusta ja tietoliikennetiedustelusta. Kahdesta ensimmäisestä tiedustelulajista käytetään yhteistä nimitystä ulkomaan tiedustelu.

Perusteltua olisi, että ulkomaan tiedustelulajien käyttäminen tulisi mahdollistaa myös kotimaan tiedustelussa, sillä mitä lähempänä kansallista turvallisuutta vakavasti uhkaava toiminta olisi, sitä tarpeellisempaa olisi saada siitä tietoa ja pyrkiä estämään toiminnan eteneminen epätoivottuun vaiheeseen. Jäljempänä, kun käytetään henkilötiedustelun ja tietojärjestelmätiedustelun käsitteitä, niillä tarkoitetaan sekä kotimaan että ulkomaan tiedustelua.

Henkilötiedustelulla tarkoitetaan tiedustelua, joka perustuu henkilökohtaisiin suhteisiin, henkilökohtaiseen kanssakäymiseen taikka henkilön tai muun kohteen henkilökohtaiseen havainnointiin. Rakentamalla luottamuksellisia yhteistoimintasuhteita toisten henkilöiden kanssa henkilötiedustelulla voidaan hankkia keskeistä tietoa turvallisuusympäristöstä ja esimerkiksi asevoimien, tiedustelupalveluiden, yksittäisten henkilöiden tai organisaatioiden toiminnasta ja niiden kiinnostuksen kohteista

Suomen maanpuolustukseen liittyvissä asioissa. Henkilötiedustelulla pystytään hankkimaan strategisen ja operatiivisen ennakkovaroituksen ja tiedustelutilannekuvan edellyttämiä tietoja.

Henkilötiedustelulla voidaan tuottaa sellaista yksityiskohtaista tietoa, jota muilla tiedustelulajeilla on vaikeaa tai mahdotonta hankkia ja sen avulla voidaan luoda edellytyksiä myös muiden tiedustelulajien tehokkaalle hyödyntämiselle.

Henkilötiedustelu voidaan jakaa kolmeen kokonaisuuteen, jotka ovat lähdeoperaatiot, yleinen henkilötiedustelu ja tukioperaatiot. Lähdeoperaatioissa tiedonhankkijana voi toimia vain henkilötiedustelukoulutuksen saanut tehtävään käsketty henkilö. Yleistä henkilötiedustelua tekevät henkilöt, jotka ovat saaneet suppeamman henkilötiedustelukoulutuksen. Yleiseen henkilötiedusteluun kuuluvat tapaamiset perustuvat usein henkilöiden virka-asemaan, ja tiedonhankinta tehdään avoimesti. Henkilötiedustelun tukioperaatioilla hankitaan tietoja henkilöistä ja kohteista.

Kuten edeltä käy ilmi, henkilötiedustelutoimivaltuutta olisi toimivaltuussääntelyn täsmällisyys ja tarkkarajaisuus huomioon ottaen hankala säännellä. Siksi henkilötiedustelun keinot tulisi säännellä nykyinen toimivaltuussäännöskehikko huomioon ottaen. Poliisilain 5 luvun salaisista tiedonhankintakeinoista henkilötiedustelun alaan voidaan katsoa kuuluvan ainakin telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, tekninen laitetarkkailu, suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen tarkkailu (tekninen kuuntelu, tekninen katselu, tekninen seuranta) teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen, peitetoiminta, valeosto ja tietolähdetoiminta.

Tietojärjestelmätiedustelulla tarkoitetaan tietojärjestelmässä käsiteltäviin tietoihin kohdistuvaa tietoteknisin menetelmin tapahtuvaa tiedustelua. Tietojärjestelmätiedustelua käsitellään jäljempänä tässä esityksessä.

Tietoliikennetiedustelulla tarkoitetaan Suomen rajan ylittävässä viestintäverkon osassa liikkuvaan tietoliikenteeseen kohdistuvaa tiedustelua.

Tiedustelutoimivaltuuksista voitaisiin säätää sotilastiedustelusta annetussa laissa. Toimivaltuuksia voitaisiin kutsua tiedustelumenetelmiksi, jotka keinollisesti ja määritelmällisesti vastaisivat poliisilain 5 luvussa säädettyjä salaisia tiedonhankintakeinoja. Tiedustelumenetelmien käytön edellytykset eroaisivat salaisten tiedonhankintakeinojen vastaavista. Koska sotilastiedustelun toimivaltuuksista säädettäisiin omassa laissaan, näin ei aiheutuisi sekaannusta salaisten tiedonhankinta keinojen tai salaisten pakkokeinojen käsitteiden kanssa.

Lisäksi voitaisiin säätää radiosignaalitiedustelusta, paikkatiedustelusta, jäljentämisestä ja ulkomaan tietojärjestelmätiedustelusta sekä tietoliikennetiedustelusta.

2.4.4 Salaiset tiedonhankintakeinot

2.4.4.1 Käyttöedellytykset

Yleiset ja erityiset edellytykset

Salaisten tiedonhankintakeinojen yleisenä edellytyksenä on poliisilain 5 luvun 2 §:n 1 momentin mukaan se, että sillä voidaan olettaa saatavan rikoksen estämiseksi tai paljastamiseksi taikka vaaran torjumiseksi tarvittavia tietoja. Telekuuntelun, tietojen hankkimisen telekuuntelun sijasta, suunnitelmallisen tarkkailun, teknisen kuuntelun, henkilön teknisen seurannan, teknisen laitetarkkailun, peitetoiminnan, valeoston ja tietolähteen ohjatun käytön yleisenä lisäedellytyksenä saman pykälän 2 momentin mukaan on, että niillä voidaan olettaa olevan erittäin tärkeä merkitys rikoksen estämi-

selle tai paljastamiselle. Peitetoiminnan ja valeoston käyttäminen edellyttää lisäksi, että käyttö on välttämätöntä rikoksen estämiseksi tai paljastamiseksi.

Eri tiedonhankintakeinojen käytölle on asetettu niin sanottuja yleisiä edellytyksiä ja erityisiä edellytyksiä. Salaisten tiedonhankintakeinojen käytön erityisinä edellytyksinä ovat ennen kaikkea ne yksilöidyt rikokset, joiden estämiseksi kutakin keinoa voidaan käyttää. Eri tiedonhankintakeinoja koskevissa säännöksissä on myös voitu asettaa muita erityisiä edellytyksiä. Kokoavasti voidaan todeta, että Puolustusvoimat voi käyttää kattavasti SKRTL:ssa säädettyjä salaisia tiedonhankintakeinoja sotilaallisen maanpuolustuksen alalla rikoslain 12 luvussa rangaistavaksi säädettyjen laittomaan tiedustelutoimintaan liittyvien rikosten ja rikoslain 13 luvussa rangaistavaksi säädettyjen valtiopetosrikosten estämiseksi.

Rikosten paljastamiseen yllä mainittuja salaisia tiedonhankintakeinoja voidaan käyttää vain, jos kysymyksessä on SKRTL:n 89 §:n 2 momentissa tarkemmin säädetty Suomen itsemääräämisoikeuden vaarantaminen, sotaan yllyttäminen, maanpetos ja törkeä maanpetos, vakoilu tai törkeä vakoilu, turvallisuussalaisuuden paljastaminen tai luvatun tiedustelutoiminta. Rikosten paljastamisen yhteydessä ei sovelleta salaisten tiedonhankintakeinojen keinokohtaisissa säännöksissä säädettyjä erityisiä edellytyksiä (HE 224/2010 vp. s.92).

Sotilastiedustelulakiin tulisi ottaa vastaavanlainen sääntely, jossa tiedustelumenetelmien käyttö porrastettaisiin sen mukaan, kuinka tuntuvasti niillä puututaan kohteena olevan henkilön perus- ja ihmisoikeuksiin. Tällöin voitaisiin käyttää SKRTL:n viittaussäännösten kautta poliisin lain 5 luvussa säädettyä tuloksellisuusodotusta sekä ilmaisuja ”erittäin tärkeä merkitys” ja ”välttämätön”. Tiedustelumenetelmien käytön tarkoituksena ei olisi estää, paljastaa tai selvittää rikoksia, vaan hankkia tietoa maanpuolustusta tai kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Kyseinen toiminta tulisi määritellä niin seikkaperäisesti kuin se ylipäänsä on mahdollista. Erityisesti silloin, kun tiedustelumenetelmiä käytetään Suomen alueella, toimivaltuuksien käytön perusteisiin tulee kiinnittää erityistä huomiota. Toimenpidekohtaisesti tulisi edelleen säätää muista keinojen käyttämisen edellytyksistä niin seikkaperäisesti kuin mahdollista, esimerkiksi siitä, kehen toimivaltuuden käyttö voidaan kohdistaa tai luvan tai päätöksen voimassaoloajasta.

Sotilastiedustelulaissa säänneltävien tiedustelumenetelmien käyttämisen tavoitteena on saada tietoa toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Sotilastiedustelulaissa tulisi määritellä, minkälaisesta toiminnasta sotilastiedustelulla hankittaisiin tietoa. Koska sotilastiedustelussa ei ole kyse rikoksen estämisestä, paljastamisesta tai selvittämisestä, ja kohteena oleva toiminta voi olla sellaista, ettei se ikinä konkretisoituessaan tulisi olemaan rikos, tiedusteluviranomaisella tulee olla mahdollisuus ryhtyä alhaisella kynnyksellä hankkimaan tietoa tällaisesta toiminnasta. Tiedustelutoimivaltuuksien käytön aloittamisen kynnykset olisi kuitenkin porrastettava riittävällä tavalla ja päätöksenteon olisi oltava riittävän korkealla tasolla sekä toimivaltuuden niin edellyttäessä, ulkopuolisen päätöksentekijän ratkaistavissa. Tällöin voidaan tiedustelumenetelmän käytön edellytykseksi perustellusti asettaa se, että tiedonhankinta kohdistuu yhteiskunnan näkökulmasta kaikkein merkittävimpiin uhkiin. Sotilastiedustelun kohteita käsitellään tarkemmin sotilastiedustelulain 4 §:n yksityiskohtaisissa perusteluissa.

Yhteiskunnan toimintojen haavoittuvuus ja vahinkojen vaikutukset korostuvat nykyaikaisessa tietoyhteiskunnassa. Oikean tiedon saatavuus ja luotettava tilannekuva Suomen kansalliseen turvallisuuteen kohdistuvista uhkista luovat edellytykset uhkien hallinnalle ja oikea-aikaiselle päätöksenteolle. Toimivaltaisella viranomaisella tulee olla tiedon hankkimisessa operatiivinen vastuu.

Rikos ja tietty henkilö

Puolustusvoimien rikosten ennalta estämistä hoitavilla virkamiehillä on SKRTL:n 89 §:n 2 momentin mukaan oikeus käyttää salaisia tiedonhankintakeinoja rikoksen estämisen lisäksi seuraavien

rikosta paljastamisessa: 1) Suomen itsemääräämisoikeuden vaarantaminen, 2) sotaan yllyttäminen, 3) maanpetos tai törkeä maanpetos, 4) vakoilu ja törkeä vakoilu, 5) turvallisuussalaisuuden paljastaminen sekä 6) luvaton tiedustelutoiminta.

Puolustusvoimien käyttämien 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 tiettyyn rikokseen tai sellaisen valmisteluun.

Tiedonhankinnan kohteena oleva henkilön tulee pystyä yksilöimään vähintään henkilön roolin tai tehtävän kautta, vaikka hän olisikin Puolustusvoimien rikostorjuntaa suorittaville virkamiehille vielä henkilöllisyydeltään tuntematon. Poliisi voi poliisilain 5 luvun perusteella kohdistaa telekuuntelua tai televalvontaa myös tuntemattomaan henkilöön IP-osoitteen tai IMEI-koodin perusteella. Jos tällaista tiettyyn henkilöön liittyvää rikosrojunnallista perustetta ei ole olemassa, ei SKRTL:n ja sitä kautta poliisinlain tiedonhankintakeinon käyttö ole mahdollista puolustusvoimissa. Muun tiedustelutiedon hankinnan on näin ollen perustettava avointen lähteiden seuraan, radiosignaalitiedusteluun, geotiedusteluun sekä tietoihin, jotka Puolustusvoimat yhteistyöverkostonsa kautta saa muilta viranomaisilta tai yksityisiltä tahoilta.

Tiedustelutoiminnalle tyypillistä on, ettei tietty henkilö ole aina tiedossa, vaan tiedustelun olennaisena tavoitteena olisi löytää sellaiset henkilöt, jotka liittyvät sotilaalliseen toimintaa tai joiden toiminta aiheuttaa uhkaa kansalliselle turvallisuudelle. Siksi tiedustelutoimivaltuuksien käyttöperusteiden kohdalla tulisi irtaantua nykyisten toimivaltuuksien rikos- ja henkilöperustaisuudesta.
Kun nykyisten tiedonhankintatoimivaltuuksien käytön erityiset edellytykset on määritelty rikosten ja niiden vakavuuden perusteella, tiedustelutoimivaltuuksien erityiset edellytykset tulisi määritellä toiminta- ja uhkalähtöisesti. Salainen tiedonhankinta tulisi mahdollistaa sellaisen toiminnan kohdalla, joka on sotilaallista tai aiheuttaa uhkan Suomen kansalliselle turvallisuudelle joko suoraan tai välillisesti. Kansalliseen turvallisuuteen kohdistuvat uhkat voisivat olla sellaisia, jotka konkretisoituessaan olisivat rikoksia, mutta johon ei vielä voida kohdistaa konkreettista ja yksilöityä rikosepäilyä. Samoin kyse voi olla toiminnasta, joka ei ole Suomen lain mukaan rikos eikä voisi sellaiseksi muodostuakaan, kuten sotilaallinen toiminta.
Tiedon hankkimisen tulisi sisältää myös Suomeen kohdistuvien ulkoisten uhkien kartoittamisen. Kyse olisi siten esimerkiksi Suomen lähialueen sotilaspoliittisen turvallisuusympäristön ja sotilaallisen toiminnan kehityksen seuraamisesta tilannekuvan muodostamiseksi. Ilmaisu kattaisi myös jatkuvan tiedonhankinnan sotilaallisesta toiminnasta ja kansalliselle turvallisuudelle uhkaa aiheuttavasta toiminnasta. Tiedonhankintaa ei siten olisi rajoitettu ajallisesti, sillä tiedustelutoiminnan kohteena olevaa toimintaa on tarpeen seurata pitkäjänteisesti ja systemaattisesti ilman, että seurattavan toiminnan välttämättä tarvitsisi olla välittömästi uhkaavaa seurannan aikana (OMML 41/2016, s. 49). Sotilastiedustelun kohteita käsitellään sotilastiedustelulain 4 §:n yksityiskohtaisissa perusteluissa.

Vaikka tiedonhankinta olisi 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.

2.4.4.2 Teletiedonhankintakeinot

Sotilaallinen toiminta sekä kansalliselle turvallisuudelle uhkaa aiheuttava toiminta on lähes poikkeuksetta järjestäytynyttä. Tämä koskee niin sotilaallista toimintaa kuin ulkovaltojen Suomeen kohdistamaa tiedustelua, sotamateriaalin kehittämistä ja levittämistä, yhteiskunnan kriittistä infrastruktuuria uhkaavaa toimintaa kuin valtioon tai yhteiskuntajärjestyksen väkivaltaiseen kumoamiseen tai

muuttamiseen tähtäävää toimintaa. Tällaiseen toimintaan osallistuvilla henkilöillä on tarve viestiä keskenään. Toiminnan kulloisestakin luonteesta riippuen viestintä voi koskea esimerkiksi toimintaan osallisten henkilöiden välisiä tehtävänantoja, tehtävien toteuttamista koskevaa raportointia, toiminnan suunnittelua, kohteita koskevaa tiedonhankintaa, osallisten motivointia tai uusien osallisten rekrytointia toimintaan. Nykyaikana viestintä on yleensä sähköistä ja se tapahtuu tietoverkoissa.

Henkilöiden välisiin sähköisiin viestiyhteyksiin kohdistuva varhaisvaiheen tiedonhankinta on keskeisessä asemassa sellaisten tietojen saamiseksi sotilastiedustelun kohteena olevasta toiminnasta, jotka mahdollistaa riittävän tilannekuvan muodostamisen ja uhkien torjuntaan ryhtymisen. Merkitystä on tiedonsaannilla niin sähköisen viestinnän sisällöstä kuin viestintään liittyvistä muista tiedoista kuten välitystiedoista. Viestinnän sisällön perusteella voidaan muodostaa kuva sotilastiedustelun kohteen konkreettisemmasta luonteesta ja toiminnan yksityiskohdista. Välitystiedot puolestaan ovat välttämättömiä toimintaan osallistuvien henkilöiden identifioimiseksi.

Puolustusvoimien suorittamassa rikostorjunnassa Puolustusvoimien rikostorjuntaa suorittavilla virkamiehillä on käytössää poliisilain 5 luvussa säädetyistä teletiedonhankintakeinoista ainoastaan poliisilain 5 luvun 25 §:ssä tarkoitettu teleosoitteiden tai telepäätelaitteiden yksilöintitiedot. Jos Puolustusvoimien rikostorjuntaa suorittavalla virkamiehellä on tieto siitä henkilöstä, jonka voidaan perustellusti olettaa syyllistyvän telekuuntelun tai televalvonnan perusterikokseen, mutta ei tämän käyttämistä yksittäisistä teleosoitteista tai telepäätelaitteista, voidaan teleosoitteiden tai telepäätelaitteiden yksilöintitiedot usein hankkia poliisilain 5 luvun 25 §:ssä säädetyn toimivaltuuden avulla. Kyseisen pykälän mukaan poliisi saa rikoksen estämiseksi hankkia teknisellä laitteella teleosoitteen tai telepäätelaitteen yksilöintitiedot, jos estettävänä on rikos, josta säädetty ankarin rangaistus on vähintään vuosi vankeutta. Toiminnassa käytettävän teknisen laitteen on oltava sellainen, ettei sitä voida käyttää muita tarkoituksia kuin teleosoitteen tai telepäätelaitteen yksilöimistä varten. Teleosoitteen tai telepäätelaitteen yksilöintitietojen saaminen poliisilain 5 luvun 25 §:ssä tarkoitetun toimivaltuuden avulla mahdollistaa sen, että osoitteeseen tai päätelaitteeseen myöhemmässä vaiheessa kohdistetaan telekuuntelua tai televalvontaa näille tiedonhankintakeinoille säädettyjen edellytysten täyttyessä.

Hallituksen esityksessä HE 266/2004 vp (s. 34) todetulla tavalla teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen toteutetaan eräänlaisen valetukiaseman avulla ilman, että on tarpeen kytkeä yksityistä teleyritystä mukaan viranomaisten tiedonhankintaan. Teknisen laitteen käyttö on toteutettava fyysisesti lähellä sitä henkilöä, jonka käyttämistä teleosoitteista tai telepäätelaitteista on määrä hankkia yksilöintitiedot. Toimivaltuuden käyttö edellyttää näin ollen käytännössä sitä, että poliisilla on tieto niin toimenpiteen kohdehenkilöstä kuin tämän olinpaikasta. Henkilön olinpaikan on luonnollisesti oltava Suomessa sillä hetkellä kun laitetta käytetään.

Muiden poliisilain 5 luvun teletiedonhankintakeinojen osalta suojelupoliisi voi suorittaa Puolustusvoimille teletiedonhankintakeinoja edellyttävän tiedonhankinnan. Suojelupoliisin käytössä olevia luottamuksellisen viestin salaisuuden suojaan puuttuvia rikoksen estämiseen ja paljastamiseen tarkoitettuja salaisia tiedonhankintakeinoja ovat poliisilain 5 luvun 5 §:ssä tarkoitettu telekuuntelu, 6 §:ssä tarkoitettu tietojen hankkiminen telekuuntelun sijasta, 8 §:ssä tarkoitettu televalvonta ja 9 §:ssä tarkoitettu televalvonta teleosoitteen tai telepäätelaitteen haltijan suostumuksella. Pakkokeinolaissa säädetään samojen keinojen käytöstä rikosten selvittämistä varten.

Edellä mainituille salaisille tiedonhankintakeinoille on yhteistä, että niiden käyttö edellyttää sen teleosoitteen tai telepäätelaitteen, johon keinon käyttö on määrä kohdistaa, tarkkaa yksilöintiä. Telekuuntelun ja telekuuntelun sijasta tapahtuvan tietojen hankkimisen osalta yksilöintivaatimuksesta säädetään poliisilain 5 luvun 7 §:n 3 momentin 5 kohdassa, jonka mukaan tiedonhankintakeinon käyttöä koskevassa vaatimuksessa ja päätöksessä on mainittava toimenpiteen kohteena oleva teleosoite tai telepäätelaite. Poliisilain 5 luvun 5 §:n 2 momentin ja 6 §:n 1 momentin mukaan tele-

kuuntelu ja sen sijasta tapahtuva tietojen hankkiminen saadaan kohdistaa vain sellaiseen teleosoitteeseen tai telepäätelaitteeseen, jonka omistaa tai jota muuten oletettavasti käyttää henkilö, jonka voidaan perustellusti olettaa syyllistyvän johonkin 5 §:n 2 momentissa erikseen mainittuun vakavaan rikokseen.

Televalvonnan samoin kuin teleosoitteen tai telepäätelaitteen haltijan suostumuksella tapahtuvan televalvonnan osalta siitä, että tiedonhankintakeinon käyttöä koskevassa vaatimuksessa ja päätöksessä on mainittava toimenpiteen kohteena oleva teleosoite tai -päätelaite, säädetään poliisilain 5 luvun 10 §:n 6 momentin 6 kohdassa. Poliisilain 5 luvun 8 §:n 2 momentin mukaan televalvonta saadaan kohdistaa vain sellaiseen teleosoitteeseen tai telepäätelaitteeseen, jonka omistaa tai jota muuten oletettavasti käyttää henkilö, jonka voidaan perustellusti olettaa syyllistyvän tietyn vakavuusasteen rikokseen tai johonkin säännöksessä erikseen mainittuun rikokseen. Niin sanottu suostumusperäinen televalvonta saadaan poliisilain 9 §:n mukaan kohdistaa vain suostumuksen antajan hallinnassa olevaan teleosoitteeseen tai telepäätelaitteeseen.

Se, että teletiedonhankintakeinon käyttöä koskevassa lupavaatimuksessa ja vaatimuksen johdosta annettavassa päätöksessä on mainittava toimenpiteen kohteena oleva teleosoite tai -päätelaite, ei tarkoita, että kyseisen päätelaitteen tai osoitteen omistavan tai sitä muuten käyttävän henkilön tulisi olla nimeltään ennalta tunnettu. Hän voi myös olla poliisille toistaiseksi nimeltään tuntematon henkilö, jonka perustellusti voidaan epäillä esimerkiksi olevan osallinen rangaistavaan tekoon. Tällöin hänet voidaan teletiedonhankintakeinon käyttöä koskevassa vaatimuksessa ja tuomioistuimen vaatimuksen johdosta tekemässä päätöksessä yksilöidä hänen hallussaan olevan tai hänen muuten oletettavasti käyttämän teleosoitteen tai telepäätelaitteen ja hänen osallisuutensa avulla (HE 224/2010 vp, s. 94).

Telekuuntelu ja televalvonta voidaan kohdistaa vain teleosoitteeseen tai telepäätelaitteeseen, joka on tietyllä varmuudella tietyn henkilön hallussa tai hänen käyttämänsä. Telekuuntelua ja televalvontaa koskevassa päätöksessä on mainittava myös henkilö, joka voi olla tuntematon. Kumpaakaan tiedonhankintakeinoa ei voida kohdistaa ainoastaan henkilöön ilman teleosoitteen tai telepäätelaitteen yksilöimistä, vaan jokaiseen teleosoitteeseen ja telepäätelaitteeseen tulee hakea erillinen lupa. Tämä on tiedustelutoiminnan rikostorjunnasta poikkeavan luonteen näkökulmasta ongelmallista, sillä tiedustelutoiminnassa on kyettävä toimimaan laveammilla kohdentamiskriteereillä toiminnan ominaispiirteistä johtuen.

Prepaid-liittymiä sekä muita anonyymiliittymiä on erittäin helppo hankkia ja ne ovat teknisen kehityksen myötä tulleet edulliseksi hankkia ja käyttää. Yhdellä henkilöllä voi olla hallussaan useita kymmeniä anonyymiliittymiä ja telepäätelaitteita, kuten kännyköitä. Tämä aiheuttaa useassa tapauksessa sen, että telekuuntelu- ja televalvonta muodostuvat työläiksi käyttää ja niiden teho heikkenee salaisina tiedonhankintakeinoina. Lisäksi siitä aiheutuu tarpeettomia henkilöstökustannuksia viranomaiselle, tuomioistuinlaitokselle ja teleyrityksille.

Tiedustelutarkoituksessa toteutettavaa telekuuntelun ja televalvonnan kohdistamista koskevaa sääntelyä olisi perusteltua väljentää koskemaan myös henkilöä. Näin telekuuntelu kohdistuisi vain tietyltä henkilöltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin, mutta henkilön hallusta löytyneisiin uusiin teleliittymiin ja telepäätelaitteisiin ei tarvitsisi henkilöperusteisen luvan voimassaoloaikana hakea useita uusia lupia. Tällä säästyttäisiin samaan henkilöön kohdistuvilta useilta lupapäätöksiltä, mikä olisi omiaan parantamaan myös lupaprosessin toimijoiden turvallisuutta. Esimerkiksi terroristisolut pyrkivät suojaamaan toimintaansa ja yhteydenpitoansa käyttäen useita eri henkilöllisyyksiä ja harhauttamaan tiedusteluviranomaista muun muassa käyttämällä useita eri puhelinliittymiä ja useita eri puhelimia.

Teletiedonhankintakeinoja koskeva edellä kuvattu sääntely vaikuttaa siihen, kuinka telekuuntelu ja televalvonta toteutetaan teknisesti. Telekuuntelu ja televalvonta suoritetaan mahdollisimman lähel-

lä tiedonhankinnan kohteena olevaa teleosoitetta tai -päätelaitetta eli pisteessä, jonka kautta ei kulje muuta viestintää kuin se, joka lähtee tiedonhankinnan kohteena olevasta osoitteesta tai päätelaitteesta taikka saapuu siihen. Verkkotopologisesti eli viestintäverkon loogisen rakenteen kannalta tarkasteltuna telekuuntelu ja -valvonta tapahtuvat viestintäverkon reunalla.

Teletiedonhankintakeinoja ei voida käyttää, jos poliisin tiedonhankinnan kohteena olevaan toimintaan liittyvässä viestinnässä käytettävät yksittäiset teleosoitteet tai -päätelaitteet eivät ole poliisin tiedossa. Teletiedonhankintakeinoja ei tuolloin voida käyttää siinäkään tapauksessa, että telekuuntelun tai -valvonnan perusterikoksesta ja sen tosiseikoista sinänsä olisi tieto tai epäilys. Teletiedonhankintakeinot eivät mahdollista tiedonhankintaa siitä, mitä viestintävälineitä tai viestintäkanavia tiedonhankinnan kohteena olevassa toiminnassa käytetään, sillä viestintävälineitä tai -kanavia koskevan tiedon olemassaolo on tiedonhankintakeinojen käytön laissa säädetty edellytys ja myös niiden teknisen toteuttamisen edellytys.

Jos Puolustusvoimilla olisi tieto siitä henkilöstä, jonka voidaan perustellusti olettaa syyllistyvän telekuuntelun tai televalvonnan perusterikokseen, mutta ei tämän käyttämistä yksittäisistä teleosoitteista tai telepäätelaitteista, voidaan teleosoitteiden tai telepäätelaitteiden yksilöintitiedot usein hankkimalla ne sitä koskevalla toimivaltuudella. Toiminnassa käytettävän teknisen laitteen on oltava sellainen, ettei sitä voida käyttää muita tarkoituksia kuin teleosoitteen tai telepäätelaitteen yksilöimistä varten. Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimista koskeva toimivaltuus mahdollistaa sen, että osoitteeseen tai päätelaitteeseen myöhemmässä vaiheessa voidaan kohdistaa telekuuntelua tai televalvontaa näille tiedonhankintakeinoille säädettyjen edellytysten täyttyessä.

Puolustusvoimien ja poliisin nykyiset teletiedonhankintakeinot soveltuvat tietojen hankkimiseen vain sellaisista jo tietyllä varmuudella tiedossa olevista, tiettyä rikostunnusmerkistöä vastaavista joko valmisteilla olevista tai oletettavasti tehdyistä rikoksista, joihin osalliset henkilöt ja henkilöiden käyttämät yksilölliset teleosoitteet ja telepäätelaitteet ovat poliisin tiedossa tiedonhankintaan ryhdyttäessä. Tiedustelutoiminnan kannalta arvioituna poliisilain mukaiset salaiset teletiedonhankintakeinot eivät sovellu uhkien havaitsemiseen ja tunnistamiseen. Tämä johtuu teletiedonhankintakeinojen luonteesta ja niiden teknisestä toteuttamistavasta.

Telekuuntelun puutteelliseen soveltuvuuden sotilastiedustelun kohteiden havaitsemisen ja tunnistamisen kannalta ratkaisevaa merkitystä ei ole esimerkiksi sillä, onko telekuuntelu ja -valvonnan käytön perusteena nykyiseen tapaan rikoksen estäminen vai voidaan kyseisiä tiedonhankintakeinoja käyttää myös tiedustelumenetelminä tietojen hankkimiseksi sotilaallisesta toiminnasta tai kansalliseen turvallisuuteen kohdistuvista uhkista. Tiedusteluperusteisesta telekuuntelusta ja televalvonnasta säätäminen ei näin ollen merkittävästi lisäisi suomalaisen yhteiskunnan kykyä havaita ja tunnistaa sen keskeisiin turvallisuusetuihin kohdistuvia tuntemattomia uhkia ja niiden taustalla olevia henkilöitä, koska menetelmien tiedusteluperusteisenkin käytön nimenomaisena edellytyksenä olisi sotilastiedustelun kohteen, sen taustalla olevien henkilöiden ja heidän käyttämiensä konkreettisten viestinvälineiden tiedossa olo sillä hetkellä kun telekuuntelun tai -valvonnan käytötön ryhdytään. Tästä erillinen asia on, että tiedusteluperusteisessa telekuuntelusta ja televalvonnasta säätämisen voidaan arvioida merkittävällä tavalla parantava tiedonsaantia sellaisesta sotilastiedustelun kohteena olevasta toiminnasta, jossa kyse ei ole rikoksesta tai joka ei ole edennyt konkreettisen ja yksilöiden rikosepäilyn asteelle. Kyse olisi tältä osin teletiedonhankintakeinojen aineellisen käyttöalan laajentamisesta, joka kuitenkaan ei muuttaisi menetelmien perusluonnetta. Sama huomio koskee teletiedonhankintakeinojen aineellisen käyttöalan laajentamista kriminalisoimalla sellaisia sotilastiedustelun kohteena olevan toiminnan muotoja, jotka nykyisin eivät ole rangaistavia. Teletiedonhankintakeinojen käytön erityisenä edellytyksenä olevien perusterikosten laajentaminen ei muuttaisi näiden tiedonhankintakeinojen perusluonnetta.

Puolustusvoimien toimialaan kuuluvien turvallisuusuhkiin liittyy se, että ne ja niihin osalliset henkilöt oleskelevat eri maissa, jolloin heidän välisensä sähköinen viestintä ylittää valtioiden rajat. Poliisilain 5 luvussa säädettyjen teletiedonhankintakeinojen puutteet korostuvat monesti silloin, kun on tarve hankkia tietoa Suomen ja jonkin ulkomaan välisestä viestinnästä. Usein kyse on tilanteista, joissa viestinnän ulkomailla oleva osapuoli esimerkiksi vieraan vallan asevoimien tai tiedustelu- ja turvallisuuspalveluiden edustaja kansainvälisen tietojenvaihdon seurauksena on jollain tarkkuudella tiedossa kun viestinnän Suomessa oleva osapuoli on tuntematon. Kyse voi olla esimerkiksi tilanteista, joissa vieraan vallan asevoimista tiedetään tai epäillään viestivän Suomessa olevan henkilön kanssa tai ohjaavan tänne lähetettyjä tai täällä muuten oleskelevia yhteistyötahoja, tai joissa on saatu tietoa, jonka mukaan vieraan valtion tiedustelupalvelu on lähettänyt Suomeen peitteellä toimivia tiedustelu-upseereita. Jos toimintaan osallistuvat Suomessa oleskelevat henkilöt ja heidän käyttämänsä viestinvälineet ei ole tiedossa, ei rajat ylittävään viestintään voida kohdistaa teletiedonhankintaa siitäkään huolimatta, että viestinnän ulkomailla olevasta osapuolesta olisi tieto. Nykyisiä teletiedonhankintakeinoja ei toisin sanoen voida käyttää rajat ylittävään sotilastiedustelun kohteena olevaan toimintaan osallisten Suomessa oleskelevien havaitsemiseen eikä heidän tunnistamiseensa, vaikka henkilöiden havaitseminen ja tunnistaminen olisi edellytys toimintaa koskevalle täsmällisemmälle tiedonhankinnalle ja viime sijassa uhkan estämiselle. Tämä on merkittävä puute tilanteessa, jossa Suomen turvallisuusympäristö on lähes kaikilla osalohkoillaan ratkaisevasti heikentynyt ja oletettavasti jatkaa heikkenemistään.

2.4.4.3 Tarkkailutyyppiset tiedonhankintakeinot

Tarkkailutyyppisiin keinoihin kuuluvat suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, tekninen seuranta (henkilön tekninen seuranta), tekninen laitetarkkailu teleosoitteen ja telepäätelaitteen yksilöintitietojen hankkiminen sekä näitä keinoja tukeva laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen.

Tarkkailutyyppiset keinot olisivat niiden tehokkuuden ja vähäisen perusoikeuspuuttumisen takia tärkeitä tiedustelumenetelmiä sotilastiedustelussa, jossa tieto hankittaisiin sotilastiedustelun kohteista. Sotilastiedustelussa käytettävien toimivaltuuksien mahdollisimman varhaisessa vaiheessa tapahtuva ja oikea kohdentaminen vähentäisi niiden henkilöiden piiriä, joihin tiedustelu kohdentuu.

Tarkkailutyyppisillä keinoilla saatavalla reaaliaikaisella tiedolla voidaan merkittävästi parantaa tilannekuvaa ja tätä kautta helpottaa päätöksentekoa sotilastiedustelun suuntaamisesta sekä sen painopisteistä. Saadulla tiedolla pystytään tehostamaan sotilastiedustelun vaikuttavuutta.

Tarkkailutyyppisten salaisten tiedonhankintakeinojen eräs ominaisuus on, että niiden käyttö tulee kohdentaa tiettyyn henkilöön. Lisäksi teknistä kuuntelua koskevassa päätöksessä tulee mainita tila tai muu paikka, johon kuuntelu kohdistuu. Teknistä seurantaa koskevassa päätöksessä on mainittava toimenpiteen kohteena oleva esine, aine tai omaisuus sekä teknisessä laitetarkkailussa toimenpiteen kohteena oleva tekninen laite tai ohjelmisto.

Tiedustelutarkoituksessa käytettävien toimivaltuuksien käytössä kysymys ei ole rikoksen estämiseen, paljastamiseen tai selvittämiseen tähtäävistä toimista. Näin ollen tietyn henkilön yksilöinnin kautta ei sotilastiedustelussa ilmene vastaavanlaista tarvetta arvioida toimivaltuuden käytön erityisiä edellytyksiä, kuten onko kyseistä henkilöä syytä epäillä tietyn seuraamusuhkan ylittävästä rikoksesta tai voidaanko hänen olettaa syyllistyvän sellaiseen. Tiedustelussa käytettävien toimivaltuuksien käytön tarkoituksena voi olla esimerkiksi tiedonhankinta tietyn henkilöryhmän organisaatiosta, ryhmään kuuluvista henkilöistä ja henkilöryhmän aktiivisuudesta tietyillä alueilla sekä ryhmän toiminnan eri muodoista. Tiedoilla voi olla merkitystä niin operatiivisessa kuin strategisessa päätöksenteossa. Muun muassa edellä kerrotuista syistä johtuen myös tarkkailutyyppisiä toimivaltuuksia tulisi voida kohdistaa rajattuun henkilöryhmään.

Sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain 89 §:n 1 momentissa viitataan Puolustusvoimien rikostorjunnassa käytettävän suunnitelmallisen tarkkailun osalta poliisilain 5 luvun 13 §:ään. Poliisin lain 5 luvun 13 §:n 1 momentissa säädetyllä tarkkailun määritelmällä on välineellistä merkitystä useiden salaisten tiedonhankintakeinojen, erityisesti teknistä tarkkailua koskevien säännösten osalta. Tällainen hetkellinen havaintojen tekeminen ei edellytä toimivaltuussääntelyä. Tilanne muuttuu toiseksi silloin, kun epäiltyä henkilöä tarkkaillaan muuten kuin lyhytaikaisesti. Tällöin kysymys on suunnitelmalliseksi katsottavasta tiedonhankintatoimenpiteestä, jossa epäillyn elämää seurataan jonkin aikaa. Tällainen tarkkailu puuttuu kohdehenkilön yksityisyyden suojaa, kun esimerkiksi seurataan, mitä hän tekee vapaa-aikanaan ja keitä hän tuolloin tapaa. Tällaisesta suunnitelmallisesta tarkkailusta tulisi sen luonteen ja viranomaistoimivaltuuksien kattavan sääntelyn vuoksi säätää laissa.

Internetissä tapahtuvan tarkkailun osalta vallitsevana käsityksenä on, että erityistä toimivaltuussääntelyä ei tarvita suoritettaessa tarkkailua yleisissä tietoverkoissa, esimerkiksi keskustelupalstalla. Tätä asiantilaa ei ehdoteta muutettavaksi. Tietoverkoissa tapahtuvan tarkkailun tulee olla passiivista ihmisten väliseen vuorovaikutukseen kohdistuvaa tiedonhankintaa muun tarkkailun tavoin. Pelkästään tietyn rakennuksen, tilan, paikan, keskustelupalstan tai muuhun vastaavan kohteen tarkkailua ei olisi tarkkailutoimivaltuuden käyttöä. Tällaisen tarkkailun sallimisesta ei ole tarpeen erikseen säätää laissa.

Suunnitelmallisessa tarkkailussa saa käyttää kiikaria, kameraa, videokameraa, valonvahvistinta tai muuta vastaavanlaista teknistä laiteta, joita nykyisinkin voidaan käyttää tarkkailussa. Tällaisten laitteiden käyttäminen ei muuta toimenpiteen luonnetta toiseksi siitä, mikä se on käytettäessä pelkästään aistein tehtäviä havaintoja. Rajaveto tekniseen katseluun tullisi siitä, että viimeksi mainitussa käytetään tiettyyn paikkaan sijoitettuja teknisiä laitteita, menetelmiä ja ohjelmistoja.

Puolustusvoimien toimialaan kuuluvien maanpuolustuksen ja vakavien turvallisuusuhkien taustalla on usein järjestäytynyt toimintaan, josta ei välttämättä voida tunnistaa yksittäisiä henkiöitä. Toimintaan voi osallistua henkilöitä, jotka eivät tietoisesti osallistu toimintaan muodostaen uhkan maanpuolustukselle tai kansalliselle turvallisuudelle. Tällaisessa tilanteessa olisi erittäin tärkeää voida tehdä toiminnasta havaintoja kokonaisuutena, vaikka ei vielä voitaisi tai olisi tarpeen tunnistaa yksittäisiä henkilöitä eikä ketään olisi syyllistymässä rikokseen. Nykyisin suunnitelmallista tarkkailua ei voi kohdistaa muuhun kuin henkilöön.

Puolustusvoimien nykyiset tarkkailutiedonhankintakeinot soveltuvat vain tietojen hankkimiseen sellaisista jo tietyllä varmuudella tiedossa olevista, tiettyä rikostunnusmerkistöä vastaavista joko valmisteilla tai oletettavasti tehdyistä rikoksista, joihin osallinen henkilö on tiedossa viranomaisen ryhtyessä tiedonhankintaan.

Tarkkailu ei nykyedellytyksillä sovellu uhkien havaitsemiseen. Kyseistä tiedonhankintakeinoa voitaisiin käyttää tiedustelumenetelmänä. Siksi tarkkailu olisi tarpeen mahdollistaa myös silloin, kun hankintaan tietoa toiminnasta, joka uhkaa maanpuolustusta tai vakavasti uhkaa kansallista turvallisuutta.

Peitellyllä tiedonhankinnalla tarkoitetaan tiettyyn henkilöön kohdistuvaa lyhytkestoisessa vuorovaikutuksessa tapahtuvaa tiedonhankintaa, jossa virkamiehen tehtävän salaamiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja. Peitelty tiedonhankinta toimivaltuuden käytön lyhytkestoisuudesta johtuen sijoittuu suunnitelmallisen tarkkailun ja peitetoiminnan välimaastoon. Menetelmässä on selkeästä peitetoiminnan kaltaisia piirteitä, mutta toiminnassa ei muodostu samanlaista luottamussuhdetta toimijan ja kohteen välille. Peitetoimintaa voi nykyisin rikosperusteisesti kohdistaa tiettyyn henkilöön, jonka ei tarvitse olla rikokseen oletettavasti syyllistyvä henkilö. Tiedustelutoiminnassa peitellyn tiedonhankinnan kohteena tulisi voida olla myös henkilöryhmä, vaikkakin varsi-

nainen kanssakäyminen ja henkilön kohtaaminen olisi toiminnallisesti kohdistettavissa henkilöryhmässä oleviin yksittäisiin henkilöihin.

Teknisen tarkkailun käsittämille salaisille tiedonhankintakeinoille on yhteistä se, että niiden käyttö edellyttää tietyn henkilön, tilan, alueen tai muun paikan yksilöimistä. Teknisen tarkkailun toimivaltuuksille yhteistä on se, että niissä kuuntelu, katselu tai seuranta tapahtuu tarkkailijan olematta läsnä tilanteessa tai sen välittömässä läheisyydessä. Teknistä tarkkailua voidaan toteuttaa tekniikka neutraalisti teknisellä laitteella taikka menetelmällä tai ohjelmistolla. Teknisen tarkkailun toimivaltuuksien käytössä voidaan siis käyttää tiettyyn esineeseen liitettävän ulkopuolisen laitteen tai esineeseen asennettavan ulkopuolisen tietoteknisen sovellutuksen lisäksi myös esineessä itsessään valmiiksi olevia ominaisuuksia, kuten esineessä olevaa paikannusteknologiaa, mikrofonia tai kameraa.

Tekniseen kuunteluun ja katseluun liittyy niiden suhde eräisiin rikoslain säännöksiin. Salakuuntelu säädetään rangaistavaksi rikoslain 24 luvun 5 §:ssä ja salakatselu rikoslain 24 luvun 6 §:ssä. Nämä rikoslain säännökset ovat nimenomaisesti suljettu pois teknistä kuuntelua ja katselua koskevissa toimivaltuussäännöksissä, jottei epätietoisuutta synny niiden suhteesta tekniseen katseluun ja kuunteluun. Jotta edellä mainittuja kriminalisoinnit eivät tulisi sovellettavaksi, olisi toimivaltuuden käytön edellytysten täytyttävä.

Teknisen katselun käytön ensisijainen tavoite on tuottaa sellaista kuvaa, jota voidaan tarvittaessa käyttää esimerkiksi tiedon analysoinnissa tai kuvamateriaalilla voi olla merkitystä sellaisenaan. Kuvan laadusta voidaan tietyissä tilanteissa tinkiä, esimerkiksi silloin, kun tarve on saada tietoa pelkästään henkilöiden tai henkilöryhmien liikkeestä tietyllä alueella. Teknisellä katselulla pystytään korvaamaan merkittävä osa muuten tarvittavasta henkilötyömäärästä. Esimerkkinä voidaan mainita tilanteet, joissa yksi tai useampi rakennus tai alue pitää saada ympärivuorokautiseen valvontaan eivätkä Puolustusvoimien virkamiehet voisivat hoitaa tarkkailua valvottavan kohteen erityispiirteiden vuoksi.

Sotilastiedustelussa olisi oleellista saada mahdollisimman ajantasaista sekä yksilöityä tietoa viestinnän sisällöstä. *Tekninen kuuntelu* mahdollistaisi kattavan ja yksityiskohtaisen tiedonsaannin tietystä toiminnasta sekä sellaiseen toimintaan liittyvistä henkilöistä ja henkilöryhmistä. Teknisessä kuuntelussa tarkoituksena olisi yhtälailla joko kohdehenkilön tai henkilönryhmän tunnistaminen tai tiedonhankinta heidän toiminnasta.

Henkilöiden, henkilöryhmien ja kuljetusten (esine, aine tai omaisuus) liikkeiden valvominen teknisen seurannan keinoin antaa Puolustusvoimille mahdollisuuden suunnitella ja kohdentaa toimenpiteitä. *Muu kuin henkilön tekninen seuranta* poikkeaa teknisestä katselusta ja kuuntelusta erityisesti siltä osin, ettei se puutu yhtä voimakkaasti perus- ja ihmisoikeuksiin. Teknisen seurannan tarkoituksenmukaisella käytöllä voitaisiin täydentää sotilastiedustelussa tavanomaista tarkkailua. On kuitenkin syytä mainita, ettei tekninen seuranta, teknisen katselun ja kuuntelun tavoin, kaikissa tilanteissa täysin korvaa virkamiehen itsensä tekemiä havaintoja. Henkilön tekninen seuranta sitä vastoin puuttuisi perus- ja ihmisoikeuksiin, kuten liikkumisvapauteen ja yksityiselämän suojaan.

*Teknisellä laitetarkkailulla t*arkoitetaan tietokoneen tai muun vastaavan teknisen laitteen taikka sen ohjelmiston toiminnan, sisältämien tietojen tai yksilöintitietojen muuta kuin yksinomaan aistinvaraista tarkkailua, tallentamista tai muuta käsittelyä rikoksen estämiselle merkityksellisen seikan tutkimiseksi.

Poliisilain 5 luvun 23 §:n 2 momentin mukaan teknisellä laitetarkkailulla ei saa hankkia tietoa viestin sisällöstä eikä 8 §:ssä tarkoitetuista tunnistamistiedoista. Vastaavanalainen säännös on pakkokeinolain 10 luvun 23 §:n 2 momentissa. Poliisi- ja pakkokeinolaista ja niiden esitöistä ilmenee välillisesti, että mainituissa säännöksissä viestin sisällöllä tarkoitetaan nimenomaan telekuuntelun ja

teknisen kuuntelun yhteydessä esiin tulevaa viestin sisältöä. Kyse on toisin sanoen reaaliaikaisesta viestinnästä kahden ihmisen välillä esimerkiksi tietokoneella tai älypuhelimella. Siten viestinnässä käytetylle laitteelle jo tallentuneet tai talletetut asiakirjat, jotka eivät ole teknisen kuuntelun tai telekuuntelun reaaliaikaisessa yhteydessä, kuuluvat teknisen laitetarkkailun piiriin.

Tiedustelun luonteesta johtuu, että siinä käytettäviä toimivaltuuksia käytettäisiin tiedustelun kohteelta salassa. Tekninen laitetarkkailu mahdollistaisi tiedustelun kohdistamisen esimerkiksi tietokoneella olevien asiakirjojen selvittämiseen. Tekninen laitetarkkailu olisi välttämätön toimivaltuus esimerkiksi paikkatiedustelun yhteydessä käytettäväksi, jos olisi tarpeen hankkia digitaalisessa muodossa olevia tietoja teknisellä laitteella olevista asiakirjoista.

Sotilastiedustelussa käytettävien toimivaltuussäännöksillä olisi voitava vastata toimintaympäristön teknisen kehittymisen asettamiin haasteisiin, mikä on otettava huomioon voimassa olevan lainsäädännön toimivuutta arvioitaessa. Tämä koskee niin käytettäviä menetelmiä kuin kohteena olevaa toimintaakin.

Teleosoitteen ja telepäätelaitteen yksilöintitietojen hankkimista koskevasta toimivaltuudesta olisi tarpeen säätää myös sotilastiedustelussa. Keinolla pystyttäisiin hankkimaan tietoja, joilla luottamuksellisen viestin suojaan puuttuvien toimivaltuuksien (telekuuntelu ja televalvonta) käyttö olisi mahdollista kohdistaa sotilastiedustelun kohteeseen, jolloin tämä olisi omiaan parantamaan sivullisten perusoikeuksien suojaa.

Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen on ennen kaikkea teknisen tarkkailun mahdollistava säännös. Teknisen tarkkailun toteutus olisi käytännössä usein mahdotonta tai ainakin erittäin vaikeaa ilman puheena olevaa toimivaltuutta.

Puolustusvoimien nykyiset tarkkailutiedonhankintakeinot soveltuvat tietojen hankkimiseen vain sellaisista jo tietyllä varmuudella tiedossa olevista, tiettyä rikostunnusmerkistöä vastaavista joko valmisteilla tai oletettavasti tehdyistä rikoksista, joihin osallinen henkilö on tiedossa viranomaisen ryhtyessä tiedonhankintaan. Tekninen tarkkailu ei sovellu tällä hetkellä uhkien havaitsemiseen ja tunnistamiseen.

2.4.4.4 Peitetoiminta ja valeosto

Peitetoiminnalla tarkoitetaan poliisilain 5 luvun 28 §:n 1 momentin mukaan tiettyyn henkilön tai hänen toimintaansa kohdistuvaa suunnitelmallista tiedonhankintaa käyttämällä soluttautumista, jossa tiedonhankinnan edellyttämän luottamuksen hankkimiseksi tai tiedonhankinnan paljastumisen estämiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka valmistetaan tai käytetään vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka valmistetaan tai käytetään vääriä asiakirjoja. Peitetoiminnan määritelmässä ei erikseen mainita henkilöryhmää, mutta tästä huolimatta peitetoimintaa voidaan kohdistaa ryhmän muodostaviin yksittäisiin henkilöihin.

Nykyisin peitetoiminnan kohteena olevat henkilöt tulisi voida yksilöidä vähintään heidän rikolliseen toimintaan liittyvien tehtäviensä avulla. Tämä puolestaan ei edellytä henkilön nimeämistä. Sotilastiedustelussa peitetoimintaa pitäisi voida kohdistaa myös tiettyyn henkilönryhmään, jossa peitetoimintaa ei kohdistettaisi kaikkiin ryhmän muodostaviin yksittäisiin henkilöihin. Eräissä tapauksissa tarpeen ei olisi tietojen hankkiminen yksittäisen henkilön toiminnasta, vaan tarpeen olisi voida soluttautua esimerkiksi tiettyyn ihmisryhmään ja tätä kautta hankkia heidän toimintaansa ohjaavasta taustaorganisaatiosta ja tämän henkiöistä tietoa. Kyse voisi olla esimerkiksi hybridivaikuttamisesta Suomen oloihin.

Peitetoimintaa ja valeostoa pidetään kovimpina salaisina tiedonhankintakeinoina, minkä takia näiden keinojen käytön edellytykset ovat erittäin tiukat. Peitetoiminnan ja valeoston käyttäminen edellyttää, että se on välttämätöntä rikoksen estämiseksi tai paljastamiseksi. Peitetoiminnan kohdalla sen käytön edellytyksenä on lisäksi, että tiedonhankintaa on rikollisen toiminnan suunnitelmallisuuden, järjestäytyneisyyden tai ammattimaisuuden taikka ennakoitavissa olevan jatkuvuuden tai toistuvuuden vuoksi pidettävä tarpeellisena. Yhtä tiukoista peitetoiminnan ja valeoston edellytyksistä on perusteltua säätää myös sotilastiedustelussa tiedustelumenetelminä käyttävien peitetoiminnan ja valeoston yhteydessä, vaikka niiden tarkoituksena ei olisikaan hankkia tietoa rikosperusteisesti.

Poliisilain 5 luvun 29 §:ssä säädetään rikoksentekokiellosta, joka vastoin pykälän otsikkoa sisältää oikeuden peitetoimintaa suorittavalle poliisimiehellä tehdä lieviä rikkomuksia. Lain 5 luvun 30 §:ssä säädetään järjestäytyneen rikollisryhmän toimintaan ja valvottuun läpilaskuun osallistumisesta. Kyseisen säännöksen mukaan peitetoimintaa suorittava poliisimies osallistuessaan järjestäytyneen rikollisryhmän toimintaan voi hankkia toimitiloja tai kulku- tai muita sellaisia välineitä, kuljettaa henkilöitä, esineitä tai aineita, hoitaa taloudellisia asioita taikka avustaa rikollisryhmää muilla näihin rinnastettavilla tavoilla. Poliisimies on rangaistusvastuusta vapaa, jos erittäin pätevin perustin on voitu olettaa, että 1) toimenpide tehdään ilman hänen myötävaikutustaankin, 2) poliisimiehen toiminta ei aiheuta vaaraa tai vahinkoa kenenkään hengelle, terveydelle tai vapaudelle taikka merkittävää vaaraa tai vahinkoa omaisuudelle, ja 3) avustaminen editää merkittävästi peitetoiminnan tavoitteen saavuttamista.

Jälkimmäisen säännöksen mukaan peitetoimintaa suorittava poliisimies voisi toisin sanoen osallistuessaan järjestäytyneen rikollisryhmän toimintaan tehdä osittain rikoslain 17 luvun 1 a §:ssä lueteltuja rangaistavia toimia. Toimivaltuuspykälässä ei mainita kyseistä rangaistussäännökset, mutta kysymykseen voi tulla myös vastuusta vapautuminen avunannosta rikokseen.

Peitetoiminta ja valeostotoiminta ovat sellaisia keinoja, joita pidetään jo nykyisin ensisijaisesti tiedustelutyyppisenä eikä välttämättä osana esitutkintaa. Myös EIT on hahmottanut poliisin epäkonventionaaliset tiedonhankintakeinot nimenomaan tiedustelutoimintana, joita arvioidaan osin eri kriteerein kuin rikosoikeudenkäyntimenettelyä tai sen osana olevaa esitutkintamenettelyä. Kun kyseisiä keinoja arvioidaan sotilastiedustelun näkökulmasta, niin katsontakanta on vielä kauempana rikoksen käsitteestä tai rikosperusteinen käyttö ei tulisi lainkaan kyseeseen.

Peitetoiminnalla voitaisiin saada yksityiskohtaista tietoa tiedustelun kohteena olevasta toiminnasta. Lisäksi Puolustusvoimilla on toimintakenttänsä tuntemus ja osaaminen, minkä takia Puolustusvoimilla voidaan katsoa olevan ainoana viranomaisena tietotaito sotilasorganisaatiossa toimimisesta myös peitetoiminnassa.

Peitetoiminnan ja valeostotoiminnan suojaaminen

Hallintovaliokunnan aikanaan esittämä kanta (HaVM 17/2000) valeoston lähtökohtaisesta ja vahvasta salassa pitämisestä vastaa esitutkintaviranomaisten nykyisin edustamaa näkemystä. Valiokunnan kannanotto on sittemmin ainakin poliisitoiminnassa omaksuttu periaatteellisesti, miten valeostoon suhtaudutaan. Hallintovaliokunta on katsonut, että jo pelkkä tieto siitä, että peitetoimintaa tai valeostoa on käytetty, saattaa johtaa toiminnan yksityiskohtien paljastumiseen. Hallintovaliokunnan mukaan syytetyn oikeus oikeudenmukaiseen oikeudenkäyntiin ei vaarannu silloin, kun peitetoiminnalta tai valeostolla saatuja tietoja ei käytetä syyteharkinnan perustana eikä oikeudenkäynnissä, vaan ainoastaan poliisitoiminnan suuntaamisessa.

Mainittu lähtökohta osoittaa valeostoilla ja peitetoiminnalla olevan merkittävä periaatteellinen ero legaliteettiperiaatteen varaan rakentuvaan rikosprosessioikeudelliseen järjestelmään nähden. Vastaavanlaista jännitettä ei voida katsoa sisältyvän tiedusteluperusteisesti käytettävään peitetoimintaan ja valeostoon, joiden perimmäisenä tarkoituksena ei ole hankkia tietoa rikosprosessia varten

eikä muun kuin sotilastiedustelutoiminnan suuntaamiseksi. Tästä käyttöedellytysperustasta huolimatta valeoston ja peitetoiminnan vahva lähtökohtainen salassa pidettävyys on välttämätöntä turvallisuussyistä ja tiedusteluoperaatioiden tuloksellisuuden kannalta. Paljastuessaan valeoston voi aiheuttaa peitehenkilön henkeen tai terveyteen kohdistuvan uhkan kostotoimien muodossa. Kostotoimenpiteet voivat kohdistua myös peitehenkilön läheisiin sekä ulkopuolisiin henkilöihin, jotka ovat mahdollisesti toimineet peitehenkilön tietolähteinä tai muuten edesauttaneet tiedustelutoimintaa. Valeoston ja peitetoiminnan pysyminen salassa on ymmärrettävää myös sen takia, että jos tällaiset toimenpiteet annettaisiin aina niiden kohteille tietoon, muodostuisi esimerkiksi vieraan vallan tiedustelupalveluun sekä siihen kuuluvien sidosryhmien selvittäminen mahdottomaksi.

Valvonta

Sen kontrollointi, miten peitetoimintaa ja valeostoa koskevia menettelyvaatimuksia noudatetaan, jää käytännössä usein sisäisesti suoritettavaksi. Myös tiedusteluperusteisesti käytettävässä peitetoiminnassa ja valeostossa on tärkeää pystyä tosiasiallisesti ja tehokkaasti valvomaan kyseistä toimintaa.

Peitetoiminnan ja valeoston valvontarakenteiden tulee olla valmiina ennen toiminnan aloittamista. Sisäisen ja puolustusministeriön suorittaman valvonnan lisäksi riippumattomalla oikeudellisella valvojalla, tiedusteluvaltuutetulla olisi merkittävä rooli peitetoiminnan ja valeostotoiminnan, kuten muidenkin tiedustelumenetelmien valvonnassa.

2.4.4.5 Tietolähteen ohjattu käyttö ja tietolähteen turvallisuudesta huolehtiminen

Tietolähteen ohjatusta käytöstä säädetään poliisilain 5 luvun 40 §:ssä. Pykälän 1 momentissa on tietolähteen määritelmä, jonka mukaan tietolähdetoiminnalla tarkoitetaan muuta kuin satunnaista luottamuksellista, poliisilain 1 luvun 1 §:ssä tarkoitettujen tehtävien hoitamiseksi merkityksellisten tietojen vastaanottamista poliisin ja muun esitutkintaviranomaisen ulkopuoliselta henkilöltä.

Koska Puolustusvoimilla ja sotilastiedusteluviranomaisella on osaaminen ja tietotaito sotilaallisesta toimintaympäristöstä, voidaan katsoa, että ainoastaan sillä on riittävä osaaminen tunnistaa sotilastiedustelun kannalta keskeiset tahot ja organisaatiot sekä tunnistaa keskeiset henkilöt, jotka voisivat toimia tietolähteinä.

Nykysääntely mahdollistaa tietolähteen ja tietoa hankkivan virkamiehen yhteydenpidon salaamiseen lähinnä poliisilain 5 luvun 46 pykälässä säädetyn tiedonhankinnan suojaamisen avulla. Tietolähteelle ei voida kuitenkaan tämän säännöksen nojalla antaa esimerkiksi uutta henkilöllisyyttä, vaan tarkoituksena on suojata toimintaa ja tietolähdettäkin tätä työtä tekevien virkamiesten kautta. Näin ollen vain virkamiehille voitaisiin tehdä pykälässä tarkoitettu suojaus ja vain he voisivat sitä käyttää.

Tietolähdettä käyttävällä viranomaisella on lähtökohtaisesti velvollisuus huolehtia tietolähteidensä turvallisuudesta tarpeen mukaan tiedonhankinnan aikana ja sen jälkeen. Ei kuitenkaan ole olemassa sääntelyä tietolähteen ennakollisesta suojaamisesta. Tiedustelutoiminnan tietolähteet saattavat joissain tapauksissa asettaa itsensä hengen ja terveyden vaaraan, jolloin henkeen ja terveyteen kohdistuva uhka voi olla valtiollinen. Kyse voi olla esimerkiksi poliittisen turvapaikan hakemisesta. Tällöin tietolähteen suojaaminen edellyttää erilaista intensiteettiä, mitä poliisilain 5 luvun tietolähdetoiminnassa on tarkoitettu. Sotilastiedusteluviranomaisen tulisi pystyä suojelemaan mahdollista tietolähdettä jo ennakollisesti, jotta tietolähde voisi luottaa saavansa asianmukaista suojelua. Pidempiaikaisessa suojan tarpeessa ja viimesijaisena keinona tulisi harkita todistajansuojeluohjelman käyttämistä, josta säädetään todistajansuojeluohjelmasta annetussa laissa (65/2914). Edellä kerrotusta johtuen olisi tarpeen säätää tietolähteen turvaamisesta, joka voitaisiin aloittaa ennakollisesti.

2.4.4.6 Etsintä

SKRTL:ssä tai poliisilaissa ei nykyisin ole paikanetsintää koskevia säännöksiä tiedonhankintatarkoituksessa. Pakkokeinolain (806/2011) 8 luvussa sen sijaan säädetään paikanetsinnästä, joka tehdään tapahtuneen rikoksen selvittämiseksi. Voimassa olevan pakkokeinolain etsinnät tehdään kohdehenkilön tietäen tai läsnä ollessa tarkoituksena hankkia näyttöä rikoksesta. On kuitenkin syytä huomioida, että pakkokeinolaissa ei ole tällä hetkellä säännöksiä tiedonhankintatarkoituksessa tiedonhankinnan kohteen tietämättä tehtävästä etsinnästä eikä siten tässä muistiossa käytetty termi "etsintä" tarkoita samaa asiaa kuin voimassa olevan pakkokeinolain etsintä.

Tiedustelutoiminnassa ilmenee tilanteita, joissa paikkaan kohdistuvan etsinnän toimittaminen olisi välttämätöntä tiedon hankkimiseksi kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Tiedonhankintavaiheen ajallinen kesto ei olisi etukäteen määriteltävissä, vaan se jäisi riippumaan siitä, minkälaista ja -laatuista tietoa suojelupoliisi lakisääteisiä valtuuksia käyttäessään saa hankittua. Jos sotilastiedusteluviranomaisen tiedonhankinta paljastuisi tiedonhankintatoimenpiteen kohdehenkilölle, vaarantaisi tämä sotilastiedustelun tiedonhankinnan tarkoituksen toteutumisen sekä saattaisi aiheuttaa sotilastiedusteluviranomaisen virkamiehelle hengen tai terveyden vaaran.

Yhteiskunnan intressi on sitä suurempi mitä vakavammasta hankkeesta tai ilmiöstä on kyse. Lähtökohtaisesti kaikki sellainen toiminta, joka vakavasti uhkaa kansallista turvallisuutta, on vahingollisuutensa takia sellaista, että mahdollisimman laaja tietojenhankinta tulisi olla mahdollista.

Esimerkiksi vieraan vallan sotilaallisen toiminnan valmistelu toisen valtion alueella on luonteeltaan suunnitelmallista, systemaattisesti päämäärään pyrkivää ja kollektiivista. Kollektiivisuuden yksi seuraus on se, että tällaisten hankkeiden mahdollistamiseksi välttämättömät osatoimenpiteet jaetaan suoritettaviksi useille tahoille. Tällöin tiedon hankkiminen koko toimintakokonaisuudesta voi osoittautua erittäin haasteelliseksi. Solu- tai verkostomaisten organisaatiomuotojen avulla pyritään minimoimaan ryhmän näkyvyys ja salaamaan suunnitelmat mahdollisimman tehokkaasti perinteisten viestintämahdollisuuksien lisäksi. Ryhmän jäsenten välinen yhteydenpito pyritään usein minimoimaan tai kommunikoinnin sisällön tulkitseminen tekemään mahdollisimman vaikeaksi ulkopuolisille. Modernin viestintätekniikan suomia teknisiä salausmahdollisuuksia ja anonymiteettisuojaa hyödynnetään tehokkaasti. Kaikki edellä mainitut tekijät myötävaikuttavat siihen, että Puolustusvoimien tiedonhankintakeinot eivät aina tuota sellaista tietoa, jonka avulla maanpuolustus voitaisiin turvata.

Edellä kerrotusta huolimatta on tosiasia, että vieraan vallan sotilaallinen toiminta ja muu Suomeen kohdistuva vaikuttamistoiminta edellyttää reaalimaailmassa tapahtuvia fyysisiä toimia. Tällaisista toimista jää yleensä erilaisia ja eriasteisia jälkiä. Jäljet voivat olla esimerkiksi luonnoksia, ryhmän sisäisen työnjaon osoittavia asiakirjoja, suunnitellun iskukohteen ennakkotiedusteluun tai -valvontaan liittyviä muistiinpanoja, matkustusasiakirjoja, tietokoneen salausohjelmalla avattuja suunnitelman toteuttamista koskevia sähköpostiviestejä taikka suunnitelman toteuttamiseksi tarvittavia aineita tai esineitä. Tietyissä tapauksissa edellä mainituista tai niiden kaltaisista seikoista voidaan saada tieto suorittamalla etsintä esimerkiksi sellaisessa tilassa, jota henkilö tai ryhmä, käyttää kokoontumisiinsa tai varastona. Toimitettava etsintä voi tuottaa tietoa, jolla voidaan olettaa olevan erittäin tärkeä merkitys sotilaallisesta toiminnasta tai kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.

Tällaisen etsinnän toimittamisesta ei ole syytä ilmoittaa toimenpiteen kohdehenkilölle, koska hänen toimintaansa kohdistuvan tiedonhankinnan jatkaminen voi olla välttämätöntä vielä etsinnän toimittamisen jälkeenkin. Etsinnän toimitushetkeen sidottu ilmoitusvelvollisuus tekisi vastaisen tuloksellisen tiedonhankinnan mahdottomaksi. Tämä voi johtua esimerkiksi siitä, että etsintä on toimitettu väärällä hetkellä. Voidaan ajatella tilannetta, jossa sotilastiedusteluviranomainen saa luotettavana pidettäviä tietoja siitä, että jonkin tuntemattoman tahon on määrä tavata kohdehenkilöä ja toimittaa

tälle tärkeä suunnitelma. Sotilastiedusteluviranomaisella olisi tieto toimituksesta, mutta ei sen tarkasta ajankohdasta. Jos sotilastiedusteluviranomainen tekee kyseisen henkilön hallitsemaan tilaan etsinnän ennen kuin tapaaminen on ohi, toimii kohdehenkilölle etsinnästä tehtävä ilmoitus sellaisena varoituksena, joka saa hänet muuttamaan toimintasuunnitelmaansa. Kokonaiskuvan varmistamiseksi etsintä voidaan joutua suorittamaan useassa kohteessa samanaikaisesti, jolloin tieto etsinnästä ei saa päätyä mahdollisten muiden kumppaniensa tietoisuuteen.

Tiedonhankinnan tehokkuus perustuu näin ollen siihen, että kohdehenkilö ei ainakaan välittömästi tule tietoiseksi häneen kohdistetuista toimenpiteistä. Kyse olisi ennemmin salaisesta tiedonhankinnasta kuin pakkokeinolaissa säädetystä etsinnästä. Pääsääntöisesti kohdehenkilölle olisi kuitenkin myöhemmässä vaiheessa ilmoitettava toimenpiteistä. Ilmoitus tulisi tehtäväksi sen jälkeen kun tiedonhankinnan tarkoitus on saavutettu. Ilmoitusvelvollisuutta voitaisiin kuitenkin lykätä tai ilmoitusvelvollisuudesta luopua, jos erittäin tärkeät intressit tapauskohtaisesti perustelisivat tätä. Ilmoitusvelvollisuuden lykkäämistä tai siitä luopumista koskevat edellytykset olisi aiheellista asettaa samalle tasolle kuin poliisilain 5 luvun mukaisissa salaisissa tiedonhankintakeinoissa. Etsintää voitaisiin kutsua paikkatiedusteluksi.

Jäljentäminen

Sotilastiedustelussa on paikkatiedustelun aikana sekä myös muutoin välttämätöntä taltioida tehdyt havainnot ja löydöt. Lähtökohtaisesti olisi oltava mahdollista jäljentää paikkatiedustelussa löydetty esine, omaisuus, asiakirja, tieto tai seikka. Paikkatiedustelun toimittamisen kannalta on tarpeen säätää vastaavantyyppisestä jäljentämisestä sotilastiedustelulain 4 luvun tiedustelumenetelmänä mitä pakkokeinolaissa jäljentämisestä menetelmällisesti säädetään. Jäljentämisestä olisi tehtävä merkinnät paikkaetsintää koskevaan pöytäkirjaan, jonka lisäksi niistä olisi jokaisesta tehtävä oma pöytäkirjansa. Jäljentämisestä olisi lisäksi ilmoitettava kohdehenkilölle tai sille, jonka omaisuudesta, esineestä tai asiakirjasta on kyse yhtä lailla mitä tiedustelumenetelmien käytöstä ilmoittamisesta säädettäisiin.

Koska lähtökohtana on, että sotilastiedustelutoiminnan ja siinä käytettävien tiedustelumenetelmien on tarkoitus pysyä sen kohteelta salassa, niin myös henkilölle kuuluvan asiakirjan, esineen tai omaisuuden haltuunottaminen ei tule kyseeseen. Siksi jäljentäminen välttämätön keino, jotta pystyttäisiin välttämään tehtyjen havaintojen ja löytöjen taltioiminen ja samalla minimoimaan paljastumisriski, kuten esimerkiksi paikkatiedustelun paljastuminen. Jos sotilastiedustelussa, esimerkiksi paikkatiedustelussa löydettäisiin vaarallisia esineitä tai aineita, voitaisiin toimia kuten poliisilain 2 luvun 14 ja 15 §:ssä on säädetty. Tältä osin on syytä huomioida myös se, että mikäli paikkatiedustelun kohteena olevasta tilasta löydetään vaarallisia esineitä tai aineita ja ne on mahdollisesti vaihdettu myös vaarattomiin, on estettävän tai paljastettavan rikoksen tai jonkun muun rikoslakirikoksen "syytä epäillä" kynnys hyvin todennäköisesti ylittynyt. Tällöin olisi siirryttävä tiedustelumenetelmien käytöstä rikosperusteisten toimivaltuuksien käyttöön, mikä ei enää olisi sotilastiedustelua, jolloin toiminta tiedustelun osalta olisi lopetettava.

Kun paikkatiedustelussa otetaan esimerkiksi kuvia paikkatiedustelun kohteena olevasta tilasta löydetyistä asiakirjoista, suoritetaan samalla asiakirjan jäljentäminen. Paikkatiedustelun aikana tai heti sen jälkeen ei välttämättä ole selvää, mikä merkitys asiakirjoilla on ja asiakirjojen tietosisällön selvittäminen voi edellyttää esimerkiksi niiden kääntämistä.

2.4.4.7 Tiedonhankinta tietoverkoista ja tietojärjestelmistä

Tietoliikennetiedustelu

Sotilastiedustelun kannalta keskeinen tieto on siirtynyt merkittävissä määrin analogisista kanavista digitaalisiin kanaviin, joiden käyttämiseen sotilastiedustelun tiedonhankintalähteenä ei tällä hetkellä

ole toimivaltuuksia. Muutoksiin vastaaminen edellyttäisi lainsäädännön tarkistamista niin, että sotilastiedustelusta vastaavat viranomaiset pystyvät hoitamaan lakisääteiset tehtävänsä riittävän tehokkaasti.

Tietoverkkojen toimintalogiikka eroaa vanhoista puhelinverkoista. Siinä missä puhelu varasi piirikytkentäisen puhelinverkon kokonaan soittajan ja vastaajan välille, internet-verkossa ja tietoliikennekaapeleissa kulkee limittäin lukuisten yhteyksien liikennettä. Lähettävä laite jakaa viestin paketteihin, jotka vastaanottajalaite kokoaa jälleen kokonaiseksi viestiksi. Kaikki paketit eivät välttämättä kulje samaa reittiä vastaanottajalle, sillä verkko reitittää kunkin paketeista kulloisenakin hetkenä kustannustehokkainta reittiä. Kahden samassa maassa olevan osapuolen välinen tietoliikenne voi reitittyä ulkomaisen yhteyspisteen kautta.

Tietoverkkojen kehittyminen on mahdollistanut esimerkiksi pilvipalvelujen yleistymisen. Pilvipalvelussa on kyse tallennuspalvelusta, josta tieto on saatavilla miltä tahansa verkon laitteelta tiedon haltijan oikeuksin. Pilvipalveluun liittyvät palvelimet voivat sijaita yhden tai useamman valtion alueella. Käyttäjällä ei välttämättä ole mahdollisuutta selvittää, mihin tiedot fyysisesti tallentuvat. Teknologian kehittymisestä johtuen voimassa olevilla rikostorjunnallisilla keinoilla ei päästä käsiksi tarvittavaan tietoon.

Tietoverkkovakoilun ja -operaatioiden merkityksen voidaan olettaa kasvavan tulevina vuosina entisestään. Syitä tälle ovat mahdollisuus toteuttaa kybertoimintaympäristössä tekoja alhaisin kustannuksin, suojautumisen vaikeus ja kalleus sekä vähäinen kiinnijäämisriski. Myös Suomen kannalta olennaiset ulkovallat panostavat hyökkäykselliseen tietoverkkokapasiteettinsa rakentamiseen. Kansallisen turvallisuuden kannalta on tärkeää, että turvallisuusviranomaisilla olisi asianmukaiset toimivaltuudet pystyä varautumaan edellä mainittujen uhkien torjumiseen.

Kuten edellä on todettu telekuuntelusta ja teletiedonhankintakeinoista, voimassa olevat teletiedonhankintatoimivaltuudet eivät mahdollista Puolustusvoimien tiedustelutarkoituksessa suorittamaa tiedonhankintaa Suomen kautta kulkevasta tietoliikenneverkoissa tapahtuvasta viestinnästä. Teknologian kehityksen myötä myös esimerkiksi asevoimien viestiliikenne on siirtynyt pääasiassa tietoliikenneverkkoihin.

Sotilaallisen toiminnan ja kansalliselle turvallisuudelle uhkaa aiheuttavan toiminnan havaitsemisen tunnistaminen ja järjestäminen sähköisessä viestintäympäristössä on teknisesti mahdollista. Havaitsemis- ja tunnistamiskyvyn luominen kuitenkin edellyttää nykyisin voimassa olevista teletiedonhankintakeinoista perusominaisuuksiltaan poikkeavaa ratkaisua, jossa tiedonhankinta toteutetaan viesti- ja tietoliikennevirtaa suodattavan järjestelmän avulla. Verkkotopologisesti tämän merkitsee sitä, että tiedonhankinta toteutetaan, päivänvastoin kuin nykylainsäädännön mukaisia teletiedonhankintakeinoja käytettäessä, viestintäverkon keskellä. Tiedonhankinnassa käytettävän suodattimen asettamisella viestintäverkon keskelle pyritään varmistamaan se, että seulontajärjestelmän läpi mahdollisimman suurella todennäköisyydellä virtaa sellaista viesti- tai tietoliikennettä, jonka voidaan olettaa liittyvän sotilastiedustelun kohteena olevaan toimintaan. Seulonnassa uhkan kannalta olennainen viestintä erotetaan muusta tietoliikenteestä tiettyjen ennakkoon asetettujen kriteerien tai seulontaparametrien avulla. Seulontaparametreiksi voidaan asettaa esimerkiksi sellaisia viestinnässä käytettäviä ilmaisuja, erityisiä viestintätapoja, IP-osoiteavaruuksia tai viestinnän aikaa ja paikkaa koskevia tietoja, joiden tiedetään tai oletetaan liittyvän tiedonhankinnan kohteena olevaan toimintaan.

Seulontaan perustuva toimintatapa voitaneen tietyiltä osin rinnastaa sellaiseen muussa turvallisuusviranomaisten toiminnassa käytettävään profilointiin, jonka avulla laajemmasta kohdejoukosta etsitään turvallisuuden kannalta olennaisia poikkeamia. Toiminnalliselta luonteeltaan viestiliikenteen seulonta vertautuu esimerkiksi profilointiin ja riskiarviointiin perustuvaan raja- ja tullivalvontaan. Raja- ja tullivalvonnassa osa rajan ylittävistä henkilöistä voidaan ottaa tarkemman tarkastelun

kohteeksi sen vuoksi, että he täyttävät tietyt esimerkiksi matkustustapaan liittyvät ennakkoon asetetut seulontaparametrit. Viestiliikenteen seulonta voidaan kuitenkin perustaa paitsi inhimillistä käyttäytymistä tai toimintatapoja koskeviin yleisiin tietoihin, myös konkreettisiin tiedonhankinnan kohteena olevaa uhkaa kuvaaviin tietoihin. Esimerkkinä tällaisesta tiedosta voidaan mainita tieto siitä, että tiedonhankinnan kohteena olevaan uhkaan liittyvässä viestinnässä käytetään sellaista ohjelmakoodia tai viestin salausta, joka on ainoastaan tietyn sotilasorganisaation käytössä.

Kuten kansainvälisestä vertailusta ilmenee, valtaosa vertailumaista käyttää tai suunnittelee ottavansa käyttöön viesti- ja tietoliikenteen seulontaan perustuvia tiedonhankintamenetelmiä. Näitä menetelmiä voidaan, niiden keskinäisistä eroista huolimatta, kutsua yhteisnimellä tietoliikennetiedustelu. Vertailumaiden käyttämän tai niiden kaavaileman tietoliikennetiedustelun tarkoituksena on havaita kansalliseen turvallisuuteen kohdistuvia uhkia, tunnistaa niiden taustalla olevia henkilöitä, tunnistaa uhkaavassa toiminnassa käytettävät teleosoitteet ja -päätelaitteet telekuuntelun ja televalvonnan mahdollistamiseksi sekä hankkia tarkempaa tietoa uhkista.

Vertailumaissa tietoliikennetiedustelua käytetään tiedustelumenetelmänä eikä rikosten estämisen, paljastamisen tai selvittämisen keinona. Tiedustelun tarkoituksena ei ole hankkia tulevaa rikosprosessia varten tietoa sellaisesta ennalta tunnetusta henkilöstä, jonka voidaan perustellusti olettaa syyllistyvän tai epäillä syyllistyneen tietyn vakavuusasteen rikokseen, vaan tarkoituksena on havaita ja tunnistaa keskeisimpiin kansallisiin turvallisuusetuihin kohdistuvia uhkia sekä jakaa uhkia koskevia analysoitua tietoa sitä tarvitseville tahoille. Tietoliikennetiedustelu poikkeaa poliisin perinteisistä tele- ja muista tiedonhankintakeinoista ja myös useimmista tiedustelupalveluiden käyttämistä menetelmistä juuri sen vuoksi, että se teknisten ominaispiirteidensä johdosta mahdollistaa aiempaa tehokkaammin esimerkiksi sotilaallisesta toiminnasta.

Tietoliikennetiedustelun avulla hankitaan vertailumaissa paitsi valtiojohdon ulko- ja turvallisuuspoliittista päätöksentekoa palvelevaa tietoa, myös tietoa, joka on tarpeen uhkien toteutumisen mahdollisimman varhaisessa vaiheessa tapahtuvaksi estämiseksi.

Tietoliikennetiedustelussa käytettävät seulontaparametrit, joista voidaan käyttää nimitystä hakuehdot, voivat seuloa tiedustelujärjestelmän läpi virtaavan viesti- ja tieto-liikenteen sisältöä tai sen muita tietoja. Muita tietoja ovat esimerkiksi sellaiset tiedot, jotka ovat tarpeen tietoliikennevirtaan sisältyvien yksittäisten viestien ohjaamiseksi niiden lähettäjältä vastaanottajalle, sekä viestinnän aikaa ja paikkaa koskevat tiedot.

Tietoliikennetiedustelun tehokkuus mutta myös sen perusoikeusvaikutukset riippuvat siitä, käytetäänkö hakuehtoina viestin sisältöä kuvaavia tietoja vai ainoastaan muita viestintään liittyviä tietoja. Tehokkuus on suurempi, jos hakuehtoina voidaan käyttää viestin sisältöä kuvaavia tietoja. Tällöin tiedusteluviranomaisella ei tarvitse olla ennakkotietoa esimerkiksi siitä, missä osoiteavaruudessa osapuolet viestivät, vaan kaikista tietoliikennevirtaan sisältyvistä viesteistä voidaan etsiä esimerkiksi sellaisia harvinaisia nimiä tai koodikielisiä ilmaisuja, joita tiedetään tai voidaan olettaa käytettävän selvitettävänä olevan esimerkiksi terroristisen toiminnan tai vieraan valtion harjoittaman vakoilun yhteydessä. Viestin sisältöä kuvaavien hakuehtojen käyttö on näin ollen tarpeen ennen kaikkea silloin, kun tiedonhankinnan kohteena olevassa toiminnassa käytettävistä viestintäkanavista ei ole tietoa tai ainoastaan hyvin yleisluontoista tietoa. Toisaalta sisällöllisten hakuehtojen käyttö muodostaa muiden hakuehtojen käyttöä suuremman puuttumisen luottamukselliseen viestintään, sillä se edellyttää kaiken läpivirtaavan viestinnän, myös kaikkien uhkan kannalta sivullisten henkilöiden viestinnän, avaamista ja hakuehtojen vertaamista viestien sisältöön.

Viestinnän sisältöä kuvaavien hakuehtojen käyttö on sallittu tai kaavaillaan sallittavaksi kaikissa niissä vertailumaissa, jotka ovat säätäneet tietoliikennetiedustelusta tai jotka valmistelevat siitä säätämistä. Sisällöllisten hakuehtojen käyttöä on kuitenkin joko lakien tai niiden perusteluiden kautta rajattu siten, että hakuehtoina saadaan käyttää vain muita kuin tavallisia yleiskieleen sisältyviä

ilmaisuja. Sallittuina hakuehtoina voivat siten tulla kyseeseen lähinnä sellaiset harvinaiset henkilönimet ja ilmaisut, jotka eivät ole yleisesti tiedossa tai käytössä ja joiden ei siten voida olettaa esiintyvän sivullisten henkilöiden viestinnässä.

Sisällöllisten hakuehtojen käyttökelpoisuutta ja tehokkuutta rajoittavat salaustekniikoiden kehittyminen ja niiden käytön yleistyminen. Viestintään liittyviä muita tietoja ei voida samalla tavalla salata kuin viestien sisältöä, koska niitä tarvitaan viestien ohjaamiseksi viestintäverkossa lähettäjältä vastaanottajalle. Viestinnän ohjaus- ja välitystietojen merkitys tietoliikennetiedustelun hakuehtoina on siten suuri. Tiedonhankintalakityöryhmän mietinnössä arvioidaan (s. 72), että tietoliikennetiedustelulla voidaan salauksesta huolimatta saada kansallisen turvallisuuden kannalta merkittävää tietoa esimerkiksi tunnistamistietojen perusteella.

Tietoliikennetiedustelua voidaan käyttää sekä sitä harjoittavaan maahan sen ulkopuolelta kohdistuvien uhkien että myös puhtaasti maan sisäisten uhkien havaitsemiseen, tunnistamiseen ja selvittämiseen. Vertailuvaltioissa tietoliikennetiedustelua käytetään yksinomaan ulkoisten uhkien tunnistamiseen, havaitsemiseen ja selvittämiseen eli ulkomaantiedustelun menetelmänä. Tästä johtuen tietoliikennetiedustelu on vertailuvaltiossa järjestetty siten, että se kohdistuu sitä harjoittavan valtion rajan ylittävään viesti- ja tietoliikenteeseen.

Vertailuvaltioiden lainsäädännöistä ja niiden perusteluasiakirjoista voidaan päätellä, että tietoliikennetiedustelu on niissä järjestetty tai aiotaan järjestää useampivaiheisena toimintana. Eri maiden lainsäädäntöjen erovaisuuksista huolimatta toimintaa voidaan yleistäen luonnehtia siten, että rajan ylittävistä tietoliikenneyhteyksistä ensin valikoidaan ne osat, joiden läpi voidaan arvioida virtaavan tiedustelun kohteena olevaan toimintaan liittyvää viestintää tai muuta tietoliikennettä. Valikoiduissa tietoliikenneyhteyksissä kulkeva viestintä ja muu tietoliikenne joko ohjataan kulkemaan tiedustelussa käytettävän tietojärjestelmän läpi tai siitä luodaan tallennettava kopio. Ensin mainitussa tapauksessa tietojärjestelmä vertaa läpi virtaavaa viestintää ja tietoliikennettä reaaliaikaisesti ennalta asetettuihin hakuehtoihin. Hakuehtoja vastaava viestintä ja muu tietoliikenne ohjataan analyysitietokantaan jatkokäsittelyä varten. Muu kuin hakuehtoja vastaava viestintä ja tietoliikenne kulkevat tiedustelujärjestelmän läpi eivätkä ne ole myöhemmin palautettavissa tarkasteltavaksi. Jälkimmäisessä tapauksessa hakuehtoja ei käytetä reaaliaikaisesti, vaan kopioitu liikenne ohjataan kokonaisuudessaan analyysitietokantaan, jossa siihen voidaan myöhemmin tehdä hakuja.

Edellä tässä esityksessä on kuvattu tietoliikennetiedustelun järjestämisen kannalta relevanttia Euroopan ihmisoikeustuomioistuimen ja Euroopan unionin tuomioistuimen oikeuskäytäntöä. Kuvauksesta ilmenee, että ihmisoikeustuomioistuin on pitänyt tietyin verrattain tiukoin reunaehdoin järjestettyä tietoliikenne-tiedustelua ihmisoikeussopimuksen 8 artiklan mukaisena.

Kun arvioidaan tietoliikennetiedustelun sallittavuutta Euroopan ihmisoikeussopimuksen ja EU-oikeuden näkökulmasta, on kansainvälisen tuomioistuinkäytännön perusteella merkitystä erityisesti sillä, että kansallinen lainsäädäntö on suhteellisuusperiaatteen mukainen. Ihmisoikeustuomioistuimen käsitystä suhteellisuusperiaatteen asettamista vähimmäisvaatimuksista ilmentää sen tapauksien Huvig v. Ranska 24.4.1990 ja Kruslin v. Ranska 24.4.1990 johdosta antamissaan ratkaisuissa luoma testi, jota se myöhemmissä ratkaisuissaan on toistuvasti soveltanut ja jossain määrin myös edelleen kehittänyt. Myös Euroopan unionin tuomioistuimen Digital Rights Ireland -tapauksen johdosta antamassa ratkaisussa oli pitkälti kyse yllä mainitun ns. Huvig/Kruslin -testin soveltamisesta. Kyseisen testin mukaan viestintäsalaisuuteen puuttumisen oikeuttavan kansallisen lainsäädännön on sisällettävä: 1) niiden henkilöiden määrittelyn, joiden viestintäsalaisuuteen puututaan, 2) niiden tekojen tai uhkien määrittelyn, jotka antavat aiheen puuttua viestintäsalaisuuteen, 3) säännökset siitä, kuinka puuttumisesta päätetään, 4) säännökset siitä, kuinka tietoja käsitellään, käytetään ja säilytetään, 5) säännökset viestintäsalaisuuteen puuttumisen kestosta ja toimenpiteiden avulla kerättyjen tietojen säilytysajoista, 6) varotoimenpiteet, kun tietoa annetaan muiden käyttöön ja 7) tietoja poistettaessa ja tuhottaessa noudatettavat menettelyt.

Tiedonhankintalakityöryhmän mietinnössä on alustavasti arvioitu, kuinka tietoliikennetiedustelusta voitaisiin Suomessa säätää, jotta sääntely täyttäisi edellä mainituista suhteellisuusperiaatetta konkretisoivista kriteereistä aiheutuvat ja laajemminkin kansainvälisestä oikeuskäytännöstä johtuvat vaatimukset.

Mietinnön mukaan Suomea velvoittavat kansainväliset ihmisoikeussopimukset sallivat tietyin reunaehdoin sekä sisäiseen että rajan ylittävään tietoliikenteeseen kohdistuvan tiedustelun. Koska Suomen kansalliseen turvallisuuteen kohdistuvat vakavimmat uhat ovat ensisijaisesti ulkoisia, todetaan mietinnössä Suomen tarpeiden liittyvän rajan ylittävän tietoliikenteen tiedusteluun. Ne uhat, joita tietoliikennetiedustelun tiedonhankinta saisi koskea, tulisi puolestaan määritellä lain tasolla mahdollisimman selkeästi ja suppeasti. Uhkien tulisi olla riittävän vakavia ja kohdistua kansallisen turvallisuuden kannalta keskeisiin turvallisuusintresseihin. Selvänä mietinnössä pidetään sitä, ettei tietoliikennetiedustelu voi olla tavanomaisena pidettävän verkko- tai muunkaan massarikollisuuden tutkintaa varten käytettävä menetelmä. Mietintö menee kuitenkin tätä pidemmälle ja suosittaa tietoliikennetiedustelusta säätämistä harkittaessa otettavan lähtökohdaksi, ettei sen käyttöä rikostutkinnallisena menetelmänä tulisi sallia (s.62–63).

Mietinnön mukaan Suomen rajan ylittävän tietoliikenteen tiedustelu tulisi toteuttaa siten, että tietoliikenteen joukosta voitaisiin seuloa mahdollisimman tehokkaasti toiminnan perusteena olevien vakavien uhkien kannalta olennainen liikenne ja estää tehtäviin kuulumattoman liikenteen päätyminen analysoinnin kohteeksi. Seulonnassa tulisi tästä johtuen käyttää riittävän tarkkoja ennakkoon määrättyjä hakuehtoja tai sellaisia kansallista turvallisuutta vaarantavan toiminnan sanallisia kuvailuja, jotka mahdollisimman konkreettisesti luonnehtisivat tiedonhankinnan kohdetta. Kuvailun kohteena kyseeseen tulisivat sellaiset viestinnälliset ja muut toimintamallit, joiden tiedetään tai voidaan olettaa liittyvän kansallista turvallisuutta vaarantavaan toimintaan (s. 64). Hakuehtojen ja suullisten kuvailujen hyväksymisen tulisi tapahtua tiedusteluviranomaisesta erillisen lupaviranomaisen toimesta, ja niiden käyttö tiedustelussa tulisi kattavasti dokumentoida jälkikäteistä valvontaa varten. Lupaviranomaiseksi mietintö ehdottaa tuomioistuinta (s. 67), ja jälkikäteisen valvonnan toteuttamiseksi se ehdottaa harkittavaksi uuden riippumattoman laillisuusvalvontaelimen perustamista (s. 69).

Mietinnössä suositellaan, että tietoliikennetiedustelussa sallittavia hakuehtoja rajoitettaisiin siten, että sellaisina tulisivat kyseeseen ainoastaan tunnistamistiedot. Esimerkkeinä tällaisista hakuehdoista mainitaan verkkolaitteita ja verkko-osoitteita kuvaavat yksilöintitiedot sekä viestinnän aikaa ja paikkaa kuvaavat tiedot (s. 64). Tiedonhankintalakityöryhmä ottaa mietinnössä näin ollen edellä käsiteltyjen vertailumaiden lainsäädännöistä poikkeavan ja niitä tiukemman kannan sisällöllisten hakuehtojen käyttöön. Kuitenkin silloin, kun tietoliikennetiedustelun tarkoituksena olisi havaita haittaohjelmien avulla toteutettavaa tietoverkkovakoilua, tulisi myös viestin sisältöä kuvaavia hakuehtoja poikkeuksellisesti voida käyttää. Sisältöä kuvaavavana hakuehtona tulisi tuollaisissa tapauksissa kyseeseen tekninen haittaohjelmatunniste (s. 64).

Mietinnössä ehdotetaan, että hakuehtojen avulla tapahtuva viesti- ja tietoliikenteen seulonta suoritettaisiin koneellisesti. Hakuehtojen käytön avulla muusta tietoliikenteestä erotellut viestit, joiden voidaan lähtökohtaisesti olettaa olevan relevantteja tiedonhankinnan kohteena olevan uhkan selvittämiseksi, saataisiin ottaa manuaalisen käsittelyn kohteeksi, jolloin myös niiden sisältö saataisiin selvittää (s. 65). Ne viestit, jotka sisällön selvittämisen perusteella todettaisiin tiedustelun kohteena olevaan uhkaan liittyviksi, saataisiin myös tallettaa. Tallettaa saataisiin myös viestit, jotka liittyvät johonkin toiseen kansalliseen turvallisuuteen kohdistuvaan laissa mainittuun uhkaan kuin siihen, jota varten tietoliikennetiedusteluun on myönnetty lupa. Kansalliseen turvallisuuteen liittymätön ylimääräinen tieto sen sijaan tulisi hävittää välittömästi, kun se on havaittu tällaiseksi. Kun mietinnössä ehdotetun tietoliikennetiedustelun tarkoituksena olisi hankkia tietoa ulkoisista uhkista Suomen rajan ylittävästä tietoliikenteestä, suositetaan mietinnössä lisäksi, että tietoliikennetiedustelun

piiriin teknisistä syistä tuleva Suomessa oleskelevien osapuolten välinen tietoliikenne olisi hävitettävä (s. 68).

Mitä tulee tietoliikennetiedustelulla saatujen tietojen käsittelyyn yleisemmin, mietinnössä todetaan, että Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö edellyttää tietojen tarkastamisesta, hyödyntämisestä, säilyttämisajoista, luovuttamisesta ja hävittämisestä riittävän täsmällistä säätämistä lain tasolla. Esimerkiksi tietojen luovuttamisen ulkomaan viranomaiselle osalta suositetaan lähtökohdaksi otettavan, että tietojen luovutuksella edistetään kansallista turvallisuutta eikä sillä vaaranneta Suomen etuja, mukaan lukien kansantaloudelliset edut (s. 68).

Tiedonhankintalakityöryhmä toteaa mietinnössä, että tietoliikennetiedustelusta säätäminen sen ehdottamalla tavalla ei johtaisi sellaiseen laajamittaiseen, erittelemättömään, pitkäaikaiseen ja rajoittamattomaan tunnistamistietojen tallentamiseen, jota kansainvälisten tuomioistuinten oikeuskäytännössä on pidetty suhteellisuusperiaatteen vastaisena (s. 65). Tiedonhankintatyöryhmän toteamus koskee nimenomaan tunnistamistietoja, mutta se soveltuu luonnollisesti myös viestinnän sisältötietoihin.

Tämän hallituksen esityksen valmistelua varten asetetun työryhmän asettamispäätöksessä todetaan, että lainvalmisteluhankkeessa otetaan huomioon tiedonhankintalakityöryhmän mietintö ja siitä saatu lausuntopalaute. Asettamispäätöksessä asetettu huomioon ottamista koskeva velvoite koskee myös tietoliikennetiedustelun järjestämistä.

Tehokkaan ennakkovaroituskyvyn ja toimintaympäristöä koskevan tilannetietoisuuden kannalta sotilastiedustelulla tulisi olla tarvittavat toimivaltuudet suorittaa rajat ylittävää tietoliikennetiedustelua. Suomen rajan ylittävää viestintäverkkoa tai sen osan omistava tai hallinnoivan tahon olisi avustettava viranomaista tietoliikennetiedustelun toteuttamisessa. Avustavasta tahosta voitaisiin käyttää nimitystä tiedonsiirtäjä. Avustamisvelvollisuus olisi verrattavissa voimassa olevan lainsäädännön teleyritysten avustamisvelvollisuuteen telekuuntelussa ja -valvonnassa Teleyritysten avustamisvelvollisuudesta olisi säädettävä erikseen.

Tiedon hankkiminen tietoverkkouhkasta

Maanpuolustusta tai kansallista turvallisuutta uhkaavat tahot voivat käyttää sähköisiä viestintäverkkoja paitsi uhkia koskevaan viestintään, myös uhkien toteuttamiseen. Aiemmin tässä esityksessä todetulla tavalla viestintäverkkojen välityksellä suoritetut kyberteot, esimerkiksi kybervakoilu, laaja-alaiset kyberhyökkäykset, painostusta sisältävät kyberoperaatiot ja valtion elintärkeisiin toimintoihin kohdistuvat kybertuhotyöt, saattavat vakavimmillaan vaarantaa valtion elinkelpoisuuden tai valtion keskeiset turvallisuusedut. Kybertekojen kohteina saattavat valtion ohella olla myös yksityiset yritykset tai yhteisöt, jolloin teot vaarantavat esimerkiksi niiden salassa pidettävän tuotekehitystiedon.

Kyberuhkien riittävän varhaisessa vaiheessa tapahtuva havaitseminen on niiden estämisen tai ainakin niiden aiheuttamien vahinkoseurausten rajaamisen edellytys. Puolustusvoimien tiedonhankintakeinot eivät sovellu kyberympäristössä suoritettujen tekojen havaitsemiseen, koska Puolustusvoimilla ei näitä uhkia koskevia tiedonhankinta toimivaltuuksia ole. Myös Suomen voimassa olevan sääntely-ympäristössä teletiedonhankintakeinojen käytön edellytyksenä on, että keinon käytön kohde, teletiedonhankintakeinojen osalta teleosoite tai telepäätelaite ja esimerkiksi tarkkailutyyppisten keinojen osalta henkilö, on tiedossa sillä hetkellä kun tiedonhankinta aloitetaan.

Suomen vallitsevassa sääntely-ympäristössä teletiedonhankintakeinojen heikko soveltuvuus kyberuhkien havaitsemiseen johtuu myös kyberuhkien ominaispiirteistä. Suomeen ja sen kansalliseen turvallisuuteen kohdistetut kyberteot pannaan yleensä toimeen maan rajojen ulkopuolella eikä toteuttaminen edellytä minkäänlaista fyysistä läsnäoloa Suomen alueella. Teot eivät tästä johtuen voi edes periaatteessa tulla Suomen viranomaisten tietoon ennen sitä hetkeä, jolloin teossa käytettävä

hyökkäysvektori, pääsääntöisesti tekninen haittaohjelma, ylittää Suomen rajan viestintäverkossa. Aikaväli tuon ajankohdan ja teon aiheuttamien vahinkoseurausten toteuttamisen välillä voi olla erittäin lyhyt. Lisäksi, kun kyse on kokonaisuudessaan sähköisissä viestintäverkoissa toteutettavista teoista, voidaan ne toteuttaa likipitäen minkä tahansa teleosoitteen tai telepäätelaitteen avulla. Kyberteossa ei tarvitse käyttää eikä siinä yleensä käytetäkään siinä maassa olevaa tai siihen maahan muuten viittaavaa teleosoitetta tai -päätelaitetta, joka on teon taustalla tai jossa tekijä muuten oleskelee. Kybertoimintaympäristö tarjoaa erinomaiset mahdollisuudet teon kohteen harhauttamiseen ja tekijän jälkien peittämiseen. Kaiken kaikkiaan kybertoimintaympäristössä toteutettaville kansallista turvallisuutta uhkaaville teoille leimallisia piirteitä ovat niiden alhaiset toteutuskustannukset, mahdollisuus käyttää samoja vektoreita toistuvasti ja useita kohteita vastaan, teoilta suojautumisen vaikeus ja kalleus sekä vähäinen kiinnijäämisriski.

Mahdollisuudet havaita ja estää kansallista turvallisuutta vaarantavia kybertekoja perustuvat nykyisin pääasiassa tietoyhteiskuntakaaren 272 §:ssä säädettyihin toimivaltuuksiin. Säännös antaa sähköisiä viestintäpalveluja hyödyntäville yrityksille, yhteisöille ja viranomaisille tietoturvastaan huolehtimisen tarkoituksessa oikeuden analysoida verkossaan tulevien ja siitä lähtevien viestien sisältöä muun muassa haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi. Säännös sallii myös viestien välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen, tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä ja muiden rinnastettavien teknisluonteisten toimenpiteiden suorittamisen.

Haitalliset ohjelmat ja käskyt tunnistetaan ensivaiheessa automaattisessa sisällöllisessä analysoinnissa ennalta tehtyjen määrittelyiden perusteella. Jos on ilmeistä, että automaattisessa analysoinnissa esiin noussut viesti sisältää haittaohjelman eikä tietoturvaa voida varmistaa automaattisin keinoin, sallii tietoyhteiskuntakaaren 272 § sen, että yritys, yhteisö tai viranomainen ottaa viestin sisällön manuaalisen käsittelyn kohteeksi.

Tietoyhteiskuntakaaren 272 §:n mukaisten toimintaoikeuksien käytössä, tapahtui se sitten tietoturvastaan huolehtivan yrityksen, yhteisön tai viranomaisten toimesta taikka HAVARO-järjestelmän puitteissa, on tekniseltä kannalta kyse pitkälti samankaltaisesta hakuehtojen käyttöön perustuvat tietoliikenteen seulonnasta ja seulonnassa esiin nousseiden viestien jatkokäsittelystä kuin tässä esityksessä ehdotetussa tietoliikennetiedustelussa. Tietoyhteiskuntakaaren 272 §:n mukaisessa toiminnassa hakuehtoina käytetään muun muassa haittaohjelmien sisältöä kuvaavia tunnisteita, haittaohjelmien levittämiseen käytettyjä teleosoitteita koskevia tunnisteita sekä sellaisia tunnisteita, jotka kuvaavat haittaohjelmille tyypillisiä liikennöintitapoja. Se, kyetäänkö toiminnassa tosiasiassa havaitsemaan kansallista turvallisuutta uhkaavaa haittaohjelmaliikennettä, riippuu seulonnassa hakuehtoina käytettävien haittaohjelmia koskevien tunnisteiden laadusta.

Yritysten, yhteisöjen ja viranomaisten toiminnassa käytettävät haittaohjelmatunnisteet ovat pääsääntöisesti sellaisia, jotka ovat kaupallisesti tai muuten yleisesti saatavilla. HAVARO-järjestelmään syötettävät tunnisteet perustuvat pääosin sellaisiin tietoihin, jotka Viestintäviraston Kyberturvallisuuskeskus on saanut kotimaisen ja kansainvälisen yhteisönsä puitteissa. Kyberturvallisuuskeskuksen keskeisiä kansainvälisiä yhteiskumppaneita ovat eri maiden valtionhallinnoissa toimivat ns. GovCERT-ryhmät.

Haittaohjelmista vaikeimmin havaittavia ja samanaikaisesti suurinta vahinkoa kansalliselle turvallisuudelle aiheuttavia ovat valtiolliset vakoilu- ja muut haittaohjelmat. Mahdollisuudet tällaisten haittaohjelmien havaitsemiseen yritysten, yhteisöjen ja viranomaisten itse toteuttamien tietoturvatoimenpiteiden puitteissa samoin kuin HAVARO-järjestelmän avulla ovat rajalliset. Syynä on ennen kaikkea se, että vakoilun ja muun vihamielisen valtiollisen toiminnan havaitsemiseksi välttämättömät tunnisteet eivät ole tietoyhteiskuntakaaren 272 §:ssä tarkoitettujen toimintaoikeutettujen tahojen käytössä eivätkä ne myöskään ole syötettävissä HAVARO-järjestelmään. Toiminnan havaitse-

miseksi tarvittavat tunnisteet ovat sellaista korkean suojatason tietoa, jota vaihdetaan tyypillisesti osana turvallisuus- ja tiedustelupalveluiden kansainvälistä yhteistyötä. Yhteistyö perustuu osapuolten väliseen luottamukseen. Yhteistyön puitteissa tapahtuvien tietojenluovutusten ehdoksi asetetaan lähes poikkeuksetta kielto luovuttaa tiedot edelleen ulkopuolisille. Koska HAVARO-järjestelmää ylläpitävä Viestintäviraston Kyberturvallisuuskeskus ei ole eikä voi olla osapuolena turvallisuus- ja tiedustelupalvelujen välisessä yhteistyössä, vaan se on tämän yhteistyön näkökulmasta ulkopuolinen, HAVARO-järjestelmään ei voida luovuttaa niittä tunnisteita, joiden merkitys kansallisen turvallisuuden suojaamiseksi olisi suurin.

Tietoyhteiskuntakaaren 272 §:n mahdollistamien tietoturvatoimenpiteiden, HAVARO mukaan lukien, tarkoituksena on toteuttaa tietoturvaa suojaamalla yksittäisiä kohdeorganisaatioita niihin kohdistuvilta loukkauksilta. Tietoturvatoimenpiteiden tarkoituksena ei ole kattaa niitä tiedontarpeita, jotka liittyvät kansallista turvallisuutta vaarantava toiminnan torjuntaan.

Tietoturvatoimenpiteiden näkökulmasta sellaiset kansallisen turvallisuuden ylläpitämisen kannalta olennaiset tiedot, kuten vakavimpien tietoturvaloukkausten syyt, olosuhteet, tekijät ja taustamotiivit eivät ole keskeisiä.

Edellä on todettu, että tietoyhteiskuntakaaren 272 §:ssä tarkoitettu toiminta teknisesti muistuttaa läheisesti tämän esityksen kansainvälistä vertailua käsittelevässä jaksossa kuvattua toimintaa, josta voidaan käyttää yhteisnimeä tietoliikennetiedustelu. Toimintojen teknisestä samankaltaisuudesta seuraa, että hakuehtoperusteiseen tietoliikenteen suodattamiseen perustuvaa tietoliikennetiedustelujärjestelmää voidaan käyttää myös haittaohjelmien tunnistamiseen.

Vertailuvaltioissa tietoliikennetiedustelulla on tärkeä asema paitsi kansallista turvallisuutta uhkaavaan toimintaan kohdistuvassa perinteisessä tiedustelussa, myös kyberuhkein havaitsemisen ja niiltä suojautumisen keinona (esim. Ruotsin mietintö ”En anpassad försvarsunderrättelseverksamhet”. Departementsserien 2005:30. Regeringskansliet/Försvarsdepartementet, s. 96–99). Tietoliikennetiedustelu mahdollistaisi ennen kaikkea niiden kyberuhkien havaitsemisen, jotka kaikkein vakavimmilla tavalla vaarantavat yhteiskunnan keskeiset turvallisuusedut.

Ulkomaan tietojärjestelmätiedustelu

Tiedonhankintalakityöryhmän mietinnössä todetusti turvallisuusviranomaisten tulisi säätää ulkomaan tietojärjestelmätiedustelusta. Ulkomaan tietojärjestelmätiedustelulla tarkoitetaan ulkomaisessa tietojärjestelmässä käsiteltävien tietojen hankinnasta tietoteknisin menetelmin.

Ulkomaan tietojärjestelmätiedustelu voidaan toteuttaa hyödyntämällä teknistä laitetarkkailun ja tietyiltä osin teknisen kuuntelun menetelmiä. Koska ulkomaan tietojärjestelmätiedustelu on tiedonhankintana pitkäkestoista ja sen käyttö edellyttää mahdollisten ulkopoliittisten liittymäpintojen tarkkaa tunnistamista sekä siihen liittyvää harkinta, ei teknistä laitetarkkailua ja teknistä kuuntelua voida pitää tarkoituksen mukaisin tiedonhankintakeinoina tältä osin. Lisäksi ulkomaan tietojärjestelmäntiedustelun kokonaisuuden kannalta ei voida pitää tarkoituksen mukaisena sitä, että sen käyttäminen edellyttäisi kahta erillistä lupaharkintaa.

Suomalaisella viranomaisella ei ole toimivaltuuksia suorittaa tiedonhankintaa Suomen rajojen ulkopuolella, vaikka tiedonhankinta tapahtuisi Suomen alueelta käsin ulkomailla olevasta tietojärjestelmästä. Lisäksi tietojärjestelmätiedustelussa olisi tarkoituksen mukaista ohittaa tietojärjestelmän suojaus tietoteknisin menetelmin, mikä ilman nimenomaista säännöstä ei olisi mahdollista suomalaiselle viranomaiselle.

2.4.5 Päätöksenteko

Päätösvalta eräiden Puolustusvoimien käyttämien salaisten tiedonhankintakeinojen käyttämisestä on edelle kerrotulla tavalla jakautunut tuomioistuimelle tai pääesikunnan apulaisosastopäällikölle tai sotilaslakimiehelle. Puolustusvoimien rikostorjuntatoimivaltuudet perustuvat poliisilain 5 luvun säännöksiin.

SKRTL:n ja poliisilain 5 luvun salaisten tiedonhankintakeinoista yhteenvedonomaisesti todettakoon, että poliisilain 5 luvun mukaisista toimivaltuuksista telekuuntelu, tietojen hankkiminen telekuuntelun sijasta ja tukiasematietojen hankkiminen edellyttävät tuomioistuimen lupaa. Myös televalvonnasta päättäminen kuuluu useimmiten tuomioistuimen toimivaltaan. Sellaisissa kiireellisissä tilanteissa, joissa poliisi voi tilapäisesti itse päättää televalvonnasta, asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta. Poliisi voi kuitenkin päättää televalvonnasta henkeä tai terveyttä uhkaavan vaaran torjumiseksi sekä henkilön suostumuksella tehtävästä televalvonnasta epäiltäessä sellaisia rikoksia, jotka suoraan liittyvät teleosoitteeseen tai telepäätelaitteeseen.

Salaisen tiedonhankintakeinon käyttöä koskeva vaatimus on poliisilain 5 luvun 45 §:n mukaan otettava viipymättä tuomioistuimessa käsiteltäväksi vaatimuksen tehneen tai hänen määräämänsä asiaan perehtyneen virkamiehen läsnä ollessa. Asia on ratkaistava kiireellisesti. Asia voidaan ratkaista kuulematta henkilöä, jonka perustellusti voidaan olettaa syyllistyvän tai syyllistyneen rikokseen, ja pääsääntöisesti kuulematta teleosoitteen tai telepäätelaitteen haltijaa.

Salaista tiedonhankintamenetelmää koskevassa lupa-asiassa annettuun päätökseen ei saa hakea muutosta valittamalla. Päätöksestä saa ilman määräaikaa kannella.

Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta ja televalvonnasta on poliisilain 5 luvun 58 §:n mukaan viipymättä ilmoitettava tiedonhankinnan kohteelle sen jälkeen, kun tiedonhankinnan tarkoitus on saavutettu. Salaisen tiedonhankintakeinon käytöstä on kuitenkin ilmoitettava tiedonhankinnan kohteelle viimeistään vuoden kuluttua sen käytön lopettamisesta. Tuomioistuin voi kuitenkin pidättämiseen oikeutetun poliisimiehen vaatimuksesta päättää, että ilmoitusta tiedonhankinnan kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan. Edellytyksenä ilmoittamisen lykkäämiselle on, että lykkääminen on perusteltua käynnissä olevan tiedonhankinnan turvaamiseksi, valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saadaan tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi.

Käytännössä tuomioistuin myöntää luvan telekuuntelun ja televalvonnan käyttöön valtaosassa tapauksista. Kielteisiä päätöksiä arvioidaan olevan vuosittain muutamia. Vuonna 2015 tuomioistuimet hylkäsivät 11 poliisin telepakkokeinovaatimusta, jotka kaikki koskivat pakkokeinolain perusteella tehtyjä hakemuksia.

Sotilastiedustelulaki perustuu olennaisilta osiltaan poliisilain 5 luvun sääntelyn varaan. Perus- ja ihmisoikeuksiin puuttumisen tuntuvuutta korostava näkökohta puhuu sen puolesta, että nykyisin käytettävissä olevien salaisten tiedonhankintakeinojen osalta tuomioistuimen päätöksentekotoimivalta säilyisi pitkälti ennallaan. Päätöksentekotoimivaltaan liittyvät perus- ja ihmisoikeuspuuttumiset keinokohtaisesti on arvioitu esitutkinta- ja pakkokeinotoimikunnan (Oikeusministeriön komiteanmietintö 2009:2) työn yhteydessä. Siksi myös sotilastiedustelulaissa tiedustelumenetelmien päätöksentekoa koskevien perusratkaisujen kohdalla on perusteltua seurata poliisilain 5 luvun sääntelyä mahdollisimman pitkälle.

Tiedustelumenetelmien lisäksi tulee säätää ulkomaan tiedustelusta päättämisestä. Tuomioistuimella ei lähtökohtaisesti ole toimivaltaa päättää toimivaltuuden käytöstä muualla kuin Suomessa. Ope-

ratiivista päätöksentekoa ei myöskään ole tarkoituksenmukaista viedä oikeudellisessa järjestelmässä uusille toimijoille ulkomaan tiedusteluun liittyvien ulkopoliittisesti sensitiivisten elementtien takia. Kansainväliseen vertailuun kuuluvien, joidenkin maiden sekä eräiden muiden maiden kohdalla ulkomaan tiedustelusta päättää tiedusteluviraston päällikkö. Ulkomaan tiedustelua koskevasta päätöksenteosta sotilastiedustelussa on perusteltua säätää vastaavalla tavalla. Poliisilain 5 luvun perusteella suojelupoliisin päällikkö päättää nykyisin kaikkein kovimpien keinojen, peitetoiminnan ja valeoston käyttämisestä, joiden päätösarviointiin liittyy vakavuudeltaan vastaavantyyppisiä seikkoja, mitä ulkomaan tiedusteluun. Tarkoituksen mukaista olisi, että sotilastiedustelun osalta päätöksenteko olisi samalla tasolla, jolloin päätöksentekijänä voisi olla pääesikunnan tiedustelupäällikkö.

Myös tiedustelumenetelmien käytöstä ilmoittamista koskeva sääntely olisi perusteltua mainituista syistä säännellä vastaavalla tavalla kuin poliisilain 5 luvussa sotilastiedusteluun liittyvät erityispiirteet huomioiden.

2.4.6 Kaikille salaisille tiedonhankintakeinoille yhteiset säännökset

Tiedonhankinnan suojaaminen

Puolustusvoimat ei voi käyttää rikostorjunnan toimivaltuuksien osalta käyttää tiedonhankinnan suojaamista. Vertailukohtana olevassa poliisilaissa tiedonhankinnan suojaamisesta säädetään lain 5 luvun 46 §:ssä. Pykälän 1 momentti koskee poliisin mahdollisuutta siirtää puuttumista rikokseen salaisen tiedonhankintakeinon käytön aikana. Edellytyksenä on, ettei puuttumisen siirtämisestä ei aiheudu merkittävää vaaraa kenenkään hengelle, terveydelle tai vapaudelle eikä merkittävää huomattavan ympäristö-, omaisuus- tai varallisuusvahingon vaaraa. Edellytyksenä on lisäksi, että puuttumisen siirtäminen on välttämätöntä tiedonhankinnan paljastumisen estämiseksi tai toiminnan tavoitteen turvaamiseksi.

Pykälän 2 momentin mukaan poliisi saa käyttää vääriä, harhauttavia tai peiteltyjä tietoja, tehdä ja käyttää vääriä, harhauttavia tai peiteltyjä rekisterimerkintöjä sekä valmistaa ja käyttää vääriä asiakirjoja, kun se on välttämätöntä jo toteutetun, käynnissä olevan tai tulevaisuudessa toteutettavan salaisen tiedonhankintakeinon käytön suojaamiseksi.

Nykyisen sääntelyn perusteella suojausta voidaan käyttää kaikissa salaisissa tiedonhankintakeinoissa (myös peitellyssä tiedonhankinnassa), koska tarve voi ilmetä esimerkiksi poliisin omilla laitteilla suoritettavassa televalvonnassa. Momentin turvin ei kuitenkaan voida antaa tietolähteelle tai kenellekään sivulliselle peitehenkilöllisyyttä, vaan tarkoituksena on suojata toimintaa.

Vääränsisältöisten kirjausten ja merkintöjen tekemistä käsitellään eduskunnan apulaisoikeusasiamiehen ratkaisussa 571/2/08. Kysymys liittyy siihen, että poliisilla on tutkintapakko, lainmukaisten kirjausten tekemisen vaatimus ja valeoston ja peitetoiminnan salassapitointressit ovat keskenään jännitteessä. Laista ei saa selvää vastausta esimerkiksi siihen, voidaanko ja missä määrin salaisen tiedonhankintamenetelmän paljastumisen estämiseksi laatia vääränsisältöisiä esitutkintapöytäkirjoja tai tutkintailmoituksia.

Kyse on monessa tapauksessa intressipunninnasta ja kokonaisharkinnasta. Lähtökohtana on, että kovin kevyesti ei kovia suojauskeinoja siihen liittyvien ongelmien ja oikeusturvasyiden johdosta tulisi tehdä. Lähtökohtaisesti väärän viranomaisasiakirjan tekemisestä aiheutuu myös väärä rekisterimerkintä julkista luottamusta nauttiviin viranomaisrekistereihin. Siksi suojauksen tekemisen tulee olla välttämätöntä.

Väärien merkintöjä ei kuitenkaan saa jättää rekistereihin, vaan pykälän 3 momentissa säädetään rekisterimerkintöjen oikaisuvelvollisuudesta.

Kyseisenlaisesta tiedonhankinnan suojaamisesta on korostunut tarve säätää myös sotilastiedustelun suojaamiseksi. Lähtökohtana on, että koko sotilastiedustelutoimintaa tulee voida suojata. Tiedustelutoimintaan liittyy monenlaisia herkkyyksiä ja kohteena voi olla toisen valtion hallinto, yksittäinen korkean intressin henkilö tai henkilöjoukko, jokin teollisuuden haara tai yksittäinen yritys. Käytännössä tiedustelussa pyritään hankkimaan tietoa kohteen tietämättä ja tahdonvastaisesti. Paljastumisriskin minimoimiseksi suojauksen käyttäminen tulisi mahdollistaa jo aikaisessa vaiheessa. Esimerkiksi omien vakoojien suojaus soluttautumalla vieraan valtion vastavakoiluorganisaatioon edellyttäisi huomattavasti intensiivisempiä suojaustoimia ja niiden aloittamista hyvin varhaisessa vaiheessa. Sotilastiedustelutoiminnassa suojauksen käyttämisen kohdalla ei olisi myöskään vastaavanlaisia oikeusturvaongelmia mitä rikosperusteisia toimivaltuuksia käytettäessä, sillä sotilastiedustelun lähtökohtaisena tarkoituksena olisi hankkia tietoa toiminnasta, joka uhkaa maanpuolustusta tai vakavasti uhkaa kansallista turvallisuutta.

Kuuntelu- ja katselukiellot

Puolustusvoimien rikostorjunnassa ei ole käytössä toimivaltuuksia, joiden takia olisi tarkoituksen mukaista säätää erityisistä kuuntelu- ja katselukielloista. Salaisia tiedonhankintakeinoja koskevan poliisilain 5 luvussa kuuntelu- ja katselukielloista on säädetty luvun 50 §:ssä. Pykälän mukaan telekuuntelua, telekuuntelun sijasta toimitettavaa tietojen hankkimista, teknistä kuuntelua ja teknistä katselua koskevista kielloista on soveltuvin osin voimassa, mitä pakkokeinolain 10 luvun 52 §:ssä säädetään.

Pakkokeinolain 10 luvun 52 §:n 1 momentin mukaan Telekuuntelua, tietojen hankkimista telekuuntelun sijasta, teknistä kuuntelua ja teknistä katselua ei saa kohdistaa: 1) rikoksesta epäillyn ja hänen oikeudenkäymiskaaren 17 luvun 13 §:n 1 tai 3 momentissa tarkoitetun oikeudellisen avustajansa tai 1 momentissa tarkoitetun tulkin taikka mainittuun avustajaan 22 §:n 2 momentissa tarkoitetussa suhteessa olevan henkilön väliseen viestiin; 2) rikoksesta epäillyn ja oikeudenkäymiskaaren 17 luvun 16 §:ssä tarkoitetun papin tai muun vastaavassa asemassa olevan henkilön väliseen viestiin; eikä 3) rikoksen johdosta vapautensa menettäneen epäillyn ja lääkärin, sairaanhoitajan, psykologin tai sosiaalityöntekijän väliseen viestiin. Pykälän 3 momentin mukaan, jos telekuuntelun, telekuuntelun sijasta tapahtuvan tietojen hankkimisen, teknisen kuuntelun tai teknisen katselun aikana tai muulloin ilmenee, että kyseessä on viesti, jonka kuuntelu ja katselu on kielletty, toimenpide on keskeytettävä ja sillä saadut tallenteet ja sillä saatuja tietoja koskevat muistiinpanot on heti hävitettävä. Pykälän 4 momentin mukaan tässä pykälässä tarkoitetut kuuntelu- ja katselukiellot eivät kuitenkaan koske tapauksia, joissa 1 tai 2 momentissa tarkoitettua henkilöä epäillään samasta tai siihen välittömästi liittyvästä rikoksesta kuin rikoksesta epäiltyä ja myös hänen osaltaan on tehty päätös telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, teknisestä kuuntelusta tai teknisestä katselusta.

Edellä kerrotut kuuntelu- ja katselukiellot on säädetty rikosprosessia ja rikosprosessuaalisia pakkokeinoja silmällä pitäen. Vaikka kuuntelu- ja katselukiellot ovat merkityksellisessä asemassa myös siviilitiedustelussa, niin niiden status näyttäytyy eri tavalla mitä rikosprosessissa. Siviilitiedustelussa kyseisiä kieltoja tulee arvioida lähes yksinomaan rikosprosessin ulkopuolisina kieltoina, joilla ei ole välitöntä kytkentää rikoksesta epäillyn oikeusturvaan. Tiedustelumenetelmillä kuitenkin puututaan yhtä lailla perus- ja ihmisoikeuksiin mitä salaisilla tiedonhankintakeinoilla, vaikka tiedustelumenetelmien varsinaisena tarkoituksena ei olekaan rikosprosessuaalinen. Sotilastiedustelussa käytettävien tiedustelumenetelmien käytössä tulee yhtä lailla säätää kuuntelu- ja katselukielloista kuin muita salaisia tiedonhankintakeinoja käytettäessä.

Poliisi- ja pakkokeinolaeissa säännellyistä rikoksen estämisestä, paljastamisesta ja selvittämisestä poiketen tiedustelumenetelmää ei kohdistettaisi rikoksesta epäiltyyn tai oletettuun tulevaan rikoksentekijään. Siviilitiedustelussa kyse olisi tiedon hankkimisesta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Myöskään sotilastiedustelun kohdehenkilöiden asemaa ja henkilörelaatioi-

ta voi olla hankala tunnistaa alkuvaiheessa eikä oikeudenkäymiskaaren 17 luvun 17 §:ssä tarkoitettujen läheisten välinen viestinnän suojaaminen ole yhtä merkityksellisessä asemassa mitä rikosprosessissa.

Sotilastiedustelun ominaispiirteiden vuoksi tulisi säätää, ettei telekuuntelua, telekuuntelun sijasta toimitettavaa tietojen hankkimista, teknistä kuuntelua ja teknistä katselua saisi kohdistaa sellaiseen viestintään, josta viestinnän osapuoli ei saisi todistaa oikeudenkäymiskaaren 17 luvun 13, 14, 16, 20 tai 22 §:n 2 momentin nojalla. Oikeudenkäymiskaaren 17 luvun 13 §:ssä säädetään oikeudenkäyntiasiamiehen ja -avustajan sekä tulkin velvollisuudesta olla luvattomasti todistamatta siitä, mitä hän on saanut tietää hoitaessaan oikeudenkäyntiin liittyvää tehtävää, antaessaan oikeudellista neuvontaa päämiehen oikeudellisesta asemasta esitutkinnassa tai muussa oikeudenkäyntiä edeltävässä käsittelyvaiheessa, antaessaan oikeudellista neuvontaa oikeudenkäynnin käynnistämiseksi tai sen välttämiseksi. Lisäksi pykälässä säädetään asianajajan ja luvan saaneista oikeudenkäyntiavustajista annetussa laissa tarkoitetun oikeudenkäyntiavustajan sekä julkisen oikeusavustajan velvollisuudesta olla luvattomasti todistamatta yksityisen tai perheen salaisuudesta tai liike- tai ammattisalaisuudesta, josta hän on muussa kuin edellä tarkoitetussa tehtävässään saanut tiedon. Oikeudenkäymiskaaren 17 luvun 14 §:ssä säädetään lääkärin ja muun terveydenhuollon ammattihenkilön velvollisuudesta olla todistamatta henkilön tai hänen perheensä terveydentilaa koskevasta arkaluonteisesta tiedosta tai muusta henkilön tai perheen salaisuudesta, josta hän asemansa tai tehtävänsä perusteella on saanut tiedon, ellei se, jonka hyväksi salassapitovelvollisuus on säädetty, suostu todistamiseen. Oikeudenkäymiskaaren 17 luvun 16 §:ssä säädetään papin ja muun vastaavassa asemassa olevan henkilön velvollisuudesta olla todistamatta siitä, mitä hän on ripissä tai yksityisessä sielunhoidossa saanut tietää, ellei se, jonka hyväksi salassapitovelvollisuus on säädetty, suostu todistamiseen. Oikeudenkäymiskaaren 17 luvun 20 §:ssä säädetään sananvapauden käyttämisestä joukkoviestinnässä annetussa laissa tarkoitetun yleisön saataville toimitetun viestin laatijan sekä julkaisijan ja ohjelmatoiminnan harjoittajan oikeudesta kieltäytyä todistamasta siitä, kuka on antanut viestin perusteena olevat tiedot tai laatinut yleisön saataville toimitetun viestin. Oikeudenkäymiskaaren 17 luvun 22 §:n 2 momentti laajentaa eräiden edellä mainittujen todistelukieltojen ja oikeuksien olla todistamatta henkilöllistä soveltamisalaa. Kyseisen lainkohdan mukaan sillä, joka on saanut 11 §:n 2 tai 3 momentissa, 13 §:n 1 tai 3 momentissa, 14 §:n 1 momentissa taikka 20 §:n 1 momentissa tarkoitetun tiedon toimiessaan lainkohdassa tarkoitetun henkilön palveluksessa tai muuten hänen apunaan, on vastaava velvollisuus tai oikeus kieltäytyä todistamasta kuin vastaavassa lainkohdassa tarkoitetulla henkilöllä. Tarpeen ei kuitenkaan olisi ulottaa viittausta koskemaan 11 §:n 2 ja 3 momenttia, joita koskevasta kiellosta ei muutenkaan esitetä säädettäväksi.

Lisäksi olisi tarpeen säätää toimenpiteistä, jos kuuntelun tai katselun aikana tai muulloin ilmenee, että kyseessä on viesti, jonka kuuntelu ja katselu on kielletty. Toimenpide olisi tällöin keskeytettävä ja sillä saadut tallenteet ja sillä saatuja tietoja koskevat muistiinpanot heti hävitettävä. Selvyyden vuoksi myös kiellon väistymisestä tulisi erikseen säätää silloin, kun uhkan lähde olisi kuuntelu- tai katselukiellon kohteena.

Tietojen luovuttaminen muille esitutkintaviranomaisille

SKRTL:ään ei sisälly säännöstä tietojen luovuttamisesta muille esitutkintaviranomaisille. Lähin esikuva on poliisilain 5 luvun 54 §, jossa säädetään ylimääräisen tiedon käyttämisestä. Poliisilain 5 luvun 53 § määrittelee ylimääräiseksi tiedoksi telekuuntelulla, televalvonnalla, tukiasematietojen hankkimisella ja teknisellä tarkkailulla saadun tiedon, joka ei liity rikokseen tai vaaran torjumiseen taikka joka koskee muuta rikosta kuin sitä, jonka estämistä tai paljastamista varten lupa tai päätös on annettu. Ylimääräinen tieto voidaan toisin sanoen määritellä informaatioksi, joka on saatu lainmukaisen tiedonhankinnan käytön sivutuotteena siten, että se ei ole ollut toimenpiteiden varsinaisena tai suunniteltuna tarkoituksena. Ylimääräistä tietoa koskeva sääntely muodostaa eräänlaisen välitilan vapaan todistusteorian mukaisen vapaan hyödynnettävyyden ja todistamiskieltoja koskevi-

en rajoitusten välillä. Tiedossa voi olla kysymys jotakin rikosta koskevasta tiedosta tai sitten täysin rikokseen liittymättömästä, mutta viranomaisen toiminnan kannalta merkityksellisestä tiedosta.

Poliisilain 5 luvun 54 §:n 1 momentin mukaan ylimääräistä tietoa saa käyttää rikoksen selvittämisessä, kun tieto koskee sellaista rikosta, jonka estämisessä olisi saatu käyttää sitä tiedonhankintakeinoa, jolla tieto on saatu. Rikoksen selvittämisellä tarkoitetaan, että tietoa on tarkoitus käyttää näyttönä syyllisyyden tukena tai tiedonhankintakeinoa koskevan ratkaisun perusteena (välitön hyödyntäminen) erotuksena esimerkiksi tutkinnan suuntaamistarkoituksesta, jolloin ylimääräisen tiedon hyödyntäminen on vapaampaa (välillinen hyödyntäminen). Ylimääräisen tiedon "näyttökäyttöä" koskevassa rajoituksessa on kysymys hyödyntämiskiellosta.

Poliisilain 5 luvun 54 §:n 2 momentin mukaan ylimääräistä tietoa voidaan aina käyttää rikoksen estämiseksi, poliisin toiminnan suuntaamiseksi ja syyttömyyttä tukevana selvityksenä. Rikoksen estämisen osalta on muistettava, että se sisältää myös jatkuvan rikoksen keskeyttämisen. Rikoksen paljastamiseen tietoa ei sen sijaan voida käyttää. Tietoa voidaan käyttää näyttönä (todisteena) aina syyttömyyden tueksi, vaikka tiedon käyttäminen voi tosiasiallisesti vahvistaa jonkun toisen syyllisyyttä. Pykälän 3 momentin mukaan ylimääräistä tietoa saa käyttää johdonmukaisesti myös hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi. Mitään lisäedellytyksiä ei ole asetettu ylimääräisen tiedon käytölle nyt puheena olevan pykälän 2 ja 3 momentin tarkoittamissa tilanteissa.

Ylimääräistä tietoa syntyy kaikenlaisten viranomaisille kuuluvien toimenpiteiden yhteydessä. Selvää on, että myös tiedustelumenetelmien käyttö väistämättä tuottaisi muutakin kuin maanpuolustusta tai kansalliseen turvallisuutta uhkaavaa tietoa. Monessa tapauksessa kyseinen tieto tulisi välittömästi hävittää irrelevanttiusperusteella, mutta osa maanpuolustuksen tai kansallisen turvallisuuden kannalta merkityksetön tieto saattaisi koskea vakavaa rikosta. Siksi tarvitaan sääntelyä ohjaamaan tällaisen tiedon eteenpäin saattamista paitsi relevanteille tiedonsaajille ylipäätään, erityisesti myös esitutkintaviranomaisille. Sotilastiedustelun ja rikosprosessin rajapintaan asemoitava, ja siinä tiedon luovuttamista esitutkintaviranomaisille säätelevä normi olisi monitahoinen ja periaatelatautunut. Rikoksen täyttymistä edeltävässä vaiheessa sen estämistavoitteella on etusija esitutkintavaihetta määrittävään rikoksen selvittämisintressiin nähden. Tällöin on kyse toimenpiteistä, jotka ovat yhtäältä välttämättömiä vaaran ja vahingon välttämiseksi ja joilla toisaalta ei pääsääntöisesti loukata yksilön oikeusturvan keskeistä ydinaluetta. Tuomioistuinvaiheessa sitä vastoin ei ole yleensä katsottu yksilön oikeusturvaintressin vastapainona olevan mitään vahvaa kilpailevaa intressiä. Sotilastiedustelussa puolestaan maanpuolustuksen ja kansallisen turvallisuuden suojaamistavoitteella on lähtökohtainen etusija rikoksen estämisintressiin ja selvittämisintressiin nähden. Sotilastiedustelussa on nimittäin kyse toimenpiteistä, jotka ovat välttämättömiä valtion tai yhteiskunnan keskeisten etujen puolustamiseksi ja niiden turvaamiseksi. Yksi tällainen etu on oikeusjärjestelmän, mukaan lukien rikosprosessijärjestelmän, toimivuus. Tämän vuoksi poliisilain 5 luvun 54 § ei sellaisenaan sovi esikuvaksi säädettäessä tiedon ilmoittamisesta rikostorjuntaan, sillä siinä ei ole otettu huomioon sotilastiedustelun maanpuolustukseen ja kansalliseen turvallisuuteen kytkeytyvää suojaamisintressiä.

Ensimmäinen lähtökohta tiedon luovuttamista rikostorjuntaa koskevalle säännökselle on, että siinä olisi asetettava ilmoitusvelvollisuus esitutkintaviranomaiselle viime kädessä rikoslain 15 luvun 10 §:ssä mainituista rikoksista, sillä jokaisella on ilmoitusvelvollisuus näin vakavista ja vielä estettävissä olevista rikoksista. Tällaisiin tekoihin liittyy jo niin suuri rikoksen estämis- ja selvittämisintressi, ettei niiden kohdalla ole kriminaalipoliittisesti hyväksyttävissä tiedustelun yhteydessä ilmenneen rikostiedon esitutkintaviranomaisille luovuttamatta jättäminen eli toimenpide, jolla voidaan välttää vakavan vaaran realisoituminen tai vahingon syntyminen taikka myötävaikuttaa törkeän rikoksen selvittämiseen. Johdonmukaista olisi edelleen, että 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. Näissä pääasiassa individualistisissa eduissa on paljon yhtäläisyyksiä niiden kollektiivisten etujen kanssa, joita tiedustelulla osaltaan pyritään suojelemaan. EIS 6 artiklan 2 kohdassa turvatun syyttömyysolettaman kannalta tulisi kuitenkin suhtautua pidättyvästi sääntelyyn, joka mahdollistaisi tiedon luovuttamisen kaikista, myös vähäisistä, rikoksista esitutkintaviranomaiselle. Samasta syystä olisi myös tarkoin arvioitava, voidaanko tietoa ylipäätään antaa esitutkintaviranomaisille rikostiedustelutarkoituksessa tai poliisin toiminnan suuntaamiseksi.

Tiedonhankinnasta ilmoittaminen

Oikeusturvakysymykset ovat salaisen tiedonhankinnan luonteesta johtuen korostetun tärkeitä niin sellaisten toimenpiteiden kohteiksi joutuvien asianosaisten ja sivullisten kannalta kyin ylipäätään koko oikeudellisen järjestelmän uskottavuuden kannalta. Eräs tärkeimmistä oikeusturvatakeista on se, että asianosainen saa tutustua viranomaisella olevaan aineistoon. Ennen kuin asianosainen voi tehdä tämän, hänellä on oltava mahdollisuus saada tieto salaisen tiedonhankinnan käytöstä. Asianosaisen tiedonsaantioikeus on myös tärkeä oikeudenmukaisen oikeudenkäynnin edellytys (PL 21 §, EIS 6 artikla 1 kappale ja KP-sopimus 14 artikla 1 kappale).

Tästä erillinen on kysymys oikeudesta saada tieto salaisen tiedonhankintakeinon käyttöä koskevasta asiakirjasta tai tallenteesta. Asianosaisen oikeudesta tiedonsaantiin säädetään viranomaisten toiminnan julkisuudesta annetun lain 11 §:ssä. Pykälän 1 momentin mukaan lähtökohta on, että asianosaisella on oikeus saada asiaa käsittelevältä tai käsitelleeltä viranomaiselta tieto muunkin kuin yleisöjulkisen asiakirjan sisällöstä, joka voi tai on voinut vaikuttaa hänen asiansa käsittelyyn. Pykälän 2 momentissa säädetään tapauksista, joissa asianosaisella, hänen edustajallaan tai avustajallaan ei ole 1 momentissa tarkoitettua oikeutta. Rajoitus koskee esimerkiksi asiakirjaa, josta tiedon antaminen olisi vastoin erittäin tärkeää yleistä tai yksityistä etua, ja asiakirjaa, joka on esitutkinnassa laadittu ennen tutkinnan lopettamista, jos tiedon antamisesta aiheutuisi haittaa asian selvittämiselle.

EIS 6 artiklan 1 kappaleen tarkoituksena on muun ohessa suojata osapuolia salaiselta oikeudenkäytöltä. Asianosaisten tasa-arvo, aseiden yhtäläisyys ja kuulemisperiaatteet ovat tärkeitä tekijöitä arvioitaessa sitä, onko oikeudenkäyntiä pidettävä kokonaisuudessaan oikeudenmukaisena. Ne edellyttävät asianosaisen mahdollisuutta esittää asiansa olosuhteissa, jotka eivät aseta häntä vastapuoleen verrattuna asiallisesti huonompaan asemaan. Asianosaisten yhdenvertaisuus edellyttää asianosaisten tasavertaista ja puolueetonta kohtelua tuomioistuimessa. Tiedonsaantioikeutta edellyttävät myös epäillyn oikeus puolustuksensa tehokkaaseen valmisteluun ja vastatodisteluun. Toisaalta on huomattava, ettei aseiden yhtäläisyysperiaatetta loukata sillä, että oikeudenkäyntiaineistosta puuttuu jotakin. Toisin on arvioitava sitä tilannetta, että toisella asianosaisella on käytössään tai tiedossaan jokin toiselta salassa oleva tai salassa pidetty seikka. Lisäksi on otettava huomioon se lähtökohta, että oikeudenkäyntivaiheessa viranomaisella ei ole oikeutta suorittaa arviota jonkin tiedon merkityksestä, vaan se on asianosaisen nimenomainen oikeus.

EIS 6 artiklan 2 kappaleessa ilmaistun syyttömyysolettaman kannalta voi olla merkityksellistä esimerkiksi se, että erilaisilla motiiveilla toimivat tietolähteet eivät halua tai kykene antamaan objektiivista tietoa tai ainakin suuntaavat tiedon hankkimisen omien motiiviensa mukaisesti. Mikäli lähtökohtana on, ettei tietolähteen henkilöllisyyttä tai ylipäätään tietolähteen käyttöä paljasteta, ei tietolähteen vastuu annetun tiedon laadusta tai sen käytöstä voi toteutua, vaan vastuu on viranomaisella.

Myös salaamisen puolesta voidaan esittää vahvoja perusteita. Tällaisia intressejä ovat ainakin tärkeät tutkinnalliset syyt. Lisäksi hengen ja terveyden suoja, valtion turvallisuus sekä salassa pidettävien taktisten ja teknisten menetelmien suojaaminen voivat edellyttää tiedon antamisen lykkäämistä tai tiedonhankinnan salaamista jopa kokonaan. Lykkäämisen pituutta määriteltäessä rikoksen selvittämisen vaarantumiselle voidaan ajatella jokin takaraja, kun taas valtion turvallisuuden

sekä hengen ja terveyden suojan tarve voi olla pidempikestoisempi, jopa pysyvä. Esimerkiksi peitetoiminnassa pelkkä tieto keinon käytöstä paljastaa käytännössä peitehenkilön aikaisemmat rikoksen estämistä tai paljastamista koskevat operaatiot ja aiheuttaa sen, ettei peitehenkilöä voida enää tulevaisuudessa käyttää. Lisäksi tieto voi pahimmassa tapauksessa vaarantaa peitehenkilön ja hänen läheistensä hengen ja terveyden. Mikäli samaan asiaan liittyy esimerkiksi sekä tietolähde että peitehenkilö, riittää jo toisen henkilön paljastuminen saattamaan molemmat henkilöt ja heidän läheisensä hengen ja terveyden vaaraan.

EIT on muun muassa ratkaisuissaan Rowe ja Davis v. Yhdistynyt kuningaskunta 16.2.2000, Natunen v. Suomi 31.3.2009, Janatuinen v. Suomi 8.12.2009, Bannikova v. Venäjä 4.11.2010 ja Bulfinsky v. Romania 1.6.2010 hyväksyt sen, ettei kaikkea aineistoa paljasteta epäillylle, jos vastakkainen intressi koskee kansallista turvallisuutta, hengen ja terveyden suojaa tai salassa pidettäviä tutkintamenetelmiä. EIS 6 artiklan 1 kappale sallii kuitenkin vain ehdottoman välttämättömät syytetyn oikeuksiin puuttumiset.

Poliisilain 5 luvun 58 §:n 1 momentti koskee telekuuntelua, tietojen hankkimista telekuuntelun sijasta, televalvontaa, suunnitelmallista tarkkailua, peiteltyä tiedonhankintaa, teknistä tarkkailua ja valvottua läpilaskua. Näiden keinojen käyttämisestä on viipymättä ilmoitettava tiedonhankinnan kohteelle kirjallisesti sen jälkeen, kun tiedonhankinnan tarkoitus on saavutettu. Ehdoton takaraja 1 momentissa on kuitenkin vuosi tiedonhankintakeinon käytön lopettamisesta, jonka jälkeen siitä on ilmoitettava tiedonhankinnan kohteelle. Kohteelle ilmoittamisesta on samalla annettava kirjallisesti tieto luvan myöntäneelle tuomioistuimelle. Kyseinen momentti ei koske tukiasematietojen hankkimista, tarkkailua ja teleosoitteen tai telepäätteen yksilöintitietojen hankkimista. Ilmoitus on yksilöitävä sellaisella tarkkuudella, että tiedonhankinnan kohde voi tarvittaessa pyrkiä selvittämään häneen kohdistetun keinon käytön perusteita. Ilmoituksessa on mainittava mistä tiedonhankintakeinosta on kysymys sekä se, missä ja milloin keinoa on käytetty. Salassa pidettäviä taktisia ja teknisiä menetelmiä ilmoituksessa ei tarvitse paljastaa. Mikäli kohteen henkilöllisyys jää epäselväksi, ilmoitus ei luonnollisesti voida tehdä. Jos kohteen henkilöllisyys myöhemmin selviää, ilmoitus on tehtävä jälkikäteen. Vaikka salaiset tiedonhankintakeinot kohdistuvat tosiasiallisesti myös muihin henkilöihin, heille ei ilmoitusta tarvitse tehdä.

Poliisilain 5 luvun 58 §:n 3 momentti koskee suunnitelmallista tarkkailua, peiteltyä tiedonhankintaa, peitetoimintaa, valeostoa ja tietolähteen ohjattua käyttöä. Pääsääntönä on, että näistä keinoista on ilmoitettava tiedonhankinnan kohteelle, jos asiassa aloitetaan esitutkinta. Jos esitutkinta aloitetaan, noudatetaan soveltuvin osin, mitä pakkokeinolain 10 luvun 60 §:ssä säädetään. Kohteelle ilmoittamisesta on samalla annettava kirjallisesti tieto luvan myöntäneelle tuomioistuimelle ja peitetoiminnan osalta pakkokeinolain 32 §:ssä tarkoitetulle tuomioistuimelle eli Helsingin käräjäoikeudelle. Sama koskee valeostoa ja tietolähteen ohjattua käyttöä pakkokeinolain 10 luvun 60 §:n 7 momentin nojalla ja noudattaen soveltuvin osin saman luvun 43 §:n 6 momentin sääntelyä. On huomattava, että ainoastaan peitetoiminnassa tuomioistuimella on rooli päätöksentekoprosessissa. Näin ei ole valeostossa ja tietolähteen ohjatussa käytössä. Tästä huolimatta kaikkien näiden keinojen osalta tuomioistuimelle on annettava kirjallisesti tieto kohteelle ilmoittamisesta.

Poliisilain 5 luvun 58 §:n 2 momentti sisältää puolestaan ilmoittamista koskevia pääsääntöjä koskevat poikkeukset. Momentin mukaan tuomioistuin voi pidättämiseen oikeutetun poliisimiehen vaatimuksesta päättää, että 1 momentissa tarkoitettua ilmoitusta tiedonhankinnan kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedonhankinnan turvaamiseksi, valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Valtion turvallisuutta koskeva peruste tulee kysymykseen käytännössä vain suojelupoliisin toimialalla. On huomattava, että päätös ilmoituksen lykkäämisestä ei velvoita viivyttelemään ilmoitusta annettuun määräpäivään saakka. Jos olosuhteet muuttuvat siten, ettei edellytyksiä ilmoittamatta jättämiselle enää ole, ilmoitus on tehtävä lykkäyspäätöksestä huolimatta (AOA Dnro 1716/2/09 ja AOA Dnro 609/2/10). Lykkäämisperusteet kattavat myös erilaiset kansainvälisiä yhteisoperaatioita

koskevat tilanteet samoin kuin tilanteet, joissa havaitaan tiedonhankinnan kohteen olleen väärä. Lykkääminen tarkoittaa siis ilmoituksen siirtämistä, mutta myös kokonaan ilmoittamatta jättäminen on mahdollista. Se voidaan edellä mainitun momentin mukaan tehdä, jos se on välttämätöntä valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoituksen lykkäämisestä tai sen kokonaan tekemättä jättämisestä päättää tuomioistuin, vaikka keinon käytöstä on päättänyt pidättämiseen oikeutettu virkamies.

Salaisen tiedonhankintakeinon käytöstä ilmoittamista koskeva säännös poliisilain 5 luvun 58 §:ssä on perusratkaisuiltaan toimiva säädettäessä tiedustelumenetelmien käytöstä ilmoittamista. Ilmoittamisen lykkääminen ja kokonaan ilmoittamatta jättäminen on syytä jättää tuomioistuimen harkintaan, jossa eri osapuolten oikeudet ja tiedonsaantitarpeet pystytään parhaiten arvioimaan. Ottaen huomioon, että sotilastiedustelulain sääntely rakentuisi tiedonhankinnalle sotilastiedustelun kohteena olevasta toiminnasta, ilmoittamisen lykkäämisen ja kokonaan ilmoittamatta jättämisen perusteisiin tulisi lisätä maanpuolustuksen ja kansallisen turvallisuuden varmistaminen. Lisäksi olisi arvioitava, minkälainen ilmoittamisjärjestely olisi niin kohteen oikeusturvan kuin käytännöllisten ilmoittamismahdollisuuksienkin kannalta asianmukaisin sotilastiedustelulakiin uutena ehdotettavien menetelmien eli paikkatiedustelun ja jäljentämisen osalta.

2.4.7 Ulkomaantiedustelu

Puolustusvoimien toimintaympäristössä viime vuosina tapahtuneiden muutosten taustalla on Suomen ulkoiseen, sisäiseen ja kansalliseen turvallisuuteen kohdistuvien uhkien ja niihin liittyvien ilmiöiden kiihtyvä kansainvälistyminen ja tietoteknistyminen. Sisäisen ja ulkoisen turvallisuuden väliset rajat ovat hämärtyneet. Kansallinen ja kansainvälinen toimintaympäristö nivoutuvat toisiinsa entistä tiiviimmin. Suomen kansalliseen turvallisuuteen kohdistuvat vakavimmat uhat ovat lähes poikkeuksetta kansainvälistä alkuperää tai niillä on kytköksiä ulkomaille. Tämän vuoksi kaikkea suomalaisen yhteiskunnan turvallisuuteen vaikuttavaa tietoa ei ole saatavissa Suomen alueelta. Yksittäinen valtio ei 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 viestiliikenne 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 yhteystoimintaa 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 kannalta kriittisen tärkeitä tietoja olisi tällaisissa tapauksissa voitava hankkia salaisten 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.

Kohdevaltion näkökulma

Kansainvälisen oikeuden yleisen periaatteen mukaan jokainen suvereeni valtio nauttii alueellista koskemattomuutta ja poliittista riippumattomuutta suhteessa muihin valtioihin. Jokainen valtio päättää itse, salliiko se ja millä ehdoilla ulkomaisten virkamiesten toimia alueellaan. Useimmat valtiot tosiasiassa tiettyyn rajaan saakka sietävät tai jopa hyväksyvät vieraiden tiedusteluviranomaisten toiminnan maaperällään. Kyse saattaa olla molempia osapuolia hyödyttävästä tiedonvaihdosta tai siitä, ettei ulkovallan avoimesti suorittama, kohdevaltion yleisiä olosuhteita koskeva tiedonkeruu vaaranna kohdevaltion tai minkään muunkaan tahon etuja. Toisissa olosuhteissa kohdevaltio saattaa suhtautua alueellaan tapahtuvaan vieraan valtion viranomaisten toimintaan torjuvasti. Toiminta saattaa tapauskohtaisesti myös täyttää jonkin kohdevaltion rikoslainsäädännössä rangaistavaksi säädetyn teon tunnusmerkistön. Toiminnan rangaistavuuteen saattaa kohdevaltiosta riippuen vaikuttaa esimerkiksi se, kuka tietoa hankkii, mitä tietoa hankitaan ja mitä menetelmää käyttäen tiedonhankinta tapahtuu. Vertailussa olevat valtiotkaan eivät ole lainsäädäntönsä tasolla asettaneet ulkomaan tiedustelun ehdoksi sitä, että kohdevaltio hyväksyy toiminnan tai että sillä ei rikota kohdevaltion lainsäädäntöä.

Ulkomaantiedustelussa olisi kyse hyväksyttävän päämäärän eli kansallisen turvallisuuden suojaamisen saavuttamisen edellyttämästä toiminnasta, joka tietyissä tilanteissa saattaa sisältää riskejä. Yksi riskeistä on se, että kyse on kohdevaltion lainsäädännön vastaisesta tai muuten sen kannalta ei-hyväksyttävästä toiminnasta. Ulkomaantiedustelussa olisi tärkeä huomioida muiden valtioiden suhtautuminen sekä niiden lainsäädäntöjen sisältö, mutta käytännön syistä huomioiminen ei voisi tapahtua toiminnasta säädettäessä, vaan vasta siihen ryhdyttäessä. Tällöin kyse olisi sen harkitsemisesta, onko toiminnasta aiheutuva etu selvästi suurempi kuin siihen liittyvät riskit.

Kolmannen valtion näkökulma

Kansainvälisen oikeuden yleisen periaatteen mukaan jokainen suvereeni valtio nauttii alueellista koskemattomuutta ja poliittista riippumattomuutta suhteessa muihin valtioihin. Tämä pätee myös silloin, kun tiedustelu tapahtuu kolmannen valtion aluetta jollakin tavalla hyväksikäyttäen. Lisäksi kansainvälisen oikeuden yleisen periaatteen mukaan valtio ei saa sallia sen aluetta käytettävän tekoihin, jotka haitallisesti ja laittomasti vaikuttavat toisiin valtioihin. Tekoa arvioitaessa merkitystä ei anneta pelkästään sille, aiheuttaako teko vahinkoa omaisuudelle tai henkilöille vaan riittävää voi olla se, että teko aiheuttaa ylipäänsä negatiivisia vaikutuksia. Ulkomaantiedustelussa kolmannen valtion alueella voitaisiin esimerkiksi tavata tietolähteinä toimivia henkilöitä tai heitä voitaisiin sieltä värvätä. Kauttakulkuvaltiota koskevan periaatteen ei voida kuitenkaan katsoa soveltuvan suoraan kansainväliseen tietoliikenteeseen, jossa normaalisti tietoliikenne liikkuu ja reititetään ennalta määrittelemättömästi sitä kautta, missä tietoliikenteen kululle ei ole esteitä.

Tiedustelutoiminta ja kansainvälinen oikeus

Kansainvälisen tuomioistuimen perussäännön 38 artiklan mukaan kansainvälisen oikeuden keskeisimmät lähteet ovat kansainväliset yleis- ja erityissopimukset, kansainvälinen tapaoikeus ja niin

sanotut yleiset oikeusperiaatteet. Rauhan ajan tiedustelutoiminnasta ei ole laadittu kansainvälisiä sopimuksia. Geneven vuoden 1949 yleissopimusten ensimmäisen lisäpöytäkirjan 46 artiklaan sisältyvillä määräyksillä sodan ajan vakoilijoiden nauttimasta suojasta taas ei ole merkitystä tässä käsiteltävän aiheen kannalta.

Vaikka tiedustelutoiminnassa on lähtökohtaisesti kyse kohdevaltion suvereniteetin loukkauksesta, ei oikeuskirjallisuudessa ole yksimielisyyttä siitä, suhtautuuko kansainvälinen oikeus tapaoikeuden ja yleisten oikeusperiaatteiden tasolla tiedustelutoimintaan hyväksyvästi vai tuomitsevasti. Tiedustelutoiminnalla ei voitane katsoa olevan kansainvälisoikeudellisesti yleisesti hyväksyttyä asemaa, koska valtiot toteamalla henkilön persona non grataksi tai muulla tavoin ei-hyväksytyksi osoittavat toistuvasti, etteivät ne hyväksy tällaista toimintaa. Toisaalta tiedustelutoimintaa ei ole kansainvälisessä oikeudessa nimenomaisesti kielletty, ja lähes kaikki valtiot harjoittavat sitä muodossa tai toisessa. Kyse on maailmanlaajuisesti vakiintuneesta toiminnasta, johon yksittäisten valtioiden asennoituminen määräytyy sen mukaan, ovatko ne kulloisessakin tapauksessa tiedustelevan valtion tai kohdevaltion roolissa.

Tiedustelutoiminnassa on yleisesti käytetty hyväksi diplomaattisia suhteita koskevalla Wienin yleissopimuksella (SopS3-5/1970) taattua diplomaattisen edustajan koskemattomuutta ja vapautta kohdevaltion rikosoikeudellisesta tuomiovallasta.

Sotilastiedustelun tiedonhankinta ulkomailla

Suomalaisilla turvallisuusviranomaisilla ei ole säädettyjä toimivaltuuksia hankkia tietoa ulkomailla. Turvallisuusympäristön muutoksesta johtuen ja tässä mietinnössä mainituilla perusteilla olisi kuitenkin tarpeen säätää ulkomaantoimivaltuuksista eli ulkomaantiedustelusta. Ulkomaantoimivaltuudet ehdotetaan sotilastiedustelutoiminnassa säädettäväksi pääesikunnalle ja Puolustusvoimien tiedustelulaitokselle ja ulkomaantiedustelussa ehdotettaisiin käytettäväksi kaikkia sotilastiedustelulaissa säädettyjä tiedustelumenetelmiä. Kansainvälisestä yhteistyöstä ja sen yhteydessä käytettävistä tiedustelumenetelmistä säädettäisiin erikseen.

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 sotilastiedustelusta ja tiedustelumenetelmän käytöstä päättäisi aina pääesikunnan tiedustelupäällikkö. 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 suorittavana sotilastiedusteluviranomainen. Sotilas- ja siviilitiedustelutoiminnan yhteensovittamisesta säädettäisiin erikseen. Ulkomaantiedustelun ulkopoliittisten ulottuvuuksia käsiteltäisiin siten myös sotilas- ja siviilitiedustelun yhteensovittamisen yhteydessä, jolloin mukana olisivat keskeiset ulkopoliittiset tahot.

Kansainvälisestä yhteistyöstä säädettäisiin erikseen ja tällöinkin ulkomailla suoritettavassa operaatiossa käytettävistä tiedustelumenetelmistä päättäisi pääesikunnan tiedustelupäällikkö. Kansainvälisen yhteistyön ja ulkomaantiedustelun ero olisi kohdevaltion tietoisuus suoritettavasta operaatiosta. Ulkomaantiedustelua tehtäisiin lähtökohtaisesti kohdevaltion tai kolmannen valtion tietämättä, kun taas kansainvälistä yhteistyötä suoritettaisiin kohdevaltion suostumukseen perustuen tai vaihtoehtoisesti kohdevaltion tietämättä yhdessä kolmannen valtion kanssa.

2.4.8 Ohjaus ja seuranta

Kuten kansainvälisestä vertailusta käy ilmi, ylimmän valtiojohdon velvollisuutta tiedustelutoiminnan ohjaukseen on pidetty merkittävänä. Ohjaus voidaan toteuttaa eri tavoilla, kuten ylimmän valtiojohdon ohjauksen kautta tai ministeritason päätöksenteolla tiedustelumenetelmien käytön edellytyksiä harkittaessa. Tämän tyyppisen ohjauksen eräs merkittävä tarkoitus on se, että tiedustelutoiminnan kannalta merkittävien hallinnonalojen näkökannat tulevat huomioiduksi tiedustelutoiminnassa yleisinä linjauksina.

Suomen hallintokulttuurissa poliittisenpäätöksen tekijän konkreettisesta osallistumista operatiiviseen päätöksentekoon ei ole pidetty mahdollisena. Sotilastiedustelutoiminnan edellyttämää ohjausta voisi antaa valtioneuvoston ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteinen kokous. Valtioneuvostosta annetun lain 24 §:n (88/2012) mukaan ulko- ja turvallisuuspolitiikkaa käsitelevän ministerivaliokunta voi kokoontua yhdessä presidentin kanssa. Tasavallan presidentti tai pääministeri voi tehdä aloitteen yhteisen kokouksen koolle kutsumiseksi. Valtioneuvoston ohjesäännön 25 §:n (494/2007) 3 momentin mukaan valiokunnan on valmistelevasti käsiteltävä tärkeä ulko- ja turvallisuuspolitiikkaa ja muita Suomen suhteita ulkovaltoihin koskevat asiat, näihin liittyvät tärkeät sisäisen turvallisuuden asiat sekä tärkeät kokonaismaanpuolustusta koskevat asiat. Valiokunta käsittelee myös sen tehtävien alaan kuuluvien asioiden yhteensovittamista koskevat kysymykset.

Sotilastiedustelu ei nykyisillä toimivaltuuksilla pysty riittävässä määrin tuottamaan tehokkaasti luotettavaa ja oikea-aikaista tietoa ylimmän valtionjohdon ja sotilasjohdolle niiden päätöksenteon tueksi. Ylimmän valtiojohdon parempi tiedonsaanti sotilastiedustelun avulla edellyttää myös sitä, että ylimmällä valtiojohdolla tulisi olla myös riittävä tietoisuus tiedustelutoiminnasta ja sen mahdollisista vaikutuksista Suomen kansainvälisille suhteille.

Ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteinen kokous voisi käsitellä jo voimassa olevan sääntelyn nojalla tiedustelutoimintaa koskevia asioita valmistelevasti. Vallitsevassa oikeustilassa ylimmällä valtiojohdolla ei kuitenkaan ole selkeää säännöspohjaa sotilastiedustelutoiminnan ohjaamiseen.

Myös muuhun kuin oikeudelliseen valvontaan liittyvät näkökohdat edellyttävät riittävää sääntelyä sotilastiedustelutoiminnan ohjaamisesta ja seurannasta sotilastiedustelun vaikuttavuuden kasvaessa.

2.4.9 Henkilötietojen käsittely

SKRTL:ssä säädetään paitsi Puolustusvoimien rikostorjunnan tietojärjestelmistä myös henkilötietojen käyttämisestä myös tietojen luovuttamisesta sotilasviranomaiselle vain silloin, kun se on tarpeen 1) valtion turvallisuuden varmistamiseksi, 2) välittömän henkeä tai terveyttä uhkaavan vaaran taikka huomattava omaisuusvahingon torjumiseksi tai 3) sellaisen rikoksen ennalta estämiseksi tai selvittämiseksi, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta. Puolustusvoimia koskevissa henkilötietosäännöksissä ei sen sijaan säädetä toimivaltuuksista, kuten pääesikunnan tiedusteluosaston salassapitosäännösten estämättä tapahtuvasta tiedonsaantioikeudesta. Tiedonluovuttamisoikeudesta ja -velvollisuudesta sen sijaan säädetään.

Puolustusministeriö on 4.8.2016 asettanut hankkeen, jonka tarkoitus on uudistaa Puolustusvoimien henkilötietojen käsittelyä koskeva lainsäädäntö. Työ on parhaillaan käynnissä ja Puolustusvoimien henkilötietolain kokonaisuudistuksen on tarkoitus tulla voimaan vuoden 2018 aikana. Koska uusilla tiedustelutoimivaltuuksilla saataisiin muiden tietojen ohella myös henkilötietoja ja koska tiedustelutoimivaltuuksista mahdollisesti säädettäisiin siten, että ne tulisivat voimaan jo ennen uudistettavaa Puolustusvoimien henkilötietolakia, olisi lakiin otettava henkilötietojen käsittelyä koskevat säännök-

set. Laissa olisi otettava huomioon oikeus saada tietoja eräistä rekistereistä ja tietojärjestelmistä sekä sotilastiedustelun reksiterien tarkastusoikeus.

Puolustusvoimien rikostorjuntatehtävää varten Puolustusvoimien on ylläpidettävä turvallisuustietorekisteriä. Puolustusvoimien rikostorjuntaa hoitavat virkamiehet eivät talleta tehtävänsä kannalta tarpeellisia henkilötietoja muihin rekistereihin. Koska sotilastiedustelutoiminta on Puolustusvoimien rikostorjunnasta erillistä toimintaa, olisi tarkoituksen mukaista säätää uudesta sotilastiedustelun tietojärjestelmästä.

Järjestelmään voitaisiin tallettaa sotilastiedustelun lakisääteisen tehtävän suorittamiseksi tarpeellisia henkilötietoja. Sotilastiedustelun tehtävä määriteltäisiin laajasti ja sen muodostuisi muustakin kuin sitä varten säädetyistä toimivaltuuksista. Suomen sotilaallinen maanpuolustus ja valtion turvallisuuden turvaaminen sekä kansallisen turvallisuuden suojaaminen eivät ole synonyymeja, mutta kaikkia näitä käytetään jo voimassa olevassa lainsäädännössä.

Sotilastiedustelun tehtävän ja siihen liittyvien henkilötietojen käsittelyn kannalta keskeistä on, että eri toimivaltuuksilla saatuja henkilötietoja voitaisiin sotilastiedustelussa käsitellä samalla tavoin ja samassa rekisterissä eikä niiden luovuttamiselle olisi eriasteisia kynnyksiä riippuen niiden saantitavasta. Sotilastiedustelun tehtävän suorittamiseksi henkilötietoja käsiteltäisiin joko käyttötarkoitussidonnaisuuden edellyttämällä tavalla tai siitä poiketen valtion turvallisuuden turvaamiseksi tai kansallisen turvallisuuden suojaamiseksi.

2.4.10 Oikeudellinen valvonta ja oikeusturva

Puolustusvoimien käyttämiä salaisia tiedonhankintakeinoja valvovat SKRTL:n 127 §:n mukaan Puolustusvoimien johto. Lisäksi tiedusteluosaston osastopäällikkö valvoo 86 §:n mukaista rikosten ennalta estämistä ja paljastamista.

Eduskunnan oikeusasiamiehen salaisiin tiedonhankintakeinoihin kohdistuva valvonta perustuu pääosin tarkastuksiin ja muuhun oma-aloitteiseen valvontaan. Kanteluita salaisten tiedonhankintakeinojen käytöstä tehdään vain vähän. Oikeusasiamies antaa eduskunnalle joka vuodelta kertomuksen toiminnastaan sekä lainkäytön tilasta ja lainsäädännössä havaitsemistaan puutteista.

Suojelupoliisin osalta perustuslakivaliokunta on edellyttänyt, että kertomukseen sisällytetään telepakkokeinoja ja peitetoimintaa varten oma jaksonsa (PeVM 15/2002 vp.).

Perustuslakivaliokunta on useita kertoja (PeVM 8/2007 vp., PeVM 17/2006 vp. ja PeVM 16/2006 vp.) yhtäältä todennut, että oikeusasiamiehellä on ollut tärkeä rooli telepakkokeinojen valvonnassa ja valvontajärjestelmien kehittämisessä. Oikeusasiamiehen laillisuusvalvonta voi valiokunnan mukaan toisaalta kuitenkin ainoastaan täydentää hallinnon sisäisiä valvontamekanismeja. Valiokunta on lisäksi muussa yhteydessä todennut olevan syytä huolehtia siitä, että telepakkokeinojen käyttöön liittyvän oikeussuojajärjestelmän, etenkin tuomioistuimen lupamenettelyn, viranomaisten sisäisen valvonnan ja oikeusasiamiehen laillisuusvalvonnan, toimivuus varmistetaan sekä säädöstasolla että käytännössä (PeVL 32/2013 vp.).

Myös oikeusasiamiehen vuotta 2014 koskevassa kertomuksessa on arvioitu, että viranomaisilta saatavat vuosittaiset raportit parantavat mahdollisuuksia seurata salaisen tiedonhankinnan käyttöä yleisellä tasolla. Konkreettisissa yksittäistapauksissa oikeusasiamiehen erityisvalvonta voi kuitenkin olla vain pistokoeluontoista. Kertomuksessa todetaan, että oikeusasiamiehen valvonta lähinnä vain täydentää viranomaisten omaan sisäistä laillisuusvalvontaa ja että sitä voidaan luonnehtia valvonnan valvonnaksi.

Uusien toimivaltuuksien myötä sotilastiedustelulla olisi oltava nykyistä kattavampi valvontajärjestelmä, jolla olisi riittävät toimivaltuudet valvonnan asianmukaiseksi suorittamiseksi. Valvontajärjestelmän tulee täyttää vaatimukset valvonnan tehokkuudesta ja riippumattomuudesta. Myös EIT on lisäksi kiinnittänyt huomiota salaisiin tiedonhankintakeinoihin kohdistuviin valvontajärjestelmiin. Tehokas valvontajärjestelmä muodostuu sekä parlamentaarisesta valvonnasta että laillisuusvalvonnasta vastaavasta viranomaisvalvonnasta. Tästä syystä valvonnasta olisi tarkoituksenmukaista säätää erillisessä laissa.

Kuten kansainvälisessä vertailussa käy ilmi, olisi tiedustelutoimintaa koskevassa sääntelyssä huolehdittava riittävistä oikeusturvajärjestelyistä. Jotta tiedustelutoiminta on mahdollista, tulee tiedustelua koskevan lainsäädännön täyttää kriteerit, joita EIT ja EUT ovat ratkaisukäytännöissään sille asettaneet. Oikeusturvan toteutumiseksi luonnollisella henkilöllä tulee olla riittävät keinot saada oma asiansa tehokkaasti tutkituksi toimivaltaisen viranomaisen toimesta. Niin ikään tiedonhankinnan kohteelle tulee tietyin edellytyksin ilmoittaa häneen kohdistuneesta viranomaisen suorittamasta salaisesta tiedonhankinnasta.

Uusien toimivaltuuksien myötä sotilastiedustelulla olisi oltava kattava valvontajärjestelmä, jolla olisi riittävät toimivaltuudet valvonnan asianmukaiseksi suorittamiseksi. Valvontajärjestelmän tulee täyttää vaatimukset valvonnan tehokkuudesta ja riippumattomuudesta. Myös ihmisoikeustuomioistuin on lisäksi kiinnittänyt huomiota salaisiin tiedonhankintakeinoihin kohdistuviin valvontajärjestelmiin. Tehokas valvontajärjestelmä muodostuu sekä parlamentaarisesta valvonnasta että laillisuusvalvonnasta vastaavasta viranomaisvalvonnasta. Suomessa ei tällä hetkellä ole viranomaista, jolla olisi riittävät toimivaltuudet tiedustelutoiminnan tehokkaaseen, riippumattomaan ja uskottavaan valvontaan sekä tiedustelutoiminnan mahdolliseen keskeyttämiseen väärinkäytöstapauksissa. Tästä syystä valvonnasta olisi tarkoituksenmukaista säätää erillisessä laissa.

Kuten kansainvälisessä vertailussa käy ilmi, on tiedustelutoimintaa koskevassa sääntelyssä huolehdittava riittävistä oikeusturvajärjestelyistä. Jotta tiedustelutoiminta on mahdollista, tulee tiedustelua koskevan lainsäädännön täyttää kriteerit, joita esimerkiksi EIT ja EUT ovat ratkaisukäytännöissään sille asettaneet. Oikeusturvan toteutumiseksi luonnollisella henkilöllä tulee olla riittävät keinot saada oma asiansa tehokkaasti tutkituksi toimivaltaisen viranomaisen toimesta. Niin ikään tiedonhankinnan kohteelle tulee tietyin edellytyksin ilmoittaa häneen kohdistuneesta viranomaisen suorittamasta salaisesta tiedonhankinnasta.

2.4.11 Tietojen luovuttaminen ja kansainvälinen yhteistyö

Tiedustelutietojen luovuttamisesta viranomaisten välillä on säädettävä lain tasolla. Tällä hetkellä tietojen luovuttamisesta säädetään muun muassa henkilötietolaissa, julkisuuslaissa, SKRTL:ssä ja kansainvälisistä tietoturvavelvoitteista annetussa laissa. Nykytilaa ei kuitenkaan voida pitää riittävänä, sillä lähtökohtaisesti tiedustelua tehdään vakavien uhkien ehkäisemiseksi, jolloin kyse ei ole rikosten torjunnasta. Tilanteissa, joissa tiedustelutoiminnan aikana ilmenisi rikokseksi katsottava tapahtuma, voitaisiin tietyissä tapauksissa asiasta ilmoittaa rikostorjuntaviranomaiselle tai esitutkintaviranomaiselle. Voimassa olevan lainsäädännön mukaan hankittuja tiedustelutietoja ei voida myöskään luovuttaa yksityisille tahoille.

Nykylainsäädännön mukaan sotilastiedustelua koskeva kansainvälinen yhteistyö ei ole mahdollista tarpeelliseksi katsotussa laajuudessa. Ilman nimenomaisia laintasoista säännöstä sotilastiedustelu ei voi suorittaa tiedusteluoperaatiota yhteistyössä kansainvälisten kumppaneiden kanssa, mikäli sellainen katsottaisiin Suomen kansallisten etujen mukaan tarpeelliseksi.

2.4.12 Reserviläisten osallistuminen sotilastiedusteluun

Reserviläisiä olisi korkean osaamistason vuoksi voitava tarvittaessa käyttää sotilastiedustelutoiminnassa. Tällä hetkellä reserviläisiä pystytään käyttämään sotilastiedustelun tehtävissä, joihin ei vaadita laissa säädettyjä toimivaltuuksia. Reserviläisiä voidaan kutsua kertausharjoituksiin myös valmiuden joustavaksi kohottamisen tilanteissa.

SKRTL:n mukaisessa tiedonhankinnassa reserviläisiä voidaan käyttää siinä vaiheessa, kun tasavallan presidentti on päättänyt ylimääräisestä palveluksesta asevelvollisuuslain 87 §:n mukaisesti.

Reserviläisinä on myös henkiöitä, jotka ovat joutuneet eroamaan sotilastiedusteluviranomaisen palveluksesta Puolustusvoimien eläkeiän takia. Täten reservissä on henkiöitä, joilla on huomattava määrä tiedustelutoimialan osaamista ja he ovat käyttäneet sekä päättäneet toimivaltuuksien käytöstä.

Kuitenkin myös normaalioloissa sotilastiedusteluviranomainen saattaisi joutua hankkimaan tavallista enemmän tiedustelutietoa toimintaympäristön muutoksista ja tilanteen kehittymisestä. Reserviläisiä olisi näin voitava käyttää etenkin tilanteessa, jossa Puolustusvoimien valmiutta tehostetaan toimintaympäristössä tapahtuneiden muutosten myötä. Reserviläisiä voidaan kutsua kertausharjoitukseen välittömästi, jos Suomen turvallisuusympäristössä ilmenee välttämättömän tarve sille.

Reserviläisten käyttäminen liittyy myös olennaiselta osin sotilaalliseen kriisinhallintaa ja kansainväliseen avun antoon. Suomen osallistuminen näihin operaatioihin nojaa suurelta osin niihin erityisen koulutuksen saaneisiin reserviläisiin. Lukuun ottamatta kriisinhallinta-alueella tapahtuvaa joukkojen omasuojaan liittyvää tiedustelutoimintaa, kriisinhallinnassa ja kansainvälisessä avunannossa reserviläisten erityisistä tiedonhankintatoimivaltuuksista ei ole säädetty.

Reserviläisten käyttö Suomessa sekä kriisinhallintaoperaatioissa ja kansainvälisessä avunannossa edellyttäisi säännöksiä toimivaltuuksista, valonnasta ja ohjauksesta, reserviläisten rikosoikeudellisesta vastuusta ja vahingonkorvausvelvollisuudesta sekä tarkkaa rajausta koskien tiedonsaantioikeuksia ja tiedonkäsittelyä. Niin ikään reserviläisten toiminnan ei tulisi sisältää julkisen vallan käyttöä.

2.4.13 Organisaatioiden mahdollisuus varautua tietoturvauhkiin

Haittaohjelmista vaikeimmin havaittavia ja samanaikaisesti suurinta vahinkoa kansalliselle turvallisuudelle aiheuttavia ovat valtiolliset vakoilu- ja muut haittaohjelmat. Tällaisia haittaohjelmia koskevat tunnisteet ovat sellaista korkean suojaustason tietoa, jota vaihdetaan tyypillisesti osana turvallisuus- ja tiedustelupalveluiden kansainvälistä yhteistyötä. Koska Viestintävirasto ei ole eikä voi olla osapuolena tässä luottamuksellisessa yhteistyössä, HAVARO-järjestelmään ei voida luovuttaa niitä tunnisteita, joiden merkitys kansallisen turvallisuuden suojaamiseksi on suurin.

Tietoyhteiskuntakaaren 272 §:n mahdollistamien tietoturvatoimenpiteiden, HAVARO mukaan lukien, tarkoituksena on toteuttaa tietoturvaa suojaamalla yksittäisiä kohdeorganisaatioita niihin kohdistuvilta loukkauksilta. Tietoturvatoimenpiteiden tarkoituksena ei ole kattaa niitä tiedontarpeita, jotka liittyvät kansallista turvallisuutta vaarantavan toiminnan havaitsemiseen ja torjuntaan. Tietoturvatoimenpiteiden suorittajan näkökulmasta sellaiset kansallisen turvallisuuden ylläpitämisen kannalta olennaiset tiedot, kuten vakavimpien tietoturvaloukkausten syyt, olosuhteet, tekijät ja taustamotiivit, eivät ole keskeisiä. Tarkoituksenmukaista olisi, että kansallisen turvallisuuden kannalta merkittävistä tietoturvauhista ja -loukkauksista voitaisiin luovuttaa tietoa eri toimijoiden välillä.

2.4.14 Yhteenveto nykytilan arvioinnista

Suomen ylin valtionjohto on kiinnittänyt huomiota tiedustelulainsäädännön tarpeeseen. Tasavallan presidentti ja valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta linjasivat marraskuussa 2013, että osana Suomen kyberturvallisuusstrategian toimeenpanoa tuli välittömästi aloittaa työ lainsäädännön kehittämiseksi.

Pääministeri Juha Sipilän hallituksen ohjelman mukaan kasvavat riskit ja uudet uhat edellyttävät koko yhteiskunnalta uudenlaista valmiutta ja varautumista. Tämä koskee erityisesti uusien ja laaja-alaisten uhkien kuten hybridivaikuttamisen, tietoverkkohyökkäysten ja terrorismin torjuntaa. Puolustusvoimien suorittamassa sotilastiedustelussa järjestelmän tarkoitus on antaa valtionjohdolle ennakkovaroituksen sotilaallisten uhkien kehittymisestä, mikä mahdollistaa valtionjohdon oikea-aikaisen päätöksenteon ja yhteiskunnan elintärkeiden toimintojen johtamisen. Sotilastiedustelun kannalta keskeinen tieto on siirtynyt merkittävissä määrin analogisista kanavista digitaalisiin kanaviin, joiden käyttämiseen sotilastiedustelun tiedonhankintalähteenä ei tällä hetkellä toimivaltuuksia. Muutoksiin vastaaminen edellyttäisi lainsäädännön tarkistamista niin, että kansallisesta turvallisuudesta vastaavat viranomaiset pystyvät hoitamaan lakisääteiset tehtävänsä riittävän tehokkaasti. Perustuslain säännökset huomioon ottaen ei voida enää pitää hyväksyttävänä sitä, että sotilastiedusteluun viitataan ainoastaan puolustusvoimista annetun lain esitöissä ja säännellään Puolustusvoimien sisäisellä normistolla.

Puolustusvoimien tehtävät koskevat maanpuolustukseen ja kansalliseen turvallisuuteen kohdistuvien uhkien torjuntaa. Uhkien torjuminen edellyttää, että ne kyetään havaitsemaan ja niistä saadaan tietoa riittävän varhain. Jotta uhkien toteutumiseen voitaisiin varautua, niistä olisi saatava tietoa riittävän varhaisessa vaiheessa.

Sotilaallista uhkaa ja kansalliseen turvallisuuteen kohdistuvia uhkia torjuvien viranomaisten tiedustelutoimivallasta ja tämän toimivallan jakautumisesta sotilas- ja siviiliviranomaisten välillä ei ole säännöksiä. Nykysääntelyssä viranomaisten tiedonhankintatoimivaltuudet perustuvat tiedustelun sijaan yksinomaan rikostorjuntaan.

Muuttuneeseen turvallisuusympäristöön liittyvät epävarmuustekijät korostavat tarvetta tuottaa riippumatonta, varmennettua ja analysoitua tietoa Suomeen kohdistuvista turvallisuusuhkista sekä poliittisen päätöksenteon että turvallisuusviranomaisten päätöksenteon tueksi. Vain todenmukainen ja mahdollisimman varhaisessa vaiheessa saatava tieto uhkien taustatahojen aikeista ja suunnitelmista takaa riittävän kyvyn varoittaa näistä ennakolta. Varhaisvaiheen tiedonsaanti parantaa suomalaisen yhteiskunnan mahdollisuuksia varautua uhkiin ja laajentaa sitä keinovalikoimaa, jonka avulla uhkien toteutuminen voidaan estää. Myös poikkeusoloihin varautumisen näkökulmasta on välttämätöntä, että tieto Suomeen kohdistuvista sotilaallisista uhista pystytään hankkimaan jo normaalioloissa.

Salaisilla tiedonhankintakeinoilla voitaisiin katsoa saatavan tietoa sotilastiedustelun kohteista, jolloin ainoastaan toimivaltuuksien käytön käyttötarkoitusta ja edellytyksiä olisi muutettava. Esimerkiksi telekuuntelulla voitaisiin saada yksityiskohtaista tietoa henkilöstä. Tiedonhankinnan kohteena oleva toiminta ei välttämättä olisi rangaistavaksi säädettyä tai edennyt niin pitkälle, että siihen voitaisiin kohdistaa konkreettinen ja yksilöity rikosepäily. Tällä hetkellä sotilastiedustelun suorittama telekuuntelu ei ole kuitenkaan mahdollista edes rikosperusteisesti.

Rikostorjunnan toimivaltuuksilla voidaan tyydyttää sotilastiedustelun toimintaympäristöstä vain pieni osa. SKRTL:n toimivaltuudet ovat rajalliset ja niillä voidaan hankkia tarvittavaa tietoa ainoastaan pienestä osasta turvallisuusympäristöä Suomen rajan sisäpuolella. Tehokas sotilastiedustelutoiminta edellyttää toiminnanharjoittajalle laajempia tiedonhankintakeinoja kuin SKRTL tällä hetkellä

antaa mahdollisuuden. Jotta tarvittava tietoa uhkista saataisiin, tietoa olisi voitava hankkia esimerkiksi Suomen viranomaisen ulkopuoliselta henkilöltä ja peitetoiminnalla sekä tietoverkoista.

Toimivaltuuksien puuttumisen tai niiden rajoitusten vuoksi on mahdollista, että Puolustusvoimat ei kykene riittävän ajoissa havaitsemaan sellaisia Suomeen tai toimintaansa kohdistuvia uhkia, jotka saattaisivat vaarantaa maanpuolustuksen turvallisuutta tai järjestelmän suorituskykyä. Käytössä olevilla toimivaltuuksilla ei kaikilta osin ajanmukaisesti kyetä vastaamaan operatiivisen toimijan käytännön toimintatapamalleissa tapahtuneeseen muutokseen.

Suomen houkuttelevuuden investointikohteena on monissa yhteyksissä katsottu perustuvan puhtaisiin tietoverkkoihin ja Suomen maineeseen korkean tietosuojan maana. Arvion puhtaista tietoverkoista kyseenalaistaa Kyberturvallisuuskeskuksen raportti, jonka mukaan tietoverkkohyökkäyksiä järjestelmällisesti seuraavissa länsimaissa havaitaan vuosittain kymmeniä tietoverkkovakoilutapauksia, joissa teknisenä apukeinona on käytetty kohdistettua haittaohjelmaa. Raportin mukaan uhka kohdistuu myös Suomeen. Näistä maista poiketen Suomessa ei tällä hetkellä ole järjestelmää, jolla erityisen vakavia kohdennettuja haittaohjelmahyökkäyksiä voitaisiin seurata. Näin ollen voidaan arvioida, että käsitys erityisen puhtaista tietoverkoista perustuu ainakin vakavimpien kybertekojen osalta puutteelliseen kansalliseen havaitsemiskykyyn.

Nykytilaa voidaan pitää epätyydyttävänä ottaen huomioon ne muutokset, joita turvallisuusympäristössä on tapahtunut. Suomalaisen yhteiskunnan toimivuus tulisi turvata erityisen vakavia ulkoisia uhkia sekä kriittiseen infrastruktuuriin kohdistuvia tekoja vastaan. Kansallisen turvallisuuden näkökulmasta keskeistä on saada riittävän varhaisessa vaiheessa tietoa Suomen turvallisuusympäristössä tapahtuvista muutoksista, ei ainoastaan esitutkinnan toteuttamiseen pyrkivä tiedonhankinta.

Kansainvälisestä kehityksestä voidaan huomioida, että digitalisaatio ja viestinnän siirtyminen tietoverkkoihin näkyy useiden eri valtioiden lainsäädännössä. Useissa valtioissa onkin käynnissä tiedustelua koskevan lainsäädännön muutosten valmistelutyö. Eri valtioiden lainsäädäntöhankkeita ovat jouduttaneet muun muassa EIT:n ja EUT:n viimeaikaiset aiheeseen liittyvät ratkaisukäytännöt. EIT:n ja EUT:n ratkaisuissa on korostettu yksityiselämän kunnioitusta ja henkilötietojen suojaa koskevien perusoikeuksien tärkeyttä erityisesti sähköisen viestinnän yhteydessä. Toisaalta EIT:n ja EUT:n voidaan katsoa huomioivan valtion turvallisuusintressin perus- ja ihmisoikeuksia rajaavana perusteena.

Uhkien menestyksekkään torjumisen edellytyksenä on se, että kansallisesta turvallisuudesta vastaavat viranomaiset mahdollisimman varhaisessa vaiheessa saavat tiedon tällaisista yhteyksistä ja niiden puitteissa käsiteltävistä kansallista turvallisuutta vaarantavista seikoista. Varhaisvaiheen tiedonsaanti parantaa suomalaisen yhteiskunnan vastekykyä ja laajentaa sitä keinovalikoimaa, jonka avulla uhkien toteutuminen voidaan estää tai siihen varautua. Tietoverkoissa tapahtuvaan viestintään kohdistettu kansallisesta turvallisuudesta vastaavien viranomaisten tiedonhankinta on maailmanlaajuisesti ollut keskeisessä asemassa esimerkiksi terroritekojen estämisessä. Uudet tiedonsaantia ja varautumista parantavat toimivaltuudet edellyttäisivät uutta sääntelyä henkilötiedustelun, tietoliikennetiedustelun ja tietojärjestelmätiedustelun osalta.

3 Tavoitteet ja keskeiset ehdotukset

3.1 Tavoitteet

Lainsäädäntöhankkeen tavoitteena on valmistella sotilastiedustelua koskevat keskeiset säännökset, sekä ajanmukaistaa Puolustusvoimien viranomaisten tiedustelua koskevat toimivaltuudet. Keskeisimpänä tavoitteena on yhteiskunnan turvallisuuden parantaminen.

Suomen ulkoinen turvallisuusympäristö kehittyy kiihtyvällä vauhdilla. Muun muassa hybridivaikuttamisen ja digitalisaation myötä tapahtuneessa toimintaympäristön muutoksessa Suomen on kyettävä entistä paremmin hankkimaan tietoa myös ilmiötason tapahtumista sekä uhkaperusteista tietoa. Lainsäädäntöä on tarpeen kehittää vastaamaan edellä mainittua muuttunutta toimintaympäristöä. Nykyisillä rikostorjuntatoimivaltuuksilla ei voida riittävän tehokkaasti ja varhaisessa vaiheessa havaita Suomen valtioon ja yhteiskunnan turvallisuuteen kohdistuvia uhkia eikä ryhtyä niistä hankitun tiedon perusteella niiden edellyttämiin toimenpiteisiin. Väärän tiedon levittäminen ja käyttäminen korostavat turvallisuusviranomaisten tarvetta tuottaa objektiivista, varmennettua ja analysoitua tietoa ylimmän valtionjohdon päätöksenteon tueksi. Tämän vuoksi tiedusteluviranomaisten tiedonhankinnan säädöspohjaa tulee kehittää.

Tiedustelutoimivaltuuksista muodostuu kokonaisuus, johon kuuluu eri tiedustelumenetelmiä, jotka täydentävät toisiaan. Kuten kansainvälisestä vertailusta käy ilmi, valtioiden tiedusteluviranomaisilla on käytössään samankaltaisia tiedusteluun tarkoitettuja toimivaltuuksia, mistä Suomessa on säädetty ainoastaan rikostorjunnan tarpeisiin. Jälkimmäisillä toimivaltuuksilla ei saada välttämättä yhteiskunnan turvallisuutta koskevaa kaikkea tarpeellista tietoa, vaan tieto joudutaan hankkimaan ja varmistamaan useilla toisiaan tukevilla tiedustelumenetelmillä.

Tiedonhankintalakityöryhmä on mietinnössään ehdottanut, että Suomeen tulisi luoda säädöspohja tietoliikennetiedustelulle, ulkomaan henkilötiedustelulle ja ulkomaan tietojärjestelmätiedustelulle. Tämän lisäksi olisi välttämätöntä luoda säädöspohja Suomessa käytettäville tiedustelutoimivaltuuksille samoista syistä mitä ulkomaan tiedustelulle. Tiedustelulajit eivät korvaa toisiaan, koska ne ovat luonteeltaan osittain erilaisia. Tietoliikennetiedustelulla on ennen kaikkea tarkoitus havaita yhteiskunnan turvallisuutta vaarantavia uhkia. Henkilötiedustelulla ja tietojärjestelmätiedustelulla hankittaisiin pääasiassa tieto jo tunnistetuista uhkista ja toiminnasta.

Puolustusvoimien tiedustelullisesta tiedonhankinnasta eli sotilastiedustelusta ei ole nimenomaisia säännöksiä laissa. Puolustusvoimista annetun lain esitöiden mukaan tiedonhankinta on osa Puolustusvoimien tehtäviä, mutta varsinaisista toimivaltuuksista siihen ei ole säädetty. Perustuslain 2 §:n 3 momentin mukaan julkisen vallan käytön tulee perustua lakiin. Perustuslain 119 §:n mukaan valtionhallinnon toimielinten yleisistä perusteista on säädettävä lailla, jos niiden tehtäviin kuuluu julkisen vallan käyttöä.

Lisäksi on kiinnitettävä huomiota turvallisuusviranomaisten toimivaltuuksien käyttöön ja käyttämisen edellytyksiin, kansalaisten oikeusturvaan ja perusoikeuksiin liittyviä kysymyksiä. Turvallisuusviranomaisten toimivaltuuksien käyttöön liittyvien säännösten laatimisessa on otettava huomioon Euroopan ihmisoikeustuomioistuimen (jäljempänä EIT) ja Euroopan unionin tuomioistuimen (jäljempänä EUT) ratkaisut sekä muut kansainväliset velvoitteet sekä perus- ja ihmisoikeusnäkökulman korostuminen esimerkiksi ihmisoikeuksien ja perusoikeuksien suojaamiseksi tehtyyn yleissopimukseen.

Laissa säädettäisiin täsmällisesti ja kattavasti Puolustusvoimien sotilastiedustelua hoitavien tahojen toimivaltuuksista, toisaalta perus- ja ihmisoikeuksien suoja ja toisaalta sotilastiedustelun tarpeet huomioon ottaen. Sama koskisi puolustusvoimien sotilastiedustelun henkilörekistereitä koskevaa sääntelyä. Niin ikään ehdotetaan säädettäväksi myös Puolustusvoimien velvollisuudesta toimia teknisenä toteuttajana siviilitiedusteluviranomaisten suorittamassa tiedustelutoiminnassa. Poikkeusoloja koskevat säännökset säädettäisiin suoraan laissa. Perustuslakivaliokunta on katsonut, ettei lainsäädäntövallan delegoinnin rajoituksia voida arvioida poikkeusololainsäädännön yhteydessä lähtökohtaisesti väljemmin kuin muun lainsäädännön yhteydessä, koska tällaisesta mahdollisuudesta ei ole perustuslaissa nimenomaisesti säädetty (PeVL 6/2009 vp).

Puolustusvoimien tiedustelulla pyritään varmistamaan osaltaan oikea, luotettava ja ajantasainen tieto valtiojohdon päätöksenteon tueksi. Sotilastiedustelu muodostaa ja ylläpitää tilannekuvaa soti-

laallisesta toiminnasta ja tuottaa tarvittaessa ennakkovaroituksen Suomeen kohdistuvasta sotilaallisesta uhasta. Muun muassa hybridisodankäynnin ja digitalisaation myötä tapahtuneessa toimintaympäristön muuttuessa Suomen on kyettävä entistä paremmin hankkimaan tietoa myös ulkomailta. Lainsäädäntöä pitää edelleen kehittää vastaamaan edellä mainittua muuttunutta toimintaympäristöä.

Sotilastiedustelulainsäädännöllä pyrittäisiin poistamaan monin paikoin puutteellinen asiantila, joka tiedustelutoimintaa nykyisin rasittaa ja samalla saattamaan Suomen tiedustelulainsäädäntö vastaamaan yleiseurooppalaista tasoa. Esityksen tavoitteena on parantaa Puolustusvoimien tiedonhankintaa Puolustusvoimien tehtäviin liittyvistä vakavista kansainvälisistä uhista ja muista varautumisen kannalta merkittävästä tiedosta siten, että Puolustusvoimilla on toimivaltuudet henkilötiedusteluun ja tietojärjestelmätiedusteluun sekä tietoliikennetiedusteluun. Niin ikään sotilastiedustelulainsäädännön tarkoitus on mahdollistaa tiedonhankinta Euroopan unionin avunantolausekkeen mukaisessa kansainvälisessä yhteistoiminnassa sekä sotilaallisissa kriisinhallintaoperaatioissa ja siten parantaa ulkomailla palvelevien suomalaisten turvallisuutta.

Esitys sisältää säännökset muun muassa Puolustusvoimien tiedustelun tarkoituksesta, toimivaltaisista viranomaisista sekä niiden tehtävistä ja toimivaltuuksista, ohjauksesta ja valvonnasta, tietojen käsittelystä ja rekisteröinnistä sekä viranomaisten yhteistyöstä. Valmisteltavien säännösten perustuslainmukaisuutta on tarkasteltu huolellisesti. Keskeistä valmistelun kannalta on ollut erityisesti perustuslain 10 §, jonka mukaan yksityiselämä, kunnia ja kotirauha on turvattu.

Perustuslain 10 §:n 3 momentti koskee viestinnän luottamuksellisuutta. Vireillä on perustuslain 10 §:n muutos, joka sallisi luottamuksellisen viestin salaisuuteen puuttumisen sotilaallisen toiminnan ja kansallisen turvallisuuden sitä edellyttäessä.

Erityistä huomiota esityksen valmistelussa on kiinnitetty Suomea velvoittaviin kansainvälisiin ihmisoikeussopimuksiin sekä Euroopan ihmisoikeustuomioistuimen ja Euroopan unionin tuomioistuimien ratkaisukäytäntöihin.

3.2 Toteuttamisvaihtoehdot ja niiden arviointi

3.2.1 Nykytilan säilyttäminen

Nykyisin Suomella ei ole sotilastiedustelulainsäädäntöä eikä Puolustusvoimille ole säädetty erityisiä toimivaltuuksia tiedon hankkimiseksi toiminnasta, joka uhkaa maanpuolustusta tai vakavasti uhkaa kansallista turvallisuutta. Puolustusvoimat toteuttaa tehtäväänsä käyttämällä rikostorjunnan toimivaltuuksia, viranomaisyhteistyöllä sekä kansainvälisellä yhteistoiminnalla.

Vaihtoehdossa, jossa nykytila säilytettäisiin, Suomella ei olisi mahdollisuuksia saada ennakolta tietoa valtioon kohdistuvasta sotilaallisesta uhkasta taikka kansallisesta turvallisuutta vakavasti vaarantavista uhkista. Tässä vaihtoehdossa tiedonhankinta olisi mahdollista ainoastaan rikosperusteisesti Suomen rajojen sisäpuolella tai tiedustelumenetelmillä, joiden ei katsottaisi edellyttävän erillistä säädösperustaa.

Ulkomailla tapahtuva ja ulkomaiden tapahtumista sekä olosuhteista saatava tieto perustuisi muiden valtioiden viranomaisten vapaaehtoisesti antamiin tietoihin. Lisäksi kansainvälisessä yhteistyössä ei välttämättä voitaisi saada kaikkea tarvittavaa tietoa sen takia, ettei Suomi voi auttaa tiedustelutoiminnassa toista valtiota. Tiedustelutietoa olisi hankittavissa niin kotimaassa kuin ulkomaillakin julkisista tai muuten vapaasti saatavilla olevista lähteistä joko maksusta tai maksutta.

Kuten nykytilan kuvauksesta ja arvioinnista on havaittu, merkittävä osa viestinnästä liikkuu nykyisin muualla kuin radioaalloilla tai telejärjestelmässä. Nykytilan säilyttämisessä tiedonhankintaa ei voi-

taisi kohdistaa tehokkaasti tietoverkoissa tapahtuvaan viestintään. Nykyisillä rikosperusteisilla toimivaltuuksilla, kuten telekuuntelulla, ei voida saada tietoa ulkomaisesta tietoliikenteestä tai Suomen kautta kulkevasta Suomen ulkopuolisen valtion alueelta lähtöisin olevasta viestistä, jonka määränpää on myös toinen valtio kuin Suomi.

Nykytilan säilyttämisen ohella on esitetty, että tulisi harkita rikostorjuntatoimivaltuuksien käyttöalan laajentamista. Ilman tiedustelulainsäädännön luomista voitaisiin harkita myös tiettyjen uusien kriminalisointien säätämistä ja rikoksen valmistelun alan laajentamista niin laajalle, että tiettyihin rikoksiksi määriteltyihin tapahtumakehityksiin päästäisiin käsiksi nykyisiä SKRTL:ssä ja poliisilaissa määritellyillä toimivaltuuksilla. Tämä ratkaisu voitaisiin mahdollistaa esimerkiksi kriminalisoimalla valtio- tai yhteiskuntajärjestystä vaarantavat hankkeet sikäli kuin ne eivät nykyisin ole rikoslain piirissä ja laajentamalla Puolustusvoimien käytössä olevien pakkokeinojen aineellista tai alueellista soveltamisalaa. Tämä jättäisi kuitenkin ulkopuolelle tiedustelutoiminnan, jossa tiedonhankinnan kohteena olevat tapahtumat eivät olisi rikoksia tai koskaan muodostuisi rikoksiksi. Lisäksi Suomen rikoslain alueellinen ulottuvuus muodostuu esteeksi ulkomailla tapahtuvassa toiminnassa.

Uuskriminalisoinnit olisivat perustuslain 8 :n rikosoikeudellisen laillisuus- eli legaliteettiperiaatteen kannalta ongelmallisia. Rikoslainsäädäntöön kohdistuu samaan tapaan kuin muuhun lainsäädäntöön rajoituksia perustuslaista ja Suomea sitovista kansainvälisistä ihmisoikeusvelvoitteista. Perusoikeudet asettavat rajoja sille, mitä tekoja voidaan säätää rangaistavaksi ja millaisia rangaistuksia tai muita seuraamuksia rikoksiin voidaan liittää. Lailla ei esimerkiksi voida säätää rangaistavaksi toimia, joihin perustuslaki nimenomaisesti oikeuttaa (PeVL 17/2006 vp. s.2, PeVL 20/2002 vp. s. 6, PeVL 33/2000 vp. s. 2, PeVL 6/1998 vp., PeVL 23/1997 vp. s. 2-37).

Uusissa kriminalisoinneissa ja kriminalisointien laajentamisessa on myös huomioitava se, että oikeusjärjestelmässä kriminalisointeja on pidettävä aina ultima ratio -vaihtoehtona, eli viimesijaisena keinona.

Perusoikeusrajoituksen hyväksyttävyyden vaatimuksen takia kriminalisoinnille on oltava painava yhteiskunnallinen tarve ja perusoikeusjärjestelmän kannalta hyväksyttävä peruste. Esimerkiksi velvoite jonkin perusoikeuden suojaamiseen voi olla hyväksyttävä peruste kriminalisoinnille (PeVL 23/1997 vp). Toisaalta esimerkiksi pelkästään symbolisista syistä ehdotettuihin kriminalisointeihin on perustuslakivaliokunnan käytännössä suhtauduttu torjuvasti (PeVL 5/2009 vp. s. 3, PeVL 26/2004 vp. s. 3–4, PeVL 20/2002 vp. s. 6–7, PeVL 29/2001 vp. s. 4).

Rikosoikeudellinen laillisuusperiaate sisältää lain täsmällisyyteen kohdistuvan erityisen vaatimuksen. Sen mukaan kunkin rikoksen tunnusmerkistö on ilmaistava laissa riittävällä täsmällisyydellä siten, että lain sanamuodon perusteella on ennakoitavissa, onko jokin teko tai laiminlyönti rangaistava (ks. esim. PeVL 38/2012 vp. s. 4, PeVL 68/2010 vp. s. 4, PeVL 58/2010 vp. s. 3, PeVL 33/2010 vp. s. 2–3, PeVL 12/2010 vp. s. 3, PeVL 17/2006 vp. s. 3–4).

Jäljempänä mietinnössä käsitellään sotilastiedustelun kohteena olevaa toimintaa. Aiemmin mietinnössä on myös todettu, että on olemassa sellaisia uhkia, jotka eivät voisi edetä rikokseksi, kuten esimerkiksi Suomeen kohdistuva ulkopuolinen sotilaallinen toiminta tai Suomen maanpuolustuksen vaarantavista omistussuhteiden muutoksista. Näin pitkälle menevät tai väljät kriminalisoinnit olisivat rikosoikeudellisen laillisuusperiaatteen kannalta ongelmallisia. Näin jouduttaisiin jättämään ulkopuolelle Suomen kansallisen turvallisuuden kannalta erittäin tärkeitä tiedustelutoimivaltuuksien käyttöperusteita, joiden kohdalla tiedonhankinnan kohteena olevat tapahtumat eivät olisi rikoksia tai koskaan muodostuisi rikoksiksi. Lisäksi Suomen rikoslain alueellinen ulottuvuus muodostuu esteeksi ulkomailla tapahtuvassa toiminnassa.

Puolustusvoimien tehtävänä on Suomen puolustaminen sotilaallisesti. Sotilastiedustelun tarkoituksena on hankkia tietoa, jolla muodostetaan muun muassa ajantasainen tilannekuva toimintaympä-

ristössämme tapahtuvasta sotilaallisesta toiminnasta tai muusta sellaisesta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Hankittujen tietojen perusteella tuotetaan tarvittaessa ennakkovaroitus poliittiselle tai sotilaalliselle johdolle, tuetaan Puolustusvoimien strategista ja operatiivista suunnittelua ja maalittamisesta sekä kriisinhallintaoperaatioista ja kansainvälisen avun antamisesta.

Poliisilain 5 luvussa säädettyjen salaisten tiedonhankintakeinojen edellytyksenä on niiden käytön sitominen tiettyyn rikokseen. Käyttöedellytysten säätämisen taustalla on tarkasteltu yhtenäisesti niitä arvoja, joita rikoslailla voidaan edistää ja suojata, sekä arvioitu tarvetta eri tekojen säätämiseen rangaistavaksi. Perusteltuna ei voida pitää sitä, että säädettäisiin rikosoikeudellisen laillisuusperiaatteen näkökulmasta epätäsmällisiä uuskriminalisointeja, jotta rikosperusteisia toimivaltuuksia olisi mahdollista käyttää tiedustelutoiminnassa.

Rikoksen rangaistusasteikot on laadittava ja perusteltava kunkin tekotyypin rangaistusarvon perusteella. Rangaistusasteikkoratkaisuja ei tehdä sen mukaan, miten rikokseen voidaan soveltaa salaisia tiedonhankintakeinoja koskevia säännöksiä, tai sen mukaan, millainen vaikutus säädetyllä rangaistuksella on rikoksen vanhentumiseen. Se, mihin enimmäisrangaistukseen salaisen tiedonhankintakeinon käyttö on sidottu, on harkittu kunkin tiedonhankintakeinon kohdalla erikseen. Salaisia tiedonhankintakeinoja ei voida systematisoida voimakkaisiin ja lieviin sillä perusteella, miten vakavaa rikosta edellytetään, jotta tiettyä tiedonhankintakeinoa voidaan käyttää. Rikoslainsäädännön näkökulmasta toimivaltuudet, joilla rikoksia estetään, paljastetaan ja selvitetään, ovat relevantteja, mutta tietyn rikoksen rangaistusmaksimin määrittäminen ei yleisen lainsäädäntökäytännön nojalla saa perustua rangaistusmaksimin nojalla käytettäväksi mahdollisesti tuleviin toimivaltuuksiin, vaan tekojen moitittavuuteen. Toisin sanoen, valmistelurikosten rangaistusasteikot on päätettävä suhteellisuusperiaatteen mukaisesti, eikä ankaria asteikkoja voida perustella toimivaltuuksilla tai niiden puutteella. Telekuuntelua voidaan käyttää vain hyvin vakavien rikosten tutkinnassa, ja nämä rikokset on lueteltu laissa.

Toinen merkittävä puute rikosperusten toimivaltuuksien soveltumisessa tiedustelutoimintaan on, että niitä voidaan kohdistaa vain tiettyyn yksilöitävissä olevaan, jonka voidaan perustellusti olettaa tulevaisuudessa syyllistyvän tai jo syyllistyneen tietyn vakavuusasteen rikokseen tai sellaisen valmisteluun. Jos tällaista tiettyyn henkilöön liittyvää rikostorjunnallista perustetta ei ole olemassa, ei poliisilain mukaisen salaisen tiedonhankintakeinon käyttö ole mahdollista. Telekuuntelu ja televalvonta lisäksi pystyttäisiin tiedustelutarkoituksessakin kohdentamaan tuomioistuimen antamalla luvalla vain tiettyjen määriteltyjen kohdehenkilöiden ja heidän hallussaan olevien liittymien tai laitteiden viestintään, ei tietoliikenteeseen tiettyjä yksilöityjä hakuehtoja käyttäen.

Kolmas huomioitava asia on, että tietoliikennetiedustelu kohdistuisi Suomen rajat ylittävään tietoliikenteeseen eli lähtökohtaisesti ulkomaiseen viestintään. Valtaosa niistä maista, joihin Suomen nykyiset ja suunnitellut tietoliikenneyhteydet menevät, voi seurata jo nykyisin oman lainsäädäntönsä perusteella alueensa läpi kulkevaa tietoliikennettä. Tietoliikennetiedustelu on lainsäädännöllä mahdollistettu ainakin Ruotsissa, Saksassa ja Venäjällä. Lisäksi Norjassa on julkaistu tietoliikennetiedustelun kehittämistä koskien mietintö. Näin ollen ainoastaan Viro on Suomen rajanaapureista maa, jonne kulkee Suomesta tietoliikennekaapeliyhteydet, ja jolla ei ole lakiin säädettyä oikeutta suorittaa tietoliikennetiedustelua. Tämä merkitsee sitä, että Suomen kansainvälisten verkkoyhteyksien kautta kulkeva tietoliikenne voi olla päätyä tiedustelun kohteeksi muiden kuin Suomen omien viranomaisten taholta.

Edellä kerrottua vaihtoehtoa nykyisten rikosperusteisten toimivaltuuksien aineellisen ja alueelliset soveltamisalan laajentamisesta ei ole pidetty kannatettavana, koska nykyisiä tiedonhankintakeinoja ei ole lainkaan mahdollista käyttää toistaiseksi tuntemattomien uhkien havaitsemista ja uhkan lähteiden tunnistamista varten. Tätä on käsitelty tarkemmin jo aikaisemmin mietinnön yleisperusteluissa. Tämän tyyppisessä tietoliikennetiedustelussa tietoliikennetiedustelun kohdentaminen edel-

lyttäisi myös teleosoitteeseen tai telepäätelaitteeseen kohdistuvien tietojen tietämistä ennakolta. Malli edellyttäisi myös laajojen tietojen säilyttämis- ja antamisvelvollisuuksien säätämistä tietoliikenteen keskeisille toimijoille, teleoperaattoreille.

Uudet kriminalisoinnit ja kriminalisointien laajentaminen eivät kuitenkaan ratkaisisi sitä ongelmaa, että Puolustusvoimilla on käytettävinään SKRTL:n mukaan ainoastaan rajoitetut tiedonhankintatoimivaltuudet. Puolustusvoimat ei pystyisi hankkimaan kattavasti tietoa esimerkiksi tietolähteiltä, telekuuntelulla tai peitellyllä tiedonhankinnalla eikä tietoverkoista tietoliikennetiedustelulla taikka tietyistä tietojärjestelmistä tietojärjestelmätiedustelulla. Kattava sotilastiedustelu edellyttäisi uusista toimivaltuuksista säätämistä SKRTL:ssä.

Nykytilan säilyttämisessä tiedonhankinta olisi mahdollista ainoastaan rikosperusteisesti Suomen rajojen sisäpuolella tai tiedustelumenetelmillä, joiden ei katsottaisi edellyttävän erillistä säädöspohjaa.

3.2.2 Sotilastiedustelulakityöryhmän ehdotus

Sotilastiedustelulakityöryhmän ehdotuksen pohjana on tiedonhankintalakityöryhmän mietintö. Näin ollen tiedonhankintalakityöryhmän tekemät ratkaisut valtaosin omaksuttiin myös sotilastiedustelulakityöryhmän mietinnössä.

Sotilastiedustelulakityöryhmä pitää perusteltuna, että ulkomaan tiedustelutoimivaltuuksien eli henkilötiedustelun ja tietojärjestelmän tiedustelun käyttö mahdollistettaisiin myös kotimaassa. Työryhmän näkemyksen mukaan tiedustelutoimivaltuuksilla pyritään torjumaan maanpuolustukseen ja kansalliseen turvallisuuteen kohdistuvia uhkia. Vaikka Suomen turvallisuutta uhkaavat vakavimmat tekijät liittyvät nykyisin usein Suomen ulkopuolisiin tapahtumiin ja ulkomaista alkuperää olevan tai siellä syntyvän uhkan seuraukset saattavat realisoitua Suomessa aiempaa herkemmin, niin ulkomaan tiedustelutoimivaltuuksilla ei kuitenkaan pystyttäisi hankkimaan maanpuolustuksen ja kansallisen turvallisuuden kannalta välttämätöntä tietoa kotimaassa maanpuolustuksen ja kansallista turvallisuutta uhkaavan toiminnan ollessa suojattavan intressin keskiössä.

Koska Puolustusvoimien rikostorjunnasta säädetään puolustusvoimista annetusta laista erillisessä laissa, työryhmä päätyi vaihtoehtoon, jossa säädettäisiin uusi sotilastiedustelulaki, joka sisältäisi säännökset sotilastiedustelutoiminnan organisoinnista, toimivaltuuksista, ohjauksesta ja seurannasta sekä sisäisestä valvonnasta.

3.2.2.1 Sotilastiedustelun organisointi

Kuten kansainvälisestä vertailusta on käynyt ilmi, tiedustelutoiminta voidaan organisoida useilla eri tavoilla. Eräissä valtioissa, kuten Sveitsi ja Saksa, on päädytty ratkaisuun, jossa ulkomaan tiedustelu on erotettu valtion sisäisestä tiedustelusta. Tässä vaihtoehdossa ulkomaan tiedustelupalvelu hankkii tietoa niin sotilas- kuin siviilitiedustelun alalla ylimmälle valtiojohdolle ja valtion sisäinen tiedustelu tähtää ennen kaikkea rikostorjuntaan. Edellä viitatuissa maissa keskitetty ulkomaan tiedustelupalvelu on siviiliviranomainen.

Keskitetyssä mallissa ulkomaan tiedustelun ohjaus on keskitetty ulkomaan tiedusteluviranomaisen hallinnonalalle. Ulkomaan tiedustelutoiminta ei vaadi erityistä yhteensovittamista eri tiedusteluviranomaisten kesken.

Tietojen luovuttaminen ulkomaan tiedustelusta sisäisen turvallisuuden käyttöön, kuten rikostiedusteluun ja rikostorjuntaa, vaatii hallinnollisia järjestelyitä, koska ulkomaan tiedustelun tehtävä on erityyppinen ja se toimii eri hallinnonalalla.

Eräissä valtioissa on päädytty ratkaisuun, jossa sotilas- ja siviilitiedustelu on erotettu toisistaan. Tällaisessa tiedustelutoiminnan organisoinnissa niin siviililuonteisten uhkien tiedustelun viranomainen sekä tiedustelun sotilaallinen toimija saavat hankkia tietoa omiin tehtäviin liittyen.

Tiedustelun kohteet voivat olla päällekkäisiä ainakin osittain sotilas- ja siviilitiedustelun toimialalla. Tiedustelutiedon luovuttaminen tiedustelutoiminnasta rikostorjuntaan toisaalta voidaan katsoa olevan helpompaa, koska tiedustelun toimijat sekä rikostorjuntaviranomaiset toimivat samalla hallinnonalalla.

Suomessa hajautettu tiedustelu sotilas- ja siviilitiedusteluun ei vaatisi uusien viranomaisten perustamista. Hajautettu tiedustelu edellyttää kuitenkin laajempaa ohjausta valtion ylimmältä johdolta tiedustelun kohteiden määrittelyssä sekä tiivistä tiedustelutoiminnan yhteensovittamista operatiivisella tasolla.

3.2.2.2 Henkilötiedustelu ja tekninen tiedonhankinta

Henkilötiedustelu voidaan jakaa toimivaltuuksiksi, joista säädetään jo tiedonhankintamenetelminä poliisilain 5 luvussa. Henkilötiedustelu jakautuu telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tukiasematietojen hankkimiseen, suunnitelmalliseen tarkkailuun, peiteltyyn tiedonhankintaan, tekniseen tarkkailuun, teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimiseen, peitetoimintaan, valeostoon, tietolähdetoimintaan, paikkatiedusteluun ja jäljentämiseen.

Lisäksi olisi tarkoituksen mukaista säätää teknisistä tiedonhankintamenetelmistä ulkomaan tietojärjestelmätiedustelusta sekä radiosignaalitiedustelusta. Tekninen laitetarkkailu ja ulkomaan tietojärjestelmätiedustelu on tiedonhankintamenetelminä samanlaiset, mutta koska ulkomaan tietojärjestelmätiedustelu on pitkäkestoista ja laaja-alaista toimintaa, jossa on tarkoin harkittava myös ulkopoliittisia näkökohtia. Myös radiosignaalitiedustelusta säädettäisiin nimenomaisesti toiminnan merkittävyyden vuoksi.

Toimivaltuuksia ehdotetaan käytettäväksi tiedon hankkimiseksi sotilastiedustelun kohteena olevasta toiminnasta.

Sotilastiedustelulaissa olisi tarkoituksen mukaista säätää kaikista toimivaltuuksista lain systematiikan ja selkeyden vuoksi.

3.2.2.3 Tietoliikennetiedustelu

Toteuttaminen

Tietoliikennetiedustelussa hankittaisiin tietoja viesteistä, jotka liikkuisivat Suomen rajan yli tietoverkoissa. Eräissä valtioissa tietoliikennetiedustelu kohdistuu lähtökohtaisesti kaikkeen viestintään siitä riippumatta, missä viestintä tapahtuu. Kaikkeen viestiliikenteeseen kohdistuva tietoliikennetiedustelu edellyttää erittäin suuria resursseja niin tiedon tallentamisen, tiedonhallinnan kuin tietojen analysoinnin osalta. Lisäksi kaikkeen tietoliikenteeseen kohdistuvaa tietoliikennetiedustelua ei voida pitää hyväksyttävänä EIS:n ja EIT:n ratkaisukäytännön kannalta vaikka sillä voitaisiinkin saada kattavasti tietoa kansalliseen turvallisuuteen kohdistuvista uhkista.

Kohdennetussa tietoliikennetiedustelussa pyritään hankkimaan tietoja tietystä tiedustelun kannalta merkityksellisestä kohteesta. Usein tietoliikennetiedustelun aloittamista edeltää jo jokin muilla keinoin saatu tieto siitä, minne tietoliikennetiedustelua on tarpeen kohdistaa. Koska tietoliikennetiedustelua on jo voitu kohdentaa etukäteen, ei tietoliikennetiedustelu vaadi yhtä mittavia resursseja kuin kohdentamaton tietoliikennetiedustelu. Kohdennetussa toteuttamisvaihtoehdossa ei men-

täisi myöskään suoraan viestin sisältöön kuin tietyissä erikseen säädetyissä tapauksissa, joita ovat esimerkiksi haittaohjelmat ja vieraan valtion asevoimien viestiliikenne.

Kohdennettu vaihtoehto voidaan katsoa myös EIT:n ratkaisukäytännön kannalta hyväksyttäväksi.

Yhtenä tietoliikennetiedustelun toteuttamisvaihtoehtona olisi kohdennettu pakkokeinotyyppinen malli, jossa tiedusteluviranomainen saisi tarvitsemansa tiedot teleoperaattorilta, eikä sillä olisi missään vaiheessa teknistä pääsyä muuhun tietoliikennekaapeleissa kulkevaan viestiliikenteeseen. Tässä mallissa tiedustelun tekninen toteuttaja olisi teleoperaattori, jolta sekä sotilastiedusteluviranomainen voisi pyytää ne tiedot, jotka niillä tuomioistuimen luvalla oikeus hankkia tietoliikenneverkosta. Pakkokeinotyyppisen ratkaisu voitaisiin mahdollistaa esimerkiksi kriminalisoimalla valtio- tai yhteiskuntajärjestystä vaarantavat hankkeet sikäli kuin ne eivät nykyisin ole rikoslain piirissä ja laajentamalla Puolustusvoimien käytössä olevien pakkokeinojen aineellista tai alueellista soveltamisalaa. Näillä keinoin ei voitaisi hankkia tietoja Suomen rajan ylittävästä tietoliikenteestä.

Tämän tyyppisessä tietoliikennetiedustelussa tietoliikennetiedustelun kohdentaminen edellyttäisi myös teleosoitteeseen tai telepäätelaitteeseen kohdistuvien tietojen tietämistä ennakolta. Malli edellyttää myös laajojen tietojen säilyttämis- ja antamisvelvollisuuksien säätämistä tietoliikenteen keskeisille toimijoille, teleoperaattoreille.

Niin ikään yhtenä toteuttamisvaihtoehtona olisi malli, jossa tietoliikenteeseen tehtäisiin automaattinen seulonta hakuehtoja hyväksikäyttämällä. Suomen rajat ylittävissä tietoliikennekaapeleissa kulkeva tiedon määrä huomioiden pelkkä automaattisia hakuehtoja hyödyntävä vaihtoehto olisi hankala toteuttaa sekä asettaisi toiminnalle erittäin suuret resurssivaatimukset.

Tietoliikennetiedustelu voidaan toteuttaa keskittämällä sen tekninen toteuttaminen yhdelle viranomaiselle tai hajauttamalla tekninen toteuttaminen useammalle viranomaiselle. Keskittämällä tekninen toteuttaminen yhdelle viranomaiselle, tietoliikennetiedustelussa tarvittava teknologia sekä teknistä toteuttamista koskevat toimintatavat ovat yhdellä viranomaisella. Muille viranomaisille voidaan säätää toimivalta antaa toimeksianto tietojen hankkimiseen tietoliikennetiedustelua käyttäen.

Teknisen toteuttamisen keskitetyssä mallissa tietoliikennetiedustelussa tarvittavat resurssit keskittyvät yhdelle toimijalle, jolloin muiden toimijoiden ei tarvitse kehittää ja hankkia resursseja tietoliikennetiedusteluun.

Tietoliikennetiedustelun edellyttämä kytkentä

Kuten edellä EIT:n ratkaisukäytännöstä voidaan nähdä, tiedusteluviranomaisella ei voi olla suoraa ja rajoittamatonta pääsyä tietoliikenneverkkoihin. Tätä voidaan ehkäistä sillä, että tietoliikennetiedustelun edellyttämän tuomioistuimen luvan mukaisen liitynnän tietoliikenneverkkoon tekisi jokin muu taho kuin tiedusteluviranomainen itse. Suomessa tällainen taho voisi olla viestintävirasto, teleoperaattori, Valtori tai valtion kokonaan omistama Suomen turvallisuusverkko Oy. Tuomioistuimen luvan mukaisen liitynnän toteuttaminen ja tältä osin luvan täytäntöönpanon ei voida katsoa olevan merkittävää julkisen vallan käyttöä, joten se voitaisiin antaa myös muun kuin viranomaisen tehtäväksi. Liitynnän toteuttamisessa ei ole kyse myöskään valvonnasta vaan täytäntöönpanotoimista.

Viestintävirasto vastaa osaltaan siitä, että tietoverkkojen toiminta on häiriötöntä ja tietoverkoissa liikkuvista haittaohjelmista saadaan tarvittava tieto toiminnanharjoittajille. Lisäksi viestintävirastossa on riittävä osaaminen ja riittävät resurssit siihen, että tiedusteluviranomainen tuomioistuimen luvan tietoliikennetiedusteluun saatuaan saisi luvan täytäntöönpanon mahdollisimman nopeasti ja asianmukaisesti. Liitynnän toteuttamisessa viestintävirasto osaltaan myös toteuttaisi tehtäväänsä, ettei tiedusteluviranomaisella olisi rajoittamatonta pääsyä tietoliikenneverkkoon. Toisaalta tieduste-

luviranomaisen avustaminen saattaisi haitata viestintäviraston mahdollisuuksia toimia alan kansainvälisessä yhteistyössä.

Toisena vaihtoehtona liitynnän voisi toteuttaa se teleoperaattori, jonka hallinnoiman viestintäverkon osaan tietoliikennetiedustelu kohdistuisi. Teleoperaattoreilla olisi tarvittava osaaminen ja resurssit liitynnän tekemiseen ja tarve tehdä toteuttaa se niin, että tietoliikenteelle aiheutuisi mahdollisimman vähän haittaa. Toisaalta teleoperaattoreille tulee jo nyt esitetyn lain mukaan uusia velvollisuuksia. Lisäksi uudet tehtävät aiheuttavat teleoperaattoreille välittömiä kustannuksia, jotka tiedusteluviranomainen olisi velvollinen korvaamaan. Teleoperaattoreiden ei myöskään voida katsoa olevan riittävän ulkopuolinen tietoliikennetiedusteluun nähden. Teleoperaattorin toimiminen liitynnän teknisenä toteuttajana voisi niin ikään olla ongelmallista ottaen huomioon tiedustelutoiminnan luonteen herkkyys ja tiedon salassapitointressi.

Kolmantena vaihtoehtona voitaisiin harkita valtion tieto- ja viestintätekniikkakeskus Valtoria. Valtorin tehtävistä ja sen tarjoamista palveluista säädetään valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä annetussa laissa (1226/2013). Valtori tuottaa valtionhallinnon toimialariippumattomat ICT-palvelut. Sen tavoitteena on, että valtion toimialariippumattomat ICT-palvelut ovat kilpailukykyisiä, laadukkaita, ekologisia, tietoturvallisia ja asiakastarpeet täyttäviä. Valtorissa toimii TUVE-yksikkö, jonka tehtävänä on tuottaa julkisen hallinnon turvallisuustoiminnasta annetussa laissa (10/2015) nimetyille valtion virastoille ja laitoksille korkean varautumisen ja turvallisuuden vaatimukset täyttäviä tieto- ja viestintäteknisiä palveluja sekä integraatiopalveluja.

Neljäntenä vaihtoehtona olisi Suomen Erillisverkot Oy:n julkisen hallinnon turvallisuusverkkotoimintaa varten perustama osakeyhtiö. Julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain 6 §:n 1 momentin mukaan Suomen Erillisverkot Oy on valtion kokonaan omistama osakeyhtiö. Lisäksi 2 momentin mukaan yhtiön tarkoituksena ei ole tuottaa liiketaloudellista voittoa sille lain mukaan kuuluvien tehtävien hoitamisessa.

3.2.2.4 Toteuttamisvaihtoehtojen arviointi

Nykytilassa viranomaisten tiedonhankinta voi tapahtua ainoastaan rikosperusteisesti. Rikosperusteinen tiedonhankinta ei kuitenkaan vastaa kattavasti niihin kysymyksiin, joihin tiedustelutoiminnalla haetaan vastauksia.

Uusien kriminalisointien ja tiettyjen kriminalisointien alan laajentamista ei myöskään voida pitää tarkoituksen mukaisena oikeusjärjestelmän näkökulmasta, sillä kriminalisoinnit on säädetty aina viimekätisiksi vaihtoehdoiksi yhteiskunnan toiminnassa. Lisäksi tämä edellyttäisi sotilastiedustelun toimialalla uusista toimivaltuuksista säätämistä.

Tiedustelutoiminnan organisoinnin osalta keskitetyssä ulkomaan tiedustelussa ulkomaan tiedustelupalvelu vaatisi Suomessa uuden viranomaisen perustamista ja täysin uusien toimintatapojen luomista viranomaisen sisällä. Lisäksi valtion sisäisen tiedonhankinnan osalta olisi harkittava toimivaltaisten viranomaisten tiedonhankintatoimivaltuuksien kehittämistä edelleen.

Puolustusministeriön hallinnonalan tarpeet koskevat Puolustusvoimien tehtäviin liittyvän tilannekuvan muodostamista ja ylläpitämistä, ennakkovaroituksen antamista sekä maalittamistukea. Tämä edellyttää toimintakentän ja kohteiden perusteellista tuntemusta ennakolta sekä ennakkotietoa siitä, millaisia käytäntöjä ja toimintatapoja toimintakentällä on. Puolustusvoimat on tutkinut ja seurannut näitä jo perustamisestaan lähtien, jolloin sotilastiedustelutoiminta olisi tarkoituksen mukaisinta toteuttaa puolustushallinnon alalla. Sisäministeriön hallinnonalan tarpeet liittyvät puolestaan kansallista turvallisuutta vaarantavien vakavien siviililuontoisten uhkien, kuten terrorismin ja vakoilun, havaitsemiseen ja niiden taustalla olevien toimijoiden tunnistamiseen. Tästä syystä siviilitiedusteluun liittyvää lainsäädäntöä voitaisiin valmistella sisäministeriön johdolla.

Esitetty tiedustelun hajautettu toimintamalli edellyttää tiedustelutoiminnan ohjaamista sekä tiivistä yhteensovittamista niin valtiohallinnossa kuin operatiivisten toimijoiden välillä.

Tietoliikennetiedustelun toteuttamisen voidaan katsoa olevan tehokkainta kohdentamalla se mahdollisimman tarkkaan tahoihin ja toimintaan, joista voidaan saada tiedustelun kannalta mahdollisimman hyödyllistä tietoa.

Sotilastiedustelussa olisi kyse tiedoista, joiden tarkoituksena olisi tuottaa maanpuolustuksen ja kansallisen turvallisuuden kannalta välttämätöntä tiedustelutietoa ulkomaisista toimijoista ja olosuhteista ylimmän valtionjohdon päätöksenteon tueksi. Lisäksi tarkoituksena olisi havaita ja tunnistaa kansalliseen turvallisuuteen kohdistuvia vakavia ulkoisia uhkia sekä kerätä niistä sellaista tietoa, joka mahdollistaa tilannekuvan muodostamisen, torjuntatoimiin ryhtymisen sekä sotilasviranomaisten osalta ennakkovaroituksen antamisen. Sotilastiedustelu ei ole samalla tavalla henkilö- ja rikossidonnaista toimintaa kuin rikosten ennalta estäminen. Tietoliikennetiedustelun tarkoituksena olisi sotilastiedustelun näkökulmasta selvittää yleisluonteisempia toimintatapoja kuin rikolliseksi toiminnaksi katsottuja tekoja.

Sotilastiedustelun yhtenä tärkeimpänä tehtävänä on tuottaa mahdollisimman reaaliaikaista tietoa turvallisuusympäristön kehityksestä, johon liittyy esimerkiksi vieraiden valtioiden asevoimien varustamiseen ja harjoitustoimintaan liittyvät kysymykset. Esimerkiksi juuri asevoimien tavanomaista varustamista ja harjoitustoimintaa ei yleisesti ottaen pidetä rikollisena toimintana, mikäli se tapahtuu kansainvälisten sopimusten ja lainsäädännön sallimissa rajoissa, jolloin toiminnan kriminalisointi kansallisen lainsäädännön tasolla ei olisi varteenotettava ratkaisu. Näin edellä kuvattu pakkokeinotyyppinen ratkaisumalli ei suoranaisesti soveltuisi sotilastiedustelun tarpeisiin.

Suomessa Puolustusvoimat on ainoa taho, joka tekee sotilastiedustelua. Sotilastiedustelu puolestaan on kriittinen osa sotilaallisen maanpuolustusta, joka puolestaan kuuluu Puolustusvoimien lakisääteisiin tehtäviin. Puolustusvoimilla itsellään puolestaan voidaan katsoa olevan paras tieto siitä, minkälaista sotilastiedustelutietoa se tarvitsee lakisääteisten tehtäviensä hoitamiseen, ja millä keinoilla tuo tieto saataisiin asianmukaisesti hankittua. Näin ei olisi tarkoituksenmukaista, että sotilastiedustelua harjoittaisi Puolustusvoimien ohessa tai sen sijaan jokin muu viranomainen. Sotilastiedustelu poikkeaa merkittävästi esimerkiksi siviilitiedustelusta, on sotilastiedustelusta tarkoituksenmukaista säätää omassa laissa.

Hallituksen strategiakokous 28.5.2015 päätyi malliin, jossa tiedustelutoiminta eriytettäisiin hallinnonalakohtaiseksi.

Tietoliikennetiedustelun teknisen suorittamisen olisi oltava viranomaistoimintaa. Toiminnassa on tarpeen käsitellä sellaista salassa pidettävää tietoa, jonka julkitulo vaarantaisi vakavalla tavalla kansallisen turvallisuuden. Lisäksi toiminnassa puututaan perusoikeuksiin tavalla, jota ei voida pitää hyväksyttävä perustuslain 124 §:n kannalta. Tästä johtuen salaisten tiedonhankintakeinoilla ja salaisilla pakkokeinoilla toteutettu tietoliikennetiedustelu ei olisi mahdollinen, sillä järjestely edellyttäisi julkisen vallan käytön siirtämistä merkittävissä määrin yksityisille toimijoille, teleoperaattoreille.

Tietoliikennetiedustelun teknisessä toteuttamisessa resurssinäkökulmasta olisi tarkoituksen mukaisinta keskittää se yhdelle viranomaiselle. Näin useat eri toimijat eivät kehittäisi omia teknisiä ratkaisujaan. Tämän voidaan myös katsoa parantavan tekniseen toteuttamiseen kohdennettujen resurssien seurantaa. Myös yksityisille toimijoille asetettavat velvollisuudet eivät muodostuisi merkittäviksi.

Tietoliikennetiedusteluviranomaiseksi olisi tarkoituksenmukaisinta nimetä sellainen viranomainen, jolla on jo valmiiksi toiminnan edellyttämä tekninen osaaminen ja kansainväliset tiedusteluyhteistyösuhteet. Tietoverkkouhkien torjuntaan osallistuvalla Kyberturvallisuuskeskuksella olisi toiminnan

edellyttämää teknistä osaamista. Sillä ei kuitenkaan ole tiedustelutiedon hankintaan liittyviä tehtäviä eikä siten myöskään tiedustelutoiminnan edellyttämiä yhteistyösuhteita. Keskusrikospoliisilla puolestaan on kansainvälisiä yhteistyösuhteita. Se on kuitenkin toimialaansa kuuluvien rikosten selvittämisestä vastaava viranomainen ja se huolehtii poliisi- ja pakkokeinolakiin liittyvien telepakkokeinojen teknisestä toteuttamisesta rikosprosessia varten. Keskusrikospoliisille ei myöskään tulisi nyt säädettäviä tietoliikennetiedustelun toimivaltuuksia, vaan siviilitiedustelun osalta tietoliikennetiedustelutoimivaltuuksia käyttäisi suojelupoliisi. Suojelupoliisilla on tiedustelutiedon hankintaan liittyvää kansainvälistä yhteistyötä, mutta ei tietoliikennetiedustelun tekniseen toteuttamiseen tarvittavia resursseja. Puolustusvoimien tiedustelulaitoksella puolestaan on sekä toiminnan edellyttämää teknistä osaamista että tiedustelutoiminnan edellyttämiä kansainvälisiä yhteistyösuhteita. Edellä mainitut seikat huomioiden Puolustusvoimien tiedustelulaitosta voitaisiin pitää tarkoituksenmukaisimpana vaihtoehtona tietoliikennetiedustelun tekniseksi toteuttajaksi.

Keskitetyssä ratkaisussa tietoliikennetiedustelun tekninen toteuttaminen osoitettaisiin sotilastiedusteluviranomaiselle (pääesikunnan tiedusteluosasto ja Puolustusvoimien tiedustelulaitos), joka toimeksiantajaviranomaisen eli suojelupoliisin toimeksiannosta toimii tietoliikennetiedustelun teknisenä toteuttajana.

Keskitettyä ratkaisua puoltaisivat toiminnan yhdenmukaisuudelle ja salassa pidettävyydelle asetettavat vaatimukset, toiminnan edellyttämä erikoistuminen ja tekninen osaaminen, toiminnasta aiheutuvat kustannukset sekä toiminnan lainmukaisuuden valvontaan liittyvät näkökohdat. EIT on edellyttänyt selkeiden menettelyiden luomista tietoliikennetiedustelulle sekä sen lainmukaisuuden kattavaa laillisuusvalvontaa. Näistä edellä mainituista asioista voidaan parhaiten huolehtia nyt keskitetyssä mallissa. Yhdenmukaisiin menettelytapoihin ja laillisuusvalvontaan liittyvät seikat puoltaisivat niin ikään sotilastiedustelun teknisen suorittamisen keskittämistä yhdelle viranomaiselle. Keskittämisen puolesta puhuvat myös taloudelliset syyt. Puolustusvoimien tiedustelulaitoksella on jo tällä hetkellä sekä toiminnan edellyttämät tekniset valmiudet että tarvittavat kansainväliset yhteistyösuhteet.

Tietoliikennetiedustelun järjestäminen edellyttäisi, että teleyrityksille tai rajat ylittävien viestintäverkkoja hallinnoivalle taholle asetettaisiin velvoite osoittaa liityntäpisteet sekä antaa tämän edellyttämät tiedot tietoliikennetiedustelun toteuttamisesta vastaavalle sotilastiedusteluviranomaiselle. Toteuttamisella ei saataisi aiheuttaa yleisen tietoliikenteen hidastumista. Liityntä tulisi suunnitella yhteistyössä viestintäverkkojen omistavien tai hallinnoivien tahojen kanssa siten, että niille sekä viestintäverkkojen toiminnalle koituvat haitat minimoitaisiin. Lähtökohtaisesti teknisestä toiminnasta yrityksille mahdollisesti aiheutuvat suorat kustannukset katettaisiin tietoliikennetiedustelua käyttävien tahojen puolelta.

Luottamukselliseen viestintään kohdistuva tiedustelu voidaan katsoa nykytilassa olevan mahdollista ainoastaan tilanteissa, joissa tiedustelun kohteena oleva taho ei nauti perusoikeussuojaa. Tästä johtuen perustuslain 10 §:n muuttaminen olisi edellytyksenä tässä esityksessä kuvatulle tietoliikennetiedustelulle sekä muiden toimivaltuuksien osalta silloin, kun ne puuttuisivat luottamuksellisen viestin suojaan.

Luottamukselliseen viestintään kohdistuva tiedustelu tulisi olla mahdollisimman kohdennettua ja rajattua. Tietoliikennetiedustelun kohteet eivät saisi olla sattumanvaraisesti valittuja. Tietoliikennetiedustelua suorittavalla viranomaisella tulee näin olla käsitys siitä, mihin viestintään tietoliikennetiedustelua kulloinkin kohdistetaan. Esimerkiksi vieraan valtion viranomaisten väliseen viestintään kohdistuva tietoliikennetiedustelu olisi tarkoituksen mukaisesti kohdennettua ja se pystyttäisiin toteuttamaan helpommin. Muihin toimijoihin kohdistuva tietoliikennetiedustelun edellyttää hakuluokkien ja automaattisten hakuehtojen käyttöä, minkä myötä tietoliikennetiedustelu voitaisiin kohdistaa mahdollisimman tehokkaasti haluttuun kohteeseen, jolloin tietoliikennetiedustelua voidaan pitää asianmukaisesti kohdennettuna.

Kohdennettu tietoliikennetiedustelu ei vaadi yhtä suurta tiedon tallettamiskapasiteettia eikä yhtä suurta tiedon analysointikykyä kuin kohdentamaton tietoliikennetiedustelu. Lisäksi vaikutusten esimerkiksi teleoperaattoreihin voidaan katsoa jäävän vähäisemmiksi.

Suomen ylimmällä valtiojohdolla olisi tilannekuvan muodostamiseksi tarve saada tietoliikennetiedustelulla hankittavaa tietoa. Tämän vuoksi myös ylimmällä valtiojohdolla tulisi olla mahdollisuus esittää tietopyyntöjä, joiden suorittamiseksi käytettäisiin tietoliikennetiedustelua. Tietopyynnöt tulisi kuitenkin kanavoida tietoliikennetiedustelun tekniselle suorittajalle Puolustusvoimien tai suojelupoliisin kautta. Näin tietopyynnön saanut viranomainen voisi tapauskohtaisesti harkita, mikä tiedustelukeino olisi tarkoituksenmukaisin tietopyyntöä koskevan tiedon hankkimiseksi.

3.3 Keskeiset ehdotukset

Hallituksen esitys on laadittu ”Suomalaisen tiedustelulainsäädännön suuntaviivoja” työryhmämietinnön ja pääministeri Juha Sipilän strategisen hallitusohjelman kirjausten pohjalta. Lainsäädäntötyön tavoitteena on luoda johdonmukainen ja ajantasainen sotilastiedustelusäännöstö, joka kaikilta osin vastaa perustuslain asettamia vaatimuksia. Esityksessä ehdotetaan täysin uutta sotilastiedustelulainsäädäntöä, josta tällä hetkellä ei ole laintasoista sääntelyä.

Esityksessä on otettu huomioon Ahvenanmaan asemaa koskevat kansainväliset sopimukset ja Ahvenanmaan itsehallintoa koskeva lainsäädäntö. Esityksen ei arvioida olevan ristiriidassa voimassaolevan sääntelyn kanssa Ahvenanmaan erityisasemaa koskien.

Yleiset säännökset (1 luku)

Lakia ehdotetaan sovellettavaksi Puolustusvoimien tiedusteluun eli sotilastiedusteluun, jolla hankitaan ennakolta, tutkitaan ja hyödynnetään puolustusvoimista annetun lain (551/2007) 2 §:ssä tarkoitettuihin tehtäviin liittyvää tietoa Suomen ulko-, turvallisuus- ja puolustuspolitiikan tueksi ja Suomeen kohdistuvien ulkoisten uhkien kartoittamiseksi. Näiden tehtävien toteuttamiseksi sotilastiedustelussa voitaisiin hankkia julkisista ja ei-julkisista tietolähteistä olevia tietoja.

Lain 2 §:ssä säädettäisiin lain suhteesta muuhun lainsäädäntöön, ennen kaikkea Puolustusvoimien rikostorjuntaan ja suojelupoliisin suorittamaan siviilitiedusteluun. 3 §:ssä säädettäisiin sotilastiedustelun tarkoituksesta.

Lain 4 §:ssä olisi lueteltu tyhjentävästi ne kohteet, joista sotilastiedusteluviranomainen saisi hankkia tietoja. Sotilastiedustelussa hankittaisiin kotimaassa ja ulkomailla tietoja 1) sotilaallisesta toiminnasta, 2) ulkomaisesta tiedustelutoiminnasta, 3) valtio- ja yhteiskuntajärjestystä uhkaavasta toiminnasta, 4) joukkotuhoaseista, 5) sotatarvikkeiden kehittämisestä ja levittämisestä, 6) valtioon tai yhteiskunnan elintärkeisiin toimintoihin kohdistuvista vakavista uhkista, 7) vieraan valtion suunnitelmista tai toiminnasta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille taikka muille tärkeille eduille, 8) kansainvälistä rauhaa ja turvallisuutta uhkaavista kriiseistä, 9) kansainvälisiin sotilaallisiin kriisinhallintaoperaatioihin kohdistuvista uhkista ja 10) Puolustusvoimien kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuuteen kohdistuvista uhkista.

Luvussa säädettäisiin myös toimintaa ohjaavista yleisistä periaatteista (5-7 §) ja esityksessä käytettävistä määritelmistä (9 §). Syrjinnän kielto (8 §) olisi toimivaltuuslainsäädännössä uuden tyyppinen säännös, mitä voidaan pitää tarkoituksenmukaisena tiedustelutoiminnan luonteen vuoksi.

Tiedustelumenetelmien käytön edellytys (10 §) vastaisi poliisilain 5 luvun salaisille tiedonhankintakeinoille säädettyä. Tiedustelumenetelmäkohtaiset erityiset edellytykset olisivat poliisilain 5 lukua vastaavasti porrastetut.

Sotilastiedusteluviranomaiset sekä ohjaus ja valvonta (2 luku)

Ehdotuksen mukaan ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteinen kokous käsittelisi valmistelevasti vuosittaiset sotilastiedustelun painopisteet (11 §). Nykyäänkin ulko- ja turvallisuuspoliittinen ministerivaliokunta valmistelee tärkeät ulko- ja turvallisuuspolitiikkaa sekä Suomen ulkosuhteita koskevat asiat, näihin liittyvät tärkeät sisäisen turvallisuuden asiat sekä tärkeät kokonaismaanpuolustusta koskevat asiat. Valmistelevasti käsitellyt painopisteet antaisi puolustusministeriö edelleen Puolustusvoimille.

Sotilastiedusteluviranomaisina toimisivat pääesikunta ja Puolustusvoimien tiedustelulaitos (12 §).

Luvussa säädettäisiin myös tiedustelutehtävästä (13 §). Tiedustelutehtävällä konkretisoitaisiin edelleen sotilastiedustelun kohteita sotilastiedustelun painopisteiden mukaisesti. Tiedustelutehtävän pohjalta sotilastiedusteluviranomainen suorittaisi konkreettisia tiedonhankinta toimenpiteitä käyttämällä tiedustelumenetelmiä.

Ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteinen kokous seuraisi painopisteiden mukaista tiedustelutoimintaa (14 §). Puolustusministeriö antaisi selvityksen vähintään vuosittain, pyynnöstä tai puolustusministeriön aloitteesta. Lisäksi seurantaan osallistuisi puolustusministeriö, jolle pääesikunta antaisi vähintään vuosittain selvityksen sotilastiedustelun laadusta ja laajuudesta sekä sen kohdentumisesta.

*Yhteistoiminta muiden viranomaisten kanssa ja kansainvälinen yhteistyö (*3 luku)

Lain 3 luvussa säädettäisiin yhteistoiminnasta suojelupoliisin ja muiden viranomaisten kanssa (15 §). Tiedustelun tarkoituksenmukaiseksi hoitamiseksi tiedustelun viranomaisten, suojelupoliisin ja sotilastiedusteluviranomaisten, olisi toimittava yhteistyössä. Tiedustelutoimintaa olisi myös yhteen sovitettava sotilas- ja siviilitiedustelun kesken.

Esityksessä ehdotetaan säädettäväksi, että edellä mainittujen painopistealueiden mukaisia tietopyyntöjä (16 §) pääesikunnalle voisivat tehdä tasavallan presidentti sekä valtioneuvoston kanslia, ulkoasiainministeriö ja puolustusministeriö. Päätöksen tietopyynnön toteuttamisesta tekisi kuitenkin sotilastiedusteluviranomainen.

Koska tiedustelutoiminnalla on merkitystä laaja-alaisesti yhteiskunnassa, tiedustelutoimintaa olisi voitava yhteen sovittaa keskeisten viranomaisten kesken (17 §). Lisäksi pykälässä otettaisiin huomioon ulkopoliittista harkintaa edellyttävät tiedustelutoiminnassa esiin nousevat tilanteet. Sotilastiedusteluviranomaisen kansainvälisestä yhteistyöstä säädettäisiin 18 §:ssä.

Tiedonhankinta toimivaltuudet (4 luku)

Lain 4 luvussa säädettäisiin sotilastiedusteluviranomaisen toimivaltuuksista. Luvussa säädetyt toimivaltuudet vastaisivat tiedonhankintakeinoina poliisilain 5 luvun salaisia tiedonhankintakeinoja ja niiden käytön edellytykset vastaisivat niitä. Toimivaltuuksia olisivat tarkkailu, suunnitelmallinen tarkkailu, tekninen tarkkailu, telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen, peitetoiminta, tietolähdetoiminta ja valeosto. Voimassa olevasta viranomaisten tiedonhankintaa koskevasta lainsäädännöstä uusina toimivaltuuksina säädettäisiin paikkatiedustelusta, jäljentämisestä, lähetyksen jäljentämisestä, radiosignaalitiedustelusta sekä ulkomaan tietojärjestelmätiedustelusta.

Puolustusvoimilla on käytössään rikosperusteisia salaisia tiedonhankintakeinoja sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain poliisilain viittausten perusteella. Uusia sotilas-

tiedusteluviranomaisen käyttämiä toimivaltuuksia voidaan pitää perusteltuina sen takia, että ainoastaan Puolustusvoimilla voidaan katsoa olevan riittävä tietotaito maanpuolustukseen kohdistuvista uhkista, sotilaallisesta toimintakentästä sekä toimintakentän tapojen ja käytäntöjen tuntemus. Tiedustelutoiminnan asianmukainen toteuttaminen edellyttää tätä taustaosaamista, jotta sotilastiedustelu pääsee hyödyntämään maanpuolustuksen kannalta kaikkein kriittisintä tietoa.

Päätöksenteko olisi porrastettu poliisilain 5 lukua vastaavasti. Esimerkiksi telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättäisi tuomioistuin pääesikunnan tiedustelupäällikön vaatimuksesta, kun taas suunnitelmallista tarkkailua koskevan päätöksen voisi tehdä tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies. Tietyissä tapauksissa olisi tarkoituksen mukaista säätää kiiremenettelystä.

Luvussa säädettyjen tiedustelumenetelmien käyttöä koskeva lupa-aika säädettäisiin pääsääntöisesti kuudeksi kuukaudeksi. Tämä ei kuitenkaan tarkoittaisi automaattisesti sitä, että lupa voitaisiin aina hakea tai päätös tehdä kuudeksi kuukaudeksi tai se tulisi myöntää kuuden kuukauden määräajaksi. Suhteellisuus- ja vähimmän haitan periaatteen mukaista harkintaa edellyttäisi säännöksissä oleva ilmaisu enintään kuudeksi kuukaudeksi kerrallaan.

Toimivaltuuden käyttöä koskevassa päätöksessä tai vaatimuksessa olisi mainittava 1) toimenpiteen perusteena oleva tiedustelutehtävä ja toimenpiteen tavoite, 2) toimenpiteen kohde (henkilö, henkilöryhmä, teleosoite, telepäätelaite, esine, alue, tila tai omaisuus), 3) tosiseikat, joihin tiedustelumenetelmän käytön edellytykset ja kohdistaminen perustuvat, 4) luvan tai päätöksen voimassaoloaika, 5) tiedustelumenetelmän käyttö johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies ja 6) mahdolliset tiedustelumenetelmän käytön rajoitukset ja ehdot.

Tiedustelumenetelmien käyttöä koskevana erityisenä vaatimuksena olisi, että vaatimukseen ja päätökseen tulisi sisällyttää tosiseikat (3 kohta). Tosiseikkojen esittäminen päätöksentekijälle velvoittaisi sotilastiedusteluviranomaisen esittämään ja perustelemaan ne tosiseikat, joiden perusteella luvan päätöksentekijä voi tehdä tiedustelumenetelmän käytön edellytysten täyttymisestä omat johtopäätöksensä. Edellytyksissä olisi kyse tiedustelumenetelmien käytön yleisistä ja erityisistä edellytyksistä. Lisäksi vaatimuksessa ja päätöksessä olisi esitettävä riittävät tosiseikat tiedustelutehtävästä ja tiedustelutehtävässä kuvastusta 4 §:ssä tarkoitetusta sotilastiedustelun kohteesta.

Luvussa tarkoitettu suunnitelmallinen tarkkailu (19–20 §) voisi kohdistua myös henkilöryhmään. Sotilastiedustelussa voisi ilmetä tarve seurata tietyn henkilöryhmän toimintaa, jolloin tiedonhankinnan tarve voi koskea tietyn henkilöryhmän organisaatiota, ryhmään kuuluvia henkilöitä ja henkilöryhmän aktiivisuutta tietyllä alueella.

Peitelty tiedonhankinta (21–22 §) voitaisiin vastaavasti kohdistaa henkilöön tai henkilöryhmään. Kuten muiden tiedustelumenetelmien osalta, myös peiteltyä tiedonhankintaa koskevassa päätöksessä tulisi kertoa tiedonhankinnan taustalla olevat tosiseikat, joiden perusteella olisi ulkopuolisen tarkastelijan, kuten valvonnan suorittajan, mahdollista tehdä tiedustelumenetelmän käytön edellytysten olemassaolosta omat johtopäätöksensä.

Tekninen tarkkailu jaoteltaisiin voimassaolevan käsityksen mukaisesti tekniseen kuunteluun (23–24 §), tekniseen katseluun (25–26 §), tekniseen seurantaan (myös henkilön tekninen seuranta) (27–28 §) ja tekniseen laitetarkkailuun (29–30 §).

Telekuuntelun (32–34 §) osalta ehdotetaan, että telekuuntelun kohteena voisi olla henkilö teleosoitteen ja telepäätelaitteen sijasta. Kun telekuuntelulupa kohdistuisi henkilöön, lupa käsittäisi telekuunteluluvan kohteena olevan henkilön hallussa olevat tai hänen oletettavasti muuten käyttämänsä teleosoitteet tai telepäätelaitteet. Telekuuntelulupa ei siis olisi teleosoite- tai telepäälaitekohtai-

nen. Lisäksi telekuuntelua olisi mahdollista kohdistaa valtiolliseen toimijaan eri edellytyksillä kuin muuhun toimijaan.

Myös televalvonnasta ja suostumusperäisestä televalvonnasta säädettäisiin tässä luvussa (35–36 §). Telekuuntelua vastaavasti, televalvontaa olisi mahdollista kohdistaa eri edellytyksillä tiedustelutehtävän kohteeseen riippuen siitä, onko kyseessä valtiollinen toimija vai muu kuin valtiollinen toimija.

Laitteen, menetelmän tai ohjelmiston asentamisesta ja poistaottamista koskevassa pykälässä (31 §) säädettäisiin sotilastiedusteluviranomaisen palveluksessa olevasta virkamiehestä, joka saisi tehdä toimenpiteen. Näin pystyttäisiin hyödyntämään paras mahdollinen tekninen osaaminen, mitä laitteen, menetelmän tai ohjelmiston asentamisessa ja poisottamisessa vaadittaisiin.

Myös teleosoitteen ja telepäätelaitteen yksilöintitietojen hankkimisesta (39 §) säädettäisiin puheena olevassa luvussa. Voimassa olevasta käytännöstä poikkeavasti, laitteiden ei tarvitsisi olla Viestintäviraston tarkastamia.

Peitetoiminnasta säädetäisiin 40–42 §:ssä ja valeostosta 47–50 §:ssä.

Laissa olisi myös säännökset ohjatusta tietolähdetoiminnasta 43–45 §:ssä. Tähän liittyvänä uutena toimivaltuutena olisi tietolähteen turvaaminen (46 §). Tietolähteen turvaamisessa olisi kyse tietolähteen ennakollisesti ja intensiivisemmästä suojaamisesta, mitä toiminnan suojaamisesta voimassa olevassa lainsäädännössä säädetään.

Lain 51 §:ssä säädettäisiin paikkatiedustelun määritelmästä. Paikkatiedustelulla tarkoitettaisiin pykälässä määritellyssä paikassa toimitettavaa tiedustelua esineen, omaisuuden, asiakirja, tiedon tai seikan löytämiseksi. Paikkatiedustelusta päättämistä koskevat säännökset olisivat 52 §:ssä. Päätöksentekotoimivalta jakautuisi sen mukaan kohdistuuko paikkatiedustelu paikkaan, johon ei ole yleistä pääsyä tai yleinen pääsy siihen on rajoitettu tai estetty paikkatiedustelun toimittajankohtana vai ei. Ensiksi mainitussa tapauksessa tuomioistuin päättäisi paikkatiedustelusta tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta. Jälkimmäisessä tapauksessa paikkatiedustelusta päättäisi pääesikunnan tiedustelupäällikkö tai tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

Lain 53 §:ssä säädettäisiin jäljentämisestä, joka olisi paikkatiedustelun lailla uusi tiedonhankintamenetelmä. Pykälän mukaan sotilastiedusteluviranomaisella olisi oikeus jäljentää asiakirja tai muu esine tietojen hankkimiseksi tiedustelutehtävän kannalta.

Jäljentämiskielloista ja telekuunteluun, televalvontaan ja tukiasematietoihin liittyvistä jäljentämiskielloista säädettäisiin pääosin vastaavalla tavalla mitä pakkokeinolain 7 luvun 3 §:ssä säädetään, sotilastiedustelutoiminnan luonne huomioon ottaen.

Lain 56 ja 57 §:ssä säädettäisiin lähetyksen jäljentämisestä ja lähetyksen pysäyttämisestä jäljentämistä varten. Menetelmällisesti kyse olisi vastaavista keinoista kuin pakkokeinolain 7 luvussa säädetään. Käyttöperusteeltaan ja -tarkoitukseltaan kyse olisi tässä yhteydessä tiedustelumenetelmistä.

Lain 60–61 §:ssä säädettäisiin radiosignaalitiedustelusta. Nykymuodossaan toimivaltuus ei vaadi erityistä sääntelyä. Sotilastiedustelutoiminnan kokonaisuuden ja sen merkityksen Puolustusvoimille kannalta toimivaltuudesta olisi kuitenkin tarkoituksen mukaista säätää nimenomaisesti.

Lain 62–63 §:ssä säädettäisiin ulkomaan tietojärjestelmätiedustelusta. Toimivaltuuden voidaan katsoa vertautuvan kotimaassa käytettävistä menetelmistä osittain tekniseen laitetarkkailuun ja

tekniseen kuunteluun. Koska toimivaltuuden käyttö olisi usein pitkäkestoista ja -jänteistä, ja koska toimivaltuuden käyttöön liittyisi ulkopoliittisia näkökohtia, joita olisi tarkoin harkittava, olisi erillisestä toimivaltuudesta ja päätöksen teosta tarkoituksen mukaista säätää erillisenä toimivaltuutena.

Tiedustelumenetelmän käytöstä päättämisestä muualla kuin Suomessa säädettäisiin 64 §:ssä. Päätöksen, esityksen ja suunnitelman sisällön osalta noudatettaisiin mitä tiedustelumenetelmiä koskevissa päätöspykälissä säädettäisiin. Ulkomaan tiedustelussa tulisi siten kirjata samat asiat tiedustelumenetelmää koskevaan päätökseen kuin kotimaan tiedustelussa. Eräitä lain säännöksiä ei kuitenkaan sovellettaisi ulkomaan tiedustelussa.

Tiedonhankinta tietoliikenteestä (5 luku)

Uutena tiedonhankintakeinona säädettäisiin toimivaltuudet rajan ylittävään tietoliikenteeseen kohdistettavaa tiedustelua varten. Tietoliikennetiedustelussa olisi kyse tiedustelutoimivaltuudesta, jonka tarkoituksena olisi tuottaa tiedustelutietoa ulkomaisista toimijoista ja olosuhteista ylimmän valtionjohdon päätöksenteon tueksi. Lisäksi tarkoituksena olisi havaita ja tunnistaa Suomeen kohdistuvia vakavia ulkoisia uhkia sekä kerätä niistä sellaista tietoa, joka mahdollistaa tilannekuvan muodostamisen, torjuntatoimiin ryhtymisen sekä sotilastiedusteluviranomaisen osalta ennakkovaroituksen antamisen. Tiedustelu ei ole samalla tavalla henkilö- ja rikossidonnaista toimintaa kuin rikosten ennalta estäminen. Tietoliikennetiedustelun kohteet olisivat yleisluonteisempia kuin rikoslaissa tarkoitettuja rikollisia tekoja.

Tietoliikennetiedustelulla tarkoitettaisiin Suomen rajan ylittävän viestintäverkon osassa ylittävään tietoliikenteeseen kohdistuvaa, tietoliikenteen automatisoituun erotteluun perustuvaa teknistä tiedonhankintaa sekä hankitun tiedon käsittely. Tietoliikennetiedustelu koskisi näin ollen ainoastaan sellaista tietoliikennettä, joka ylittää valtakunnanrajan siirtymällä suomalaisesta viestintäverkosta ulkomaiseen viestintäverkkoon tai päinvastoin. Merkittävä osa suomalaisesta tietoliikenteestä olisi jo näin rajattu tietoliikennetiedustelun ulkopuolelle.

Tietoliikenteeseen kohdistuvan tiedustelun yleisenä edellytyksenä olisi toiminnan tuloksellisuus. Tätä edellytystä sovellettaisiin silloin, kun tietoliikennetiedustelu voitaisiin kohdistaa pelkästään valtiollisen toimijan tietoliikenteeseen (68 §). Tämä edellytys perustuisi siihen, että valtiot ja niihin rinnastuvat tahot eivät nauti luottamuksellisen viestinnän salaisuuden suojaa.

Muissa tapauksissa tietoliikennetiedustelun erityisenä edellytyksenä olisi tuloksellisuuden lisäksi välttämättömyys, mikä on korkein viranomaisten toimivaltuuksia koskevan lainsäädännön tuntema edellytyskynnys (70 §). Välttämättömyysedellytystä sovellettaisiin sekä niissä tapauksissa, joissa tietoliikennetiedustelun kohteena sinänsä on vieras valtio, mutta hakuehtojen käytön piiriin voi tulla muutakin tietoliikennettä, että niissä tapauksissa, joissa tietoliikennetiedustelun kohde nauttii suoraan luottamuksellisen viestin salaisuuden suojaa.

Välttämättömyysedellytys tarkoittaisi viimesijaisuutta eli sitä, että tietojen hankkiminen muulla keinolla olisi mahdotonta tai kohtuuttoman vaikeaa. Edellytyksen soveltaminen edellyttäisi sekä tietoliikennetiedusteluun lupaa hakevalta puolustusvoimien tiedustelulaitokselta että lupavaatimuksen ratkaisijan olevalta tuomioistuimelta vertailua yhtäältä 4 luvussa säädettyjen toimivaltuuksien ja tietoliikennetiedustelun välillä. Jos muiden tiedustelumenetelmien käyttö ei olisi mahdotonta tai kohtuuttoman vaikeaa, tulisi niitä käyttää ensisijaisina keinoina.

Viestintäverkon määritelmään sisältyisi vaatimus tiedonsiirron sähkömagneettisesta toteutustavasta, mutta muuten se olisi luonteeltaan teknologianeutraali. Koska valtaosa Suomen ja ulkomaiden välisestä tietoliikenteestä välittyy valokuituja pitkin tiedonsiirtoon käytettävissä kaapeleissa, kohdistuisi tietoliikennetiedustelu käytännössä pääasiassa kaapelivälitteiseen tietoliikenteeseen. Viestin-

täverkon käsitteen teknologianeutraalisuudella varmistettaisiin kuitenkin lain soveltuvuus myös muissa teknisissä ympäristöissä ja muuttuvien viestintäteknologioiden olosuhteissa.

Luvussa säädettäisiin myös viestintäverkon teknisten tietojen analysoimiseksi välttämättömästä tietojen hankkimisesta (66 §). Näiden tietojen analysointi olisi välttämätön edellytys sille, että tietoliikennetiedustelu voitaisiin kohdistaa mahdollisimman tarkasti tiettyyn Suomen rajan ylittävään viestintäverkon osaan. Analysoinnin kohteena olisivat tietoliikennevirrat. Lisäksi viestintäverkon omistajille ja haltijoille säädettäisiin velvollisuus (95 §) avustaa antamalla viestintäverkon valinnan kannalta tarpeelliset hallussaan olevat tiedot Puolustusvoimien tiedustelulaitokselle.

Tietoliikennetiedustelu perustuisi menetelmällisesti tietoliikenteen automatisoituun erotteluun. Tämä erottaisi sen muista sähköiseen viestintään kohdistuvista tiedustelumenetelmistä, kuten telekuuntelusta ja televalvonnasta. Kyse ei olisi yksittäiseen tiedossa olevaan teleosoitteeseen tai telepäätelaitteeseen kohdistuvasta tiedonhankinnasta, vaan automaattisin menetelmin tapahtuvasta tietoliikenteen suodattamisesta sellaisessa kohdassa viestintäverkkoa, jonka kautta tiedustelun kohteena olevan tietoliikenteen voidaan olettaa kulkevan. Tietoliikenteen suodattamiseen perustuva ratkaisu mahdollistaisi uhkaan liittyvän viestinnän havaitsemisen ja sen taustalla olevien tahojen tunnistaen ja paikallistamisen. Suodattaminen toteutettaisiin vertailemalla valittua tietoliikennevirtaa hakuehdoiksi kutsuttaviin ennakkoon asetettuihin kriteereihin, eli hakuehtoihin ja hakuehtojen luokkiin.

Hakuehtoina saisi käyttää muita kuin luottamuksellisen viestin semanttista sisältöä kuvaavia tietoja, ennen kaikkea tietoliikenteen ohjaus- ja välitystiedot eli sellaiset tietoverkolle taikka lähettävälle tai vastaanottavalle tietojärjestelmälle tarkoitettuja ohjeita, komentoja ja muita metatietoja, joilla vaikutetaan viestin kuljetukseen ja ohjaamiseen viestintäverkossa ja tietojärjestelmässä. Hakuehtoina sallittuja tietoja olisivat myös esimerkiksi tiedot jonkin salausohjelman käytöstä.

Hakuehto ei saisi kuvata viestin sisältöä. Viestin sisältöä kuvaava hakuehdon käytön voidaan katsoa sisältävän syvällisemmän puuttumisen sivullisten luottamuksellisen viestinnän suojaan, sillä toiminta edellyttää kaiken suodatuksen piirissä olevan viestinnän tietoteknistä avaamista sen selvittämiseksi, vastaako sen sisältö hakuehtoa. Viestin sisällön on perinteisesti katsottu muodostavan luottamuksellisen viestin salaisuuden ydinalueen.

Viestin sisältöä kuvaavan hakuehdon käytöstä olisi kuitenkin kaksi tarkkaan rajattua poikkeusta. Sisältöä kuvaavaa hakuehtoa saataisiin ensinnäkin käyttää silloin, kun tietoliikennetiedustelu voidaan kohdistaa pelkästään vieraan valtion tai sellaiseen rinnastuvan tahon tietoliikenteeseen (68 §), eli tietoliikenteeseen, joka ei nauti luottamuksellisen viestin salaisuuden suojaa. Poikkeuksen soveltaminen tulisi kyseeseen vain, jos siinä tietoliikennevirrassa, johon hakuehtoja käytetään, ei ole mitään luottamuksellisen viestin salaisuuden suojaa nauttivaa sivullista viestintää.

Toinen poikkeus koskisi haitallista tietokoneohjelmaa tai käskyä. Haitallisen tietokoneohjelman tai -käskyn sisältöä kuvaavat hakuehdot olisivat erilaisia teknisiä merkkijonoja eivätkä luonnollisen kielen sanoja tai ilmaisuja. Haittaohjelmia koskevien hakuehtojen erityisluonteen vuoksi niitä saataisiin verrata myös viestintäsalaisuuden piiriin kuuluvien viestien sisältöön.

Hakuehdot tai hakuehtojen luokat eivät olisi Puolustusvoimien tiedustelulaitoksen vapaasti valittavissa tiedustelumenetelmän käytön aikana, vaan ne olisi lueteltava tuomioistuimen päätöksessä.

Tuomioistuimen lupapäätös on katsottu EIT ratkaisukäytännössä tärkeäksi oikeusturvatakeeksi, jos toimenpiteellä puututaan luottamuksellisen viestin suojaan. Tietoliikennetiedustelua koskevat asiat käsiteltäisiin Helsingin käräjäoikeudessa, niin kuin on muidenkin tuomioistuimen käsittelyä edellyttävien tiedustelumenetelmien osalta asian laita.

Tuomioistuimelle esitettävässä lupavaatimuksessa muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvan tiedustelun osalta (71 §) olisi esitettävä 1) tiedustelutehtävä, jota varten tietoliikennettä hankittaisiin, 2) tiedustelun kohdetta koskevat tosiseikat, 3) tosiseikat, joihin tietoliikennetiedustelun käytön edellytykset perustuvat, 4) tiedonhankinnassa käytettävät hakuehdot tai hakuehtojen luokat sekä perustelut niille, 5) viestintäverkon osa, johon tiedustelu kohdistetaan sekä perustelut kohdistamiselle, 6) luvan voimassaoloaika kellonajan tarkkuudella, 7) viestinnän keräämisen ja tallentamisen suorittamista valvova ja johtava Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies ja 8) mahdolliset tietoliikennetiedustelun rajoitukset ja ehdot. Valtiolliseen toimijan tietoliikenteeseen kohdistuvassa tiedustelussa lupavaatimuksessa esitettävät seikat eivät olisi yhtä tarkat (69 §).

Tuomioistuimen myöntämän luvan voimassaoloaika voitaisiin myöntää korkeintaan kuudeksi kuukaudeksi kerrallaan.

Suodattamisen piirissä ei olisi missään yksittäisessä tietoliikennetiedustelun käyttötapauksessa kaikki se tietoliikenne, joka ylittää Suomen rajan viestintäverkossa. Tietoliikennetiedustelun käyttö edellyttäisi, että Puolustusvoimien tiedustelulaitoksella olisi tieto tai epäilys jonkin sotilastiedustelun kohteen konkreettisesta olemassaolosta ja sen tosiseikoista. Kohteen kulloinenkin luonne ja kohteesta tiedossa olevat tosiseikat vaikuttavat siihen, missä viestintäverkon osassa tietoliikenteen voidaan olettaa ylittävän Suomen rajan. Vieraiden valtiotoimijoiden tietoliikenteen esimerkiksi voidaan olettaa ylittävän rajan muissa viestintäverkon osissa kuin muiden toimijoiden viestinvaihdon. Kuten sanotusta käy ilmi, voidaan katsoa, ettei tietoliikennetiedustelussa olisi kyse kaikkeen mahdolliseen tietoliikenteeseen kohdistuvasta tiedustelusta eli niin sanotusta massavalvonnasta.

Tietoliikennetiedustelua koskevassa lupavaatimuksessa olisi mainittava se Suomen rajan ylittävä viestintäverkon osa, jossa kulkevaan tietoliikenteeseen hakuehtoja saataisiin käyttää. Hakuehtoja ei saataisi käyttää muissa kuin lupapäätöksessä mainituissa viestintäverkon osissa liikkuvaan tietoliikenteeseen. Se, kuin laajassa osassa rajan ylittävää viestintäverkkoa hakuehtoja olisi kussakin tapauksessa tarpeen käyttää, riippuisi muun muassa tiedustelun kohteen luonteesta ja kohteen taustalla olevien henkilöiden oletettavasti käyttämistä viestintämenetelmistä.

Tietoliikennetiedustelun toteuttaminen edellyttäisi, että viestintäverkon rajan ylittävään osaan olisi ennakkoon rakennettu liitynnät. Liityntöjen rakentaminen tapahtuisi niiden yritysten myötävaikutuksella, jotka omistavat tai hallitsevat viestintäverkon rajan ylittävää osaa (97 §). Lisäksi Suomen rajan ylittävän viestintäverkon osan omistava tai hallitseva taho olisi velvollinen antamaan hallussaan olevia tietoja sen arvioimiseksi, mistä viestintäverkon osasta tietystä paikasta tuleva tietoliikenne reitittyisi Suomen rajan yli.

Kun tietoliikennetiedusteluun olisi saatu tuomioistuimen lupa, tehtäisiin luvanmukaiseen viestintäverkon osaan kytkentä (72 §). Kytkennän tekemisellä luvanmukaisessa viestintäverkon osassa kulkeva tietoliikenne ohjautuisi suodatukseen. Kytkennän tekijänä ja luvanmukaisen tietoliikenteen luovuttajana olisi Suomen Erillisverkot Oy. Tehtävä olisi osoitettu tiedusteluviranomaisista riippumattomalle taholle sen varmistamiseksi, että tiedusteluviranomaiset eivät saa laajempaa pääsyä tietoliikenteeseen kuin tuomioistuimen lupapäätös sallii.

Puolustusvoimien tiedustelulaitoksen oikeus tallentaa tietoliikennetiedustelun avulla hankittuja tietoja samoin kuin tallennettujen tietojen poistaminen ja luovuttaminen tietojärjestelmästä määräytyisi tietojen käsittelyä koskevien säännösten mukaan. Luvussa olevat erityiset säännökset koskisivat tietoliikennetiedustelun käyttöä rajoittavia erityisiä tiedustelukieltoja ja velvollisuutta hävittää viipymättä eräät tietoliikennetiedustelulla saadut tiedot. Ehdotetut tiedustelukiellot ja hävittämisvelvollisuudet rajoittaisivat merkittävästi sitä, mitä tietoliikennetiedustelutietoja Puolustusvoimien tiedustelulaitos tietojärjestelmään saataisiin tallentaa.

Luvussa säädettäisiin myös tietoliikennetiedustelun teknisestä toteuttamisesta suojelupoliisin puolesta (73 §). Tekninen toteuttaminen kattaisi teknisen analyysin tuottamisen suojelupoliisin toimeksiannosta sekä tuomioistuimen suojelupoliisille myöntämän luvan perusteella tapahtuvan tiedonhankinnan suojelupoliisille. Jälkimmäisessä tapauksessa Puolustusvoimien tiedustelulaitoksella ei olisi pääsyä hankitun tietoliikenteen sisältöön vaan kyse olisi ainoastaan tietoliikenteen hankinnasta ja sen luovuttamisesta sellaisenaan suojelupoliisille.

Tietoliikennetiedustelua ei käytettäisi Suomen sisäisessä viestintäverkossa kulkevan tietoliikenteen tiedusteluun tai Suomessa oleskelevien osapuolten välisen tietoliikenteen tiedusteluun. Viimeksi mainitussa tapauksessa tietoliikenne saattaa kuitenkin reitittyä lähettäjältä vastaanottajalle rajan ylittävän viestintäverkon osan kautta. Lisäksi olisi tarkoituksenmukaista, ettei tietoliikennetiedustelun piiriin tulisi viestintää, josta osapuolella olisi velvollisuus tai oikeus kieltäytyä todistamasta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n taikka 22 §:n 2 momentin nojalla. Koska edellä tarkoitettuja tapauksia koskevia hakuehtoja ei voida teknisesti toteuttaa tietoliikennetiedustelussa, säädettäisiin luvussa erillisesti tietojen hävittämisvelvollisuudesta (74 §). Puolustusvoimien tiedustelulaitoksen olisi hävitettävä tieto tällaisissa tapauksissa välittömästi sen käytyä ilmi.

Tiedustelutietojen ilmoittaminen eräissä tilanteissa (6 luku)

Luvussa 6 säädettäisiin sotilastiedustelutietojen ilmoittamisesta eräissä tapauksissa. Luvun mukaan kyseessä voisi olla tietyissä tapauksissa ilmoitusvelvollisuus esitutkintaviranomaiselle tai rikostorjuntaviranomaiselle. Kyseessä olisi poikkeus tiedustelumenetelmillä saadun tiedon käyttötarkoitussidonnaisuudesta. Tietyin 77 tai 78 §:ssä tarkoitetuin edellytyksin tiedustelumenetelmällä saatua tietoa voitaisiin ilmoittaa esitutkintaviranomaiselle tai rikostorjuntaviranomaiselle.

Lisäksi tietyissä tilanteissa tiedustelumenetelmällä hankittua tietoa voitaisiin ilmoittaa yksityiselle toimijalle (78 §).

Sotilastiedustelun suojaaminen ja turvaaminen, tietojen hävittäminen sekä tiedonhankinnasta ilmoittaminen (7 luku)

Luvussa säädettäisiin sotilastiedustelun suojaamisesta (81–82 §). Suojaaminen kattaisi koko sotilastiedustelutoiminnan ja mahdollistaisi siten laajemman toiminnan suojaamisen kuin voimassa olevassa lainsäädännössä.

Luvussa säädettäisiin myös sotilastiedusteluviranomaisen virkamiehen turvaamisesta peitellyssä tiedonhankinnassa, peitetoiminnassa tai valeostossa (83 §).

Tiedonhankinnasta ilmoittamisesta (87 §) säädettäisiin vastaavantyyppisesti, mitä poliisilain 5 luvun 58 §:ssä salaisen tiedonhankintakeinon käytöstä ilmoittamisesta säädetään.

Tiedustelutietojen hävittämistä koskeva pykälä (84) koskisi ensisijaisesti 4 luvussa säädettyjä toimivaltuuksia. Pykälää täydentäisi tiedonhankintaa tietoliikenteestä (5 luku) koskevat erilliset säännökset.

Kiiretilanteessa saadun tiedon hävittäminen (86 §) koskisi kaikkia tiedustelumenetelmiä, myös tietoliikennetiedustelua.

Lisäksi säädettäisiin tiedustelutietojen hävittämisestä (84 §) ja tiedustelutehtävään liittymättömän tiedon käyttämisestä (85 §).

Puolustusvoimien muun virkamiehen ja asevelvollisten osallistuminen sotilastiedusteluun sekä kansainvälinen toiminta (8 luku)

Myös muilla Puolustusvoimien virkamiehillä kuin sotilastiedusteluviranomaisen palveluksella olevilla virkamiehillä on tiedustelun kannalta olennaista osaamista (88 §). Tätä osaamista voitaisiin käyttää ainoastaan sotilastiedusteluviranomaisen alaisuudessa.

Tiedustelutehtävän suorittamiseen voisivat osallistua sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa tietyissä tapauksissa riittävän koulutuksen saaneet reserviläiset (89 §). Sotilastiedustelussa olisi voitava myös etupainotteisesti ennen liikekannallepanoa voitava käyttää reserviläisiä valmiustilannetta tehostettaessa.

Koska Puolustusvoimien kansainvälisiin operaatioiden osallistuvan organisaation keskeisinä toimijoina ovat reserviläiset, näiden toimivaltuuksista näissä tehtävissä säädettäisiin erikseen (90 §).

Luvussa säädettäisiin lisäksi asevelvollisuuslain mukaisessa palveluksessa olevan virkavastuusta sekä vahingonkorvausvastuusta (91 ja 92 §).

Ilmaisukielto, yksityisten yhteisöjen velvollisuudet ja oikeudet sekä tietojen saanti eräiltä tahoilta (9 luku)

Luvussa säädettäisiin ilmaisukiellosta sotilastiedustelua avustaneelle ulkopuoliselle henkilölle sekä sotilastiedusteluviranomaisen mahdollisuudesta saada tietoja yksityisiltä yhteisöiltä ja henkilöiltä (93 §).

Lisäksi luvussa säädettäisiin teleyrityksen ja tiedonsiirtäjän velvollisuuksista sekä näille ja kytkennän suorittajalle maksettavista korvauksista (94–100 §). Edellä tarkoitetut tahot ovat keskeisessä asemassa viestintäverkkoon kohdistuvien tiedustelumenetelmien käytössä. Lisäksi säädettäisiin yksityisen yhteisön ja henkilön tiedonantovelvollisuudesta (101 §).

Sotilastiedustelun tietojärjestelmä ja muut henkilörekisterit (10 luku) *ja sotilastiedustelun valvonta puolustushallinnossa* (11 luku)

Luvussa 10 säädettäisiin henkilötietojen käsittelyn keskeisistä yleisistä periaatteista. Sotilastiedusteluviranomaisen tehtävien erityisluonteen vuoksi olisi tarkoituksenmukaista, että henkilötietojen käsittelyä koskeva sääntely ei jäisi pelkän yleislainsäädännön soveltamisen varaan. Toimivaltaiselle viranomaiselle asetettaisiin tiedustelutoimintaa koskevat henkilötietojen käsittelyn erityisvaatimukset.

Luvussa 11 säädettäisiin sotilastiedustelutoiminnan sisäisestä valvonnasta puolustushallinnossa. Sisäinen valvonta tarkoittaa toiminnan valvontaa tiedusteluorganisaation sisällä sekä hallinnonalan yleistä valvontaa ja puolustusministeriön suorittamaa valvontaa. Ulkoisesta laillisuusvalvonnasta ja parlamentaarisesta valvonnasta säädettäisiin erikseen.

Erinäiset säännökset (12 luku)

Luvussa säädettäisiin tiedustelutoiminnan yleisistä menettelyistä, kuten määräaikojen laskemisesta (126 §), tiedustelukielloista (127 §), tallenteiden tarkastamisesta ja tutkimisesta (128-129 §), pöytäkirjasta (130 §), vaitiolovelvollisuudesta ja -oikeudesta (131-132 §) ja virkamerkistä (133 §).

Lisäksi säädettäisiin tuomioistuinmenettelystä (134 §). Sotilastiedustelun asiat käsiteltäisiin Helsingin käräjäoikeudessa. Helsingin käräjäoikeudelle on maan laajin kokemus salaisten tiedonhankinta- ja pakkokeinoasioiden käsittelemisestä, voidaan katsoa, että kyseisellä instanssilla olisi riittävä erikoisosaaminen myös tiedustelumenetelmiä koskevissa asioissa.

4 Esityksen vaikutukset

4.1 Taloudelliset vaikutukset

4.1.1 Vaikutukset julkiseen talouteen

Esityksen vaikutukset julkiseen talouteen aiheutuvat erityisesti uusien toimivaltuuksien säätämisestä Puolustusvoimille. Lisäksi esityksestä aiheutuu muita kustannuksia lupaviranomaiselle sekä puolustusministeriölle viranomaisten välisen yhteistyön syventämisen vaatimista resursseista.

Tietoliikennetiedustelu

Tietoliikennetiedustelun edellyttämien ylläpitokustannusten arvioidaan aiheuttavan noin 700 000 euron vuotuiset lisäkustannukset Puolustusvoimille.

Tietoliikennetiedustelun toimivaltuuksista arvioidaan aiheutuvan noin 1,2 miljoonan euron vuosittaiset lisäkustannukset Puolustusvoimille. Kustannukset muodostuvat yrityksille tietoliikennetiedustelusta aiheutuneiden kulujen korvaamisesta sekä Puolustusvoimille tietoliikennetiedustelun edellyttämistä laite- ja konesalivuokrista ja muista toiminnan kuluista.

Hallintokulujen ja toimintamenojen arvioidaan aiheuttavan noin 350 000 euron lisäkustannukset vuonna 2018, jonka jälkeen lisäkustannusten arvioidaan olevan noin 700 000 euroa vuodessa. Tämä pitää sisällään suojelupoliisin puolesta suoritettavan tietoliikennetiedustelun.

Puolustusvoimien tiedustelulaitokselle ohjattava tietoliikenne edellyttää ulkopuolisen toimijan tekemää kytkentää tuomioistuimen luvassa tarkoitettuun viestintäverkon osaan. Ulkopuolisesta toimijasta aiheutuvat kustannukset tarkentuvat jatkovalmistelussa, mutta tämän hetkisen arvion mukaan tähän olisi osoitettava muutama henkilötyövuosi.

Muuten tietoliikennetiedustelun edellyttämät järjestelmäinvestoinnit ja henkilöstöresurssit pystytään kohdentamaan kehittämisohjelmien puitteissa normaalina Puolustusvoimien toimintana.

Muut toimivaltuudet

Uusien toimivaltuuksien käyttöön ottaminen edellyttää sotilastiedusteluviranomaisten käyttämien menetelmien, laitteistojen, järjestelmien ja analyysitoimintojen kehittämistä. Uusien toimivaltuuksien mukaisen tiedonhankinnan kehittäminen ja hankitun tiedon turvallinen hyödyntäminen edellyttävät tarvittavien laitteiden hankkimista ja järjestelmien rakentamista etupainotteisesti. Tämä edellyttää 3,4 miljoonan euron lisärahoitusta kohdistuen vuodelle 2018. Toimivaltuuksien käytöstä ja järjestelmiin liittyvistä ylläpitokustannuksista arvioidaan aiheutuvan noin 800 000 euron vuosittaiset lisäkustannukset.

Edellä tarkoitetuista toimivaltuuksista aiheutuu lisäksi hallinto- ja toimintamenoihin, kuten koulutuskustannuksiin, toiminnan aloittamiseen liittyen ensimmäisen vuoden lisäkustannukset vuonna 2018 arvioidaan olevan noin 450 000 euroa, jonka jälkeen vuosittaiset lisäkustannukset olisivat noin 900 000 euroa. Osa teletiedonhankintakeinojen aiheuttamista kustannuksista katettaisiin sisäministeriön rahoituskehyksestä.

Uudet toimivaltuudet edellyttävät erikoiskoulutettua henkilöstöä, tiedonhankinnan ja henkilöstön suojaamista sekä tarpeen mukaan ympärivuorokautista päivystystä. Kustannukset aihetuvat henkilöstömäärän lisäyksestä, jota ei ole otettu huomioon Puolustusvoimien kehittämisohjelmissa tai kehyksissä. Henkilöstön lisäyksestä arvioidaan aiheutuvan noin miljoonan euron lisämäärärahan

tarve vuodessa lain voimaan tultua ja myöhemmin sotilastiedustelutoiminnan kehittyessä noin kolmen miljoonan euron vuosittaisen kustannukset.

Ulkomaan tietojärjestelmätiedustelun ja radiosignaalitiedustelun aiheuttamat kustannukset voidaan kattaa Puolustusvoimien kehittämisohjelmien puitteissa.

Tiedustelutoimintaan liittyvä päätöksenteko ja valvonta

Sotilastiedustelutoiminnan sisäinen valvonta edellyttää lisäresursointia pääesikuntaan. Tiedustelutoiminnan tekninen ja laillisuusvalvonta olisi järjestettävä niin, että valvonta on tehokasta, toimivaa ja uskottavaa. Tiedustelutehtävien hoitamiseen ja sisäiseen laillisuusvalvontaan olisi osoitettava lisäresursseja neljän henkilötyövuoden verran. Uusista tehtävistä aiheutuvien lisäkustannusten arvioidaan olevan noin 160 000 euroa (2 htv) vuonna 2018, jonka jälkeen lisäkustannusten arvioidaan olevan noin 320 000 euroa (4 htv) vuodessa. Lisäksi tiedustelutoiminnan valvonta aiheuttaisi lisäkustannuksia, jotka johtuvat henkilön kouluttamisesta uusiin tehtäviin.

Lain voimaantulo edellyttää puolustusministeriön laillisuusvalvonnan resurssien riittävyyden tarkastelua. Tätä ei kuitenkaan voida tarkkaan arvioida etukäteen. Arvion mukaan tämä toiminta voitaisiin aloittaa kuitenkin nykyresurssien puitteissa ottaen huomioon, että puolustusministeriön suorittama valvonta ei ole yhtä laaja-alaista ja konkreettista kuin Puolustusvoimien sisäinen laillisuusvalvonta.

Lisäksi esityksestä aiheutuisi hallinnollisia kuluja Puolustusvoimille. Hallinnolliset kulut aiheutuisivat valvontaan liittyvästä myönnettyjen tuomioistuinlupien ilmoittamisesta ulkopuoliselle tiedustelun valvontaviranomaiselle.

Muut vaikutukset

Toimivaltuuksien käytön lupaviranomaisena toimivalle tuomioistuimelle aiheutuu lisäkustannuksia käsiteltävien asioiden lisääntymisen myötä. Tiedustelutoiminnan lupa-asioiden käsittely aiheuttaa myös kustannuksia riittävien tietoturvallisten tilojen ja tietojärjestelmien rakentamisesta.

Sotilastiedusteluviranomaiselle esitettyjen tietopyyntöjen esittäjille aiheutuu lisäkustannuksia, kuten käännätyskuluja. Näiden vaikutusten ei arvioida olevan merkittäviä.

Ilmoittamisvelvollisuudesta ja -oikeudesta esitutkintaviranomaiselle ja rikostorjuntaviranomaiselle aiheutuu hallinnollisia kuluja. Näiden kulujen ei arvioida olevan merkittäviä.

Sotilastiedusteluun liittyvästä yhteistyöstä muiden viranomaisten ja valtion ylimmän johdon kanssa sekä sotilastiedustelutoiminnan ohjauksesta aiheutuu lisäkustannuksia puolustusministeriölle. Tämä aiheuttaa yhden henkilötyövuoden lisäresurssitarpeen ministeriöön. Perustettavan viran pääasiallisena tehtävänä olisi sotilastiedustelutoimintaan liittyvän poliittisen päätöksenteon valmistelu, toiminnan ja resurssien suunnittelu sekä yhteistyön kehittäminen kansallisesti ja kansainvälisesti. Virka olisi perustettava jo ennen lain voimaantuloa, jotta sotilastiedustelutoiminnan alkaessa toiminnan ohjaus ja yhteistyö muiden viranomaisten kanssa olisi asianmukaista. Viran vuosikustannusten arvioidaan olevan noin 90 000 euroa vuodesta 2018 alkaen.

Ehdotettujen toimivaltuuksien käyttämisestä arvioidaan aiheutuvan noin 100 000 euron kustannukset oikeusministeriön hallinnonalalle.

Kokonaisarvio

Uusien viranomaistehtävien aiheuttama kokonaislisäkustannus arvioidaan olevan alkuvaiheessa noin 5,7 miljoonaa euroa vuositasolla. Lisäksi esityksellä arvioidaan olevan kertahankinnoista johtuen noin 3,4 miljoonan euron vaikutukset kohdistuen vuodelle 2018.

Yhteenveto lakiesityksen taloudellisista vaikutuksista puolustushallinnolle	S2018	S2019 (lain arvioitu voimaantulo)	S2020	S2021->
Kertaluonteiset investoinnit				
-laite- ja tietojärjestelmäkustannukset	3 400 000	-	-	-
Henkilöstökulut (Puolustusvoimat)				
operatiivinen	600 000	1 000 000	2 000 000	3 000 000
sisäinen valvonta (htv)	160 000 (2 htv)	320 000 (4 htv)	320 000 (4 htv)	320 000 (4 htv)
Henkilöstökulut (Puolustusministeriö)				
ohjaus ja seuranta (htv)	90 000 (1 htv)	90 000 (1 htv)	90 000 (1 htv)	90 000 (1 htv)
Muut vuotuiset kulut yhteensä				
Tietoliikennetiedustelu				
laite- ja konesalivuokrat, korvaukset yrityksille	-	1 200 000	1 200 000	1 200 000
hallinto- ja toimintamenot	350 000	700 000	700 000	700 000
ylläpitokustannukset	-	700 000	700 000	700 000
Muut toimivaltuudet				
laitteiden ja tietojärjestelmien ylläpito	-	800 000	800 000	800 000
hallinto- ja toimintamenot, mukaan lukien koulutus	450 000	900 000	900 000	900 000
Yhteensä	5 050 000	5 710 000	6 710 000	7 710 000

Edellä mainittuja lisäkustannusten lopulliseen toteutumisajankohtaan ja kohdentumiseen eri vuosille vaikuttaa säännösehdotusten voimaantuloajankohta.

Lisäkustannuksia ei voitaisi kattaa puolustusministeriön hallinnonalan nykyisten vuosittaisten määrärahojen sekä valtioneuvoston vuosille 2017 - 2020 antaman valtiontalouden kehyspäätöksen

puitteissa. Lisäresurssien toteuttamistapa tulee arvioida valtion talousarvion valmistelun yhteydessä.

4.1.2 Vaikutukset kansantalouteen ja yrityksille

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

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

Kansantalouden ja sen osana toimivien yritysten toimintaedellytysten kannalta on tärkeää, että Suomeen luotava säädösperusta tiedusteluviranomaisten toiminnalle on selkeä. Riittävän täsmällinen ja tasapainoinen lainsäädäntö luo yritysten toiminnan suunnittelun ja investointipäätösten kannalta ennakoitavuutta. Tiedustelua koskevan sääntelyn ja tietosuojan merkityksen korostuessa digitaalisilla markkinoilla täsmällisen, tasapuolisen ja oikeasuhtaisen sääntelyn voidaan arvioida parhaimmillaan olevan Suomelle kansainvälisillä markkinoilla myönteinen kilpailutekijä. Muun muassa tästä syystä lakiehdotukset on pyritty laatimaan näitä kriteerejä vastaaviksi.

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

Hallinnolliset vaikutukset yrityksille

Esityksellä arvioidaan olevan jonkin verran vaikutuksia yrityksiin. Vaikutukset kohdistuvat erityisesti teleyrityksiin ja Suomen rajan ylittävien viestintäverkkojen omistajiin.

Sotilastiedustelulle esitetyistä toimivaltuuksista yrityksille välittömiä ja välillisiä kustannuksia aiheuttavat uudet teletiedonhankintatoimivaltuudet ja tietoliikennetiedustelu. Uudet toimivaltuudet ja yrityksille säädettävät tiedonantovelvollisuudet lisäisivät yritysten hallinnollisia kustannuksia.

Esityksestä aiheutuisi yrityksille hallinnollisia kustannuksia. Tiedonhankintatoimivaltuuksien lisääntyessä yrityksille aiheutuvat viranomaispalvelukustannukset kasvaisivat elinkeinoelämän eri toimi-

aloille kohdistuvien viranomaiskyselyiden, tiedustelujen tai muiden velvoitteiden kautta. Yrityksille aiheutuneita kustannusten ei voida kuitenkaan katsoa kasvavan merkittävästi, koska Puolustusvoimille säädettävien uusien toimivaltuuksien voidaan arvioida vähentävän rikostorjuntaan perustuvien kyselyiden määrää sekä rikostorjunnassa poliisin antaman avun kautta tapahtuvia kyselyitä.

Uusista teletiedonhankinta keinoista teleyrityksille aiheutuvien hallinnollisten kustannusten ei voida katsoa kasvavan merkittävästi, sillä osa rikostorjuntaperusteisesti haetuista teletiedonhankintaluvista ohjautuisi tiedusteluperusteiseksi teletiedonhankinnaksi.

Teletiedonhankintakeinoista aiheutuneet kustannukset korvattaisiin teleyrityksille siten, kuin tietoyhteiskuntakaaren 299 §:ssä säädettäisiin, mikä on vallitseva asian tila jo nykyisin teletiedonhankintakeinojen osalta.

Suomen rajan ylittävien viestintäverkkojen omistajille hallinnollisia kustannuksia aiheutuisi tietoliikennetiedusteluun liittyvästä tietojenantovelvollisuudesta sekä Suomen rajan ylittävään viestintäverkon osaan tarjottavasta liityntäpisteestä.

Tietoliikennetiedustelun edellyttämä tietojen antovelvollisuuden perusteella tulevat kyselyt eivät kasvattaisi Suomen rajan ylittävien viestintäverkkojen omistajien hallinnollisia kustannuksia merkittävästi. Tietojenantovelvollisuus koskee tietoja, joita viestintäverkon omistajalla on jo hallussaan, eikä omistajan edellytetä tältä osin ryhtyvän uusiin toimenpiteisiin tietojen hankkimiseksi.

Tietoliikennetiedustelun teknisten ratkaisujen toteuttaminen vaatii teknisten laitteistojen asentamista Suomen rajan ylittäviin viestintäverkon osiin. Laitteistot edellyttävät tiloja viestintäverkon osan omistajan tiloista. Lisäksi laitteistojen asennustyöt sekä jatkuvaluonteinen ylläpitäminen ja kehittäminen vaativat viestintäverkon omistajan henkilöstön osallistumista, jotta viestintäverkon toiminnalle ja viestintäverkon omistajan tai haltijan liiketoiminnalle aiheutuisi mahdollisimman vähän haittaa. Näistä töistä aiheutuneet välittömät kustannukset korvattaisiin viestintäverkon osien omistajille ja hallitsijoille. Lisäksi kytkennän suorittajalle, Suomen Erillisverkot Oy:lle, toiminnasta aiheutuneet kustannukset korvattaisiin omakustannusperusteisesti.

Vaikutukset tutkimus- ja kehitystoimintaan sekä uuden yritystoiminnan syntyyn

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

Viranomaisten teknologiainvestoinnit saattavat luoda tietyille korkean teknologian yrityksille myönteisiä mahdollisuuksia turvallisuusviranomaisten tarvitsemien palvelujen ja teknologian kehittämiseen.

Vaikutukset kansainväliseen kilpailukykyyn

Elinkeinoelämä toimii globaalissa, kansainvälisen talouden ja arvoverkostojen toimintaympäristössä. Globaalissa kilpailussa pienetkin tekijät vaikuttavat valtioiden kilpailukykyyn. Yritykset sijoittavat toimintonsa maakohtaisesti optimoiden koko yritystoimintansa omien yrityskohtaisten kilpailuetujen perusteella. Sijoittautumispäätökset ovat kokonaisarviointeja yritysten liiketoiminnan kannalta, jois-

sa huomioidaan tekijöitä kuten esimerkiksi markkinatekijät, verotus, energian saatavuus, teknologinen osaaminen, suomalaisten korkea koulutustaso sekä luotettavuus ja rehellisyys, työvoimaan liittyvät velvoitteet, kehittynyt infrastruktuuri ja yhteiskunta, yhteiskunnallinen ja poliittinen vakaus, kulutuskäyttäytyminen ja ilmastotietoisuus, sääntely ja sen ennustettavuus, vakaus, tarkkarajaisuus, hallinnollinen taakka sekä mahdolliset oikeudelliset riskit. Lainsäädäntö on siis yksi päätöksentekoon vaikuttavista lukuisista seikoista.

Suomen elinkeinorakenne on muuttunut palvelukeskeiseksi ja talous innovaatiolähtöiseksi. Suomi on siirtynyt osaamis- ja teknologiaintensiivisille aloille, joiden klusterit houkuttelevat ulkomaisia suoria sijoituksia. Suomen erityiseksi vahvuusalaksi on noussut informaatio- ja viestintäteknologia. Tietointensiivisen teollisuuden taloudellinen merkitys onkin kasvussa. Esityksen vaikutukset yritystoiminnalle ovat erilaiset riippuen muun muassa yrityksen toimialasta, koosta ja sen harjoittamasta kansainvälisestä toiminnasta.

Täsmällinen, tasapuolinen ja oikeasuhteinen lainsäädäntö vahvistaa Suomen mainetta ennustettavana ja luotettavan toimintaympäristönä. Tämä koskee jo Suomessa olevia ja Suomeen mahdollisesti investoivia toimijoita.

Lainsäädäntötyössä on arvioitu sääntelyn vaikutuksia Suomen kansainväliseen kilpailukykyyn sekä Suomen houkuttelevuuteen investointikohteena. Olennaista ICT-alan yritysten kilpailukyvyn kannalta on, että sääntely ei velvoita yrityksiä heikentämään tuotteidensa tai palveluidensa luotettavuutta esimerkiksi salausavaimien luovuttamisen, takaporttien asentamisen, salaustuotteiden käyttöön liittyvien rajoitteiden tai muiden liiketoiminnalle haitallisten velvoitteiden seurauksena.

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

Esityksen esivalmistelussa (työryhmän mietintö Suomalaisen tiedustelulainsäädännön suuntaviivoja) selvitettiin tietoliikennetiedustelun mahdollisia kielteisiä vaikutuksia Suomeen kohdistuviin investointeihin. Vaikutuksia todettiin olevan vaikea arvioida, mutta tietoliikennetiedustelusta varsin yksityiskohtaisesti ja julkisesti säätänyttä Ruotsia käytettiin vertailukohteena. Selvityksessä ei havaittu sellaista poikkeamaa ulkomaisten investointien yleisessä kehityksessä, joka voitaisiin selittää Ruotsin tietoliikennetiedustelua koskevan lainsäädännön vaikutuksella. Selvityksen mukaan Ruotsin tietoliikennetiedustelua koskevan lainsäädännön voimaantulolla ei ole selkeää merkitystä Ruotsiin suuntautuneiden ulkomaisten investointien kehitykselle verrattuna Suomeen ja Tanskaan. Ruotsi onkin menestynyt esimerkiksi Data Center Risk Index -vertailussa Suomea paremmin. Lisäksi Suomi on edelleen saanut uusia datakeskusinvestointeja lainsäädäntötyön ollessa meneillään.

Nykyisin viranomaisten kyky kansallista turvallisuutta vakavasti vahingoittavien valtiollisten vakoiluohjelmien tai -operaatioiden havaitsemiseen on rajallinen. Tietoliikennetiedustelu kuitenkin täydentäisi merkittävällä tavalla Suomen suojautumista vakavimpia tietoverkkouhkia vastaan. Tietoliikennetiedustelusta olisi siten hyötyä myös elinkeinoelämän suojautumisessa kaikkein vakavimpia tietoverkkouhkia vastaan.

4.2 Vaikutukset viranomaisten toimintaan

Sotilastiedustelun avulla tunnistettavat uhat ovat kansainvälisiä, vakavia ja kohdistuvat valtion keskeisiin turvallisuusintresseihin. Sotilastiedustelun uusilla toimivaltuuksilla pystyttäisiin tuottamaan Suomen turvallisuuden kannalta merkityksellistä tietoa ulkomaisista toimijoista ja olosuhteista päätöksenteon tueksi. Esitetyt toimivaltuudet antaisivat ylimmälle valtionjohdolle sekä Puolustusvoimien johdolle paremman kyvyn reagoida Suomea vaarantaviin uhkiin.

Ehdotus vaikuttaisi Puolustusvoimien tehtäväkenttään. Uusien toimivaltuuksien myötä sotilastiedustelun tehtäväkenttä laajenee ja tiedonhankinta kasvaa. Ehdotuksen täytäntöönpano asettaa korkea laadulliset, koulutukselliset, oikeudelliset ja sotilastiedusteluviranomaisen rakenteen vaatimukset.

Ehdotus vaikuttaisi olennaisella tavalla viranomaisten välisiin suhteisiin. Ensinnäkin toimivaltuuksien mahdollistama tiedonlisä parantaisi sotilastiedusteluviranomaisen kykyä informoida ylintä valtiojohtoa Suomen turvallisuusympäristössä tapahtuvista muutoksista. Toiseksi se tiivistää sotilastiedusteluviranomaisen ja suojelupoliisin yhteistoimintaa erityisesti tietoliikennetiedustelussa ottaen huomioon, että sen tekninen toteutus on tarkoitus keskittää Puolustusvoimien tiedustelulaitokselle. Kolmanneksi ehdotus vaatisi muokkaamaan tiedustelun valvontajärjestelmän sisäisten ja ulkoisten toimijoiden keskinäissuhteet kokonaan uudella tavalla, sillä oikeusministeriössä valmisteltavana olevassa tiedustelutoiminnan valvontalaissa ehdotetaan muun muassa perustettavaksi tiedustelutoiminnan laillisuusvalvontaa varten uusi viranomainen.

Ehdotetun sääntelyn mukaiset toimivaltuudet loisivat Puolustusvoimille paremman kyvyn hoitaa sen lakisääteisiä tehtäviä sekä sille suunniteltuja uusia tehtäviä, jotka liittyvät kansainväliseen avunantoon.

Puolustusvoimien sisällä esityksellä olisi huomattavia vaikutuksia eritoten tiedustelutoimialan työmääriin. Ehdotuksen laajimmat viranomaisvaikutukset kohdistuisivat sotilastiedusteluviranomaisen tehtäviin ja menettelytapoihin. Uusista toimivaltuuksista säätäminen olisi merkittävä, sillä sotilastiedusteluviranomaisen tiedonhankinta ei liittyisi rikoksen käsitteeseen. Sen lisäksi sotilastiedusteluviranomaisen alueellinen toimivalta ulottuisi Suomen rajan ulkopuolelle. Tästä tehtävänmuutoksesta aiheutuvia toiminnallisia, koulutuksellisia, järjestelmä- ja menetelmäkehityksellisiä ja laillisuusvalvonnallisia vaikutuksia sotilastiedusteluviranomaisen työhön.

Ehdotus edellyttää uusien tehtävien mukaisen koulutusjärjestelmän kehittämistä. Sotilastiedustelussa käytettävät toimivaltuuksien käyttöperuste, käyttöön liittyvät taktiset näkökohdat, uudet toimivaltuudet ja tiedustelumenetelmien kohdentaminen eroavat rikostorjunnassa käytössä olevista tiedonhankintakeinoista, joten riittävän koulutus ja perehtyneisyys edellyttää panostuksia koulutukseen ja toimintatapojen kehittämiseen myös kansainvälisten yhteistyötahojen avustuksella.

Ehdotuksessa esitettävät sotilastiedustelun kohteisiin keskittyvä tiedonhankinta paljastanee vain harvoin vakavia, vähintään kuuden vuoden seuraamusuhkaa kantavia rikoksia eli rikoksia, joita koskisi ilmoituspakko esitutkintaviranomaiselle. Ehdotukseen sisältyvä säännös ilmoituksesta rikostorjuntaan vaikuttaneekin tehtäviä enemmän menettelytapoihin, kuten siihen, miten ja missä laajuudessa sotilastiedusteluviranomainen ilmoittaisi epäilystä tai vielä estettävissä olevasta rikoksesta esitutkintaviranomaiselle.

Ehdotuksessa syvennettäisiin edelleen sotilastiedusteluviranomaisen ja suojelupoliisin muutoinkin vakiintunutta yhteystyötä nimenomaisella säännöksellä. Tiivistyvä sotilas-siviilitiedusteluyhteistyö tarkoittaisi ennen kaikkea toimintatapojen yhtenäistämistä ja sen varmistamista, että tiedustelutoiminta ei kohdistu samoihin kohteisiin. Yhteistyö vaikuttaisi pidemmällä aikavälillä oletettavasti myös sotilastiedusteluviranomaisten ja suojelupoliisin operatiivisia menettelytapoja ja sen oikeudel-

lisia tulkintoja lähentävästi. Täyden luottamuksen olosuhteissa yhteistyö sotilastiedusteluviranomaisen ja suojelupoliisin välillä voisi ilmetä jopa kaluston ja osaamisen keskinäisenä jakamisena.

Hallituksen esityksen mukaisessa keskitetyssä ratkaisumallissa, jossa tietoliikennetiedustelun tekniseksi suorittajaksi nimettäisiin Puolustusvoimien tiedustelulaitos, kohdistuisivat resurssivaikutukset ensisijaisesti Puolustusvoimiin.

Ehdotuksen mukaan kaikki tiedustelumenetelmiä koskevat lupa-asiat käsiteltäisiin Helsingin käräjäoikeudessa. Helsingin käräjäoikeudessa työskentelee useita pakkokeinoasioihin keskittyviä käräjätuomareita, mikä mahdollistaa erikoistumisen tiedustelumenetelmiä koskeviin lupa-asioihin sekä tiedustelumenetelmien käytöstä ilmoittamista koskeviin kysymyksiin. Helsingin käräjäoikeudelle osoitettaisiin myös tiedustelumenetelmien käytöstä ilmoittamiseen liittyviä tehtäviä, kuten päättämistä ilmoituksen lykkäämisestä tai sen kokonaan tekemättä jättämisestä. Käräjäoikeuden työmäärä olisi näin ollen riippuvainen tiedustelumenetelmien käyttöä ja pääsääntöisestä kohteelle ilmoittamisesta poikkeusta merkitsevien vaatimusten määrästä. Kun pakkokeinotuomari pystyy ratkaisemaan keskimäärin 60 lupa-asiaa kuukaudessa, ehdotuksella ei todennäköisesti olisi kovinkaan suurta vaikutusta Helsingin käräjäoikeuden tehtävämäärään.

Helsingin hovioikeudelle ehdotettava tehtävä tiedustelumenetelmiä koskevien lupa-asioiden kantelutuomioistuimena ei vaikuttane sen työmäärää käytännössä juuri lainkaan. Ehdotus edellyttäisi kuitenkin erityisesti Helsingin käräjäoikeuden tuomareiden koulutusta ottaen huomioon tiedustelumenetelmiä koskevien vaatimusten täysin uudentyyppinen perusteleminen ja sotilastiedustelun kohteista johtuva korostunut tulkintataito.

Tiedustelutoimintaa koskevien asioiden käsittely edellyttää riittävän korkean turvallisuusluokan tiloja. Näiden tilojen saatavuus oikeuslaitoksessa on varmistettava. Asioita voitaisiin käsitellä myös puolustushallinnon tiloissa.

Tiedustelutoiminnan luonne ja toiminnan hyväksyttävyys edellyttävät korostunutta oikeudellista valvontaa. Ulkoisen laillisuusvalvonnan riippumattomuuden ja läpinäkyvyyden turvaamiseksi tällaisesta valvonnasta ei ole tarkoituksen mukaista säätää tiedustelutoimintaa koskevassa laissa. Tämän takia oikeusministeriön hallinnonalalle perustettaisiin uusi tiedustelutoiminnan valvontaan keskittyvä viranomainen. Myös tiedustelutoiminnan parlamentaarisen valvonnan voidaan katsoa kuulua valvonnan kokonaisuuteen.

Esityksellä ei rajoitettaisi ylimpien laillisuusvalvojien toimintaan ja esityksen arvioidaan lisäävän ylimpien laillisuusvalvojien työmäärään. Tähän olisi kuitenkin vaikutuksia oikeusministeriön valmistelemalla tiedustelutoiminnan valvontaa koskevalla lailla.

Ehdotukseen sisältyvä säännös tiedustelumenetelmien käytön valvonnasta ja delegointisäännös valtioneuvoston asetuksella annettavista tarkemmista säännöksistä lisäisi niin sotilastiedusteluviranomaisen kuin puolustusministeriön raportointi- ja selvitysvelvoitteita siihen nähden mitä salaisen tiedonhankinnan käyttöä koskevista raportointi- ja selvitysvelvoitteista jo nykyisin johtuu. Koska Puolustusvoimien tehtävä estää ja paljastaa maanpuolustuksen alalla Suomeen kohdistuvaa tiedustelutoimintaa ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyviä rikoksia, raportointi- ja selvitysvelvoitteet kattaisivat lain voimaantulon jälkeen paitsi salaisten tiedonhankintakeinojen ja niiden suojaamisen käytön ja valvonnan myös samat tarkastuskohteet tiedustelumenetelmiä koskien. Ehdotuksen seurannaisvaikutuksena lisääntyisi myös puolustusministeriön tilastoraportointi koskien viranomaistarpeita varten säilytettäviä tietoja.

Puolustusvoimien sisäisessä laillisuusvalvonnassa pyritään hyödyntämään jo olemassa olevaa laillisuusvalvontamekanismia, jossa laillisuusvalvontaa suorittaa Puolustusvoimien asessorin alainen Pääesikunnan oikeudellisen osasto. Puolustusvoimien sisäiseen laillisuusvalvontaan tulee

kuitenkin kytkeä myös teknistä valvontaa suorittava komponentti, sillä teknistä tietotaitoa vaativaan laillisuusvalvontaan Puolustusvoimien oikeudellisella toimialalla tällä hetkellä ei ole vaadittavia resursseja tai osaamista.

Puolustusministeriön laillisuusvalvontatehtävien voidaan arvioida lisääntyvän hieman uuteen toimintaa liittyvien ohjaus- ja valvontatehtävien takia. Puolustusministeriön valvonta kohdistuisi ennen kaikkea puolustusvoimien sisäisen laillisuusvalvonnan valvontaan ja järjestämiseen.

Sotilastiedustelutoiminnan ohjaus sekä yhteistoiminta ylimmän valtiojohdon, valtioneuvoston sekä operatiivisten toimijoiden välillä vaikuttaa puolustusministeriön työmäärää lisäävästi.

Ehdotetulla sääntelyllä selkeytettäisiin tiedustelua harjoittavien turvallisuusviranomaisten toimivallan jakoa. Myös vakiintuneelle yhteistyölle luotaisiin entistä selkeämpi säädöspohja.

Ehdotettavat uudet säännökset huomioon ottaen on selvää, että sotilastiedustelulainsäädäntöä soveltavat virkamiehet niin sotilastiedustelussa kuin laillisuusvalvonnassa tulevat tarvitsemaan laajamittaista koulutusta uuden lainsäädännön käyttöön ottamisen yhteydessä.

Telekuuntelu, televalvonta ja tukiasematietojen hankkiminen kasvattavat hieman keskusrikospoliisin suorittamien tehtävien määrää, sillä sotilastiedustelun tarvitsema toimivaltuuksien käyttö toteutettaisiin tällä hetkellä käytössä olevia järjestelyjä hyödyntäen. Toisaalta salaisten tiedonhankintakeinojen käytön voidaan katsoa hieman vähentyvän Puolustusvoimissa, mikä vähentää myös suojelupoliisin Puolustusvoimille suorittamaa tiedonhankintaa.

Ehdotetut tiedustelun toimivaltuuden ja kansainvälisen yhteistyön voidaan katsoa lisäävän Puolustusvoimien kansainvälistä yhteistyötä, mikä edellyttää resurssien kohdentamista tähän.

Sotilastiedustelusta säätäminen parantaisi osaltaan tiedustelutoimintaan osallistuvien oikeusturvaa. Lisäksi selkeä ja läpinäkyvä sääntely lisää oikeusvarmuutta ja parantaa yhteiskunnallista luottamusta sitä kautta, että eri toimijat pystyvät paremmin arvioimaan sotilastiedustelutoiminnan yhteiskunnallista vaikuttavuutta.

4.3 Yhteiskunnalliset vaikutukset

4.3.1 Kansalaisten asema yhteiskunnassa ja kansalaisyhteiskunnan toiminta

Ehdotuksella ei olisi merkittäviä vaikutuksia kansalaisten asemaan yhteiskunnassa ja kansalaisyhteiskunnan toimintaa, kansalaisten arvoihin ja asenteisiin, perusoikeuksien ja oikeusturvan toteutumiseen, kansalaisten keskinäiseen toimintaa ja oikeussuhteisiin sekä kansalaisyhteiskunnan toimintaan.

Ehdotuksella ei arvioida olevan merkittäviä vaikutuksia kansalaisryhmin asemaan ja käyttäytymiseen. Epävarmuutta tiedustelun asianmukaisesta kohdentumisesta voitaisiin ehkäistä säätämällä sotilastiedustelutoiminnan periaatteista ja sillä, että tiedustelutoimintaan kohdistuu riippumaton oikeudellinen ja parlamentaarinen valvonta.

Sotilastiedusteluviranomaisen toimivaltuudet antavat mahdollisuuden puuttua luottamuksellisen viestin suojaan sekä yksityiselämään. Uusi toiminta saattaa aluksi joissain yksittäisissä tapauksissa kaventaa henkilön omaa halua käyttää sananvapauttaan ja aiheuttaa itsesensuuria henkilön viestinnässä. Vaikutuksia voidaan kuitenkin arvioida erittäin vähäisiksi. Toisaalta riippumaton ja tehokas sotilastiedustelutoiminnan oikeudellisen ja parlamentaarisen valvonnan voidaan katsoa ehkäisevän tällaisia vaikutuksia.

Kansainvälinen yhteistyö voi vaikuttaa yhteiskunnallisesti lisäämällä kiinnostusta sotilastiedustelun toimintaa kohtaan.

Reserviläisten käyttäminen tietyissä tilanteissa sotilastiedustelutoimintaan lisää asevelvollisten mahdollisuuksia osallistua Puolustusvoimien toimintaan. Puolustusvoimat voivat hyödyntää asevelvollisten erityisosaamista entistä laajemmin ja tämän voidaan katsoa osaltaan parantavan maanpuolustustahtoa. Puolustusvoimat voivat kehittää asevelvollisuutta suuntaan, jossa asevelvollisille voitaisiin tarjota heidän erityisosaamistaan kehittävää koulutusta. Puolustusvoimien omaa tarvetta ajatellen esitettävällä lainsäädännöllä Puolustusvoimiin avautuu tehtäviä, joissa tarvitaan nykyisestä Puolustusvoimien toiminnasta poikkeavaa osaamista ja ominaisuuksia.

4.3.2 Vaikutukset rikostorjuntaan ja turvallisuuteen

Ehdotus lisäisi sotilastiedusteluviranomaisen itse hankkiman ja kumppaneilta saaman tiedon määrää. Siltä osin kuin tästä tiedosta voidaan erottaa maanpuolustuksen alalla tiedusteluun liittyviä rikoksia tai maanpuolustuksen vaarantavaa toimintaa, Puolustusvoimat vastaisi nykyiseen tapaan niiden estämisestä ja paljastamisesta. Muiden rikoslajien osalta sotilastiedusteluviranomaisen olisi viipymättä ilmoitettava esitutkintaviranomaiselle, jos tiedustelumenetelmän käytön aikana ilmenee rikoslain 15 luvun 10 §:ssä tarkoitettu vielä estettävissä oleva rikos. Sotilastiedusteluviranomainen saisi lisäksi luovuttaa esitutkintaviranomaiselle tietoa sellaisen rikoksen estämiseksi, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta.

Tiedustelumenetelmien säätämisellä luotaisiin edellytykset hankkia tietoa toiminnasta, joka muodostaa uhkan Suomen maanpuolustukselle taikka vakavasti uhkaa kansallista turvallisuutta. Kyse olisi ennen muuta tiedonhankinnasta maan ylimmälle johdolle ja ylimmälle sotilasjohdolle tilannekuvan muodostamiseksi sekä Suomen turvallisuusympäristön kehittymisestä. Ehdotuksilla ei olisi merkittävissä määrin yleistä rikoksia estävää vaikutusta, joskin yksittäistapauksissa saatettaisiin pystyä estämään tilanteen kehittyminen vakavan rikoksen tekemiseen. Toisaalta tiedustelumenetelmien säätäminen saattaa osaltaan nostaa kynnystä rikolliseen toimintaan ryhtymiseen.

Yksittäistapauksissa saatettaisiin pystyä estämään tilanteen kehittyminen vakavan rikoksen valmistelusta sen täytäntöön panemiseen. Ehdotuksen rikostorjunnallinen vaikutus kanavoituisi kuitenkin rikosten selvittämismahdollisuuksia voimakkaammin esitutkintaviranomaisten kykyyn estää niille ilmoitettuja rikoksia.

Lisäksi sotilastiedusteluviranomaisen hankkimaan tietoa voidaan ilmoittaa Puolustusvoimien toiminnan suuntaamiseksi, mikä vaikuttaisi suotuisasti Puolustusvoimien mahdollisuuteen reagoida esiin nouseviin turvallisuusuhkiin sekä uuden tyyppisiin vaikuttamismahdollisuuksiin.

Esitys mahdollistaa yhteiskuntaan kohdistuvien uhkien tunnistamisen ja tunnistamisen jälkeen uhkien torjunnan, kriittisen infrastruktuurin ja yhteiskunnan taloudellisen elinkelpoisuuden säilyttämisen edellyttämän yhteistyön julkisen ja yksityisen sektorin välillä. Tietoa hyödynnettäisiin esimerkiksi kansallisen yhteisen uhkatilannekuvan ylläpitämiseksi. Esityksen mukaan tiedustelutietoa voitaisiin tarvittaessa luovuttaa yksityisille yhteisöille vakavien uhkien torjunnan aloittamiseksi tai merkittävien taloudellisten tappioiden estämiseksi.

Sotilastiedustelukyvyn voidaan arvioida nostavan vieraiden valtioiden kynnystä kohdistaa Suomeen vakoilua tai tietoverkkojen kautta muuta haitallista toimintaa. Ehdotuksella voidaan siten olettaa olevan suotuisia vaikutuksia Suomen digitaalisen ympäristön turvallisuuteen, erityisesti tietoturvallisuuteen ja tietojärjestelmäturvallisuuteen.

4.3.3 Tietoyhteiskuntavaikutukset

Sotilastiedustelulainsäädännöllä on nähtävissä sekä suoria että välillisiä tietoyhteiskuntavaikutuksia, jotka aiheutuvat ennen muuta ehdotetusta uudesta tietoliikennetiedustelutoimivaltuudesta. Sotilastiedustelulakiin ehdotettavista muista toimivaltuuksista aiheutuva vaikutus on vähäisempi, sillä digitaaliselta luonteeltaan ne ovat samoja tiedonhankintakeinoja, joista säädetään poliisilain 5 luvussa salaisina tiedonhankintakeinoina (telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, tekninen kuuntelu).

Tietoyhteiskuntavaikutusten suuruuteen voidaan olennaisesti vaikuttaa lainsäädäntöteknisillä ratkaisuilla. Siksi lainsäädännön ratkaisumalleja valittaessa on alusta alkaen arvioitu sääntelystä aiheutuvia vaikutuksia sekä huomioitu lainsäädäntöhankkeen johdosta aiheutunut julkinen keskustelu.

Tieto- ja viestintäteknologia yritysten kilpailukykykyyn aiheutuvat vaikutukset sivuavat tietoyhteiskuntavaikutuksia. Niistä on tässä luvussa käsitelty vain suorat vaikutukset.

Vaikutukset tietoyhteiskunnan palveluiden käyttäjiin

Tietoliikennetiedustelulla tarkoitettaisiin Suomen rajan ylittävän viestintäverkkoon kohdistuvaa, tietoliikenteen automatisoituun erotteluun perustuvaa teknistä tiedonhankintaa. Tietoliikennetiedustelulla arvioidaan olevan vaikutuksia tiedustelukysymyksen kannalta sivullisten henkilöiden luottamuksellisen viestinnän suojaan. Puuttumisen intensiteettiä on lainsäädäntöteknisillä valinnoilla rajattu niin, ettei kenenkään oikeuksiin puututa enempää kuin on välttämätöntä tietoliikennetiedustelun suorittamiseksi.

Ensinnäkin tietoliikennetiedustelu on toteutettava liikenteen solmukohdassa. Teknisesti tarkasteltuna perinteinen telekuuntelu kohdistuu aina yksittäiseen teleosoitteeseen (tai rajalliseen teleosoitteiden joukkoon), jolloin telekuuntelu voidaan toteuttaa verkkoteknisesti lähellä tiedonhankinnan kohteena olevaa osoitetta. Tällöin tiedonhankinnassa käytettävä seula voidaan usein asettaa verkossa sellaiseen pisteeseen, jonka kautta kulkee vain vähän tiedonhankintalupaan kuulumatonta liikennettä. Tehokkaan tietoliikennetiedustelun edellytyksenä puolestaan on, että tietoliikennetiedustelujärjestelmä näkee mahdollisimman suuren osan tiedustelukysymyksen kannalta olennaisesta tietoliikenteestä. Tätä voidaan havainnollistaa reaalimaailman vertauksella: Jos viranomainen saa vihjetiedon, että yksittäisellä huolintaliikkeellä on vaarallisen huonokuntoisia rekka-autoja, viranomaisen tiedonhankinta on mahdollista kohdistaa vain yksittäisen huolintaliikkeen varikkoon. Jos kuitenkin viranomainen haluaisi tunnistaa mahdollisimman tehokkaasti liikenteestä vaarallisen huonokuntoisia rekka-autoja, liikennevirran havainnointi on keskitettävä liikenteen solmukohtiin.

Koska tietoliikennetiedustelu tapahtuu pisteessä, jonka kautta kulkee suuri osa verkon liikenteestä, tietoliikennetiedustelun kohdentaminen tapahtuu ennalta määriteltyjen tarkkojen kriteerien mukaisesti.

Toiseksi on huomioitava, että verkko toimii irrallaan ajasta ja paikasta. Vaikka tietoliikennetiedustelua käytetään ainoastaan valtakunnan rajat ylittävään tietoliikenteeseen, hakuehtovertailun piiriin voi Internetin toimintatavan vuoksi päätyä myös maan sisäistä tietoliikennettä. Esimerkiksi ruuhka- tai vikatilanteessa yhteys kahden kotimaisen teleyrityksen välillä saattaisi reitittyä ulkomailla sijaitsevan reitittimen kautta. Ylipäätään tietoliikenteen osapuolten sijaintipaikka ei Internet-verkossa ole aina teknisesti suoraan pääteltävissä. On mahdollista, että vasta tiedusteluanalyytikon toteuttaman manuaalisen käsittelyn yhteydessä selviää jatkokäsittelyyn seuloutuneen tietoliikenteen kotimainen luonne. Siksi ehdotukseen on otettu erityinen tiedustelukielto, jonka mukaan tietoliikennetiedustelua ei saisi kohdistaa viestiin, jonka lähettäjä ja vastaanottaja ovat Suomessa.

Vaikutukset tietoturvallisuuteen sekä kriittisen tietoinfrastuktuurin suojaan

Tietoliikennetiedustelulla arvioitaisiin olevan positiivinen vaikutus tietoturvallisuuteen sekä kriittisen infrastruktuurin suojaan.

Tiedon turvaaminen ja tietoturvapoikkeamien havainnointi on yleisesti tehokkainta toteuttaa mahdollisimman lähellä suojattavaa tietoa. Aiemmin suoja toteutettiinkin tiedon omistavassa organisaatiossa. Tiedon merkitys tietoyhteiskunnan keskeisimpänä tuotantotekijänä on kuitenkin kasvanut. Samaan aikaan digitaalipalveluiden pitkien ulkoistusketjujen myötä organisaatioiden edellytykset hallita omaan tietopääomaansa kohdistuvia riskejä ovat jossain määrin heikentyneet. Tiedon eheys, luottamuksellisuus sekä saatavuus ovat nykyään niin olennaisia suojattavia intressejä, että koko yhteiskunnan on osallistuttava niiden suojaamiseen. Tiedon omistavien organisaatioiden, ICT-palveluntarjoajien sekä tietoturvapalveluita tuottavien yritysten tietoturvatoiminnan lisäksi tarvitaan tehokkaasti toimivia viranomaisia.

Tietoliikennetiedustelu parantaa toimivaltaisten viranomaisten edellytyksiä havaita sekä kriittiseen infrastruktuuriin kohdistuvaa kyberkartoitusta että valtiollista kybertiedustelua, joka kohdistuu korkean teknologian tutkimus- sekä tuotekehitystietoon. Sekä Suomen kriittinen tietoinfrastruktuuri että korkean teknologian tuotekehitystieto ovat suurelta osin yksityisten yritysten hallussa. Siksi tietoliikennetiedustelulakiin on luotu edellytykset luovuttaa tietoturvauhkia koskevaa tietoa sekä viestintävirastolle että vieraan valtion tiedonhankinnan kohteena oleville yrityksille vahinkojen estämistä varten. Tietoturvallisuuden ylläpito edellyttää monen toimijan yhteistyötä, johon tietoliikennetiedustelu toisi yhden komponentin lisää.

Vaikutukset tietoyhteiskuntapalveluiden tarjoajiin

Sotilastiedustelulain 4 lukuun esitetyillä tiedonhankintatoimivaltuuksista telekuuntelulla, tietojen hankkimisella telekuuntelun sijasta ja televalvonnalla olisi vaikutuksia tietoyhteiskunnan palveluntarjoajista ainakin teleyrityksiin, joilla on velvoite avustaa viranomaista teletiedustelumenetelmissä kytkentöjen toteuttamiseksi. Sotilastiedusteluviranomaiselle esitettävät toimivaltuudet laajentaisivat näiden tiedustelumenetelmien käyttöön oikeutettujen määrää. Vaikutusta voidaan kuitenkin pitää nykytilaan vertailtuna neutraalina tai jossain määrin yrityksiin kohdistuvia velvoitteita vähentävänä. Telekuuntelun ja televalvonnan käytön peruste muuttuisi rikosperusteisesta tietyn toiminnan ja uhkien havaitsemiseen ja lupa voitaisiin myöntää korkeintaan kuudeksi kuukaudeksi kerrallaan. Nykyistä pidempikestoisiksi esitettävät tiedonhankintaluvat vähentäisivät pitkäkestoisissa tiedonhankintaoperaatioissa teleyrityksille aiheutuvaa henkilöresurssikuormitusta. Lisäksi Puolustusvoimien suorittamassa rikostorjunnassa suojelupoliisilta pyydetty tiedonhankinta tässä luvussa tarkoitetuilla tiedonhankintakeinoilla arvioidaan vähentyvän.

Uuden tietoliikennetiedustelun vaikutus tietoyhteiskuntapalveluiden tarjoajiin on suurempi, sillä vastaavaa sääntelyä ei tällä hetkellä ole. Tietoliikennetiedustelulla asetettaisiin yritykselle uusia velvoitteita, joista aiheutuvat välittömät kustannukset mukaan lukien henkilökustannukset korvattaisiin.

Sääntelyssä ei ehdoteta yrityksille velvoitteita heikentää ohjelmistotuotteidensa tai tietoyhteiskunnan palveluidensa asiakaslupausta esimerkiksi salausavaimien luovuttamisen, takaporttien asentamisen, salaustuotteiden käyttöön liittyvien rajoitteiden muodossa.

5 Asian valmistelu

5.1 Valmisteluvaiheet ja -aineisto

Ehdotus hallituksen esitykseksi on valmisteltu puolustusministeriön 1.10.2015 asettamassa työryhmässä. Työryhmän tehtävänä on ollut valmistella ehdotus sotilastiedustelua koskevaksi lainsäädännöksi eli säännökset muun muassa Puolustusvoimien tiedustelun tarkoituksesta, toimivaltaisista viranomaisista sekä niidentehtävistä ja toimivaltuuksista, ohjauksesta ja valvonnasta, tietojen käsittelystä ja rekisteröinnistä sekä viranomaisten yhteistyöstä. Hankkeen keskeisin tavoite on ollut kansallisen turvallisuuden parantaminen.

Työryhmässä on ollut edustus puolustusministeriön lisäksi tasavallan presidentin kansliasta, valtioneuvoston kansliasta, ulkoasiainministeriöstä, oikeusministeriöstä, sisäministeriöstä sekä pääesikunnasta.

Työryhmään on kutsuttu pysyvät asiantuntijat Elinkeinoelämän keskusliitto EK:sta, Helsingin yliopistosta, ulkoasiainministeriöstä, liikenne- ja viestintäministeriöstä, suojelupoliisista ja Puolustusvoimista.

Sotilastiedustelua ja samanaikaisesti sisäministeriössä valmisteltavana olevat siviilitiedustelua koskevat säännösehdotukset ovat keskenään yhteen sovitettuja.

Esityksessä on otettu huomioon tiedonhankintalakityöryhmän mietintö ja siitä saatu lausuntopalaute.

Tiedonhankintalakityöryhmä

Puolustusministeriö asetti 13.12.2013 työryhmän kehittämään lainsäädäntöä turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista. Työryhmässä oli puolustusministeriön lisäksi edustus tasavallan presidentin kansliasta, ulkoasiainministeriöstä, oikeusministeriöstä, sisäministeriöstä, valtiovarainministeriöstä, liikenne- ja viestintäministeriöstä, työ- ja elinkeinoministeriöstä, Poliisihallituksesta ja pääesikunnasta. Lisäksi työryhmään kutsuttiin pysyviä asiantuntijoita.

Työryhmän tehtävänä oli kehittää lainsäädäntöä turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista ja arvioida Suomen lainsäädännön kehittämistarvetta siten, että Suomessa kyetään huolehtimaan kansallisesta turvallisuudesta tietoverkoissa esiintyvien uhkien torjumiseksi. Työryhmän tehtävänä oli lisäksi koota yhteen näkemyksiä tietoverkkojen kautta Suomen turvallisuuteen kohdistuvista uhkista ja niiden vaikutuksista Suomen turvallisuudelle ja kilpailukyvylle, selvittää turvallisuusviranomaisten tiedonhankintaa koskeva nykytila ja kehittämisehdotukset, tarkastella tarvittavilta osin turvallisuusviranomaisten tiedonhankintaa koskevaa lainsäädäntöä eräissä muissa maissa, tuottaa vaikutusarviointi eri kehittämisvaihtoehdoista ja selvitetyn pohjalta tehdä lainsäädännön kehittämisehdotukset sekä esitys niiden toimeenpanon edellyttämistä toimista.

Arvioitaessa tiedonhankintaan tietoverkoissa liittyviä mahdollisia sääntelytarpeita kävi ilmi, että lainsäädännön kehittämistä olisi tarkasteltava laajemmin turvallisuusviranomaisten tiedustelutehtävää varten. Turvallisuusviranomaisten tiedonhankintakyvyn parantamisessa ei olisi ensisijaisesti kyse tietoturvan parantamisesta vaan viranomaisten paremmista mahdollisuuksista estää vakavia kansallista turvallisuutta uhkaavia tekoja.

Työryhmä luovutti mietintönsä puolustusministeriölle 14.1.2015 (Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö). Mietintöön liitettiin yksi eriävä mielipide sekä kaksi lausumaa.

Mietinnössä arvioitiin tiedustelua koskevan lainsäädännön kehittämistarpeita. Työryhmä ehdotti harkittavaksi, että hallitus käynnistäisi tarvittavat toimenpiteet tiedustelua koskevan säädösperustan luomiseksi. Kansallisesta turvallisuudesta vastaaville sotilas- ja siviiliviranomaisille tulisi harkita toimivaltuuksia rajat ylittävään tietoliikenteeseen kohdistettavaan tiedusteluun, jotta turvallisuusympäristön muutoksiin voitaisiin vastata. Tietoliikennetiedustelun tekninen suorittaminen olisi tarkoituksenmukaista keskittää yhdelle viranomaiselle.

Puolustusvoimille ja suojelupoliisille tulisi harkita toimivaltuuksia ulkomaan tiedusteluun, jossa hankittaisiin tietoja henkilöiltä ja tietojärjestelmistä. Koska ulkomaan tiedusteluun liittyy ulkopoliittisesti sensitiivisiä elementtejä, sitä koskevassa päätöksenteossa olisi otettava huomioon valtion ylimmän johdon linjaukset. Ohjaus- ja vastuusuhteet tulisi arvioida mahdollisen jatkovalmistelun yhteydessä.

Tietoliikennetiedusteluun tulisi liittää riippumaton lupamenettely. Tietoliikennetiedustelua ja ulkomaan tiedustelua varten tulisi luoda riippumaton valvontajärjestelmä.

Tietoliikennetiedustelua koskevan lainsäädännön valmistelua harkittaessa olisi erityisesti otettava huomioon jokaiselle perus- ja ihmisoikeutena turvattu luottamuksellisen viestin salaisuuden suoja. Tiedustelutarkoituksessa toteutettavasta tietoliikennetiedustelusta ei näyttäisi olevan mahdollista säätää perustuslakia muuttamatta, pelkästään vieraan valtion tietoliikenteeseen kohdistuvaa tiedustelua ehkä lukuun ottamatta.

Työryhmän mietinnöstä pyydettiin lausuntoa 150 eri taholta (ministeriöltä, viranomaiselta, puolueelta, järjestöltä, yritykseltä ja yhteisöltä). Lausuntopyyntö oli myös julkisesti saatavilla puolustusministeriön internet-sivuilla. Lisäksi lausunto pyydettiin erikseen oikeustieteen asiantuntijoilta. Lausunnon antoivat 74 tahoa. Lausunnoista on laadittu lausuntotiivistelmä, joka on julkaistu puolustusministeriön internet-sivuilla. Lausunnoissa yhdyttiin laajasti mietinnön lähtökohtana esitettyyn arvioon toimintaympäristön muutoksesta digitalisoituvassa tietoverkkojen yhteiskunnassa. Lainsäädännön nykytilan aukollisuus katsottiin ongelmalliseksi ja säädöspohjan luomista pidettiin perusteltuna. Mietinnössä esitetyt kehittämisehdotukset ja johtopäätökset jakoivat kuitenkin mielipiteitä. Ongelmallisena pidettiin viranomaisten tiedonsaantitarpeen ja yksityisyyden suojan välisen jännitteen yhteensovittamista.

5.2 Lausunnot ja niiden huomioon ottaminen

6 Ahvenanmaan asema

Perustuslain 120 §:n mukaan Ahvenanmaan maakunnalla on itsehallinto sen mukaan kuin Ahvenanmaan itsehallintolaissa erikseen säädetään. Ahvenanmaan itsehallintolaissa (1144/1991) säädetään muun muassa Ahvenanmaan kotiseutuoikeudesta, lainsäädäntövallan jakautumisesta valtakunnan ja maakunnan kesken, lainsäädäntövallan valvonnasta, hallinnosta, lainkäytöstä, kieli- ja kulttuuriasioista ja maakunnan taloudenhoidosta.

Ahvenanmaan maakuntapäivät (lagtinget) on eduskuntaa vastaava ylin itsehallintoelin. Maakunnan hallintoa hoitavat maakuntahallitus (Ålands landskapsregering) ja sen alaiset viranomaiset. Ahvenanmaan maakunnan lääninhallitus ja valtion keskushallinnon viranomaiset huolehtivat valtakunnan yleiseen hallintoon kuuluvien tehtävien hoitamisesta maakunnassa. Ahvenanmaan valtuuskun-

ta (Ålandsdelegationen) on maakunnan ja valtakunnan yhteinen elin, joka hoitaa laissa erikseen mainittuja tehtäviä, joihin kuuluu muun muassa itsehallintoon kuuluvien asioiden asiantuntijatehtävät, lausuntojen antaminen valtioneuvostolle ja ministeriöille.

Ahvenanmaan itsehallintoa koskeva lainsäädäntövalta kuuluu maakunnalle. Itsehallintolain 27 §:ssä luetellaan asiat, joita koskevan yleisen lain säätäminen on jätetty valtakunnan toimielinten asiaksi. Itsehallintolain 18 §:ssä luetellaan asiat, joita koskeva säädäntövalta kuuluu maakuntapäiville. Lainkäyttö Ahvenanmaan maakunnassa kuuluu yleensä asianomaisille valtion toimielimille. Tuomiovaltaa käyttävät siten valtakunnan tuomioistuimet tai muut valtakunnalliset viranomaiset, joille on uskottu tuomitsemisvaltaa. Sama koskee myös hallinto-oikeudellista lainkäyttöä.

Ahvenanmaa on ollut demilitarisoitu Krimin sodan päättymisestä vuonna 1856 lähtien. Tämän jälkeen siellä on oleskellut sotajoukkoja ainoastaan maailmansotien aikana. Ahvenanmaan demilitarisaatiosta on sovittu Suomen, Saksan, Tanskan, Ruotsin, Britannian, Ranskan, Italian, Latvian ja Puolan kesken vuoden 1922 sopimuksella Ahvenanmaan saarten linnoittamattomuudesta (SopS 1/1922). Lisäksi Ahvenanmaan saarten demilitarisaatiosta on erikseen sovittu vuonna 1940 Suomen ja Neuvostoliiton välillä (SopS 24/1940). Molemmat sopimukset kieltävät Suomea rakentamasta alueelle mitään kiinteitä puolustuslaitteita, sotilaslentokenttiä tai muita sotilaallisiin tarkoituksiin suunniteltuja laitteita. Sotatilanteessa Suomella on vuoden 1922 sopimuksen mukaan oikeus miinoittaa Ahvenanmaan vesiä ja sijoittaa alueelle sen puolueettomuutta uhkaavan hyökkäyksen torjumiseksi tarpeellisia joukkoja. Sopimuksen perusperiaatteena on kuitenkin, että allekirjoittajavallat jättäisivät sotatilanteessakin Ahvenanmaan sotatoimien ulkopuolelle.

Edellä mainitut Ahvenanmaan sopimukset määrittävät muun muassa Suomen Puolustusvoimien oikeudet ja velvollisuudet Ahvenanmaan alueella. Ahvenanmaan saarten linnoittamattomuutta ja neutralisoimista koskevan sopimuksen (1922) 4§:ssä on määritetty oikeudet alusten käyntien osalta. Suomella on 7§:n mukaan velvollisuus valvoa Ahvenanmaan vyöhykettä ja valmistautua sen puolustamiseen. Ahvenanmaan vyöhykkeellä tarkoitetaan vuoden 1922 (Ahvenanmaansaarten linnoittamattomuutta ja puolueettomuutta koskeva sopimus) ja vuoden 1940 (sopimus Suomen ja Sosialistisen Neuvostotasavaltain Liiton välillä Ahvenanmaan saarista) sopimusten määrittämää aluetta.

Merivoimat voi aika ajoin käydä tarkastamassa saaria korkeintaan kahdella sota-aluksella (sopimuksen 4.2b art). Käytännössä näistä tarkastuksista ja vierailusta on etukäteen ilmoitettu Ahvenanmaan maakuntahallitukselle. Nämä käynnit suunnitellaan etukäteen. Ahvenanmaan maakunnan alueella saa olla kerrallaan korkeintaan kaksi merivoimien alusta. Yksittäinen tarkastuskäynti saa kestää enintään 48 tuntia. Aikarajoitus ei koske aluerikkomuksen torjunta- tai virka-aputehtävää. Merivoimien komentaja vahvistaa vuosittaisen merivoimien tarkastuskäyntisuunnitelman ja myöntää luvat suomalaisten sota-alusten käynneille ja kauttakulkuun Ahvenanmaan vyöhykkeelle. Ennalta laaditusta tarkastussuunnitelmasta poikkeavat tilanteenmukaiset käynnit käsitellään erikseen.

Merivoimien alukset tekevät vuoden aikana pääsääntöisesti 1-2 tarkastuskäyntiä Ahvenanmaan vyöhykkeelle Ahvenanmaan aluevesien sisäpuolelle. Tarkastuskäynnit kattavat myös Ahvenanmaan saariston. Kiireellisessä alueloukkauksen torjuntatehtävässä päätöksen Ahvenanmaan aluevesille menosta tekee aluksen päällikkö. Mikäli kyseessä on pelastustehtävä tai Ahvenanmaan itsehallintoviranomaisen esittämä avunpyyntö kiireelliseen tehtävään, aluevesille menon käskee asianomainen johtoporras, joka vastaa tiedon saattamisesta viipymättä Merivoimien päivystävälle esiupseerilla, joka vastaa tapauksen ilmoittamisesta Ahvenanmaan Maaherralle.

Merivoimien joukko-osastot sisällyttävät toimintasuunnitelmiinsa Ahvenanmaalle suunnittelemansa tarkastuskäynnit. Maarianhaminassa käyntiin tulee olla selkeät perusteet, jotka tuodaan esiin suunnitelmassa. Harjoituksiin liittyviä käyntejä koskevat tarkennetut suunnitelmat ja lupa-

anomukset on esitettävä Merivoimien komentajalle harjoitussuunnitelmien ja käskyjen esittelyjen tai hyväksymisen yhteydessä. Merivoimien Esikunta laatii vuosittain tilaston merivoimien alusten käynneistä Ahvenanmaan alueella.

Asevelvollisuuslain (1438/2007) 3 §:n 3 momentin mukaan asevelvollisuuden suorittamisen sijasta suoritettavasta palveluksesta säädetään Ahvenanmaan itsehallintolain 12 §:ssä. Asevelvollinen, jolla on Ahvenanmaan kotiseutuoikeus, saa asevelvollisuuden suorittamisen sijasta palvella vastaavalla tavalla luotsi- ja majakkalaitoksessa tai muussa siviilihallinnossa. Kunnes tällainen palvelu on järjestetty, ovat edellä tarkoitetut maakunnan asukkaat vapautettuja asevelvollisuuden suorittamisesta. Vapautus ei koske sitä, joka on 12 vuotta täytettyään muuttanut maakuntaan. Asevelvollisen muuttaessa vakituisesti Ahvenanmaan maakunnasta muualle Suomeen, aluetoimisto saa vakituisen osoitteen muutoksesta tiedon väestötietojärjestelmän kautta. Aluetoimisto tarkistaa alle 30-vuotiaan osalta vapautusperusteen olemassaolon ja tarvittaessa määrää asevelvollisen aluetoimiston järjestämään tarkastukseen asevelvollisuusasioiden hoitamista varten.

Väestötietojärjestelmästä ei ole saatavissa tietoa Ahvenanmaan asukkaiden kotiseutuoikeudesta. Tämän vuoksi Ahvenanmaan alueen kunnista vastaava Puolustusvoimien aluetoimisto lähettää vuosittain Ahvenanmaalla asuvien kutsuntaikäisten nimilistan maakuntahallitukselle, joka tarkastaa henkilöiden kotiseutuoikeuden ja palauttaa listan tarvittavilla kotiseutuoikeustiedoilla täydennettynä aluetoimistolle, joka puolestaan ilmoittaa asevelvollisuudesta vapauttamisesta siihen oikeutetuille. Muille kutsunnanalaisille aluetoimisto järjestää kutsunnat Maarianhaminan kaupungissa asevelvollisuuslain 127 §:n mukaisesti. Kutsuntalautakunnassa maakunnan kuntia edustaa Maarianhaminan kaupunginhallituksen valitsema edustaja tai tämän varahenkilö.

7 Riippuvuus muista esityksistä

Sisäministeriössä on vireillä siviilitiedustelua koskeva lainsäädäntöhanke, jossa ehdotetaan säädettäväksi poliisilain muuttamisesta, tietoliikennetiedustelusta siviilitiedustelussa sekä henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamisesta.

Esitykseen sisältyvän sotilastiedustelua koskevan lakiehdotuksen 2 §:ssä olisi viittaussäännös edellä mainittuihin lakeihin. Tietoliikennetiedustelun teknisestä toteuttamisesta suojelupoliisille säädettäisiin lakiehdotuksen 73 §:n 2 momentin mukaan tietoliikennetiedustelusta siviilitiedustelussa annetun lain 10 §:ssä. Tietojen luovuttamista suojelupoliisille koskevan 113 §:n mukaan rekisteripitäjä saisi salassapitosäännösten estämättä luovuttaa rekistereistä henkilötietoja, jos tiedot ovat tarpeen poliisilain 5 a luvussa tai tietoliikennetiedustelussa siviilitiedustelussa annetussa laissa tarkoitettua tiedustelua varten. Asianosaisjulkisuuden rajoittamista eräissä tapauksissa koskevassa 137 §:ssä olisi siviilitiedusteluun liittyvissä rajoituksissa viittaussäännös poliisilain 5 a lukuun.

Oikeusministeriössä on valmisteltu ehdotus perustuslain muuttamiseksi koskien luottamuksellisen viestin suojan rajoittamista tiedon hankkimiseksi sotilaallisesta toiminnasta ja muusta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Muutoksella mahdollistettaisiin luottamuksellisen viestin salaisuuden suojaan puuttuvia tiedustelutoimivaltuuksia koskevan lainsäädännön säätäminen.

Oikeusministeriössä on lisäksi valmisteltu sotilas- että siviilitiedustelutoiminnan laillisuusvalvontaa koskeva ehdotus hallituksen esitykseksi.

Valtioneuvoston kansliassa on valmisteltu hallituksen esitys (HE 261/2016 vp) laiksi valtioneuvoston tilannekeskuksesta. Kyseisen hallituksen esityksen mukaan valtioneuvoston tilannekeskuksen tehtävänä olisi muun muassa hoitaa ja koordinoida tilannekuvan ylläpitämiseen, kokoamiseen ja yhteensovittamiseen liittyviä poikkihallinnollisia tehtäviä, mikä liittyy tähän esitykseen sisältyvään tiedustelutoiminnan yhteensovittamista koskevaan pykäläehdotukseen lain 17 §:ssä.

Puolustusministeriö on asettanut työryhmän, jonka tehtävänä on selvittää henkilötietojen käsittelyä puolustushallinnossa koskevan lainsäädännön muutostarpeet ja valmistella ehdotus tarvittaviksi säädösmuutoksiksi. Hanke liittyy EU:n tietosuojalainsäädännön kokonaisuudistukseen ja henkilötietojen suojaa koskevan lainsäädännön tarkistamiseen. Tietosuojadirektiivi on pantava täytäntöön viimeistään 6.5.2018. Yleistä tietosuoja- asetusta aletaan soveltaa 25.5.2018. Hallituksen esitys puolustushallinnon henkilötietoja koskevaksi uudeksi lainsäädännöksi annettaisiin eduskunnalle syysistuntokaudella 2017.

Esitykseen sisältyvään lakiehdotuksen 10 lukuun on sisällytetty sotilastiedustelun tietojärjestelmää ja muita henkilörekistereitä koskevia säännösehdotuksia. Tarkoituksena on, että jatkovalmistelussa tämä sääntely siirrettäisiin valmisteltavana olevaan uuteen puolustushallinnon henkilötietolakiin.

YKSITYISKOHTAISET PERUSTELUT

1 Lakiehdotuksen perustelut

Laki sotilastiedustelusta

1 luku. Yleiset säännökset

1 §. *Lain soveltamisala.* Pykälässä säädettäisiin lain soveltamisalasta. Tämän lain tarkoittamaa tiedustelua suorittaisi Puolustusvoimat ja toimintaa kutsuttaisiin sotilastiedusteluksi. Tiedustelutoiminnan tavoitteena olisi tuottaa varhaisvaiheen tietoa, joka mahdollistaa uhkiin, riskeihin, mahdollisiin tapahtumakehityksiin ja muutoksiin vaikuttamisen ja varautumisen. Sotilastiedustelun yleisenä tehtävänä on sotilasstrategisen tilannekuvan muodostamiseksi seurata Suomen turvallisuusympäristön kehitystä, määrittää ympäristön muutokset ja tuottaa tietoa vallitsevasta tilanteesta.

2 §. *Suhde muuhun lainsäädäntöön.* Pykälän 1 momentissa säädettäisiin lain suhteesta muuhun sotilastiedustelutoimintaa lähellä olevaan toimintaan.

Hallituksen esityksessä eduskunnalle poliisilain muuttamisesta annettavaksi laiksi (HE /2017) poliisilain 5 a luvun mukaan suojelupoliisi hoitaisi siviilitiedusteluun liittyviä tehtäviä.

HE /2017 mukaan 5 a luvussa tiedustelumenetelmien soveltamisalaksi määriteltäisiin suojelupoliisin suorittamaa tiedustelua, jolla hankitaan tietoa toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Sääntelyllä korostettaisiin sitä, että suojelupoliisi olisi ainoa siviilitiedusteluviranomainen, jolla olisi oikeus käyttää poliisilain 5 a luvussa säädettyjä keinoja.

Lisäksi HE /2017 5 a luvun soveltamisalassa olisi viittaus säännös tietoliikennetiedustelusta siviilitiedustelussa annettavaan lakiin. 5 a luvun siviilitiedusteluun liittyvänä toimivaltuutena olisi erillislaissa säädettynä tiedonhankinta Suomen rajat ylittävissä tietoliikennekaapeleissa liikkuvaan tietoliikenteeseen kohdistuva tiedonhankinta.

Suomessa rajat ylittävissä tietoliikennekaapeleissa liikkuvaan tietoliikenteeseen kohdistuvan tiedonhankinnan tekninen toteuttaminen olisi keskitettynä yhdelle Puolustusvoimien toimijalle, jolla olisi velvollisuus toteuttaa poliisilta tulevat kyseistä tiedonhankintakeinoa koskevat toimeksiannot. Teknistä toteuttajaa koskeva sääntely olisi sotilastiedustelulaissa.

Tiedustelutoiminnan luonteesta johtuen sen valvontaan on kiinnitettävä erityistä huomiota. EIT:n ratkaisukäytännössä on korostettu, että valvonnan on oltava riippumatonta ja tiedusteluviranomaisen hallinnonalan ulkopuolista. Tiedustelutoiminnan oikeudellinen valvonta olisikin keskitetty erilliselle viranomaiselle, josta säädettäisiin erikseen. Pykälän 2 momentin mukaan sotilastiedustelusta olisi erotettava Puolustusvoimien rikosten ennalta estäminen, paljastaminen ja selvittäminen, josta säädetään sotilaskurinpidosta ja rikostorjunnasta puolustusvoimista annetussa laissa (255/2014, SKRTL). SKRTL 86 §:n 1 momentin mukaan Puolustusvoimien rikosten ennalta estämisessä ja paljastamisessa huolehditaan sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaa ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyvien rikosten ennalta estämisestä ja paljastamisesta. SKTRL 89 §:n 2 momentissa säädetään rikoksista, joidenka paljastamisessa saadaan käyttää salaisia tiedonhankintakeinoja. SKRTL:ssä tarkoitettu rikostorjunnan soveltamisala liittyy rikoksen käsitteeseen, joka on erotettava tiedustelun kohteena olevista uhkista ja toiminnasta sekä niiden kehittymisestä. SKRTL:än toimivaltuuksia käyttää pääesikunnan tiedusteluosasto. Koska rikostorjunnan toimivaltuudet ovat osittain samankaltaiset

tässä esityksessä ehdotettavien toimivaltuuksien kanssa, mutta niitä käytetään eri tarkoituksessa, olisi erityistä huomioita kiinnitettävä siihen, ettei sotilastiedustelun toimivaltuuksia ja rikostorjunnan toimivaltuuksia käyttäisi samat henkilöt.

Pykälän 3 momentissa olisi säädetty lain suhteesta henkilötietolakiin sekä viranomaisten toiminnan julkisuudesta annettuun lakiin. Henkilötietojen käsittelystä sotilastiedustelussa säädettäisiin jäljempänä.

Säännös olisi informatiivinen viittaussäännös henkilötietolakiin (523/1999) ja viranomaisten toiminnan julkisuudesta annettuun lakiin (julkisuuslaki), joita sovellettaisiin, jollei tässä laissa toisin säädetä.

Henkilötietolaissa säädetään henkilötietojen käsittelyn yleisistä periaatteista: käsittelyn yleisistä edellytyksistä, arkaluonteisten tietojen ja henkilötunnuksen käsittelystä sekä henkilötietojen siirrosta ulkomaille, rekisteröidyn oikeuksista, tietoturvallisuudesta ja henkilötietojen säilyttämisestä, ilmoitusmenettelystä sekä henkilötietojen käsittelyn ohjauksesta ja valvonnasta.

Julkisuuslaissa säädetään muun muassa oikeudesta saada tieto ja muusta henkilötietojen luovuttamisesta viranomaisen henkilörekisteristä sekä henkilötietojen salassa pitämisestä.

3 §. *Sotilastiedustelun tarkoitus.* Pykälässä määriteltäisiin sotilastiedustelun tarkoitus. Sotilastiedustelun tarkoitus olisi rajattu liittymään Puolustusvoimien lakisääteisiin tehtäviin. Puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdan mukaan Puolustusvoimien tehtävänä on Suomen sotilaallinen puolustaminen. Puolustusvoimien tehtävänä on lisäksi momentin 2 kohdan mukaan muiden viranomaisten tukeminen sekä 3 kohdan mukaan osallistuminen kansainväliseen sotilaalliseen kriisinhallintaan ja sotilastehtäviin muussa kansainvälisessä kriisinhallinnassa.

Hallituksen esityksessä 94/2016 vp. uolustusvoimista annettuun lakiin esitetään 2 §:n 1 momenttiin uutta 3 kohtaa, jolloin nykyinen 3 kohta, joka koskee sotilaallista kriisinhallintaa, siirtyisi 4 kohdaksi. Puolustusvoimien kolmanneksi tehtäväksi määriteltäisiin osallistuminen kansainvälisen avun antamiseen ja muuhun kansainväliseen toimintaan.

Kansainvälinen toiminta sisältyy sinänsä jo nyt kiinteästi kaikkiin Puolustusvoimien lakisääteisiin tehtäviin eli Suomen sotilaalliseen puolustamiseen, muiden viranomaisten tukemiseen ja osallistumiseen kansainväliseen sotilaalliseen kriisinhallintaan sekä sotilastehtäviin muussa kansainvälisessä kriisinhallinnassa. Suomen sotilaallista puolustusta pyritään vahvistamaan myös kansainvälisellä yhteistyöllä. Yhteistyötä tehdään EU:ssa sekä toisten valtioiden ja kansainvälisten järjestöjen, kuten YK:n ja Naton sekä maaryhmäjärjestelyjen kanssa.

Kansainvälistä apua voitaisiin uuden 3 kohdan mukaisesti antaa toiselle valtiolle, Euroopan unionille tai kansainväliselle järjestölle esimerkiksi EU:n yhteisvastuulausekkeen tai keskinäisen avunannon lausekkeen tilanteissa taikka aluevalvonnassa siten kuin jäljempänä 12 §:ssä säädettäisiin. Esimerkkeinä säännöksessä tarkoitetusta muusta kansainvälisestä toiminnasta voidaan mainita Suomen omista tarpeista lähtevä yhteistoiminta.

Sotilastiedustelu tuottaisi oikeaa ja riippumatonta tietoa riittävän aikaisessa vaiheessa ylimmän valtiojohdon ja ylimmän sotilasjohdon päätöksenteon tueksi puolustusvoimista annetun lain 2 §:ssä määriteltyjen Puolustusvoimien tehtäviin liittyen. Tietoa hankittaisiin vain tässä laissa myöhemmin määritellyistä sotilastiedustelun kohteista. Sotilastiedustelulla hankittu tieto mahdollistaisi ylimmän valtionjohdon sekä ylimmän sotilasjohdon oikea-aikaisen ja oikeaan tietoon perustuvan päätöksenteon sekä strategisen, operatiivisen ja taktisen ennakkovaroituksen antamisen sekä jo olemassa olevien viranomaisresurssien tehokkaan käyttämisen, mutta myös viranomaisresurssien tehokkaan suunnittelun, kehittämisen, ylläpidon ja lisäyksen tilanteen niin vaatiessa.

Tiedon hankkiminen sisältäisi myös Suomeen kohdistuvien ulkoisten uhkien kartoittamisen. Kyse olisi siten esimerkiksi turvallisuusympäristön kehityksen seuraamisesta tilannekuvan muodostamiseksi. Ilmaisu kattaisi myös jatkuvan tiedonhankinnan sotilastiedustelun kohteista. Tiedonhankintaa ei siten olisi rajoitettu ajallisesti, sillä tiedustelutoimintaa on usein tarpeen seurata pitkäjänteisesti ja systemaattisesti ilman, että seurattavan toiminnan välttämättä tarvitsisi olla välittömästi uhkaavaa seurannan aikana (OMML 41/2016, s. 49).

Pykälässä oleva maininta uhkien tunnistamisesta viittaisi toimintaan, jota ei vielä voitaisi konkretisoida tietyksi kohteeksi. Tapahtumaketjut ja toiminta voivat näyttää aluksi muulta kuin konkreettista uhkaa aiheuttavalta toiminnalta. Tiedon saaminen riittävän varhaisessa vaiheessa näistä tapahtumista ja toiminnasta mahdollistaa niiden tavoitellun päämäärän tunnistamisen sekä sen, kenen etua ja hyötyä niillä tavoitellaan. Tämä mahdollistaisi myös riittävän riskiarvioinnin ja ulko- turvallisuus- ja puolustuspoliittisen arvion siitä, kuinka todennäköisesti ja missä tilanteissa Suomi voisi joutua tällaisten tapahtumaketjujen ja toiminnan kohteeksi. Uhkien tunnistamisessa keskeisenä kysymyksenä on se, mikä taho uhkan takana on.

Sotilastiedustelusta keskeisenä kohteena on esimerkiksi sotilaallinen toiminta. Sotilaallinen toiminta voi olla Suomen ulkoinen uhka, jonka taustalla voi olla valtiollinen tai ei-valtiollinen toimija (OMML 41/2016 s. 48). Sotilaallisessa toiminnassa usein liikutellaan suuria joukkokokonaisuuksia ja asejärjestelmiä. Joukkokokonaisuuksien ja asejärjestelmien sijoittaminen kertoo jo itsessään tietoa sotilaallisen toimijan toimintavalmiudesta rauhanaikana esimerkiksi sotilaallisissa harjoituksissa.

Uhkien tiedustelu kattaisi myös esimerkiksi Puolustusvoimien tarvitseman maalittamistuen ja Puolustusvoimien tarvitsemien paikka- ja olosuhdetietojen tuottamisen.

4 §. *Sotilastiedustelun kohteet.* Pykälässä olisi lueteltuna ne sotilastiedusteluun liittyvät asiat ja uhkat, joista sotilastiedustelulla voitaisiin hankkia tietoja. Sotilastiedustelun lisäksi kansallista turvallisuutta koskevista uhkista sekä niitä koskevasta tiedonhankinnasta säädettäisiin siviilitiedustelulaissa. Sotilastiedustelun kohteet liittyisivät aina Puolustusvoimien lakisääteisiin tehtäviin.

Sotilastiedustelun tiedonhankinta kohdistuu ennen kaikkea asioihin, jotka eivät ole rikosperusteisia tai edes suunnitteluvaiheessa olevia rikoksia. Sotilastiedustelun kohteena oleva toiminta voisi olla täysin laillista tiedonhankinnan vaiheessa, mutta toiminta saattaisi joissain tilanteissa muuttua laittomaksi rikosperusteiseksi toiminnaksi tiedustelun kohteena olevan toiminnan edetessä. Edellä tarkoitetut rikosperusteiset tilanteet eivät enää olisi sotilastiedustelun toimialassa vaan asia kuuluisi sotilasvastatiedusteluun.

Yhteiskunnan tärkeimpänä suojattavana etuna voidaan pitää valtion suvereenisuutta, jolla tarkoitetaan täysivaltaisuutta suhteessa ulkovaltioihin ja oikeutta muista riippumattomalla tavalla käyttää ylintä valtaa omien rajojensa sisällä. Muina keskeisinä suojattavina etuina voidaan pitää puolustuskyvyn lisäksi kansainvälistä toimintaa. Suomen keskeisten suojattavien etujen piiriin kuuluu esimerkiksi se, että Suomi voi toteuttaa omaa ulko- ja turvallisuuspolitiikkaansa ja toimia osana kansainvälistä yhteisöä sekä noudattaa kansainvälisiä velvoitteittaan moni- ja kahdenvälisten valtiosopimusten osapuolena. Suomen velvollisuutena on lisäksi omalta osaltaan osana kansainvälistä yhteisöä pyrkiä puuttumaan toimintaan, jonka on katsottu globaalisti vakavasti uhkaavan kansainvälistä turvallisuutta.

Sotilastiedustelun kohteena on toiminta, joka uhkaa edellä mainittuja etuja tai muita yhteiskunnan perustoimintoja. Yhteiskunnan perustoimintoja uhkaava toiminta ei kohdistuisi ensisijaisesti kehenkään yksilönä, vaan yleisemmin valtioon tai yhteiskuntaan. Kuitenkin esimerkiksi yksittäisiin henkilöihin kohdistuvat väkivallanteot voisivat olla säännöksessä tarkoitettua toimintaa, jos ne laajuudeltaan tai merkitykseltään olisivat yhteiskunnan kollektiivisten turvallisuusetujen kannalta merkittäviä

ja voisivat siten muodostaa vakavan uhan sille. Ilmaisulla uhka tarkoitettaisiin tilanteita, joissa Suomen turvallisuus ei ole välittömästi vaarantumassa. Toisaalta sotilaallisen toiminnan ei tarvitse uhata Suomen kansallista turvallisuutta tullakseen tämän säännöksen mukaisesti sovellettavaksi. Sotilaallinen toiminta voi liittyä useisiin pykälän kohtiin ja sillä tarkoitettaisiin sekä valtiollista että ei-valtiollista toimintaa (OMML 41/2016, s. 48 ja 49). Toisaalta sotilaallinen ei-valtiollinen toimija voisi olla esimerkiksi terrorijärjestö, jonka toiminta linkittyy merkittävästi aseelliseen konfliktiin tai sisällissotaan.

Kaikkia tiedustelun kohteita ei voida jakaa selkeästi sotilas- ja siviililuonteisiin. Tästä johtuen olisikin tarkoituksen mukaista, että sotilastiedustelu ja siviilitiedustelu voisivat hankkia tietoa osittain samoista kohteista. Sotilastiedustelun ja siviilitiedustelun tiedonhankinta voisi kohdistua samaan laajempaan uhka- tai asiakokonaisuuteen, mutta kumpikin toimija hankkisi tietoja omasta osa-alueestaan. Tiedusteluviranomaisten yhteistyöllä tiedusteluviranomaisen ulkopuoliselle ylimmälle valtiojohdolle voitaisiin toimittaa kokonaisvaltaisempi kuva tarkasteltavasta kokonaisuudesta.

Sotilastiedustelun tiedustelumenetelmien käytön osalta on korostettava sitä, että Puolustusvoimien tehtävien kannalta tiedustelumenetelmien soveltamisala on syytä rajata tiedon hankkimiseen sotilaallisesta toiminnasta ja kaikkein vakavimmista Suomen koskemattomuutta vaarantavasta toiminnasta.

EIT:n vakiintuneen ratkaisukäytännön mukaan Euroopan ihmisoikeussopimuksen (EIS) 8 artiklassa turvattuja oikeuksia rajoittavan lain on oltava muun ohella vaikutuksiltaan ennakoitava. Ennakoitavuus edellyttää ennen kaikkea lain riittävää täsmällisyyttä sen osoittamiseksi, missä olosuhteissa sekä millä edellytyksillä kansalaiset voivat joutua salaisten viranomaistoimenpiteiden kohteeksi (Weber ja Saravia v. Saksa, kohta 96 ja 97). EIT on toisaalta useasti muistuttanut, että jo asian luonnosta seuraa, että kansalliseen turvallisuuteen kohdistuvat uhat ovat luonteeltaan erilaisia ja toisinaan myös ennakoimattomia, minkä vuoksi niitä voi olla vaikea määritellä etukäteen (Kennedy v. Yhdistynyt kuningaskunta, kohta 159). Tämän pykälän sisältämässä sotilastiedustelun kohteiden luettelossa on pyritty yhteen sovittamaan yhtäältä vaatimus lain ennakoitavuudesta ja täsmällisyydestä sekä toisaalta tarve voida hankkia tietoa myös uusista uhkista. EIT:n ratkaisukäytäntöä on käsitelty tarkemmin yleisperusteluissa.

Vaikka tiedonhankinta voi olla luonteeltaan pitkäkestoista, jokaisen tiedustelumenetelmän kohdalla säädettäisiin erikseen päätöksen voimassaoloajasta. Voimassaoloajan päättyessä tiedustelumenetelmän käytöstä olisi joko päätettävä uudelleen tai se 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.

Pykälän merkitys kohdistuu niin tietopyynnön esittäjän, tiedustelutehtävän antavan, tiedustelumenetelmän käyttöä esittävän vaatimuksentekijän kuin vaatimuksen perusteella päätöksen tekevään tahoon tai luvan myöntäjään. Lisäksi pykälä ohjaa sotilastiedustelun tiedustelutehtävän laatimista sekä tiedustelumenetelmien käyttöä. Jäljempänä säädettävien päätöksentekoa koskevissa säännöksissä edellytettäisiin yksilöimään ja perustelemaan tiedustelutoimenpiteen perusteena olevan tiedustelutehtävän perustuminen pykälässä säädettyihin kohteisiin. Tiedustelumenetelmiä koskevassa päätöksenteossa ja tiedustelun toteuttamisessa olisi lisäksi aina otettava huomioon yleiset säännökset perusoikeuksien ja ihmisoikeuksien kunnioittamisesta, suhteellisuusperiaate ja vähimmän haitan periaate.

Sotilastiedustelun kohteista merkittävimpänä voidaan pitää sotilaallista toimintaa. Käsitteenä sotilaallinen toiminta on kokonaisvaltainen niin, että pykälässä olevan listan useat kohdat voisivat mennä sen alle. Yleisperusteluissa kuvattu EIT:n ratkaisukäytäntö ja perustuslain vaatimukset kuitenkin edellyttävät etenkin tiedustelutoiminnasta säädettäessä lainsäädännöltä tarkkarajaisuutta.

EIT:n kannanotot on otettu huomioon tämän pykälän luettelon laadinnassa, ja sotilastiedustelun kohteista on pyritty säätämään mahdollisimman yksityiskohtaisesti ja kattavasti. Pykälän luettelossa lueteltaisiin ne laajemmat kokonaisuudet, joista voitaisiin hankkia tietoa sotilastiedustelulla. Se, mitä tiedonhankinnan keinoja tiedonhankinnassa voitaisiin käyttää, edellyttäisi aina tapauskohtaista harkintaa ja tiedonhankinnan kohteena olevan toimijan tunnistamista joko valtiolliseksi toimijaksi tai muuksi toimijaksi.

Tässä laissa säädettäväksi ehdotettavissa tiedustelumenetelmiä koskevissa päätöksentekosäännöksissä edellytettäisiin aina yksilöimään ja perustelemaan tiedustelumenetelmän perusteena oleva tässä pykälässä tarkoitettuun toimintaan perustuva tiedustelutehtävä. Päätöksentekijän harkittavaksi jäisi, onko tietyn tiedustelumenetelmän käyttäminen tietyssä tilanteessa perusteltua ja missä laajuudessa.

Tiedustelumenetelmän käytön edellytyksenä ei olisi, että toiminnan taustalla oleva taho olisi tunnistettu sillä hetkellä kun tiedustelumenetelmän käyttöön ryhdytään. Tiedustelumenetelmiä voitaisiin käyttää myös uhkien havaitsemiksi ja niiden aiheuttajina olevien tahojen tunnistamiseksi. Tiedustelumenetelmän kohteena voisi myös olla henkilö tai henkilöryhmä, jolla voidaan olettaa olevan tietoa tässä pykälässä tarkoitetusta toiminnasta. Tiedustelua voitaisiin kohdistaa sekä valtiolliseen että ei-valtiolliseen toimijaan tai sellaiseen henkilöön, joka toimii valtiollisen toimijan puolesta tai hyväksi.

Pykälän 1 kohdan mukaan sotilastiedusteluviranomainen voisi hankkia tietoja sotilaallisesta toiminnasta. Sotilaalliselle toiminnalle tyypillistä ovat suuret joukkokokonaisuudet, sotilaallinen järjestäytyminen, sotilaallinen kouluttautuminen ja varustautuminen vahvemmin kuin tavanomaisilla voimankäyttövälineillä. Lisäksi sotilaallinen toiminta vaatii usein vahvaa taloudellista resursointia. Usein tällaisen toiminnan taustalla on valtio, tosin sotilaallista toimintaa voidaan organisoida muidenkin tahojen toimesta, kuten valtion johtoa vastaan kapinoivien joukkojen toimesta. Viimeksi mainitussa tilanteessa on kiinnitettävä huomiota toiminnan järjestäytyneisyyteen, taloudellisiin resursseihin, organisointiin sekä siihen, minkälaiseen voimankäyttöön kyseinen taho mahdollisesti pystyy.

Kohdassa tarkoitettua sotilaallista toimintaa ei olisi rajattu koskemaan erityisesti Suomeen kohdistuvaksi sotilaalliseksi toiminnaksi. Puolustusvoimien olisi voitava hankkia laajasti tietoa vieraan valtion sotilaallisesta toiminnasta ja sen kehityksestä ilman, että voitaisiin katsoa tämän aiheuttavan välitöntä sotilaallista uhkaa Suomelle.

Sotilaallinen toiminta kattaa toiminnan, kuten sotilaallisen voimankäytön, valmistelun, suunnitelmat ja aikeet. Edellä mainitut asiat vaikuttavat olennaisesti siihen, minkälainen todellinen uhka Suomelle tai muulle taholle olisi mahdollisesti muodostumassa ja antaa lisäaikaa varautumiseen uhkaa vastaavasti. Sotilaallisen ennakkovaroitus edellyttää sitä, että pystytään laajasti arvioimaan erilaisia tapahtumakehityksiä. Näihin liittyvää tietoa voidaan saada esimerkiksi muualla maailmassa tapahtuvasta sotilaallisesta toiminnasta ja miten eri konflikteissa sotilaallinen toimija toimii tai on toiminut.

Sotilastiedustelun tiedonhankinnan kohteena olisivat lähialueen sotilaspoliittinen ja sotilaallinen kehitys. Teknologian kehittymisen myötä sotilaalliset uhkat voivat kohdistua Suomeen myös kauempaa kuin lähialueelta. Sotilastiedustelun tiedonhankinnan kohteena olisi etenkin Suomea vastaan kohdistuva sotilaallinen uhka, jonka kehittymiseen liittyvä tieto voi olla esimerkiksi sotasuunnitelmat, joukkojen ryhmittyminen sekä asejärjestelmien kehittäminen. Hankitun tiedon pohjalta tehdään analyysi, jonka avulla erilaisia turvallisuusympäristön epävarmuustekijöitä pyritään jäsentämään, vähentämään ja myös hyödyntämään.

Sotilaallisena toimintana voidaan sotilaallisen voimankäytön uhan lisäksi pitää sen vahingollisuuteen rinnastettavia uhkia, kuten uhka biologisten aseiden käytöstä tai laajuudeltaan aseelliseen

hyökkäykseen rinnastuvaa tietoverkkohyökkäyksestä elintärkeään infrastruktuuriin. Sotilaallisiin uhkiin varautumisessa on merkittävää se, että uhkista ja niiden kehittymisestä saadaan mahdollisimman varhaisessa vaiheessa tietoa. Puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdan a alakohdan mukaan Puolustusvoimien tehtävänä on osana Suomen sotilaallista puolustamista alueellisen koskemattomuuden turvaaminen ja puolustusvoimista annetun lain 4 §:n mukaan Puolustusvoimat turvaa Suomen aluetta, kansan elinmahdollisuuksia ja valtiojohdon toimintavapautta sekä puolustaa laillista yhteiskuntajärjestystä tarvittaessa sotilaallisin voimakeinoin aseellisen hyökkäyksen tai sitä vastaavan ulkoisen uhan kohdistuessa Suomeen.

Vieraiden valtioiden välinen sota tai sodanuhka voi olennaisesti myös vaikuttaa Suomen ulko- ja puolustuspoliittisiin suhteisiin ja vaikeuttaa Suomen mahdollisuuksia toimia kansainvälisessä yhteisössä.

Pykälän 2 kohdassa tiedonhankinta voisi koskea ulkomaista tiedustelutoimintaa. Kansainvälisen oikeuden yleisen periaatteen mukaan jokainen suvereeni valtio nauttii alueellista koskemattomuutta ja poliittista riippumattomuutta suhteessa muihin valtioihin. Jokainen valtio päättää itse, salliiko se ja millä ehdoilla ulkomaisten virkamiesten toimia alueellaan. Edellä on todettu, että useimmat valtiot tosiasiassa tiettyyn rajaan saakka sietävät tai jopa hyväksyvät vieraiden tiedusteluviranomaisten toiminnan maaperällään. Kyse saattaa olla molempia osapuolia hyödyttävästä tiedonvaihdosta tai siitä, ettei ulkovallan avoimesti suorittama, kohdevaltion yleisiä olosuhteita koskeva tiedonkeruu vaaranna kohdevaltion tai minkään muunkaan tahon etuja. Toisissa olosuhteissa kohdevaltio saattaa suhtautua alueellaan tapahtuvaan vieraan valtion viranomaisten toimintaan torjuvasti. Toiminta saattaa tapauskohtaisesti myös täyttää jonkin kohdevaltion rikoslainsäädännössä rangaistavaksi säädetyn teon tunnusmerkistön. Toiminnan rangaistavuuteen saattaa kohdevaltiosta riippuen vaikuttaa esimerkiksi se, kuka tietoa hankkii, mitä tietoa hankitaan ja mitä menetelmää käyttäen tiedonhankinta tapahtuu.

Puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdan a alakohdan mukaan Suomen sotilaalliseen puolustamiseen kuuluu Suomen alueellisen koskemattomuuden turvaaminen. Lisäksi kohdan b alakohdan mukaan Suomen sotilaalliseen puolustamiseen kuuluu kansan elinmahdollisuuksien, perusoikeuksien ja valtiojohdon toimintavapauden turvaaminen ja laillisen yhteiskuntajärjestyksen puolustaminen. Vieraan vallan tiedustelutoiminnan onnistuessa tällainen toiminta voi vaarantaa edellä tarkoitetuissa lainkohdissa tarkoitetut Suomen sotilaalliseen puolustamiseen kuuluvat edut.

Vieraiden valtioiden harjoittamalla tiedustelulla tarkoitetaan vieraan valtion toimintaa, jonka päämääränä on oman valtion etujen edistämiseksi tai Suomen tai toisen vieraan valtion vahingoksi hankkia tietoa, jonka salassapitoon kohdevaltiolla on erityinen intressi. Vieraan valtion tiedonhankinnan kohteena voi olla esimerkiksi Suomen ulko-, turvallisuus- ja energiapolitiikka, kuten Suomen maanpuolustuksen kehitys, päätöksenteon perusteet, strategisentason päätöksenteko ja sotilaallinen suorituskyky, Suomen sotilaallinen valmius, yhteiskunnan kriisinsietokyky, huoltovarmuus sekä korkeateknologia sekä sen tutkimus ja tuotekehitys. Tiedonhankinnan lisäksi vieraiden valtioiden tiedustelutoiminnan päämääränä voi olla vaikuttaminen muun muassa edellä mainittuihin kohteisiin liittyvään päätöksentekoon vieraan valtion etujen edistämiseksi tai Suomen tai toisen vieraan valtion vahingoksi.

Jäljempänä säädettävillä tiedustelumenetelmillä voitaisiin hankkia tietoa esimerkiksi siitä, miten vieraan valtion tiedustelu toimii, ketkä toimivat ulkomaisen tiedustelupalvelun lukuun tai hyväksi tai mitkä ovat heidän avoimet ja salaiset tiedonhankintakeinonsa sekä -kohteensa. Tiedonhankinta voisi koskea myös esimerkiksi sitä, mitkä ovat vieraan valtion tiedustelupalvelulleen osoittamat Suomea koskevat tiedonhankintatavoitteet ja -prioriteetit. Tiedustelumenetelmillä voitaisiin myös havaita ja tunnistaa henkilöitä, jotka paljastavat salassa pidettävää tietoa vieraan valtion tiedustelupalvelulle, joita vieraan valtion tiedustelupalvelu pyrkii tähän toimintaan värväämään tai jotka pyr-

kivät vieraan valtion tiedustelupalvelulta saamiensa käskyjen ja ohjeiden mukaisesti vaikuttamaan päätöksentekoon Suomen tai toisen vieraan valtion vahingoksi.

Tiedustelutoiminta kattaisi myös tilanteet, joissa tiedustelua tehtäisiin tietoverkkojen välityksellä kehittyneitä haittaohjelmia käyttäen. Tiedustelutoiminta olisi ymmärrettävä tekniikka neutraaliksi ja se kattaisi kaikki tilanteet, joissa toiminnan tavoitteena on hankkia tietoa esimerkiksi edellä kuvatuista vieraan valtion intresseissä olevista kohteista.

Eri valtioiden tiedustelutoiminta on voitu organisoida hyvinkin monilla eri tavoilla, kuten edeltä kansainvälisestä vertailusta käy ilmi. Tämän takia ei voida katsoa tarkoituksen mukaiseksi eritellä, minkä tyyppisestä tiedustelupalvelusta sotilastiedustelussa voisi hankkia tietoja.

Kohdan mukainen tiedustelupalveluiden toiminta kattaisi myös tilanteet, joissa esimerkiksi kahden eri vieraan valtion sotilastiedustelupalvelua tapaisivat Suomen alueella tai muuten käyttäisivät hyväkseen Suomen aluetta omassa toiminnassaan kohdistamatta kuitenkaan tiedustelua esimerkiksi Suomen maanpuolustukseen. Aktiivinen puuttuminen edellä mainittuun toimintaan olisi tärkeää Suomen sitoutumattomuuden varmistamiseksi.

Pykälän 3 kohdan mukaan sotilastiedustelu voisi hankkia tietoa valtio- ja yhteiskuntajärjestystä uhkaavasta toiminnasta. Kohta liittyisi puolustusvoimista annetun lain 2 §:n 1 kohdan b alakohdassa tarkoitettuihin Puolustusvoimien tehtäviin, jonka mukaan Puolustusvoimien tehtävänä on osana Suomen sotilaallista puolustamista kansan elinmahdollisuuksien, perusoikeuksien ja valtiojohdon toimintavapauden turvaaminen ja laillisen yhteiskuntajärjestyksen puolustaminen.

Valtio- ja yhteiskuntajärjestystä uhkaavalla toiminnalla tarkoitettaisiin valtio- ja yhteiskuntajärjestyksen sellaisia kumoamis- ja muutospyrkimyksiä, joissa käytetään väkivaltaisia keinoja, niillä uhkaamista tai muuta valtiosäännön vastaista menettelytapaa. Suomen perustuslain mukaisesti valtiojärjestyksellä tarkoitetaan sellaisia asioita kuin valtiosääntöä, kansanvaltaisuutta, oikeusvaltioperiaatetta, valtiollisten tehtävien jakoa ja parlamentarismia. Valtion oikeusjärjestyksen keskeisen osan puolestaan muodostavat oikeusnormit, jotka ohjaavat valtion jäsenten käyttäytymistä ja siten yhteiskuntaelämää.

Valtio- ja yhteiskuntajärjestystä uhkaava toiminta voisi ilmetä esimerkiksi suunnitelmana käyttää asevoimaa valtionsisäisen vallankaappauksen tai -kumouksen toteuttamiseksi taikka suunnitelmana liittää Suomi vieraan vallan alaisuuteen. Suomen valtio- ja yhteiskuntajärjestystä uhkaavana toimintana voitaisiin pitää myös esimerkiksi pyrkimyksiä väkivaltaisesti estää eduskuntaa käyttämästä lainsäädäntövaltaa taikka pakottaa hallitusvaltaa käyttäviä henkilöitä tekemään tai jättämään jotain tekemättä heidän valtiollisissa tehtävissään. Uhkaavan toiminnan taustalla voisi olla vieraan valtion pyrkimykset ja uhkaava toiminta voisi sisältää sotilaallisen toiminnan piirteitä, esimerkiksi hybridivaikuttamisen keinoja. Tietoa voitaisiin hankkia esimerkiksi siitä, mitä suunnitelmia tai valmisteluja edellä mainittuja pyrkimyksiä ajavalla toimijalla on ja ketkä henkilöt Suomesta tai ulkomailta käsin osallistuvat tällaiseen toimintaan.

Pykälän 4 kohdan mukaan sotilastiedusteluviranomainen voisi hankkia tietoa joukkotuhoaseista, kuten kemiallisista ja biologisista aseista, toksiiniaseista sekä ydinaseista ja radiologisista aseista. Kohdan tarkoittama toiminta liittyisi puolustusvoimista annetun lain 2 §:n 1 kohdan a ja b alakohtien tehtävään. Ydinaseet ja niiden rooli voimankäytössä ovat palanneet turvallisuuspoliittiseen keskusteluun. Uhkana on myös muiden joukkotuhoaseiden ja niihin liittyvän vaarallisen materiaalin sekä tietotaidon leviäminen. Kemialliset aseet määritellään muun muassa kemiallisten aseiden kehittämisen, tuotannon, varastoinnin ja käytön kieltämistä sekä niiden hävittämistä koskevassa yleissopimuksessa (SopS 19/1997). Biologisten aseiden ja toksiiniaseiden taustalla taas on Genevessä vuonna 1925 tehty pöytäkirja tukahduttavien, myrkyllisten tai muiden samankaltaisten kaasujen sekä bakteriologisten keinojen käytön kiellosta sodassa (SopS 23/1929). Ydinaseista puolestaan

määrätään muun muassa ydinaseiden leviämisen estämisestä tehdyssä niin sanotussa ydinsulkusopimuksessa (SopS 11/70). Radiologisten aseiden määrittelyä tehdään esimerkiksi terroristisen pommi-iskujen torjumista koskevassa kansainvälisessä yleissopimuksessa (SopS 59/2002).

Joukkotuhoaseperustaisen tiedustelun kohteena voisi olla niin henkilö tai henkilöryhmä kuin valtiollinen toimijakin. Kyse voi olla esimerkiksi tiedonhankinnasta muualla kuin Suomessa tapahtuvasta joukkotuhoaseen valmistamisesta, hankkimisesta, varastoinnista, hallussapidosta tai kuljettamisesta.

Joukkotuhoaseisiin kytkeytyvä tyypillinen haitta on mahdollisuus erittäin suuren vahingon syntymiseen. Haittaa voidaan pitää vakavana myös sen pitkäkestoisuuden vuoksi. Tällaista haittaa aiheuttaisi esimerkiksi radioaktiivista ainetta ympäristöön levittävä räjähdys taajaan asutulla alueella. Tiedonhankinnalla varmistettaisiin osaltaan riittävät mahdollisuudet torjua joukkotuhoaseiden aiheuttamaa vahinkoa.

Joukkotuhoaseet eivät välttämättä muodosta suoraa uhkaa Suomelle, mutta niiden aiheuttamaan uhkaan olisi pysyttävä varautumaan kansallisesti ja toisaalta niistä saatava tieto voi vaikuttaa Suomen mahdollisuuksiin toimia kansainvälisillä foorumeilla. Lisäksi kansainvälisen turvallisuuden järkkymisellä voi olla merkitystä välillisesti myös Suomen turvallisuustilanteeseen.

Pykälän 5 kohdan mukaan sotilastiedustelussa voitaisiin hankkia sotatarvikkeiden kehittämiseen ja levittämiseen liittyvää tietoa. Kohdan tarkoittamilla tiedot liittyisivät puolustusvoimista annetun lain 2 §:n 1 kohdan a ja b alakohdissa tarkoitettuihin Puolustusvoimien tehtäviin. Tietoa saisi hankkia niin valtiollisesta kuin ei-valtiollisesta toimijasta tai toimijajoukosta. Asejärjestelmien kehittäminen ei välttämättä muodosta suoraa uhkaa Suomelle. Asejärjestelmien kehittämisestä saatavalla tiedolla olisi kuitenkin suuri merkitys Puolustusvoimien toiminnan kannalta, jotta asejärjestelmiä vastaan pystyttäisiin tarvittaessa toimimaan tehokkaasti ja uhkan konkretisoituessa niiden aiheuttamat vahingot minimoimaan.

Tiedustelutoiminnan perustuessa tässä kohdassa tarkoitettuun sotatarvikkeiden kehittämiseen, huomiota olisi aina kiinnitettävä siihen, mikä taho sotatarvikkeita kehittää. Sotilaallisessa toiminnassa tarvittavien sotatarvikkeiden kehittäminen voi tapahtua yksityisen sektorin toimesta. Tällöin tiedustelumenetelmien käytön edellytykset ovat tiukemmat kuin valtiollisen toimijan suorittama sotatarvikkeiden kehitystyö. Huomiota on myös kiinnitettävä siihen, onko yksityinen sotatarvikkeita kehittävä taho valtion suorassa määräysvallassa ja kuinka merkittävää ohjausta valtio voi kehitystyötä tekevään tahoon käyttää. Tavanomaista kaupallista sopimusta valtiollisen toimijan ja yksityisen yhtiön välillä ei voida lähtökohtaisesti pitää sellaisena, minkä perusteella yksityistä tahoa voitaisiin pitää valtiollisena toimijana.

Kohdassa tarkoitetut sotatarvikkeet sekä niiden kehittäminen ja levittäminen liittyisivät olennaisesti sotilasstrategisen tilannekuvan muodostamiseen sekä Suomen turvallisuusympäristön kehittymiseen ja näiden muodostamiin uhkiin varautumiseen. Sotatarvikkeiden levittäminen nostaa riskiä siitä, että tietyssä valtiossa on muodostumassa sotilaallinen toimija tai tietyn valtion sotilaallinen toimija vahvistuu ja vaarantaa kansainvälistä rauhaa. Sotatarvikkeiden levittäminen kattaisi myös niiden kauttakuljetuksen.

Puolustusvoimien tehtävät ja sotilastiedustelu eivät kuitenkaan liity kansainvälisen rikollisuuden, kuten laittoman asekaupan, ennaltaehkäisyyn ja torjuntaan.

Lisäksi ulkovallat ja ulkomaiset toimijat voivat yrittää hankkia Suomen teollisuuden osaamista omaan käyttöönsä muuten kuin normaaliksi katsottavalla tavalla. Sotilastiedustelun tiedonhankinta voisikin kohdistua esimerkiksi tällaisiin tilanteisiin ja sen selvittämiseen, mikä taho oikeasti yrittää hankkia suomalaisen puolustusteollisuuden osaamista käyttöönsä.

Pykälän 6 kohdan mukaan sotilastiedustelun kohteena voisi olla valtioon tai yhteiskunnan elintärkeisiin toimintoihin kohdistuvat vakavat uhat. Kohta liittyisi olennaisesti puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdan b alakohtaan, jonka mukaan Puolustusvoimien tehtävänä on kansan elinmahdollisuuksien, perusoikeuksien ja valtiojohdon toimintavapauden turvaaminen ja laillisen yhteiskuntajärjestyksen puolustaminen. Yhteiskunnan elintärkeät toiminnot ovat poikkihallinnollisia, yhteiskunnalle välttämättömiä toimintokokonaisuuksia, joiden on oltava turvattuina kaikissa tilanteissa. Lisäksi puolustusvoimista annetun lain 4 §:n mukaan Puolustusvoimat turvaa Suomen aluetta, kansan elinmahdollisuuksia ja valtiojohdon toimintavapautta sekä puolustaa laillista yhteiskuntajärjestystä tarvittaessa sotilaallisin voimakeinoin aseellisen hyökkäyksen tai sitä vastaavan ulkoisen uhan kohdistuessa Suomeen.

Säännöksessä tarkoitetut yhteiskunnan elintärkeät toiminnot ovat yhteiskunnalle välttämättömiä toimintakokonaisuuksia, joiden tulee olla turvattuina kaikissa tilanteissa. Kokonaisuuteen kuuluvat muun muassa valtion johtaminen, kansainvälinen toiminta, valtakunnan sotilaallinen puolustaminen, sisäisen turvallisuuden ylläpitäminen ja talouden ja infrastruktuurin toimivuus. Näitä elintärkeitä toimintoja uhkaavalla toiminnalla tarkoitettaisiin esimerkiksi niiden merkittävään heikentämiseen tai keskeyttämiseen pyrkivää toimintaa. Tietoa voitaisiin hankkia siten esimerkiksi toiminnasta, jossa pyritään keskeyttämään tai tuhoamaan sellaisia yhteiskunnalle keskeisiä toimintoja kuten sähköntuotanto, tietoliikenne ja tietojärjestelmät, kuljetuslogistiikka, yhdyskuntatekniikka, elintarvikehuolto tai rahoitus- ja maksujärjestelmä.

Valtioon tai yhteiskunnan elintärkeisiin toimintoihin kohdistuva uhka voisi olla kyseessä myös silloin, kun kyseessä olisi vieraiden valtioiden välinen sota tai sodanuhka sekä muu vaikutuksiltaan näihin verrattava Suomen ulkopuolinen tapahtuma. Hankittavalla tiedolla voitaisiin varautua tilanteen nopeaankin negatiiviseen kehittymiseen Suomen osalta mahdollisimman hyvin.

Tietoteknisiin järjestelmiin kohdistuvat vakavat hyökkäykset voivat vaikuttaa julkisiin palveluihin, liike-elämään sekä hallintoon ja siten koko yhteiskunnan toimintaan niin merkittävästi ja laajasti, että niiden vaikutuksia joissakin tapauksissa voitaisiin verrata aseelliseen hyökkäykseen. Tietoa voitaisiin hankkia esimerkiksi Suomen huoltovarmuutta vaarantavista omistussuhteiden muutoksista tai toiminnasta, jossa vieras valtio kartoittaa tietoverkoissa eurooppalaisen energiajakeluverkoston tietoteknisen ohjausjärjestelmän rakennetta ja teknisiä haavoittuvuuksia tarkoituksenaan mahdollisesti hyödyntää tietoa sähköverkon lamauttamisessa.

Valtaosa Suomen kriittisestä tietoliikenneinfrastruktuurista ja sen palveluista on yksityisen sektorin omistamaa ja tuottamaa, mistä johtuen sen merkitys yhteiskunnan elintärkeiden toimintojen turvaamisessa on tärkeä. Tiedonhankinnalla pyrittäisiin turvaamaan valtiojohdon toimintavapaus ja puolustamaan laillista yhteiskuntajärjestystä. Puolustusvoimilla on erityisosaamista poikkeusoloihin liittyen, jota voitaisiin hyödyntää tämän kohdan tarkoittamissa tilanteissa myös muuna aikana kuin poikkeusoloissa. Kohdan perusteella hankitut tiedot olisivat poikkeusoloihin varautumisen kannalta keskeisiä ja ne saattaisivat joissain tapauksissa johtaa tilanteeseen, jossa saatujen tietojen perusteella olisi tarkoituksen mukaista ottaa käyttöön valmiuslain toimivaltuudet.

Pykälän 7 kohdan mukaan sotilastiedustelun kohteena voisivat olla vieraan valtion suunnitelmat tai toiminta, joka voisi aiheuttaa vahinkoa Suomen kansainvälisille suhteille taikka muille tärkeille eduille. Vieraan valtion vahinkoa aiheuttavalla toiminnalla tarkoitettaisiin esimerkiksi toimintaa, jossa pyrittäisiin vihamielisellä tavalla vaikuttamaan Suomen päätöksentekoon. Vieraan valtion vihamielisen vaikuttamisen keinovalikoima voi olla laaja ja se voi vaihdella maailmapoliittisen tilanteen mukaan poliittisista, taloudellisista ja informaatiovaikuttamisen keinoista aina viranomaistoiminnan taktiseen laiminlyöntiin tai poikkeukselliseen aktivoitumiseen, jolle ei löydy tosiasialliseen toimintaympäristöön liittyvää perustetta.

Kohta liittyisi puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdan b alakohtaan, jonka mukaan Puolustusvoimien tehtävänä on kansan elinmahdollisuuksien, perusoikeuksien ja valtiojohdon toimintavapauden turvaaminen ja laillisen yhteiskuntajärjestyksen puolustaminen. Valtiojohdon päätöksentekoon saatetaan pyrkiä vaikuttamaan poliittisilla ja taloudellisilla painostuskeinoilla sekä disinformaatio-operaatioilla, jotka saattaisivat johtaa ulkovallan sotilaalliseen voimankäyttöön Suomea vastaan. Sotilastiedustelun toiminnalla pyrittäisiin selvittämään painostuskeinojen todelliset tarkoitusperät ja sen taustalla olevat toimijat. Painostuskeinojen taustojen selvittämisellä on suora yhteys ennakkovaroituksen antamiseen sotilaallisen uhan kehittymisestä. Oikea-aikainen ja objektiivinen tieto korostuvat poliittisiin ja taloudellisiin painostuskeinoihin ja disinformaatio-operaatioihin varautumisessa sekä mahdollistavat valtiojohdon vapaan toiminnan tällaisten painostuskeinojen kohdistuessa Suomeen ja auttaa ennakoimaan uhkan kehittymistä.

Vieras valtio voi pyrkiä toteuttamaan toimenpiteensä siten, ettei kohdevaltio voi olla varma onko kyseessä vieraan valtion ohjaama tavoitteellinen operaatio vai ei. Tällaista toimintaa voi olla esimerkiksi se, että suomalaiseen ja ulkomaiseen kansalaismielipiteeseen pyritään vaikuttamaan levittämällä järjestelmällisesti väärää tietoa Suomen politiikasta julkisuudessa. Tietoa voitaisiin tällöin hankkia siitä, mikä taho tai ketkä on Suomeen kohdistetun informaatiovaikuttamisen takana sekä siitä, mitä tällaisella toiminnalla tavoitellaan.

Toisaalta kohdan mukaista toimintaa voisi olla esimerkiksi toisessa valtiossa käynnistynyt tai näköpiirissä oleva vallankaappaus tai -kumous, minkä yhteydessä tiedonintressi liittyisi ainakin siihen, miten kyseisen valtion poliittinen tilanne kehittyy. Poliittisen tilanteen kehityksellä voi olla merkittäviäkin vaikutuksia Suomen ulko-, turvallisuus- ja puolustuspoliittiseen tilanteeseen.

Tämän kohdan mukaisesti päätöksentekijän tapauskohtaisen harkinnan varaan jäisi se, voitaisiinko esimerkiksi tietoliikennetiedustelua käyttää tiedonhankkimiseksi Suomen edulle vahinkoa aiheuttavasta toiminnasta.

Pykälän 8 kohdan mukaan sotilastiedustelussa saisi hankkia tietoa kansainvälistä rauhaa ja turvallisuutta vaarantavasta kriisistä.

Tiedustelu olisi sallittua tämän kohdan nojalla siitä riippumatta, onko kriisin aiheuttaja tai osapuoli valtiollinen vai ei-valtiollinen toimija. Valtiotoimijoiden rinnalle on noussut laajeneva joukko ei-valtiollisia toimijoita, joiden tavoitteet ja toimintatavat ovat uhka kansainväliselle tai yksittäisten maiden ja niiden asukkaiden turvallisuudelle. Näin ollen tiedonhankinta voitaisiin tämän kohdan perusteella kohdistaa paitsi aseelliseksi selkkaukseksi eskaloituneeseen toimintaan, myös sellaiseen toimintaan, joka vasta ennakoi kansainvälisen rauhan rikkoutumisen uhkaa. Tällaiset uhkat voivat syntyä hyvin monenlaisista tekijöistä, kuten väestökehityksestä, valtioiden välisistä muuttoliikkeistä, ruokapulasta tai luonnonvarojen niukkuudesta. Kansainvälistä rauhaa ja turvallisuutta vaarantavaa kriisiä, ja sitä kautta tiedustelutarvetta saattavat aiheuttaa myös eri puolilla maailmaa toimivat tahot, jotka rajoittavat demokraattisten instituutioiden toimintaa sekä kaventavat perusvapauksia ja ihmisoikeuksia, ilmaisunvapautta ja sosiaalisen median toimintaa.

Suomi osallistuu kansainväliseen kriisinhallintaan muun muassa kriisien ehkäisemiseksi ja rajoittamiseksi, niistä aiheutuneiden tuhojen korjaamiseksi ja yhteiskunnan häiriöttömän toiminnan palauttamiseksi sekä suuronnettomuuden tai luonnonkatastrofin aiheuttamien tuhojen lieventämiseksi. Konfliktien ennalta ehkäisemiselle ja ennakoivalla toiminnalle annetaan nykyistä enemmän painoarvoa. Tämän vuoksi kohdassa sallittaisiin tiedustelu myös kriisinhallintaoperaatiota tai siihen osallistuvia henkilöitä vaarantavasta toiminnasta. Tietoa voitaisiin hankkia esimerkiksi ennakollisesti kriisinhallintaoperaatioalueen olosuhteista ja alueelle lähetettävien asiantuntijoiden turvallisuuteen vaikuttavista tekijöistä. Tiedonhankintaa näistä seikoista saisi luonnollisesti jatkaa myös operaation aikana. Kohdan perusteella hankitut tiedoilla olisi olennainen yhteys kohdan 8 perus-

teella hankittaviin tietoihin. Tiedonhankinnan perusteena olisi Yhdistyneiden kansakuntien peruskirja sekä puolustusvoimista voimista annetun lain 2 §:n 3 tai 4 kohdassa tarkoitettu tehtävä.

Pykälän 9 kohdan mukaan sotilastiedustelun kohteen voisi olla kansainvälisten kriisinhallintaoperaatioiden turvallisuuteen kohdistuvat uhkat. Kohdan tarkoittama tiedonhankinta perustuisi puolustusvoimista annetun lain 2 §:n 4 kohtaan sekä sotilaallisesta kriisinhallinnasta annetun lain (211/2006) 1 §:ään, jonka mukaan Suomi voi osallistua sotilaalliseen kriisinhallintaan muun muassa kansainvälisen rauhan ja turvallisuuden ylläpitämiseksi tai palauttamiseksi taikka humanitaarisen avustustoiminnan tukemiseksi tai siviiliväestön suojaamiseksi. Siviilikriisinhallinnasta säädetään siviilihenkilöstön osallistumisesta kriisinhallintaan annetussa laissa (1287/2014).

Tietoa hankittaisiin etenkin kriisinhallintaoperaation alueen olosuhteista ja suomalaisten kriisinhallintajoukkojen turvallisuuteen vaikuttavista tekijöistä, kuten siitä, kohdistuuko kriisinhallintaoperaation suomalaisiin asiantuntijoiden väkivaltaisen iskun uhkaa sekä missä, milloin ja kenen toimesta mahdolliset väkivallanteot olisi tarkoitus toteuttaa. Sotilaallisessa kriisinhallintaoperaatiossa suoritettava tiedonhankinta olisi tapahduttava kriisinhallintaoperaatiota johtavan organisaation määräysten ja ohjeistuksen mukaisesti.

Tiedonhankinta kriisinhallintaoperaation olosuhteista voisi olla myös ennakollista, jolloin tietoa hankittaisiin kriisinhallintaoperaatioon osallistumiseen liittyvän päätöksenteon tueksi alueella vallitsevista olosuhteista.

Pykälän 10 kohta liittyisi vireillä olevaan puolustusvoimista annetun lain muuttamiseen (HE 94/2016 vp.) Puolustusvoimien tehtävistä. Esityksen mukaan valtionjohto voisi päättää avun antamisesta toiselle valtiolle apua tietyissä tilanteissa, kuten terrori-iskun, luonnononnettomuuden, suuronnettomuuden tai muun vastaavan tapahtuman johdosta. Puolustusvoimien tiedon tarve perustuisi HE 94/2016 ehdotettuun puolustusvoimista annetun lain uuteen 2 §:n 3 kohtaan.

Vaikka tietoa saataisiin ensisijaisesti avunpyynnön esittäneeltä taholta, tietoa olisi tarve voida hankkia esimerkiksi luonnononnettomuusalueen kartoittamiseksi ja lähetettävän avun saattamiseksi tarkoituksen mukaisesti perille mahdollisimman turvallisesti. Lisäksi kyse voisi olla vaativista monikansallisista evakuointioperaatioista, erityisesti, kun kyse on Euroopan unionin kansalaisten evakuoinnista ja evakuointitehtävän toteuttaminen muutoin esimerkiksi kansainvälistä pelastustoimintaa hyödyntäen ei ole mahdollista.

Tilanteet saattaisivat myös liittyä Euroopan unionin taisteluosastojen ja Naton nopean toiminnan joukkojen käyttämiseen muussa kuin sotilaallisessa kriisinhallinnassa. Näiden joukkojen käyttö on mahdollista kaiken tyyppisissä kriiseissä, myös luonnononnettomuuksissa tai ihmisen aiheuttamissa onnettomuuksissa.

Kohdan mukaan sotilastiedustelua voitaisiin tehdä myös Lissabonin sopimuksen avunantolausekkeen mukaisen päätöksenteon tueksi kansainvälisessä yhteistyössä aseellisen hyökkäyksen torjunnassa. Puolustusvoimat pystyisi hankkimaan ennakolta tietoa operaatioon osallistumiseen liittyvistä seikoista, ennen kuin päätös osallistumisesta Suomen rajojen ulkopuolella suoritettavaan operaatioon tehdään.

Hankittavilla tiedoilla pyrittäisiin tukemaan myös muita suomalaisia viranomaisia näiden kansainvälisessä toiminnassa.

Yhtenä esimerkkinä kohdan tarkoittamista tilanteista voidaan mainita suomalaisten erityisosaajien lähettäminen ulkomaisiin erityistehtäviin. Suomi voi tarvittaessa lähettää kansainvälisiin tehtäviin erityisosaajia tuhoamaan joukkotuhoaseita sekä analysoimaan niiden käyttöä. Tieto aseiden kehittämisestä ja leviämisestä antaisi Suomelle mahdollisuuden tulevaisuudessakin olla joukkotuho-

aseiden tuhoamisessa ja analysoinnissa kansainvälisessä kärjessä sekä kehittää tätä erityisosaamista.

Joukkotuhoaseiden tuhoamiseen liittyvissä erityisoperaatioissa tiedustelutiedolla olisi erityinen tarve esimerkiksi toimintaympäristöstä ja turvallisuusuhista operaation valmisteluvaiheessa. Operaation alettua tiedustelutiedolla voitaisiin lisäksi varmistaa operaation tavoitteiden saavuttaminen, esimerkiksi tuhottavaan materiaaliin kohdistuvien turvallisuusuhkien kehittymisestä.

Avun pyyntö voisi koskea myös osallistumista tiedonhankintayhteistyöhön muiden valtioiden viranomaisten kanssa. Tilanteissa voisi olla kyse suureen joukkoon ihmisiä kohdistuneesta iskusta. Kansainvälisestä yhteistyöstä säädettäisiin tarkemmin jäljempänä erikseen.

5 §. *Suhteellisuusperiaate.* Pykälän mukaan sotilastiedusteluviranomaisen toimenpiteiden olisi oltava puolustettavia suhteessa tiedonhankinnan merkittävyyteen. Suhteellisuusperiaatteen tavoitteena on tiedonhankinnan kohteena olevien henkilöiden oikeuksiin puuttumisen rajaaminen asian laadun perusteella, mutta toisaalta viranomaisvoimavarojen tarkoituksenmukainen kohdentaminen. Suhteellisuusperiaate ohjaisi osaltaan kaikkea tiedustelutoimintaa. Suhteellisuusperiaate pitäisi sisällään sen, että tiedonhankintatoimenpiteiden mitoittamisessa ja henkilöiden oikeuksiin puuttumisessa on otettava huomioon uhkan merkittävyys maanpuolustukselle ja kansalliselle turvallisuudelle sekä uhkan toteutumisen todennäköisyys. Todennäköisesti toteutuvasta vakavasta Suomen maanpuolustukseen tai kansalliseen turvallisuuteen kohdistuvasta uhkasta olisi tarkoituksen mukaista hankkia tietoja laajemmin ja tuntuvammin oikeuksiin puuttuvalla keinolla.

Tiedonhankintatoimenpidettä olisi arvioitava sillä tavoiteltavaan päämäärää nähden. Tiedonhankintatoimenpiteiden mitoittamiseen vaikuttaa esimerkiksi se, kuinka oleellinen merkitys tietyllä toimenpiteellä on uhkaan liittyvien tietojen hankinnan kannalta.

Suhteellisuusperiaate sisältäisi myös perustuslain vaatimuksen perusoikeuksien ja ihmisoikeuksien turvaamisen toteuttamisesta. Tiedonhankinnan tavoitteiden saavuttamisessa tulisi kunnioittaa tiedonhankinnan kohteeseen liittyvien henkilöiden perus- ja ihmisoikeuksia. Tiedustelun mahdollisimman hyvä kohdentaminen toteuttaisi suhteellisuusperiaatetta. Tiedustelun tulisi kaikissa tilanteissa aina olla mahdollisimman kohdennettua ja perus- ja ihmisoikeuksia kunnioittavaa. Sotilastiedustelulainsäädännön nojalla tapahtuva harkinta tulisi olla aina perus- ja ihmisoikeusmyönteisesti.

Suhteellisuusperiaatteen mukaisesti kokonaisharkinnassa on kiinnitettävä huomiota toiminnan tai uhkan vakavuuteen ja sen mahdollisesti aiheuttamaan vahinkoon sekä tiedustelutoiminnan käytöstä aiheutuvaan yksityiselämän tai luottamuksellisen viestin salaisuuden loukkaukseen.

Tiedustelun toimenpiteen käyttöä harkittaessa voitaisiin ottaa huomioon myös toimenpiteiden kohteena olevan henkilön oikeuksiin puuttumisen kesto. Jos sotilastiedustelun viranomaisella olisi jo tieto tarkasta kohteesta, tilanteessa saattaisi tulla kyseeseen enemmän kohteen oikeuksiin puuttuva keino, jos muiden keinojen käyttö sinänsä puuttuisi henkilön oikeuksiin vähemmän, mutta samalla muodostaisi pitkäkestoisemman puuttumisen tämän oikeuksiin.

Suhteellisuusperiaatteen kohdalla on huomioitava se, ettei sillä ole samanlaista merkitystä valtiolliseen toimijaan, kuten sotilaallisen toimijaan kohdistuvassa tiedustelussa. Vieraan valtion viranomaisorganisaation viestintä ei nauti perusoikeussuojaa. Suhteellisuusperiaatteella saattaisi kuitenkin olla merkitystä kokonaisharkinnassa arvioitaessa sitä, kuinka paljon muuta viestintään kuin viranomaisviestintää tiedustelun kohteeksi joutuisi kulloisessakin tiedonhankinnan tapauksessa.

Suhteellisuusperiaate liittyisi läheisesti vähimmän haitan periaatteeseen molempien pyrkiessä mahdollisimman vähäiseen puuttumiseen henkilön oikeuksiin.

6 §. *Vähimmän haitan periaate.* Vähimmän haitan periaate vaikuttaisi suhteellisuusperiaatteen kanssa samansuuntaisesti. Pykälän tarkoittaman vähimmän haitan periaatteen mukaan tiedonhankintatoimivaltuuden käytöllä kenenkään oikeuksiin ei saisi puuttua enempää kuin on välttämätöntä tiedustelun käytön tarkoituksen saavuttamiseksi. Sotilastiedustelulla ei saisi myöskään aiheuttaa kenellekään tarpeettomasti vahinkoa tai haittaa. Tiedonhankinnan tavoitteeseen pääsemiseksi viranomaisen olisi ensisijaisesti käytettävä sitä toimivaltuutta, joka vähiten puuttuu perus- ja ihmisoikeuksiin. Toimivaltuuden riittävyys arvioitaisiin aina tapauskohtaisesti.

Vähimmän haitan periaatteen mukaisesti tiedonhankintatoimivaltuuksista olisi aina valittava ensisijaisesti se, joka on kohdennettavissa parhaiten kohteeseen, josta tiedustelutehtävän päämäärän kannalta tarkoituksen mukaiset tiedot olisivat saatavissa. Periaatteen soveltamisessa olisi otettava huomioon myös toimivaltuuden käytön kohdentaminen. Mahdollisimman kohdennettu tiedonhankinta ehkäisee osaltaan myös sivullisille aiheutuvia negatiivisia vaikutuksia, kuten pelkoa siitä, että heidän yksityisyyttään loukataan..

Vähimmän haitan periaatteella turvataan osaltaan perus- ja ihmisoikeuksien toteutuminen. Perusoikeuksien ja ihmisoikeuksien soveltaminen tuo entistä selkeämmin myös viranomaisten harkintavallan osaksi viranomaisen ratkaisuharkintaa toimivaltuuksien käyttötilanteessa. Sotilastiedustelu-viranomaisen toimivaltuussäännösten perusoikeusmyönteisestä soveltamisesta perusoikeusjärjestelmän periaatteineen voidaan myös nähdä rajoittavan harkitsijan oikeudellisen harkinnan ulkopuolelle jäävää harkintavaltaa ja tätä kautta mielivaltaa.

Vähimmän haitankin osalta olisi otettava huomioon valtiollisen ja ei-valtiollisen toimijan väliset erot perusoikeussuojassa. Vieraan valtion viranomaisorganisaation ei voida katsoa nauttivan perusoikeussuojaa. Tästä johtuen tunnistettuun vieraan valtion viranomaisorganisaatioon saataisiin kohdistaa merkittävämpiä tiedustelun keinoja kuin yksityiseen henkilöön. Kokonaisharkinnassa olisi kuitenkin huomioitava se, missä määrin tiedustelun keinon käyttäminen kohdistuisi muihin kuin vieraan valtion viranomaisorganisaatioon. Lisäksi vieraan valtion viranomaisorganisaation edustaja voi olla osan ajasta myös yksityisenä henkilönä, jolloin hän nauttii perusoikeussuojaa.

7 §. *Tarkoitussidonnaisuuden periaate.* Pykälän mukaan sotilastiedustelun toimivaltuuksia saa käyttää vain säädettyyn tarkoitukseen.

Periaate liittyisi siihen, että sotilastiedustelun toimivaltuuden käytön tulee perustua nimenomaiseen säännökseen. Puututtaessa yksilön oikeuksiin tai velvollisuuksiin säännöksen tulee olla laissa. Tarkoitussidonnaisuuden periaate koskisi kaikkea sotilastiedustelutoimintaa.

8 §. *Syrjinnän kielto.* Lakiin otettaisiin voimassa olevaan muiden viranomaisten toimivaltuussääntelyyn nähden uusi periaate. Lain 8 §:ssä säädettäisiin syrjimättömyyden periaatteesta. Periaatetta voidaan pitää perusteltuna tiedustelutoiminnassa sen luonteen vuoksi. Lisäksi periaate vahvistaisi perustuslain 6 §:n 2 momentin yhdenvertaisuusperiaatetta tiedustelutoiminnassa.

Pykälän mukaan sotilastiedustelun toimenpiteiden kohdentaminen olisi toteutettava mahdollisimman syrjimättömästi niin, ettei tiedustelutoimintaa voida kohdentaa ainoastaan alkuperää, kansalaisuutta, kieltä, uskontoa, vakaumusta, mielipidettä, poliittista toimintaa, ammattiyhdistystoimintaa, perhesuhteita, seksuaalista suuntautumista koskeviin tietoihin. Kohdentamisessa olisi käytettävä aina tiettyjä henkiöitä tai henkilöryhmiä koskevia muita tietoja. Tiedustelutoiminnasta pitäisi aina lähtökohtaisesti kohdentaa aina tiettyyn henkilöön tai henkilöryhmään, jolloin kohdentaminen ei voisi tapahtua laajaan ihmisryhmään kohdistuvin perustein.

Kohdentaminen edellä tarkoitetuilla tiedoilla saattaisi kuitenkin olla tietyissä tilanteissa välttämätöntä edellä tarkoitetuilla tiedoilla, kuten esimerkiksi kansalaisuuden perusteella. Tämä edellyttäisi kuitenkin objektiivisia ja riittäviä perusteita.

Kiellolla ehkäistäisiin vähemmistöjen syrjintää ja sen aiheuttamaa nöyryyttämisen ja leimatuksi tulemisen tunnetta vähemmistöjen edustajissa.

9 §. *Määritelmät.* Pykälässä määriteltäisiin lain keskeiset määritelmät. Pykälän 1 kohdassa määriteltäisiin kytkennän suorittaja. Kytkennän suorittajalla tarkoitettaisiin julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain (10/2015) 6 §:ssä tarkoitettua verkko- ja infrastruktuuripalvelujen tuottajaa eli Suomen Erillisverkot Oy -nimistä osakeyhtiötä. Osakeyhtiö olisi valtion täysin omistama edellä tarkoitetun lainkohdan perusteella.

Pykälän 2 kohdassa määriteltäisiin sijaintitieto. Määritelmä vastaisi tietoyhteiskuntakaaren 3 §:n 19 kohtaa. Sijaintitiedolla tarkoitettaisiin viestintäverkosta tai päätelaitteesta saatavaa tietoa, joka ilmaisee liittymän tai päätelaitteen maantieteellisen sijainnin ja jota käytetään muuhun tarkoitukseen kuin viestinnän välittämiseen. Sijaintitieto voitaisiin myös saada päätelaitteesta, jotta epäselvyyttä ei ilmenisi siitä, sovelletaanko sijaintitietoihin liittyvää sääntelyä myös esimerkiksi satelliittipohjaiseen paikannukseen. Sijaintitiedoilla voidaan ilmaista muun muassa liittymän tai päätelaitteen leveysaste, pituusaste ja korkeus, matkan suunta, sijainnin tarkkuus, se osa verkkoa, jossa liittymä tai päätelaite paikannetaan tietyllä hetkellä sekä sijaintitiedon tallentamisen ajankohta. Välitystiedot sisältävät myös esimerkiksi tukiasemakohtaisia sijaintitietoja. Se, pidetäänkö sijainnin ilmaisevaa tietoa välitystietona vai sijaintitietona ratkeaa tiedon käyttötarkoituksen perusteella. Jos sijainnin ilmaisevaa tietoa käytetään viestinnän toteuttamisessa, kysymyksessä on välitystieto. Tällöin liittymän tai päätelaitteen sijainnin ilmaiseva tieto on välttämätön viestinnän toteuttamiseksi.

Pykälän 3 kohdassa määriteltäisiin teleyritys. Määritelmä vastaisi tietoyhteiskuntakaaren 3 §:n 27 kohtaa. Teleyrityksellä tarkoitettaisiin sitä, joka tarjoaa verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille eli harjoittaa yleistä teletoimintaa. Ehdotetussa teleyritysmääritelmässä teleyrityksen asema määräytyisi toiminnan luonteen perusteella. Sillä, onko kyseessä yritys vai esimerkiksi kaupunki, ei tulisi olla teleyritys-aseman kannalta merkitystä. Toiminnan vastikkeellisuudella ei ole myöskään merkitystä.

Yleisellä teletoiminnalla tarkoitetaan edelleen verkko- tai viestintäpalvelun tarjoamista käyttäjäpiirille, jota ei ole ennalta rajattu. Käyttäjäpiirin rajaamattomuuden arvioinnissa on otettava huomioon esimerkiksi verkon ja palvelun luonne, verkon ja käyttäjäpiirin laajuus ja käyttäjäksi pääsemisen edellytysten rajoittavuus.

Yrityksen tai muun yhteisön omaa tarvettaan varten ylläpitämä viestintäpalvelu voidaan katsoa selkeästi etukäteen rajatulle käyttäjäpiirille tarjotuksi. Esimerkiksi yrityksen työntekijöilleen ja koulun opiskelijoilleen tarjoamia palveluja ei käyttäjäpiirin lukumääräisestä suuruudesta tai verkon laajuudesta riippumatta voida pitää yleisenä teletoimintana.

Muita esimerkkejä rajatusta käyttäjäpiiristä ovat taksikeskuksen ja taksien sisäinen viestintäpalvelu taksien välittämiseksi tai vastaava bussiliikenteen sisäinen viestintäpalvelu. Edellä kuvatuissa esimerkeissä käyttäjäpiiriin kuuluminen liittyy selvästi yhteisön jäsenyyteen, joka on tiukasti rajattu. Esimerkeissä on myös selvää, että viestintäpalvelu ei ole syy yhteisöön liittymiselle.

Edellä tarkoitetut esimerkit eivät siis ole tässä laissa tarkoitettuja teleyrityksiä eivätkä näin ollen näitä tahoja koskisi tässä laissa määritellyt velvollisuudet.

Jos palvelun käyttäjäpiiri sen sijaan muodostuu yhteisöstä, joka on hyvin laaja tai johon liittyminen on hyvin vapaata, käyttäjäpiiriä ei voida pitää ennalta rajattuna. Esimerkiksi kahvilan tai hotellin asiakkailleen tarjoama viestintäpalvelu koskee sinänsä hyvin vapaasti valikoituvien asiakkaiden piiriä, mutta käyttäjäpiirin laajuus on näissä tapauksissa niin pieni, että kokonaisuutena palvelun tarjontaa ei yleensä voida katsoa yleiseksi teletoiminnaksi. Sen sijaan esimerkiksi se, että viestintäpalvelu toimii vain tietyllä sovelluksella tai tietyllä päätelaitteella, ei lähtökohtaisesti tee käyttäjä-

piiristä ennalta rajattua. Samoin verkon tai palvelun saatavuutta vain tietyllä maantieteellisellä alueella ei yksinään voida pitää laissa tarkoitetulla tavalla ennalta rajatun käyttäjäpiirin tunnusmerkkinä. Sovellussidonnaiset viestintäpalvelut ovat tyypillisiä esimerkiksi internetissä tarjottavissa puhe- ja pikaviestintäpalveluissa ja sovellukset ovat muiden tuotteiden tavoin vapaasti käyttäjien hankittavissa. Samoin on arvioitava esimerkiksi päätelaitteisiin kuuluvia matkaviestinyrityksestä riippumattomia viestintäpalveluja, joita voivat olla esimerkiksi pikaviestintä, sähköposti ja teksti- tai multimediaviestit.

Sovellussidonnaisia viestintäpalveluja lähellä ovat erilaiset verkkoyhteisöjen ja sosiaalisen median viestintäpalvelut, joissa yhteisöön ja viestintäpalvelun käyttäjäksi liittyminen on siinä määrin vapaata, että yhteisön jäsenyyttä ei yksinomaan voida pitää käyttäjäpiirin ennalta rajaamisena.

Verkkojen kannalta voidaan joutua arvioimaan ennalta rajaamatonta käyttäjäpiiriä maantieteelliseltä peitoltaan vähäisissä tai hallinnointitavaltaan uudenlaisissa verkoissa. Esimerkiksi lähiverkot, kuten WLAN-verkot, joissa tarjotaan internetyhteyspalvelua, voivat olla alueellisesti varsin suppealla alueella, mutta jos niiden käyttäjäpiiri valikoituu vapaasti, maantieteellinen peitto ei yksinään tee käyttäjäpiiristä ennalta rajattua. Joukkoviestintäverkon teleyrityksiä määriteltäessä ennalta rajaamattoman käyttäjäpiirin arvioiminen ei ole samalla tavalla tulkinnanvaraista kuin kohdeviestinnässä, sillä joukkoviestinnän viestintäpalvelu eli ohjelmistojen siirtäminen tai lähettäminen on jo lähtökohtaisesti luonteeltaan rajaamatonta. Sen sijaan joukkoviestintäverkossa joudutaan arvioimaan teletoiminnan ja sisältöihin liittyvän ohjelmistotoiminnan eli televisio- tai radiotoiminnan tai tilausohjelmapalvelun rajanvetoa.

Kytkennän suorittajan tehtävät olisivat luvussa tarkoitettujen lupien toimeenpanemista, eli kytkennän suorittaja ohjaisi jäljempänä tässä luvussa tarkoitetun luvan mukaisesta viestintäverkon osasta tulevan tietoliikenteen Puolustusvoimien tiedustelulaitokselle, jonka jälkeen Puolustusvoimien tiedustelulaitos hankkisi luvan mukaisesti tietoliikenteestä tiedot.

Pykälän 4 kohdassa määriteltäisiin tiedonsiirtäjä. Tiedonsiirtäjällä tarkoitettaisiin sitä, joka omistaa tai hallitsee Suomen rajan ylittävää viestintäverkon osaa. Määritelmällä on merkitystä sen varmistamiseksi, että tässä laissa säädettäväksi ehdotetut velvollisuudet avustaa viranomaisia tietoliikennetiedustelun toteuttamisessa kohdentuvat oikeaan tahoon. Velvollisuuksissa avustaa tietoliikennetiedustelun toteuttamisessa olisi kyse yhtäältä tämän lain 94 §:ssä säädettäväksi ehdotetusta velvollisuudesta antaa ilman aiheetonta viivytystä Puolustusvoimien tiedustelulaitokselle tietoliikennetiedustelun kohdentamiseksi tarpeelliset hallussa olevat tiedot. Toiseksi kyse olisi 94 §:ssä määritellystä myötävaikuttamisvelvollisuudesta, jonka asettamisella varmistettaisiin se, että rajan ylittävään viestintäverkon osaan, käytännön tasolla tiedonsiirtoyhteyteen, voidaan rakentaa niin sanottu liityntäpiste, eli tietoliikennetiedustelun toteuttamispiste. Liityntäpisteiden kautta tuomioistuimen luvassa tarkoitetusta viestintäverkon osasto voitaisiin siirtää tietoliikenne Puolustusvoimien tiedustelulaitoksen jatkokäsittelyyn. Kytkennän tekeminen ja sitä seuraava tietoliikenteen siirtäminen olisi osa tietoliikennetiedustelun teknistä toteuttamista. Tietoliikenteeseen kohdistuvassa tiedustelussa tuomioistuimelle esitettävässä lupavaatimuksessa olisi mainittava se tiedonsiirtäjä, jonka omistamasta tai hallinnoimasta viestintäverkon osasta tietoliikenne ohjattaisiin Puolustusvoimien tiedustelulaitokselle.

Määritelmässä käytettäisiin viestintäverkon määritelmää, jonka takia tiedonsiirtäjän määritelmä olisi tekniikkaneutraali.

Tiedonsiirtäjän käsite kattaisi sekä rajan ylittävän viestintäverkon osan omistajan että rajan ylittävän viestintäverkon osan haltijan. Haltijalla tarkoitettaisiin sellaista koti- tai ulkomaista yritystä tai yhteisöä, joka tosiasiassa hallitsee rajan ylittävää viestintäverkkoa tai sen osaa esimerkiksi vuokrattuaan sen operoitavakseen omistajana olevalta yritykseltä tai yhteisöltä. Tiedonsiirtäjänä pidettäisiin näin ollen tahoa, jolla on tekniset edellytykset päättää siitä, missä viestintäverkon osassa

jokin tietoliikenne kulkee. Tietoteknisesti tarkasteltuna tiedonsiirtäjä olisi se taho, joka ohjaa verkkoliikennettä ns. OSI-viitemallin (Open Systems Interconnection Reference Model) kahden alimman kerroksen, fyysisen sekä siirtoyhteyskerroksen, tasolla. Tiedonsiirtäjän käsitteen ulkopuolelle jäisi tällöin sellainen yritys tai yhteisö, joka on vuokrannut tiedonsiirtäjältä käyttöönsä tiedonsiirtokapasiteettia ilman tietoteknistä mahdollisuutta vaikuttaa itsenäisesti siihen, missä verkon osassa mikäkin osa tietoliikennettä kuljetetaan.

Määritelmä olisi tarkempi kuin esimerkiksi tietoyhteiskuntakaaren 3 §:n 36 kohdassa tarkoitettu viestinnän välittäjä. Tiedonsiirtäjä ei käsittäisi esimerkiksi erilaisten sähköisten palveluiden tarjoavia yrityksiä ja määritelmän piiriin lukeutuisi määrällisesti vähemmän eri tahoja, tämän esityksen aikaan noin kymmenkunta.

Pykälän 5 kohdan mukaan sotilastiedustelulaissa tiedustelumenetelmillä tarkoitettaisiin 4 ja 5 luvuissa säädettyjä toimivaltuuksia. Sotilastiedustelussa käytetään myös muita tiedustelumenetelmiksi luettavia tiedonhankintakeinoja, kuten avointen lähteiden tiedustelu, kuvaustiedustelu ja geotiedustelu, joista ei ole tarpeen säätää erikseen.

Pykälän 6 kohdassa määriteltäisiin tietoliikenteen tekniset tiedot. Tietoliikenteen teknisillä tiedoilla tarkoitettaisiin viestiin liittyviä muita tietoja kuin viestin merkityksellistä sisältöä.

Tietoliikenteen teknisiä tietoja ovat muun muassa viestin välitystiedot. Välitystiedolla tarkoitetaan oikeus- tai luonnolliseen henkilöön yhdistettävissä olevaa tietoa, jota viestinnän välittäjä käsittelee viestien välittämiseksi. Tietoliikennetiedustelussa sisällöksi tulkittaisiin lähettäjän vastaanottajalle tarkoittama semanttinen sisältö, kun taas tekniseksi tiedoksi katsottaisiin esimerkiksi viestin ohjaustieto, mikä on tietoverkolle sekä lähettävälle ja vastaanottavalle tietojärjestelmälle tarkoitettu ohje, komento tai muu metatieto, jolla vaikutetaan viestin kuljetukseen ja ohjaamiseen verkossa sekä tietojärjestelmässä. Muista tietoliikenteen teknisiä tietoja olisivat tilaajaan tai käyttävään yhdistettävissä olevia viestinä koskevia tietoja, jota viestintäverkoissa käsitellään viestin siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi, viestintäverkosta tai päätelaitteesta saatavia sijaintitietoja, joka ilmaisee liittymän tai päätelaitteen maantieteellisen sijainnin ja jota käytetään muuhun kuin viestin välittämiseen.

Tietoliikenteen tekniset tiedot käsittäisivät myös tietyissä tilanteissa muut tekniset tiedot, kuten erilaiset salaustekniikat. Etenkin suuret organisaatiot, jotka ovat tiedustelun kannalta olennaisia, ovat saattaneet kehittää omia tietoliikenteen salaustekniikoita, jotka ovat ainoastaan tekniikan kehittäneen organisaation käytössä. Salaustekniikasta kertovat tiedot eivät ilmaise vielä itsessään viestin merkityksellistä sisältöä, vaan ovat viestin teknistä tietoa.

Viestin merkityksellisellä sisällöllä tarkoitettaisiin tässä yhteydessä viestin ymmärrettävää tekstimuotoa, joka on esimerkiksi viestin salaus purkaen saatettu johonkin kielellisesti ymmärrettävään luettavaan muotoon.

Oman erityiskysymyksensä tietoliikenteen joukossa muodostavat verkon sisäinen signalointiliikenne, suoranainen hyökkäysliikenne sekä esineiden Internetin ohjausliikenne. Tietoliikenneverkossa ei siis tosiasiallisesti ole kyse vain viestiverkosta, jossa kulkisi ainoastaan viestisisältöä, vaan verkossa kulkee myös verkon toimintaan vaikuttavia signalointisanomia, muiden digitaalisten järjestelmien ohjausliikennettä sekä suoranaista verkon toiminnan lamauttamiseen tähtäävää hyökkäysliikennettä. Internetverkon keskeisiä suunnitteluperiaatteita ovat tehokkuus ja vikasietoisuus. Kaikki liikenne, yhtä lailla viestintä kuin verkon sisäinen signalointikin kuljetetaan saman viitekehyksen mukaisesti määritellyillä liikenneprotokollilla. Signalointisanomia ovat esimerkiksi internetin kontrollisanomat (ICMP), joilla verkon laitteet voivat välittää toisilleen tilannetietoa jonkin linkin ruuhkaisuudesta sekä nimipalvelukyselyt, joilla viestisovellus selvittää mihin verkko-osoitteeseen jollekin domain-nimelle tarkoitettu viesti lähetetään. On selvää, ettei signalointiliikennettä voida pitää luot-

tamuksellisen viestin salaisuuden suojaa nauttivana viestintänä. Toisaalta signalointiliikenteelle on ominaista, että se on tunnistettavissa otsikkotiedon perusteella, jolloin ensimmäisenä hakukriteerinä voidaan aina pitää otsikkotietoa eikä erityistä sisältöhaun mahdollistavaa poikkeussäännöstä tarvita.

Esineiden internet tuo verkkoon ohjausliikennettä, jota ei sitäkään voida sinällään pitää viestintänä. Kuitenkaan sitä johtopäätöstä ei voida tehdä, että ilman ihmisen myötävaikutusta tapahtuva laitteiden ja ohjelmistojen välinen tietoliikenneliikenne ei missään tilanteessa olisi viestintää. Tyypillinen esimerkkitapaus ohjelmistojen välisestä viestinnästä olisi pörssikauppaa käyvä robottiohjelmisto, jonka transaktioihin liittyy henkilön intentio salassa pidettävästä viestinnästä. Siksi esineiden ohjausliikenteelle ei ole haluttu tehdä sisältöhaun mahdollistavaa poikkeussäännöstä tässä laissa.

Pykälän 7 kohdassa määriteltäisiin tunnistamistieto. Tunnistamistiedon määritelmä vastaisi asiallisesti voimassa olevan poliisilain tunnistamistieto. Tunnistamistieto määriteltäisiin tietoyhteiskuntakaaren (917/2014) 3 §:n 7 kohdassa tarkoitettuun tilaajaan tai mainitun pykälän 30 kohdassa tarkoitettuun käyttäjään yhdistettävissä olevaa viestiä koskevaksi tiedoksi. Tunnistamistiedon käsite eroaisi näin ollen tietoyhteiskuntakaaressa tarkoitetusta välitystiedosta.

Pykälän 8 kohdassa määriteltäisiin valtiollinen toimija. Valtiollisella toimijalla tarkoitettaisiin vieraan valtion viranomaista tai sellaiseen rinnastuvaa toimijaa. Kuten aiemmin tässä esityksessä on todettu, vieras valtion viranomainen ei nauti perusoikeussuojaa. Vieraan valtion viranomaisen edustajat olisivat myös käsitteen piirissä. Vieraan valtion viranomaiseen rinnastuva taho kattaisi tilanteet, joissa esimerkiksi valtiossa ei olisi viranomaiseksi tunnistettavaa tahoa, mutta joka hoitaisi valtion asioita, kuten viranomainen. Tahoa voitaisiin arvioida esimerkiksi sitä kautta, voisiko Suomi tai suomalainen viranomainen tehdä sopimuksen tällaisen tahon kanssa tai voisiko taho olla kansainvälisen järjestön toiminnassa mukana.

Toisaalta valtiollinen toimija voisi olla myös yksityinen taho, kuten yritys, muu ryhmittymä tai jopa yksittäinen henkilö. Tällöin olennaista on arvioida esimerkiksi sitä, toimiiko tällainen taho valtion määräysvallassa tai sen ohjauksessa taikka ottaako valtio tällaisen tahon toiminnasta vastuun itselleen. Esimerkiksi kaupalliseen yksityisoikeudelliseen sopimukseen perustuvia yrityksen velvollisuuksia valtiollista toimijaa kohtaan ei voida pitää sellaisena, minkä perusteella yritystä voitaisiin pitää valtiollisena toimijana. Huomiota olisikin kiinnitettä esimerkiksi siihen, minkälainen tosiasiallinen määräysvalta ja ohjaus valtiollisella toimijalla olisi yritykseen.

Muiden ryhmittymien osalta edellä sanotun lisäksi huomiota olisi kiinnitettävä siihen, kuinka järjestäytynyttä toiminta on, kuinka merkittävät resurssit ryhmittymällä on käytössää esimerkiksi aseellisen hyökkäyksen tekemiseksi ja voisiko tällainen hyökkäys tekona rinnastua vaikutuksiltaan vieraan valtion tekemäksi sekä pyrkiikö ryhmittymä toimimaan valtion tavoin.

Pykälän 9 kohdan mukaan viestintäverkolla tarkoitettaisiin toisiinsa liitetyistä johtimista sekä laitteista muodostuvaa järjestelmää, joka on tarkoitettu viestien siirtoon tai jakeluun johtimella, radioaalloilla, optisesti tai muulla sähkömagneettisella tavalla.

Oleellista määritelmän kannalta on järjestelmän käyttötarkoitus viestien siirtoon tai jakeluun, sähkömagneettinen tekninen toteutustapa ja teknologianeutraalius. Viestintäverkkoon kuuluu esimerkiksi siirtojärjestelmiä sekä kytkentä- tai reitityslaitteistoja ja muita välineitä – myös verkkoelementtejä, jotka eivät ole aktiivisia. Määritelmä on yläkäsite muille laissa käytetyille viestintäverkoille, joita ovat ehdotuksen mukaan joukkoviestintäverkko, maanpäällinen joukkoviestintäverkko, kaapelitelevisioverkko ja matkaviestinverkko.

Pykälän 10 kohdan mukaan yhteisötilaajalla tarkoitettaisiin tietoyhteiskuntakaaren 3 §:n 41 kohdassa tarkoitettua yhteisötilaajaa. Lainkohdan mukaan yhteisötilaajalla tarkoitetaan viestintäpalve-

lun tai lisäarvopalvelun tilaajana olevaa yritystä ja yhteisöä, joka käsittelee viestintäverkossaan käyttäjien viestejä, välitystietoja tai sijaintitietoja.

10 §. *Tiedustelumenetelmien käytön edellytykset.* Pykälässä 1 momentissa säädettäisiin kaikille tiedustelumenetelmille yleisistä edellytyksistä, joidenka olisi täytyttävä ennen kuin tiedustelumenetelmää voitaisiin käyttää. Kakkia säänneltäviä tiedustelumenetelmiä koskevana yhteisenä edellytyksenä olisi, että sillä voidaan olettaa saatavan tiedustelutehtävän kannalta tarpeellisia tietoja. Kyse olisi tuloksellisuus vaatimuksesta, jolloin tiedustelumenetelmän käytön odotusarvona on sen hyödyllisyys.

Tiedustelumenetelmien käytön edellytykset olisivat porrasteiset. Tiedustelumenetelmien käytön edellytysten porrasteisuus vastaisi sitä, mitä sotilaskurinpidosta ja rikosrojunnasta puolustusvoimista annetun lain 89 §:ssä ja poliisilain 5 luvun 2 §:ssä säädetään salaisista tiedonhankintakeinoista.

Tiedustelumenetelmien käytölle, joka rajoittaisi voimakkaasti kohteena olevan henkilön perusoikeuksia, olisi säädetty lisäedellytyksiä tiedustelumenetelmäkohtaisesti. Tiedusteluprosessissa tiedustelumenetelmiä käytettäisiin täysin tunnistamattoman kohteen osalta niin, että prosessi alkaisi lievempiä tiedustelumenetelmiä käyttäen. Toisaalta, jos sotilastiedustelun viranomaisella olisi lähtötilanteessa tiedustelutehtävän kohteen kannalta riittävän tarkat tiedot käytössään, kyseeseen saattaisi tulla enemmän perusoikeuksiin puuttuva toimivaltuuksien käyttö. Tätä ilmentäisi laissa eräille toimivaltuuksille asetettu edellytys, jonka mukaan tiedustelumenetelmän käytöllä (telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, henkilön tekninen seuranta, tekninen laitetarkkailu, tietolähteen ohjattu käyttö ja paikkatiedustelu) olisi voitava olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Peitetoiminnan ja valeoston käyttäminen edellyttäisivät lisäksi, että menetelmän käyttö on välttämätöntä tiedon saamiseksi sotilastiedustelun kohteesta.

Tiedustelumenetelmien käyttöä harkittaessa olisi otettava aina huomioon tiedustelumenetelmien käytön periaatteet. Tiedustelumenetelmän käyttö saattaisi jo lähtötilanteessa puuttua kohteena olevan tahon perusoikeuksiin merkittävästi, mutta se saattaisi olla hyväksyttyä yleisten periaatteiden näkökulmasta, jos sillä muuten aiheutettaisiin vähemmän haittaa kohteelle ja sivullisille.

Tiedustelumenetelmien käytön olisi aina perustuttava tiedustelutehtävään, joka on tarkemmin kuvatta edellä 13 §:n yksityiskohtaisissa perusteluissa. Tiedustelutehtävän olisi aina liityttävä sotilastiedustelun painopisteisiin ja sotilastiedustelun kohteisiin. Edellä tarkoitettujen edellytysten lisäksi tiedustelumenetelmäkohtaisesti säädettäisiin tiedustelumenetelmän käytön kestosta sekä lupahakemukseen tai päätökseen kirjattavista seikoista. Esimerkiksi telekuuntelua koskevassa lupahakemuksessa tulisi esittää tuomioistuimelle muun muassa tosiseikat, joihin telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen edellytykset ja telekuuntelun kohdistaminen perustuisivat.

Tiedustelumenetelmiä ei sotilastiedustelun kohteena olevien toiminnan ja ilmiöiden vuoksi olisi mahdollista kohdistaa aina tiettyyn henkilöön tai henkilöryhmään eikä toimivaltuuden käytön erityisenä edellytyksenä olisi rikostunnusmerkistön täyttävä teko, kuten on salaisten tiedonhankintakeinojen kohdalla edellytyksenä.

Tiedustelumenetelmiä käytettäessä sotilastiedustelun periaatteiden asema olisi korostunut silloin, kun tiedustelun kohteena olisi taho, joka nauttii perusoikeussuojaa. Perusoikeuksien ja ihmisoikeuksien kunnioittaminen, suhteellisuus ja pyrkimys vähimpään haittaan ovat kaikki tärkeitä periaatteita myös tiedustelumenetelmiä käytettäessä. Näiden periaatteiden noudattaminen varmistaa osaltaan tiedustelumenetelmien käytön edellytyksiä koskevan tulkinnan pysymisen sallituissa rajoissa ja ohjaa sotilastiedusteluviranomaista tarkoituksen mukaisimman tiedustelumenetelmän käyttöön.

Perustuslakivaliokunta on lausunnossaan (PeVL 32/2013, s. 4 ja PeVL 33/2013, s. 4) arvioinut poliisilakiin ja pakkokeinolakiin sisältyvien yleisten periaatteiden sekä salaisten tiedonhankintakeinojen ja salaisten pakkokeinojen käytön yleisten ja erityisten edellytysten merkitystä lupaa haettaessa ja tuomioistuimen harkitessa luvan myöntämistä. Toisin kuin edellä tarkoitettujen lakien kohdalla, tiedustelumenetelmien käytön edellytyksiä ei ole mahdollista porrastaa rikosten vakavuuden perusteella, koska tiedustelutoiminnan kohteena eivät ole rikokset. Tämä asettaa päätöksentekijälle korostuneen tiedonsaantioikeuden luvan ehtojen arvioimiseksi. Jotta tuomioistuimella olisi näissä tapauksissa mahdollisuus huolellisesti harkita luvan myöntämisen tarvetta ja laajuutta, niin sillä tulee olla käytössää riittävät tiedot. Lisäksi ulkopuolisen valvonnan merkitys korostuu.

Yleisten edellytysten lisäksi tiedustelumenetelmäkohtaisesti olisi säädetty erityisiä edellytyksiä. Vaatimus erittäin tärkeästä merkityksestä täyttyy hallituksen esityksen poliisilaiksi (HE 224/2010 vp., s. 38-43 sekä 90 ja 91) mukaan silloin, kun salaisen tiedonhankinnan suorittaminen muulla tavalla olisi muuten hyvin työlästä tai tiedustelutehtävän pitkittymisestä aiheutuisi erityistä vaaraa tai kohtuuttomia kustannuksia . Vaatimus erittäin tärkeästä merkityksestä edellyttäisi siis, että tiedustelutehtävän suorittamisesta muulla tavalla seuraa se, että tiedustelutehtävän suorittamisen pitkittymisestä aiheutuisi erityistä vaaraa Suomelle ja yhteiskunnalle sotilastiedustelun kohteena olevan toiminnan kehittyessä kohti konkreettisen vaaran aiheuttamista. Lisäksi tiedustelutoiminnassa olennaista on se, ettei toiminta paljastu ulkopuolisille, mikä voisi pahimmillaan vaarantaa olennaisesti Suomen maanpuolustuksen.

Viime kädessä luvan myöntämisessä ja toimivaltuutta käytettäessä olisi käytettävä kokonaisharkintaa, jossa merkitystä on annettava myös suhteellisuusperiaatteelle ja vähimmän haitan periaatteelle.

Pykälän 2 momentissa olisi säädetty siitä, että tiedustelumenetelmiä voitaisiin käyttää salassa niiden kohteelta. Tällä tarkoitettaisiin sitä, ettei tiedustelumenetelmää käyttävän viranomaisen tarvitsisi erikseen ilmoittaa kohteelle tai sivullisille siitä, että esimerkiksi alueella tai tilassa suoritettaisiin sotilastiedustelua. Mikäli henkilö olisi joutunut tiedustelumenetelmien käytön kohteeksi perusteettomasti tai muuten, olisi tästä ilmoitettava jälkikäteen kuten 86 §:ssä säädetään.

Pykälän 3 momentin mukaan tiedustelumenetelmän käyttö olisi lopetettava ennen päätöksessä mainitun määräajan päättymistä, jos käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole. Tiedustelumenetelmiä ei voitaisi missään tapauksessa käyttää kauempaa kuin tarpeen, vaikka lupa olisikin voimassa. Tällä korostettaisiin sitä, ettei tiedustelumenetelmiä voida missään tapauksessa käyttää kauempaa kuin on tarpeen, vaikka lupa olisikin vielä olemassa. Selvää on, että tiedustelumenetelmän käyttö olisi lopetettava viimeistään silloin, kun luvan voimassaolo päättyy.

2 luku. Sotilastiedustelun viranomaiset sekä ohjaus ja seuranta

11 §. *Sotilastiedustelun ohjaus ja johtaminen.* Pykälän 1 momentissa säädettäisiin sotilastiedustelun ohjaamisesta ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteisen kokouksen valmistelevasti käsittelemien painopisteiden avulla. Ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteinen kokous käsittelisi vuosittaiset painopisteet valmistelevasti.

Ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteinen kokoukseen osallistuvat tasavallan presidentin lisäksi muut ulko- ja turvallisuuspolitiikan keskeiset tahot. Valtioneuvoston ohjesäännön 25 §:n 1 momentin mukaan ulko- ja turvallisuuspoliittisessa ministerivaliokunnassa ovat pääministeri, ulkoministeri, puolustusministeri sekä neljä muuta valtioneuvoston määräämää ministeriä. Edellä tarkoitetun pykälän 2 momentin mukaan, jos asiat koskevat sisäministeriön hallinnonalaa, kokoukseen kutsutaan myös sisäministeri.

Ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteisen kokouksen valmistelevasti käsittelemillä painopisteillä tarkoitettaisiin Suomelle ulko- ja turvallisuuspoliittisesti merkittäviä pitkäaikaisia kehityslinjoja, joista tarvittaisiin tarkempaa tietoa ylimmän valtionjohdon päätöksenteon tueksi. Painopisteet voisivat kohdistua esimerkiksi tiettyyn alueeseen tai tiettyyn asiakokonaisuuteen. Kyseessä eivät olisi yksittäiset sotilaalliset uhkat tai toiminta taikka yksittäiset Suomen kansallista turvallisuutta vaarantavat uhkat.

Painopisteisiin voivat vaikuttaa myös lyhytaikaiset tapahtumat ja kehityskulut. Jos tällaisilla kehityskuluilla olisi pitkäaikaisia vaikutuksia, painopisteitä voitaisiin tarvittaessa mukauttaa.

Puolustusministeriö valmistelisi ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteisen kokouksen valmistelevasti käsittelemät painopisteet, kuten se on tähänkin mennessä tehnyt kyseisiin kokouksiin menevien asioiden kohdalla.

Lisäksi on voimassa se, mitä sotilaskäskyasioiden päätöksenteosta säädetään puolustusvoimista annetun lain 31 ja 32 §:ssä.

Pykälän 2 momentin mukaan sotilastiedustelua ohjaisi hallinnollisesti puolustusministeriö. Vaikka puolustusministeriön ohjausrooli perustuukin valtioneuvostosta annettuun lakiin ja valtioneuvoston ohjesääntöön (494/2007), asiasta olisi tarkoituksen mukaista säätää nimenomaisesti sotilastiedustelutoiminnan merkittävyyden ja laajuuden vuoksi. Säännöksellä ei olisi tarkoitus vaikuttaa puolustusministeriön normaaliin Puolustusvoimien ohjaukseen. Puolustusministeriö ohjaisi edelleen Puolustusvoimia ja sotilastiedustelua sen osana talous-, resurssi- ja budjettiohjauksella sekä säädösohjauksella.

Lisäksi puolustusministeriöllä on merkittävä rooli sotilastiedustelun hallinnonalan valvonnassa ja sotilastiedustelun vuosittaisten painopisteiden valmistelussa. Puolustusvoimat on puolustusministeriön alainen puolustusvoimista annetun lain 24 §:n mukaisesti.

Pykälän 2 momentin mukaan puolustusministeriön myös antaisi Puolustusvoimille 1 momentissa tarkoitetut ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteisen kokouksen valmistelevasti käsittelemät painopisteet. Kyseessä olisi hallinnonalan sisäinen määräys, jossa vahvistettaisiin painopisteet. Puolustusministeriön antaman määräyksen jälkeen Puolustusvoimat olisi velvoitettuja painopisteitä seuraamaan.

Valmistelevasti käsiteltyjen painopisteiden mukaisesti jäljempänä säädetyssä pykälässä tarkoitetut viranomaiset voisivat antaa tiettyä tarkempaa kysymystä koskevan tietopyynnön pääesikunnalle. Tietopyynnön perusteella sotilastiedustelun viranomaiset muotoilisivat tarkemmat tiedustelutehtävät, jonka toteuttamisessa voitaisiin käyttää muun muassa tiedustelumenetelmiä.

Pykälän 3 momentissa säädettäisiin sotilastiedustelun johtamisesta, joka kuuluisi pääesikunnalla. Pääesikunta vastaisi sotilastiedustelun johtamisesta käytännössä jakamalla sotilastiedustelunviranomaisten kesken heidän suoritettavakseen tietopyyntöjen perusteella laaditut tiedustelutehtävät. Tietopyynnöistä ja tiedustelutehtävistä säädettäisiin jäljempänä. Pääesikunnalla olisi myös vastuu siitä, että sotilastiedustelutoiminta olisi ylimmän valtiojohdon antamien tiedustelun painopisteiden mukaista.

Pääesikunta vastaisi johtamisen osalta myös tiedustelun tarvittavasta yhteensovittamisesta siviilitiedusteluviranomaisen kanssa.

12 §. *Sotilastiedusteluviranomaiset.* Pykälän 1 momentissa määriteltäisiin sotilastiedusteluviranomaiset. Pääesikunta vastaisi sotilastiedustelun kokonaisuudesta ja sen johtamisesta sekä ohjaamisesta Puolustusvoimien sisällä. Puolustusvoimien organisaatiorakenne perustuu puolustusvoi-

mista annettuun lakiin, Puolustusvoimien työjärjestykseen sekä muihin säädöksiin. Pääesikunnan työjärjestyksen mukaan pääesikunnan tiedusteluosasto vastaisi sotilastiedustelun tehtäväkokonaisuuden hoitamisesta.

Sotilastiedustelun toimialaan kuuluvat sotilastiedustelu sekä sotilasvastatiedustelu, jotka sisältävät tiedonhankinnan, tiedon käsittelyn sekä raportoinnin. Pääesikunta johtaa Puolustusvoimien tiedustelulaitosta ja puolustushaarojen tiedustelua sekä sotilastiedustelutoimialan kansallista ja kansainvälistä yhteistoimintaa.

Sotilastiedustelun voimavarojen käyttöä ja kohdentamista ohjaa ensisijaisesti ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteisen kokouksen antamat linjaukset. Painopisteiden perusteella ylimmän valtiojohdon tai sotilasjohdon antaman yksittäisen tietopyynnön käsittelystä päättäisi pääesikunta. Pääesikunta osallistuu tiedustelumenetelmin hankitun tiedon analysointiin ja raportointiin.

Sotilastiedustelun toimivaltuuksia käyttävänä viranomaisena toimisi pääesikunta, eli pääesikunnan tiedusteluosasto, ja Puolustusvoimien tiedustelulaitos, jotka eri tiedustelumenetelmin hankkisivat tarpeellisen tiedon, analysoisivat sen sekä raportoisivat sen eteenpäin. Puolustusvoimien tiedustelulaitos on suoraan pääesikunnan alainen sotilaslaitos, jota pääesikunta ohjaa.

Pääesikunnan tiedusteluosasto käyttää jo tällä hetkellä rikostorjuntaan liittyviä toimivaltuuksia SKRTL:n perusteella. Rikostorjunnan tiedonhankintakeinot ovat osittain samankaltaiset kuin tässä laissa säädettäväksi tarkoitetut toimivaltuudet. Koska tiedusteluosastolla olisi kokemusta salassa pidettävästä tiedonhankintatoiminnasta, tarkoituksenmukaista olisi, että se käyttäisi myös tässä esityksessä esitettyjä toimivaltuuksia, jollei toisin ole jäljempänä erikseen säädetty.

Sotilastiedusteluviranomainen suorittaisi tietopyynnön perusteella annettuun tiedustelutehtävään perustuvan tiedonhankinnan sekä tutkisi ja analysoisi hankitut tiedot. Tämän pohjalta sotilastiedusteluviranomainen tekisi tietopyynnön vaatimukset täyttävän lopputuotteen pääesikunnalle, jonka pääesikunta sen käsiteltyään toimittaisi edelleen tietopyynnön tehneelle viranomaiselle.

Pääesikunnan tiedustelupäällikkö ja erityisesti tiedustelumenetelmien käyttöön perehtyneet virkamiehet päättäisivät merkittävissä määrin tässä laissa säädettävien toimivaltuuksien käyttämisestä.

Sotilastiedusteluviranomaiset saisivat tukea tiedonhankinnassa myös muilta Puolustusvoimien osilta. Puolustushaarat osallistuisivat tiedustelutoimintaan erityisesti aluevalvontatehtäviä suorittaessaan tuottaen toiminnassaan samalla tiedustelun kannalta tarpeellista tietoa. Ilmavoimissa ja merivoimissa aluevalvonta tukee tiedustelutoimintaa ja päinvastoin. Myös Maanpuolustuskorkeakoulu ja Puolustusvoimien tutkimuslaitos tekevät tutkimusta ja analyysejä, jotka hyödyttävät tiedonhankintaa. Lisäksi tiedustelulaitos voi saada olennaisia tietoja esimerkiksi Puolustusvoimien Logistiikkalaitokselta, jonka työntekijät toimivat aktiivisesti sotatarvikkeiden hankinnassa. Kyse ei ole varsinaisesti tiedustelusta, vaan tiedustelun kannalta merkityksellistä tietoa saadaan normaalien työtehtävien ohessa.

Tietyissä tilanteissa olisi tarkoituksen mukaista käyttää tiedustelun avustavissa tehtävissä Puolustusvoimien erityiskoulutuksen saaneita joukkoja. Näillä joukoilla olisi tiedustelumenetelmien käyttöön erityiskoulutus ja ne olisivat näissä tehtävissä sotilastiedusteluviranomaisen alaisia. Näillä joukkoja käyttävä sotilastiedusteluviranomainen olisi vastuussa joukon toiminnasta.

Myös reserviläisiä olisi voitava käyttää tietyissä tilanteissa. Varusmiespalveluksessa osa varusmiehistä koulutetaan sotilastiedustelun tehtäviin. Reserviläisiä voitaisiin käyttää lähinnä tilanteissa, joissa olisi saatu tietoa valmiustilanteen sellaisen tehostamisen tai kohottamisen tueksi, joka ei vielä vaadi muiden kuin tiedusteluun koulutettujen reserviläisten kutsumista kertausharjoitukseen

mutta jossa sotilastiedusteluun tarvitaan lisäresursseja tiedon hankkimiseksi Suomea uhkaavan tilanteen kehittymisestä. Reserviläisten osallistumisesta säädettäisiin jäljempänä.

Pykälän 2 momentin mukaan puolustushaarat voisivat käyttää radiosignaalitiedustelua tämän lain tarkoituksessa, kuten jäljempänä säädettäisiin. Päätöksentekoon sovellettaisiin kuitenkin samoja säännöksiä kuin toimivaltuuden käytöstä muuten on voimassa. Tilanteissa, joissa puolustushaarat suorittaisivat sotilastiedustelua, toiminta tapahtuisi pääesikunnan johdossa ja valvonnassa. Puolustushaarat toimittaisivat edelleen keräämänsä tiedot pääesikunnalle, joka tekisi niistä edelleen analyysin tietopyynnön esittäneelle viranomaiselle.

13 §. *Tiedustelutehtävä.* Pykälässä määriteltäisiin tiedustelutehtävä. Laissa säädettyjen toimivaltuuksien käyttö perustuisi tietyn tiedustelutehtävän toteuttamiseen. Tiedustelutehtävällä tarkoitettaisiin pääesikunnan tiedustelupäällikön sotilastiedusteluviranomaiselle antamaa toimeksi antoa tiedustelutiedon hankkimiseksi.

Tiedustelutehtävän tarkoituksena olisi aina hankkia tietoa lain 4 §:ssä säädetyistä sotilastiedustelun kohteista. Tiedustelutehtävä voisi perustua jäljempänä säädettyyn toisen viranomaisen tietopyyntöön tai lain 3 §:ssä säädettyyn sotilastiedustelun tarkoitukseen. Sotilastiedustelun tarkoituksen mukaisesti sotilastiedustelussa hankittaisiin tietoa ulkoisista uhkista ylimmän valtiojohdon päätöksenteon tueksi ja puolustusvoimista annetun lain 2 §:ssä tarkoitettujen Puolustusvoimien tehtävien suorittamiseksi. Sotilastiedustelun tarkoitukseen perustuvia tietopyynnöt tulisivat Puolustusvoimien sisältä, kuten puolustushaaroista tai pääesikunnan alaisilta laitoksilta.

Tiedustelutehtävällä määriteltäisiin tarkemmin ne konkreettiset kohteet, joista hankituilla ja käsitellyillä tiedoilla pystyttäisiin vastaamaan tietopyyntöön. Tiedustelutehtävän suunnittelisi pääesikunta. Tiedonhankinnan ja hankitun tiedon käsittelyn ja tarvittavan analysoinnin toteuttaisi tiedonhankinnan suorittava sotilastiedusteluviranomainen. Lisäksi pääesikunta osallistuisi hankitun tiedon analysointiin sekä tietopyyntöön vastaamiseen. Tiedustelutehtävällä kohdistettaisiin ja rajattaisiin edelleen sotilastiedustelun toimivaltuuksien käyttöä. Tiedustelutehtävällä määriteltäisiin konkreettisemmin ne asiat, tiedontarpeet ja tiedustelun kohdistuminen, joista tiedustelutehtävän toteuttamiseksi hankittaisiin tietoa. Tiedustelutehtävä voitaisiin kohdistaa esimerkiksi tiettyyn laajaan maantieteelliseen alueeseen, sillä tapahtuvaan toimintaan tai muuhun vastaavaan, josta voitaisiin tarvittavia tietoja tietopyyntöön vastaamiseksi olettaa saatavan.

Tiedustelutehtävässä ei vielä määriteltäisi yksityiskohtaisesti kohteita esimerkiksi henkilötasolla tai tietyn tilan tai alueen tasolla, vaan ne määrittelisi tiedustelutehtävän perusteella tiedonhankintaa toteuttavan sotilasviranomaisen toimesta. Tiedustelutehtävän ja konkreettisten kohteiden kautta sotilastiedusteluviranomainen määrittelisi tapauskohtaisesti ne toimivaltuudet, joita käyttämällä tarvittavaa tietoa olisi hankittavissa.

Sotilastiedustelu on rikosperusteiseen tiedonhankintaan ja esimerkiksi rikostorjuntaan verrattuna pidempikestoisempaa ja tiedustelutehtävät lähtökohtaisesti ennakkoon tarkoin suunniteltu. Tiedustelutehtävän tavoitteena voi olla esimerkiksi kerätä tietoa kohdevaltion asevoimien toiminnasta ja siihen liittyvistä seikoista. Jos tiedustelutehtävän kohde on merkittävä, sen kesto voisi olla hyvinkin pitkäaikainen. Näin tarkoituksena ei olisi yksittäisen rikoksen estäminen tai selvittäminen, vaan varhaisen vaiheen tiedon kerääminen kokonaiskuvan saamiseksi ja ennakkovaroituksen varmistamiseksi.

14 §. *Sotilastiedustelun seuranta.* Pykälän 1 momentin mukaan puolustusministeriö olisi velvollinen vähintään kerran vuodessa toimittamaan selvityksen valtioneuvoston ulko- ja turvallisuuspoliittiselle valiokunnan ja tasavallan presidentin yhteiselle kokoukselle tiedustelun painopisteiden perusteella tehdystä tiedonhankinnasta siltä osin kuin se kuuluu sotilastiedusteluviranomaisen toimialalle. Jos painopisteiden mukaisista kohteista hankitut tiedot sitä edellyttävät, selvitys voidaan tehdä use-

amminkin ulko- ja turvallisuuspoliittisen valiokunnan ja tasavallan presidentin yhteisen kokouksen pyynnöstä tai puolustusministeriön omasta aloitteesta.

Pykälän tarkoittamassa seurannassa ei olisi kyse oikeudellisesta valvonnasta, vaan tarkoituksena olisi toimittaa ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteiselle kokoukselle tietoja kokouksen valmistelevasti käsittelemistä painopisteistä ja niiden nojalla hankituista tiedoista. Tällä varmistettaisiin ylimmän valtiojohdon tietoisuus Suomen turvallisuusympäristöstä ja siinä tapahtuneista muutoksista.

Pykälän 2 momentin mukaan pääesikunta olisi velvollinen antamaan vuosittain tai puolustusministeriön pyynnöstä selvityksen puolustusministeriölle tiedustelutoiminnasta. Säännös olisi merkityksellinen puolustusministeriön hallinnonalan yleisen ohjauksen, tuloksellisuuden seurannan ja lainmukaisuuden valvonnan kannalta. Sotilastiedustelun ulkopuolisesta ja sisäisestä laillisuusvalvonnasta säädettäisiin lisäksi erikseen.

Puolustusministeriön saaman selvityksen olisi oltava kattavampi kuin ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteiselle kokoukselle annettava selvitys. Selvityksestä olisi käytävä ilmi kaikki ulko- ja turvallisuuspolitiikka käsittelevän ministerivaliokunnan ja tasavallan presidentin valmistelevasti käsittelemien painopisteiden nojalla toteutetut tiedustelutehtävät ja niiden perusteella annetut vastaukset eri viranomaisten tietopyyntöihin.

3 luku. Yhteistoiminta muiden viranomaisten kanssa ja kansainvälinen yhteistyö

15 §. *Yhteistyö suojelupoliisin ja muiden viranomaisten kanssa.* Kasvavat riskit ja uuden tyyppiset uhat edellyttävät koko yhteiskunnalta jatkuvaa valmiutta ja varautumista. Lisäksi kokonaisturvallisuusajattelua vahvistetaan kansallisesti, EU:ssa ja kansainvälisessä yhteistyössä.

Sotilaalliset tai Suomen kansalliseen turvallisuuteen kohdistuvat uhkat eivät välttämättä ole itsestään selvästi sotilastiedustelun tai siviilitiedustelun tiedonhankinnan ensisijaisia kohteita. Uhkat saattavat olla luonteeltaan sellaisia, että niistä saattaa muodostua esimerkiksi sotilaallisia uhkia ajan kuluessa ja tapahtumakulkujen edetessä. Tiedusteluviranomaisten olisi voitava vaihtaa saumattomasti tietoa ja siirtää tiedustelutehtävä toiselle tiedusteluviranomaiselle, mikäli tiedonhankinnankohde paljastuisi enemmän siviili- tai sotilastiedustelun kohteeksi.

Hallintolain (434/2003) 10 §:n yleinen säännös viranomaisten yhteistyöstä ja velvollisuudesta pyrkiä edistämään viranomaisten välistä yhteistyötä. Tiedonhankinnan tavoitteiden saavuttaminen sekä tiedonhankinnan tarkka ja asianmukainen kohdentaminen edellyttävät yhteistyötä tiedusteluviranomaisten kesken. Lisäksi yhteistyö edistää yhtenäisten menettelytapojen ja käytäntöjen toteutumista.

Viranomaisten yhteistyöllä varmistuttaisiin myös siitä, että sotilastiedusteluviranomainen sekä siviilitiedusteluviranomainen olisivat riittävällä tasolla tietoisia toistensa toteuttamasta tietojenhankinnasta niin, etteivät esimerkiksi suoritettavat tiedusteluoperaatiot vaarantuisi tai estyisi toisen viranomaisen toiminnan takia. Lisäksi viranomaisten resurssien takia ei voida pitää tarkoituksen mukaisena sitä, etteivät tiedusteluviranomaiset voisi jakaa kalustoaan ja osaamistaan toiselle tiedusteluviranomaiselle.

Yhteistyössä olisi kuitenkin erityistä huomiota kiinnitettävä siihen, että tiedustelu pidettäisiin erillään rikosperusteisesta toiminnasta. Toimivaltuuksien käyttötarkoitus ja edellytykset poikkeavat merkittävästi toisistaan. Sotilastiedustelun toimivaltuuksia ei saisi käyttää rikostorjunnan tai esitutkinta- ja pakkokeinolakien toimivaltuuksien laajentamiseksi.

Pykälän 2 momentin mukaan sotilastiedusteluviranomaiset voisivat tehdä yhteistyötä myös muiden viranomaisten kanssa. Sotilastiedustelutoiminta on lähellä rikostorjuntaa ja on muutenkin erittäin salassa pidettävää toimintaa. Yhteistyötä saattaisi kuitenkin olla tarpeen tehdä myös muiden viranomaisten, kuten Rajavartiolaitos ja Tulli, normaaleihin tehtäviin liittyen. Kyseessä olisi viranomaisten taktinen toiminta, jossa ei olisi kyse sotilastiedustelun toimivaltuuksien käyttämisestä.

Toiminnan luonteesta ja toimivaltuuksista johtuen saattaisi tulla tilanteita, joissa toisen viranomaisen kanssa on syytä toimia yhteistyössä sotilastiedustelutehtävän asianmukaiseksi suorittamiseksi. Kyse voisi olla esimerkiksi peitetoiminnan tai tietolähteen paljastumisen estämisestä.

Kuten 1 momentissa, momentin yhteistyöllä tarkoitettaisiin käytännön yhteistyötä tiedustelutehtävän suorittamiseen liittyen, mikä ei tarkoittaisi toisen viranomaisen tehtävien suorittamiseen osallistumista tai tietojen antamista rikostorjuntaan.

Pykälän 3 momentissa säädettäisiin asetuksenantovaltuudesta. Asetuksessa annettaisiin tarkempia säännöksiä sotilastiedusteluviranomaisen ja suojelupoliisin välisestä yhteistyöstä.

16 §. *Tietopyyntö*. Pykälän 1 momentin mukaan sotilastiedustelun kohteista hankittavia tietoja koskevia tietopyyntöjä voisi antaa Suomen ylin valtiojohto, jonka tiedonsaantitarpeita sotilastiedustelu ensisijaisesti palvelee. Tietopyynnön perusteella sotilastiedusteluviranomaiset muodostaisivat yksittäiset tiedustelutehtävät, joiden perusteella sotilastiedustelutoiminnanharjoittaja harkitsisi, mitä tiedonhankinnankeinoja kyseistä toimeksiantoa koskien olisi tarkoituksenmukaisinta käyttää. Sotilastiedusteluviranomainen keräisi tietoja sekä laatisi kerättyjen tietojen pohjalta analyysin toimeksiannon kohteesta.

Pykälässä säädetyt tietopyynnöt liittyisivät lain 11 §:ssä tarkoitettuihin painopisteisiin.

Pykälässä säädetyllä ei olisi tarkoitus vaikuttaa normaaliin viranomaisyhteistyöhön ja sen perusteella vaihdettaviin tietoihin.

Tietopyynnössä viranomainen antaisi mahdollisimman tarkan kuvauksen tiedonhankinnan kohteesta ja tietotarpeesta sekä kuvaisi sen, miten tiedonhankinnan kohde vastaa valtioneuvoston ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteisen kokouksen antamia painopisteitä. Tietopyynnön pohjalta pääesikunta määrittelisi tiedustelutehtävät ja sen pohjalta sotilastiedusteluviranomainen tekisi päätöksen, mitä tiedustelumenetelmiä tiedonhankkimiseksi olisi syytä käyttää. Sotilastiedusteluviranomainen hankkisi tässä laissa tarkemmin määritellyt tarvittavat luvat ja päätökset toimivaltuuksien käyttämiselle. Edellä sanotusta pitää kuitenkin erottaa siviilitiedusteluviranomaisen esittämä toimeksianto tietoliikennetiedustelun käytölle, mistä säädettäisiin jäljempänä erikseen.

Tietopyyntöjen pohjalta pääesikunnan tiedustelupäällikkö antaisi tiedustelutehtävän sotilastiedusteluviranomaiselle, joka päättäisi tarkemmin, millä tiedustelumenetelmillä tarvittavat tiedot pystyttäisiin hankkimaan tarkoituksen mukaisimmin ja laatisi hankittujen tietojen pohjalta tietopyynnön mukaisen selvityksen sen esittäjälle. Sotilastiedustelun viranomainen voisi käyttää myös tietopyyntöön vastaamiseksi laadittua raporttia tarvittavilta osin sotilastiedustelutoiminnasta laadittavaan selvitykseen ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteiselle kokoukselle.

Pykälän tarkoittamista tietopyynnöistä olisi erotettava tasavallan presidentin Puolustusvoimien ylipäällikkönä antamat sotilaskäskyt. Sotilaskäskyjen päätöksenteko menettelyyn ei olisi tarkoitus puuttua käsiteltävänä olevalla lainsäädännöllä. Sotilaskäskymenettelyä on käsitelty edellä tämän esityksen yleisperusteluissa. Lisäksi tietopyynnöistä olisi erotettava Puolustusvoimien sisäiset tietotarpeet, eli sotilastiedustelun tarkoitukseen perustuvat tiedustelutehtävät.

17 §. *Sotilas- ja siviilitiedustelun yhteensovittaminen.* Pykälässä säädettäisiin tiedustelun yhteensovittamisesta. Pykälän 1 momentin mukaan tiedonhallinnallisesti tiedustelun yhteensovittamisella varmistettaisiin tiedustelun kannalta merkittäviin ulko- ja turvallisuuspoliittisiin tietopyyntöihin reagoiminen, tiedustelutoimintaan kytkeytyvien eri hallinnonalojen näkemysten huomioon ottaminen ja tässä prosessissa saavutetun näkemyksen jakaminen asianmukaisille tahoille.

Toiminnallisesti yhteensovittamisessa olisi kyse tiedustelun painopisteiden osoittamisesta ja koordinoinnista sekä tiedustelutoiminnan tehtävien jakamisesta sotilas- ja siviilitiedustelun välillä tiedustelun kohteita ja uhan luonnetta koskevan tarkoituksenmukaisuusharkinnan perusteella. Tämän harkinnan yhteydessä voitaisiin arvioida esimerkiksi muualla kuin Suomessa toteuttavaan sotilas- ja siviilitiedusteluun mahdollisesti liittyviä ulkopoliittisia ulottuvuuksia ja vaikutuksia Suomen kasainvälisiin suhteisiin.

Tiedustelutoiminnan yhteensovittamisessa ei sitä vastoin olisi kyse tiedustelun valvonnasta tai operatiiviseen toimintaan, kuten tiedustelumenetelmien käyttämisestä päättämiseen, ulottuvasta ohjauksesta.

Pykälän 1 momentin mukaan tasavallan presidentti, valtioneuvoston kanslia, ulkoasiainministeriö, puolustusministeriö ja sisäministeriö sovittaisivat yhteen sotilas- ja siviilitiedustelutoimintaa. Yhteensovittaminen voitaisiin tehdä samassa kokoonpanossa kuin valtioneuvostossa toimivan tilannekuvan koordinaatioryhmä. Koordinaatioryhmään ovat kuuluneet valtioneuvoston kanslian valtiosihteeri, ulkoasiainministeriön valtiosihteeri, sisäministeriön ja puolustusministeriön kansliapäälliköt ja tasavallan presidentin kanslian kansliapäällikkö sekä asiantuntijajäseninä suojelupoliisin päällikkö ja pääesikunnan tiedustelupäällikkö. Yhteensovittamiseen osallistuvat tahot saisivat tarvittavan hallinnollisen tuen edustamiltaan viranomaisilta.

Tiedustelun yhteensovittamisessa tarkennettaisiin tarvittaessa pääesikunnalle toimitettuja tietopyyntöjä, yhteensovittamisella avustettaisiin tiedustelukysymysten tarkentamisessa ja ohjattaisiin tarvittaessa tietopyyntöjä toimivaltaiselle tiedusteluviranomaiselle.

Pykälän 2 momentin nojalla tiedustelun yhteensovittamisessa voitaisiin käsitellä ohjaavasti ja yhteen sovittavasti ulko- ja turvallisuuspoliittisesti merkittävät tietopyynnöt ja toimivaltuuksien käyttö. Tällaisia asioita voisivat olla etenkin erityisiä toimivaltuuksia edellyttävät tiedonhankintaoperaatiot, tai operaatiot, joita voidaan pitää ulkopoliittisesti arkaluonteisina. Momentin tarkoittamassa tiedustelun yhteensovittamiseen ei sisältyisi valvontaan liittyviä asioita eikä operatiivista päätöksentekoa vaan yhteensovittamisessa otettaisiin huomioon esimerkiksi eri hallinnonalojen näkemykset tilanteissa, joissa tiedustelutoiminnasta voisi syntyä Suomen kansainvälisille suhteille merkittävää haittaa.

Tiedustelun yhteensovittamisessa voitaisiin myös tarkastella tilannekohtaisesti tietopyyntöjen toteuttamiseen käytettäviä toimivaltuuksia ja arvioi niiden käyttämiseen liittyviä ulkopoliittisia riskejä. Yhteensovittamisessa käsiteltävät asiat eivät olisi tavanomaisiksi katsottavia tietopyyntöjä.

Tiedustelun yhteensovittaminen varmistaisi osaltaan myös tiedon kulun asian mukaisille tahoille esimerkiksi ulkomaan tiedusteluun liittyen. Toisaalta toimivaltainen viranomainen voisi yhteensovittamisessa saada toimintansa kannalta olennaista tietoa ja tukea operatiiviseen päätöksentekoonsa.

Sotilaskäskyasiana päätettäviä tiedusteluasioita ei tarvitsisi sovittaa yhteen vaan ne menisivät suoraan sotilastiedusteluviranomaisten käsiteltäväksi sotilaskäskynä. Sotilastiedustelulailla ei olisi tarkoitus muuttaa sotilaskäskyasioita koskevaa päätöksentekomenettelyä.

18 §. *Kansainvälinen yhteistyö.* Pykälässä säädettäisiin sotilastiedusteluviranomaisen kansainvälisestä yhteistyöstä. Yhteistyöllä tarkoitettaisiin kaikkea kansainvälistä tiedustelu- ja turvallisuusviranomaisten välistä yhteistyötä sotilastiedusteluviranomaisen ja muiden maiden vastaavien elinten välillä. Kansainvälisellä yhteistyöllä tarkoitetaan esimerkiksi tietojen vaihtoa, teknisen tuen antamista, koulutusyhteistyötä, virkamiesvaihtoa ja kansainvälistä yhdyshenkilötoimintaa. Yhteisillä tiedusteluoperaatioilla tarkoitettaisiin yhteisiä tiedonhankinnan operaatioita, joissa käytettäisiin tämän lain 4 luvussa säädettyjä tiedustelumenetelmiä. Kansainvälisen yhteistyön olisi aina oltava Suomen kansallisten etujen mukaista.

Tiedustelun alalla ei ole voimassa kansainvälisiä oikeudellisesti sitovia yleissopimuksia. Valtiot Suomi mukaan luettuna ovat tehneet aihetta sivuavia korkeintaan yhteisymmärryspöytäkirjojen tasolla olevia järjestelyitä, joilla ei ole kansainvälisoikeudellista sitovuutta tai velvoittavuutta. Yhtenä syynä tähän on tiedustelutoiminnan ensisijainen tarkoitus, mikä on jokaisen maan oman kansallisen edun parantaminen. Tämä ei kuitenkaan tarkoita sitä, ettei kansallinen etu voisi olla yhtenäinen eri valtioiden kesken ja saavutettavissa parhaiten yhteistyöllä eri valtioiden tiedusteluviranomaisten kesken.

Sotilastiedustelun viranomaisen olisi toiminnassaan aina noudatettava lain 1 luvussa säädettyjä suhteellisuusperiaatetta ja vähimmän haitan periaatetta sekä EIS:n, Euroopan unionin sekä Suomen lainsäädäntöä.

Tietojen luovuttamisessa etenkin Euroopan unionin ulkopuolelle korostuu Euroopan unionin tietosuojaa koskevat säädökset sekä Euroopan unionin tuomioistuimen oikeuskäytäntö. Euroopan unionin tuomioistuin on muun muassa katsonut henkilötietojen yleisen siirron loukkaavan yksityiselämän kunnioittamista koskevan perusoikeuden keskeistä sisältöä, mikäli henkilötietojen vastaanottajavaltion kansallinen säännöstö mahdollistaa viranomaisten yleisen pääsyn sähköisen viestinnän sisältöön ilman, että viranomaisten oikeutta käyttää tai säilyttää henkilötietoja on rajoitettu, ja mikäli vastaanottajavaltion kansallinen säännöstö ei anna yksilölle mahdollisuutta käyttää oikeussuojakeinoja omassa asiassaan.

Pykälän tarkoittamalla kansainvälisellä yhteistyöllä ei olisi tarkoitus puuttua esimerkiksi puolustushaarojen kansainväliseen yhteistyöhön, minkä säädösperusta on aluevalvontalain 42 §:ssä. Puolustushaarat saavat tehtäviensä hoitamiseksi tietoa esimerkiksi toisen valtion käyttämistä sotalaivoista, mikä voi olla ulkomaisen yhteistyökumppanin kannalta kiinnostavaa tietoa myös tämän valtion tiedusteluviranomaisten näkökulmasta. Vaihdettavia tietoja ei kuitenkaan olisi katsottavissa tässä mielessä tiedustelutiedoksi, vaan tietoja vaihdetaan osana aluevalvontayhteistyötä. Jos tietojen hankkimiseen tarvittaisiin tässä laissa tarkoitettuja toimivaltuuksia, tietoja tulisi käsitellä ja vaihtaa tämän lain mukaisesti.

Pykälän 1 momentin mukaan sotilastiedusteluviranomainen voisi osallistua Suomen kansallisten etujen mukaisesti tehtäviinsä liittyen kansainväliseen yhteistyöhön. Sotilastiedustelun tehtäviin liittyvät uhkat ovat usein luonteeltaan kansainvälisiä, joista ulkomaisilla tiedustelupalveluilla ja turvallisuuspalveluilla on mahdollisuus saada tietoja.

Kansallisella edulla tarkoitettaisiin sitä, että kansainvälisellä yhteistyöllä olisi arvioitu olevan Suomen edun mukaista eikä sillä heikennettäisi suomalaisen yhteiskunnan eri osa-alueita. Esimerkiksi Suomen kansallisen edun mukaista ei olisi tietyn suomalaisen yrityksen yrityssalaisuuksien luovuttaminen sotilastiedusteluviranomaisen ulkomaiselle yhteistyökumppanille.

Momentin 1 kohdan mukaan sotilastiedusteluviranomainen voisi vaihtaa hankkimiaan tietoja ulkomaisten tiedustelupalveluiden ja turvallisuusviranomaisten kanssa. Sotilastiedusteluviranomaisen hankkimilla tiedoilla voi kansallisen turvallisuuden takaamisen ohella olla suurta merkitystä kansainvälisesti esimerkiksi sotilaallisten uhkien ja kriisien kehittymisen kannalta. Tietojen luovuttami-

sessa olisi otettava aina huomioon tämän lain rekisterisäännökset sekä tietojen luovuttamista koskeva EU-oikeus.

Sotilastiedusteluviranomaisella olisi oikeus luovuttaa vain sellaista tietoa, jota sillä on oikeus hankkia. Luovutettavien tietojen olisi aina liityttävä 4 §:ssä tarkoitettuihin sotilastiedustelun kohteisiin ja uhkiin. Luovutettava tieto ei saisi olla tiedonhankinnassa syntynyttä ylimääräistä tai muuta tietoa, jota sotilastiedusteluviranomaisella ei olisi ollut oikeus hankkia tai käyttää, vaan sotilastiedusteluviranomaisen olisi voitava käyttää ja hankkia tietoa itsenäisestikin omaan käyttötarkoitukseensa. Tiedonvaihto voisi koskea esimerkiksi vieraan valtion aseteollisuutta.

Sotilastiedusteluviranomainen voisi vastaanottaa tehtäviinsä liittyviä tietoja ulkomaisilta tiedustelupalveluilta ja turvallisuusviranomaisilta. Sotilastiedustelun tehtäviin liittyvät uhkat ovat usein luonteeltaan kansainvälisiä, joista myös ulkomaisilla tiedustelupalveluilla ja turvallisuuspalveluilla on mahdollisuus saada tietoja, joita sotilastiedusteluviranomaisella ei ole ollut mahdollisuus saada omilla toimivaltuuksillaan. Lisäksi etenkin henkilötiedustelun osalta kyse on pitkäaikaisesta ja suunnitelmallisesta toiminnasta, johon sotilastiedusteluviranomaisella ei ole ollut vielä mahdollisuuksia tai mistä sotilastiedusteluviranomaisella ei ole vielä kokemusta. Sotilastiedusteluviranomainen voisi saada olennaista tietoa oman ulkomaan henkilötiedustelun käynnistämiseen kansainvälisen yhteistyön kautta.

Kohdan tilanteita voisivat olla esimerkiksi kansainvälisissä sotilaallisissa kriisinhallintaoperaatioissa tehtävä tiedonhankintaoperaatiota vastaan kohdistuvista uhkista, mutta myös operaatioon osallistumista koskevaa olennaista tietoa voitaisiin saada kansainvälisen yhteistyön avulla.

Tiedustelutoiminnan kansainväliseen yhteistyöhön liittyy aina epävarmuus vaihdettavien tietojen luotettavuudesta. Sotilastiedusteluviranomaisen luovuttamien tietojen laatu olisi aina varmennettava ja niihin olisi mahdollisuuksien mukaan lisättävä tietoja, joiden avulla vastaanottaja voisi arvioida tietojen oikeellisuutta, täydellisyyttä, ajantasaisuutta ja luotettavuutta. Mikäli ilmenisi, että luovutuksen kohteena on esimerkiksi virheellisiä tietoja tai että tietoja olisi luovutettu lainvastaisesti, asiasta olisi ilmoitettava viipymättä vastaanottajalle. Arvio tietojen luotettavuudesta olisi tehtävä heti analysoitaessa saatuja tietoja.

Toisaalta myös vastaanotettava tieto olisi aina heti analysoitava ja arvioitava sen lainmukaisuus. Jos tieto olisi epätarkkaa, sotilastiedusteluviranomainen ei saisi tietoa käyttää tai tiedot sisältäisivät tietoja asioista, joita sotilastiedusteluviranomainen ei saisi käyttää, olisi tieto hävitettävä tai pyrittävä varmistamaan niiden todenperäisyys.

Momentin 2 kohdan mukaan sotilastiedustelun viranomainen voisi osallistua tiedustelutietojen hankkimiseen ja arvioimiseen liittyvään kansainväliseen yhteistoimintaan. Edellä 4 §:ssä erääksi sotilastiedustelun kohteeksi on mainittu myös kansainväliset operaatiot ja tapahtumat. Osana näitä Suomen sotilastiedusteluviranomaiset voisivat osallistua kansainvälisiin tiedusteluoperaatioihin, jotka perustuvat esimerkiksi Euroopan unionin jäsenvaltion perussopimuksen nojalla pyytämään kansainväliseen apuun.

Pykälän 2 momentin mukaan pääesikunnan tiedustelupäällikkö päättäisi kansainvälisestä yhteistyöstä Suomessa tai ulkomailla sekä siihen liittyvien toimivaltuuksien käytöstä. Momentin viittaus kansainvälisessä yhteistyössä käytettävien toimivaltuuksien käytöstä viittaisi jäljempänä säädettyyn päätöksen tekomenettelyyn muualla kuin Suomen alueella ja tiedustelumenetelmien käytöstä.

Pykälän 3 momentissa kansainvälisillä velvoitteilla tarkoitettaisiin lähinnä kansainvälisiä tietoturvallisuussopimuksia, joita Suomi on jo solminut useiden merkittävien yhteistyötahojen kanssa. Lisäksi viitattaisiin kansainvälisistä tietoturvavelvoitteista annettuun lakiin, jolla on etusija soveltamisessa viranomaisten toiminnan julkisuudesta annetun lain (621/1999) sijaan.

4 luku. Tiedonhankintatoimivaltuudet

Luvussa säädettäisiin yleisistä tiedonhankintatoimivaltuuksista, jotka olisivat samantyyppisiä kuin jo poliisilla ja Puolustusvoimilla voimassa olevat rikoksen ennalta estämisen tiedonhankintatoimivaltuudet.

Luvussa säädettävien toimivaltuuksien lisäksi sotilastiedusteluviranomaisella on käytössään myös tiedonhankinnan keinoja, joiden käyttämiseen ei tarvita erityistä toimivaltuussääntelyä. Tällaisia ovat avointen lähteiden tiedustelu, kuvaustiedustelu ja geotiedustelu. Kyse on tiedonhankinnasta, jonka ei voitaisi katsoa loukkaavan yksityisyyden suojaa. Avointen lähteiden tiedustelua ei voida katsoa sellaiseksi viranomaisen toiminnaksi, josta perustuslain mukaan olisi säädettävä lailla.

Avointen lähteiden tiedustelulla tarkoitetaan muun muassa sotilastiedusteluviranomaisen tiedon hankintaa julkisista tiedotusvälineistä, julkisista viranomaisrekistereistä, julkisesti saatavilla olevista tietokannoista sekä julkisuudessa esitetyistä lausunnoista. Avoimista lähteistä saatu informaatio koostuisi tiedoista, jotka olisivat jokaisen yksityisen henkilön laillisesti saatavilla esimerkiksi pyytämällä tai itse havainnoimalla. Tyypillisiä tiedonlähteitä ovat kirjallisuus, tilastot, kartat, lehdet, julkaisut, yleisölle suunnatut televisio- ja radiolähetykset, viranomaiset sekä sosiaalinen media. Internetiä ei avointen lähteiden tiedustelussa käsitetä omana tiedonlähteenään, vaan kanavana, josta tietoa hankitaan. Avointen lähteiden tiedustelu voidaan jakaa tiedonhankintaan sekä mediaseurantaan, jonka pääasiallisena tarkoituksena on tiedustelutilannekuvan muodostamisen tukeminen.

Avointen lähteiden tiedustelua käytetään muiden tiedonhankintakeinojen tukena tai itsenäisenä tiedustelukeinona. Avointen lähteiden tiedonhankinnalle on ominaista tiedon suuri määrä ja disinformaation mahdollisuus. Toisaalta tiedonhankinnan vahvuuksiin kuuluvat sen nopeus, edullisuus, maantieteellinen rajoittamattomuus ja mahdollisuus kerätä tietoja tulevista tapahtumista. Pelkästään avoimiin lähteisiin perustuva tiedustelutieto on suojaustasoltaan muita tiedustelutietoja alhaisempi, jolloin tiedon käyttötapakin on monipuolisempi.

Kuvaustiedustelussa sotilastiedusteluviranomainen voi esimerkiksi elektro-optisin ja tutkakuvauksen keinoin hankkia tietoa alueesta, alueen kehityksestä ja sillä tapahtuvasta toiminnasta. Kuvaustiedustelu on strategisen tason tilannekuvan muodostamiseen liittyvän tiedon hankkimista, kyse ei ole tietojen hankkimisesta yksittäisistä ihmisistä. Tietoa hankittaisiin laajoista alueista ja niillä tapahtuvasta kehityksestä, jolla voi olla merkitystä Puolustusvoimien toiminnan kannalta, esimerkiksi vieraan valtion joukkojen sijoittamisessa tapahtuvista muutoksista.

Kuvaustiedustelu olisi välttämätöntä muun muassa turvallisuuspoliittisesti merkittävien tapahtumien arvioimiseksi riippumattomasti sekä itsenäisesti. Sotilastiedusteluviranomaisen näin hankkimat tiedot tukevat suoraan Suomen ulkopolitiikkaa muun muassa siinä, mikä valtio levittää joukkotuhoaseita. Kuvaustiedustelua voidaan käyttää myös esimerkiksi suomalaisen kriisinhallintajoukon turvallisuuden (omasuoja eli force protection) parantamiseksi. Kuvaustiedustelulla ei hankittaisi tietoja yksittäisistä henkilöistä eikä sitä voitaisi kohdistaan yksityisyyden suojaan kuuluviin asioihin.

Geotiedustelun keinoin sotilastiedelusteviranomainen voi muodostaa laajemman kuvan esimerkiksi vieraan valtion maantieteellisistä ja alueen toimintaympäristön olosuhteista. Geotiedustelun tarkoituksena on kuvata, arvioida ja esittää tietyt kohteet, alueet, luonnonilmiöt ja olosuhteet. Geotiedustelussa käytetään hyväksi muun muassa kansallista ja kansainvälistä paikkatieto- ja kuva-aineistoa, olosuhdetietoja sekä tilastollisia aineistoja. Sotilastiedusteluviranomainen voi myös tilata ulkopuolisilta toimijoilta tällaista tietoa oman tiedustelunsa tueksi.

Edellä tarkoitettujen tiedonhankintakeinojen lisäksi sotilastiedusteluviranomainen saa tiedustelun kannalta tarpeellista tietoa esimerkiksi Puolustusvoimien muilta yksiköiltä. Tällaista tietoa tuotetaan osana Puolustusvoimien normaaliin toimintaan. Sotilastiedustelun kannalta tarpeellista tietoa voi

syntyä esimerkiksi Maanpuolustuskorkeakoulun tutkimustyössä taikka aluevalvonnan yhteydessä. Lisäksi tietoa voidaan saada viranomaisyhteistyön kautta.

Henkilötiedustelulla tarkoitetaan henkilökohtaiseen kanssakäymiseen taikka henkilön tai muun kohteen henkilökohtaiseen havainnointiin perustuvaa tiedonhankintaa. Henkilötiedustelua voidaan harjoittaa esimerkiksi sosiaalisen median palveluiden välityksellä. Henkilötiedustelussa tiedonhankinta kohdistuu ihmisiin sekä heidän hallussaan oleviin asiakirjoihin ja sähköisiin tallenteisiin, jonka takia henkilötiedustelun toimivaltuuksista olisi säädettävä nimenomaisesti lailla.

Henkilötiedustelulla hankitaan keskeistä tietoa turvallisuusympäristöstä sekä esimerkiksi asevoimien, tiedustelupalveluiden, yksittäisten henkilöiden tai organisaatioiden toiminnasta sekä niiden kiinnostuksen kohteista Suomen maanpuolustukseen liittyvissä asioissa. Tiedot voivat koskea myös esimerkiksi asiakirjoja, suunnitelmia, yleistä mielialaa taikka henkilöiden välisiä suhteita. Henkilötiedustelua voitaisiin tässä luvussa säädettyjen toimivaltuuksien turvin toteuttaa ulkomailla tapahtuvan toiminnan ohella ulkomaisiin kohteisiin myös Suomessa. Henkilötiedustelun tiedonhankintatoimivaltuuksia olisivat esimerkiksi suunnitelmallinen tarkkailu, tekninen tarkkailu ja tietolähteen käyttäminen. Henkilötiedustelu kykenee tuottamaan sellaista yksityiskohtaista ja syvää, korkeimman suojaustason tietoa, jota muilla tiedustelulajeilla on vaikea tai mahdotonta tuottaa. Henkilötiedustelun avulla voidaan luoda edellytyksiä myös muiden tiedustelulajien tehokkaalle hyödyntämiselle.

Henkilötiedustelun tiedonhankintamenetelmillä pyritään aktiivisesti hankkimaan tietoa esimerkiksi asevoimien, tiedustelupalveluiden, yksittäisten henkilöiden tai organisaatioiden toiminnasta sekä niiden kiinnostuksen kohteista Suomen maanpuolustukseen liittyvissä asioissa.

Henkilötiedustelussa käytettävät tiedustelutoimivaltuudet muistuttaisivat toimivaltuuksina monilta kohdin jo nykyisin Puolustusvoimillakin osin käytössä olevia salaiseen tiedonhankintaan tarkoitettuja poliisilain 5 luvussa säädettyjä toimivaltuuksia. Henkilötiedustelun tiedonhankintamenetelmillä ei kuitenkaan, toisin kuin Puolustusvoimien rikostorjunnassa, hankita tietoa mahdollisesti tapahtuvista tai jo tapahtuneista rikoksista. Puolustusvoimien suorituskyvyn kehittämisen kannalta on olennaista saada tietoa esimerkiksi lähialueiden valtioiden aikeista ja suunnitelmista oman suorituskykynsä kehittämiseksi. Kyse saattaa olla tiedoista, joita ei ole saatavissa tavanomaisista dokumenteista tai viesteistä vaan esimerkiksi ihmisten keskenään käymistä keskusteluista, joista tiedon voi toimittaa vain keskusteluun osallistunut toinen osapuoli. Tällaisen tiedon hankkimisessa avustajan käytöllä ja siihen liittyvällä ehdottoman täydellisellä luottamuksella on keskeisen korostunut rooli.

Henkilötiedustelun tiedonhankintatoimivaltuuksilla pyrittäisiin tiedonhankinnan lisäksi myös suojaamaan ja varmistamaan tiedustelutoiminnan tapahtuminen riittävän turvallisesti ja luotettavasti. Kaikissa tilanteissa ei ole esimerkiksi tietolähteen turvallisuuden takaamiseksi tarkoituksen mukaista esiintyä tiedusteluviranomaisena tai tiedustelutehtävän suorittamisen turvaamiseksi ottaa yhteys mahdolliseen tietolähteeseen. Sotilastiedusteluviranomaisen tiedonhankintatarkoituksen paljastuminen voitaisiin estää käyttämällä esimerkiksi vääriä henkilötietoja tai peitehenkilöllisyyttä. Paljastuminen olisi syytä estää tarvittaessa jo ennen kuin sotilastiedusteluviranomainen tekisi esimerkiksi ratkaisun tietolähteen käyttämisestä. Sotilastiedusteluviranomaisen tulisi voida varmistua myös vapaaehtoisesti sotilasviranomaista avustavan henkilön todellisesta vapaaehtoisuudesta tehtävään ja muista motiiveista.

Henkilötiedustelu voi tapahtua niin Suomen alueella kuin Suomen rajan ulkopuolella. Henkilötiedustelu kohdistuu nimenomaisesti ulkomaisiin kohteisiin ja olosuhteisiin, vaikka ne olisivatkin Suomen alueella. Tarkoituksena on tuottaa tilannekuvan ja suorituskyvyn tueksi välttämätöntä tietoa, jonka pohjalta ylin valtiojohto johtaa välttämätöntä tietoa ulko-, turvallisuus- ja puolustuspoliittisen päätöksentekonsa tueksi.

Ulkomailla tapahtuvan henkilötiedustelun luonteesta johtuen toiminnan yleismaailmallisena lähtökohtana on, että tarvittavat tiedot pyritään hankkimaan kevyimmällä mahdollisella keinolla. Käytännössä tiedustelu perustuu usein yhteystoimintaa 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 ulkomaan tiedustelutoiminta 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.

Ulkomaan henkilötiedustelua voidaan harjoittaa myös siten, että viestintä tapahtuu tietoverkon viestintäpalveluiden välityksellä Suomesta.

Henkilötiedusteluun esitettävien Puolustusvoimille uusien tiedonhankintakeinojen käyttöönotto velvoittaisi sotilastiedusteluviranomaista varmistumaan siitä, että tiedustelua toteuttava henkilöstö on asianmukaisesti koulutettu ja henkilöstö on muutenkin hankkinut riittävän perehtyneisyyden tehtäviinsä. Toimivaltuuksien käytännön koulutuksessa olisi osin mahdollista hyödyntää Puolustusvoimien rikostorjunnan tehtävissä nykyisin palvelevien virkamiesten ammattitaitoa. Heillä olisi pidempiaikaista kokemusta rikosperusteisesta sotilasvastatiedustelun ja henkilötiedustelun tehtävistä. Joitain osia koulutuksesta voitaisiin mahdollisesti suunnitella ja toteuttaa myös yhteistoiminnassa suojelupoliisin kanssa, kansainvälisellä yhteistyöllä saatavalla koulutuksella sekä muulla perehtymisellä.

Reserviläiskoulutuksesta Puolustusvoimat vastaisi osana normaalia asevelvollisten kertausharjoitusjärjestelmää asevelvollisuuslain 32 §:n mukaisesti. Toiminnan erityisluonteen vuoksi toimivaltuuksien koulutusta ei olisi mahdollista hankkia vapaaehtoisesta maanpuolustuksesta annetun lain (556/2007) mukaisin toimenpitein.

Lain 4 luvussa säädettäisiin myös muista kuin perinteisiksi katsottavista tiedustelumenetelmistä. Näitä olisivat radiosignaalitiedustelu sekä ulkomaan tietojärjestelmätiedustelu. Näissä olisi kyse nimenomaisesti teknisin menetelmin toteutettavasta tiedonhankinnasta, jossa kohteena ei pääasiallisesti ole henkilöiden välinen toiminta eikä niistä voi saada tietoa henkilökohtaisesti tilanteeseen osallistumalla. Lisäksi puheena olevia tiedustelumenetelmiä käytettäisiin Suomen alueelta kohteen ollessa Suomen alueen ulkopuolella.

Luvussa säädettyjen tiedonhankintatoimivaltuuksien käytön osalta on huomioita se, mistä sotilastiedustelun kohteesta niillä hankittaisiin tietoa. Vireillä olevan perustuslain 10 §:n 3 momenttia koskevan muutosehdotuksen mukaan luottamuksellisen viestin salaisuutta voidaan rajoittaa lailla, jos kohteena on sotilaallinen toiminta tai kansallista turvallisuutta vakavasti uhkaava toiminta. Koska kaikki sotilastiedustelun kohteisiin liittyvä toiminta ei ole katsottavissa sotilaalliseksi toiminnaksi tai kansallista turvallisuutta vakavasti vaarantavaksi toiminnaksi, kuten yksityisen yrityksen tuotekehitys, kaikki tiedustelumenetelmät eivät ole kaikissa tilanteissa käytettävissä. Näin ollen tiedustelumenetelmän käytöstä päättävän tahon olisi päätöstä tehdessään tai lupaa antaessaan kiinnitettävä erityistä huomiota siihen, onko tiedustelumenetelmän käytön kohde sellainen, jonka luottamuksellisen viestin salaisuuteen voidaan puuttua.

19 §. *Tarkkailu ja suunnitelmallinen tarkkailu.* Pykälän 1 momentissa määriteltäisiin tarkkailu. Tarkkailu olisi mahdollista, jos 10 §:ssä tarkoitetut yleiset edellytykset täyttyvät. Lisäksi toiminnassa tulisi ottaa huomioon yleiset periaatteet. Tarkkailu olisi henkilöön, esineeseen, aineeseen, omaisuuteen, tilaan, tai alueeseen tiedonhankintatarkoituksessa kohdistuvaa havainnointia. Toimenpiteelle on luonteenomaista havaintojen tekeminen huomaamattomasti. Tarkkailu voidaan toteuttaa siten, ettei tiedonhankinnan kohde havaitse olevansa kohteena, vaikka sinänsä havainnointi toteutettaisiin täysin avoimesti. Kysymykseen tulee siten sekä havaintojen tekeminen sinänsä salaa että niiden tekeminen tiedonhankintatarkoitus salaten.

Havaintojen tekeminen viittaa havainnoitsijan läsnäoloon tarkkailun kohteen kanssa esimerkiksi samassa tilassa tai tilanteessa sekä havainnoitsijan ja tarkkailun kohteen välisen vuorovaikutuksen passiivisuuteen. Tämä ei estä vuorovaikutusta kohteen kanssa tilanteessa, jossa on vaarana esimerkiksi tiedonhankinnan paljastuminen. Havaintojen tekijä voi tarvittaessa poistua tilanteesta vuorovaikutuksen keinoin, käytännössä esimerkiksi keskustelemalla tiedonhankinnan kohteen kanssa.

Tarkkailun kohteena voisi olla henkilöiden lisäksi myös esimerkiksi suuri erä tiettyä ainetta tai muuta omaisuutta, jota voidaan käyttää esimerkiksi sotilaalliseen toimintaan verrattavan vahingon aiheuttamiseen. Lisäksi yhteiskunnan toiminnan kannalta kriittisten alueiden ja kohteiden kartoittaminen ja maalittaminen ovat Suomeen kohdistuvan sotilaallisen tiedustelutoiminnan keskeisiä kohteita. Tarkkailua voitaisiin käyttää edellä kuvatuista kohteista kiinnostuneiden henkilöiden kartoittamisessa.

Tarkkailussa saisi käyttää omien aistihavaintojen tukena muun ohessa kiikaria, kameraa, videokameraa, valonvahvistinta tai muuta vastaavanlaista teknistä laitetta. Tällä tarkoitettaisiin havainnoinnin yhteydessä muun muassa teknisellä laitteella, menetelmällä tai ohjelmistolla tapahtuvaa kuvan tai äänen tallentamista, tiedon keräämistä ja niiden käsittelyä. Kuvan ja äänen tallennus havainnoinnin yhteydessä olisi tarpeellista esimerkiksi erilaisten tapahtumien dokumentoimisessa sekä niiden todentamisessa jälkikäteen. Apuvälineiden tulisi olla havaintojen tekijän hallinnassa koko havainnoinnin ajan.

Pykälän 2 momentin mukaan suunnitelmallisella tarkkailulla tarkoitetaan muun kuin lyhytaikaisen tarkkailun kohdistamista henkilöön tai henkilöryhmään, jonka voidaan perustellusti olettaa liittyvän tiedustelutehtävään. Tiedustelumenetelmien käyttöedellytysten mukaisesti tiedustelumenetelmää voidaan käyttää salassa sen kohteelta, mikä tarkoittaisi myös tarkkailua vastaavasti, että vuorovaikutusta kohteen kanssa tulisi välttää.

Suunnitelmalliselle tarkkailulle ei voida määrittää mitään vähimmäiskestoa. Tällaiseen tarkkailuun tarvittava vähimmäisaika riippuisi tapauskohtaisista olosuhteista. Tarkkailu voitaisiin katsoa suunnitelmalliseksi myös silloin, kun tarkkailu ei kerrallaan kestä pitkää aikaa, mutta se toistetaan jonkin ajan kuluttua. Lyhytkestoisuuden arvioinnin kannalta merkityksellistä olisi siis ensimmäisen ja viimeisen tarkkailutoimenpiteen välinen aika. Suunnitelmalliselle tarkkailulle olisi tyypillistä sen seuraaminen, mitä rikoksesta epäilty tekee ja keitä henkilöitä hän tapaa. Momentin mukaan ainoastaan siinä tarkoitetun henkilön tai henkilöryhmän suunnitelmallinen tarkkailu olisi mahdollista. Muihin kuin häneen tai heihin kohdistuva tarkkailu olisi siten mahdollista ainoastaan lyhytkestoisena yksittäisenä toimenpiteenä lähinnä siitä syystä, että oikean tarkkailukohteen varmistamiseksi käytännössä joudutaan kohdistamaan havaintojen tekemistä myös muihin ihmisiin.

Pykälän 3 momentin mukaan sotilastiedusteluviranomainen voisi käyttää suunnitelmallista tarkkailua, jos sillä olisi erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Erittäin tärkeä merkitys -kynnystä on selostetta aiemmin tässä esityksessä 10 §:n yksityiskohtaisissa perusteluissa.

Suunnitelmallisella tarkkailulla ei saisikaan hankkia tietoa esimerkiksi sattuman varaisista henkilöistä, vaan havainnoinnin kohdistumisen kohteeseen olisi aina voitava olla perusteltua. Tämä tarkoittaisi sitä, että sotilastiedusteluviranomaisella olisi jo ennakkoon käsitys siitä, että tiettyyn tiedustelutehtävän kannalta merkitykselliseen kohteeseen kannattaisi kohdistaa havainnointia. Tiedustelutehtävä itsessään rajaisi jo kohteet, joista voidaan olettaa saatavan olennaista tietoa. Toimivaltuuden käyttämisestä päättävän tulisi olla vakuuttunut siitä, että juuri kyseistä kohdetta havainnoimalla voitaisiin saada tiedustelutehtävän kannalta tarpeellisia tietoja.

Pykälän toimivaltuuksien kohdentamista rajoittaisi 4 momentin kielto kohdistaa toimivaltuuden käyttöä vakituiseen asumiseen käytettävään tilaan.

20 §. *Suunnitelmallisesta tarkkailusta päättäminen.* Pykälän 1 momentin mukaan suunnitelmallisesta tarkkailusta päättäisi tiedustelumenetelmien käyttöön erityisesti perehtynyt lakimies tai virkamies. Päätös olisi tehtävä jokaisen havainnoinnin kohteen osalta erikseen ja siinä olisi yksilöitävä jokaisen havainnoinnin kohteeksi joutuva henkilö.

Päätöksenteosta suunnitelmallisesta tarkkailusta olisi tarpeen säätää erotuksena tarkkailusta, koska toiminta on pitkäkestoisempaa ja suunnitelmallisempaa. Tästä johtuen toimivaltuus puuttuu yksityiselämän suojaan laajemmin kuin tarkkailu.

Päätöksentekijänä suunnitelmallisessa tarkkailussa olisi tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.Tiedustelumenetelmien käytössä voi tulla eteen tulkinnanvaraisia tilanteita toimivaltuuksien rajojen suhteen. Tämän takia olisi tarkoituksenmukaista, että päätöksentekijä olisi perehtynyt tiedustelumenetelmien käyttöön. Tiedustelumenetelmät ovat kokonaisuutena laaja valikoima keinoja, jotka ovat lähellä toisiaan. Tiedustelumenetelmien koko keinovalikoiman kirjon tunteminen on edellytyksenä päätöksentekijällä, sillä muussa tilanteessa päätöksentekijällä ei olisi riittävästi pohjaa sen harkitsemiseksi, mikä tiedustelumeneltemä on tietyssäkin tilanteessa tarkoituksenmukaisin ja sallittu.

Perehtyneisyysvaatimus voisi täyttyä joko salaiseen tiedonhankintaan liittyvällä koulutuksella tai riittävällä kokemuksella salaisen tiedonhankinnan käyttämisestä taikka tiedustelumenetelmien käyttämisestä. Lisäksi virkamiehen olisi oltava perehtynyt tiedustelutoimivaltuuksia koskevaan lainsäädäntöön. Tiedustelumenetelmien käyttöön ei ole tiettyä koulutusohjelmaa, joten riittävä perehtyneisyys voitaisiin saavuttaa muilla keinoin. Sotilastiedusteluviranomaisen sisäisen harkinnan varaan jäisi se, keillä katsottaisiin olevan riittävä perehtyneisyys tiedustelumenetelmien käyttöön. Viime kädessä riittävästä perehtyneisyyden arvioinnista vastaisi sotilastiedusteluviranomaisen johtaja.

Momentissa olisi tarkoituksen mukaista mainita myös erikseen sotilaslakimies. Sotilaslakimiehellä on koulutuksensa puolesta perehtyneisyys etenkin lainsäädännöllisiin kysymyksiin. Tämän takia sotilaslakimiehellä olisi tarvittava osaaminen päätöksen edellyttämien perusteluiden laatimisesta, juridisesta argumentoinnista sekä tulkinnanvaraisten tilanteiden rajanvedosta. Tiedustelumenetelmien käyttöön perehtyminen vaatii aikaa, joten riittävän perehtyneisyyden saavutettuaan myös muut virkamiehet voisivat tehdä päätöksiä.

Pykälän 2 momentin mukaan päätös voitaisiin tehdä enintään kuudeksi kuukaudeksi kerrallaan. Päätöksentekijän harkintaa rajaisivat aiemmin laissa säädetyt suhteellisuus- ja vähimmän haitan periaatteet sekä tarkoitussidonnaisuuden ja syrjimättömyyden periaatteet. Säännöksessä tarkoitetut kuuden kuukauden päätöksen kestoaika ei kuitenkaan automaattisesti tarkoittaisi sitä, että päätös voitaisiin aina tehdä kuudeksi kuukaudeksi. Harkittaessa päätöksen voimassaoloaikaa, erityistä huomiota olisi kiinnitettävä suhteellisuus- ja vähimmän haitan periaatteisiin. Siksi lupaa hakiessa sekä sitä myönnettäessä tulisi harkita tiedustelumenetelmän käytön ajallisen keston tarpeellisuutta tapauskohtaisesti.

Pykälän 3 momentissa säädettäisiin vaatimuksessa ja päätöksessä mainittavista seikoista. Momentin 1 kohdassa toimenpiteen perusteena olevalla tiedustelutehtävällä tarkoitettaisiin 13 §:ssä tarkoitettua tiedustelutehtävää, joka perustuisi 4 §:ssä oleviin sotilastiedustelun kohteisiin ja 16 §:ssä tarkoitettuun tietopyyntöön tai Puolustusvoimien hallintoyksikön toimeksiantoon. Tiedustelutehtävän tulisi olla tiedustelumenetelmän käytön perusteena. Lisäksi päätöksessä tulisi ilmetä toimenpiteen tavoite, mihin tiedustelumenetelmän käytöllä pyrittäisiin. Tavoite tulisi määritellä riittävällä tarkkuudella.

Momentin 2 kohdassa säädettäisiin edellytyksestä sisällyttää päätöksen tiedustelumenetelmän käytön kohde. Suunnitelmallisen tarkkailun kohteena voisi olla henkilö tai henkilöryhmä. Päätöksessä tulisi osoittaa perustellusti, että tietty henkilö tai henkilöryhmä liittyy tiedustelutehtävään.

Sotilastiedustelussa voi ilmetä tarve seurata tietyn henkilötyhmän toimintaa passiivisesti tai aktiivisesti. Suunnitelmallisessa tarkkailussa tiedonhankinta olisi kuitenkin enemmän passiivista. Koska tiedustelumenetelmän käytössä kysymys ei olisi rikostorjuntaan tähtäävistä toimista, niin tietyn henkilön yksilöinnin kautta ei sotilastiedustelussa ilmene vastaavanlaista tarvetta arvioida toimivaltuuksien käytön erityisiä edellytyksiä, kuten onko kyseistä henkilöä syytä epäillä tietystä rikoksesta tai voidaanko hänen olettaa syyllistyvän sellaiseen. Sotilastiedustelussa olisi tarkoituksena esimerkiksi hankkia tietoa tietyn henkilöryhmän organisaatiosta, ryhmään kuuluvista henkilöistä ja henkilöryhmän aktiivisuudesta tietyillä alueilla sekä ryhmän toiminnan eri muodoista. Tiedoilla voisi olla merkitystä päätöksenteossa muihin tiedustelumenetelmiin liittyen niin operatiivisella kuin strategisella tasolla. Sotilastiedustelun suorittamassa suunnitelmallisessa tarkkailussa toimivaltuuden käytön kynnyksenä on se, että suunnitelmallisella tarkkailulla voidaan olettaa saatavan tietoja tiedustelutehtävään.

Momentin 3 kohta olisi päätöksenteon kannalta merkityksellinen. Kohdan mukaan vaatimukseen ja päätökseen tulisi sisällyttää ne tosiseikat, joihin suunnitelmallisen tarkkailun edellytykset ja kohdistaminen perustuisivat. Tosiseikkojen esittäminen päätöksentekijälle velvoittaa esittämään ja perustelemaan ne tosiseikat, joiden perusteella päätöksentekijä voisi tehdä omat johtopäätöksensä edellytysten täyttymisestä. Mainituissa edellytyksissä olisi kyse 10 §:n tiedustelumenetelmien yleisistä edellytyksistä ja toimivaltuutta koskevassa 19 §:ssä mainituista edellytyksistä. Lisäksi päätöksessä olisi esitettävä riittävät tosiseikat tiedustelutehtävästä ja sen pohjana olevasta lain 4 §:ssä tarkoitetusta sotilastiedustelun kohteesta sekä 9 §:ssä tarkoitetusta tietopyynnöstä tai muusta toimeksiannosta. Suhteellisuusperiaatteen kannalta tärkeässä asemassa olisi erityisesti se, kuinka vakavasta toiminnan ilmenemismuodosta olisi kysymys.

Momentin 4 kohdan mukaan päätökseen olisi sisällytettävä suunnitelmallista tarkkailua koskevan päätöksen voimassaoloaika.

Momentin 5 kohdan mukaan päätöksessä olisi mainittava suunnitelmallisen tarkkailun suorittamista johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies.

Momentin 6 kohdan mukaan vaatimukseen tai päätökseen tulisi sisällyttää mahdolliset suunnitelmallisen tarkkailun rajoitukset ja ehdot. Päätöksessä voitaisiin asettaa suunnitelmalliselle tarkkailulle rajoituksia ja käyttöehtoja.

21 §. *Peitelty tiedonhankinta.* Pykälän 1 momentin mukaan peitellyllä tiedonhankinnalla tarkoitettaisiin tiettyyn henkilöön kohdistuvaa lyhytkestoisessa vuorovaikutuksessa tapahtuvaa tiedonhankintaa, jossa sotilastiedusteluviranomaisen tehtävän salaamiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja.

Peitellyn tiedonhankinnan käytön tilanteista voidaan mainita esimerkkinä tilanne, jossa tiedustelutehtävään liittyvältä kohteelta pitäisi arkipäiväisessä tilanteessa kysyä tämän matkakohteesta tai kielitaidon selvittämiseksi niin, ettei virkamiehen tarvitse paljastaa omaa henkilöllisyyttään.

Lisäksi toimivaltuuden piiriin kuuluisi esimerkiksi tietyn henkilölle tarkoitetun lähetyksen toimittaminen perille lähettinä esiintyen. Tällaisissa tilanteissa on mahdollista, että lähetyksen ottaa vastaan muu kuin 2 momentissa tarkoitettu henkilö. Peiteltyä tiedonhankintaa voisi olla myös se, että Puolustusvoimien tiedustelulaitoksen virkamies tarjoilijaksi tekeytyneenä harjoittaa tiedonhankintaa ravintolassa mainitun henkilön läheisyydessä. Tarkkaa aikarajaa peitellyn tiedonhankinnan kestolle ei voida antaa, koska vuorovaikutuksen toinen osapuoli voi omilla toimillaan pitkittää tilannetta, vaikka tiedonhankinnan tavoite olisikin jo saavutettu. Epäluonteva irtautuminen tilanteesta voisi myös paljastaa tiedonhankinnan.

Erotuksena tarkkailusta ja suunnitelmallisesta tarkkailusta toimivaltuuden käytölle olisi luonteenomaista nimenomaan pyrkimys henkilökohtaiseen tapaamiseen tai vastaavaan vuorovaikutukseen tiedustelutehtävään liittyvän kohteen kanssa, ei kuitenkaan vastaavanlaiseen pitkäaikaiseen kanssakäymiseen ja erityisen luottamussuhteen muodostamiseen kuin peitetoiminnassa. Peitellyssä tiedonhankinnassa ei siten olisi kysymys soluttautumisesta.

Toimivaltuutta ei saisi käyttää peitetoimintaa koskevan sääntelyn kiertämiseksi. Muutenkaan ei olisi tarkoitus korvata peitetoimintaa koskevaa sääntelyä. Peitetoiminnan käynnistäminen olisi kuitenkin tarpeettoman raskas menettely tällaista lyhytkestoista yksittäistä tiedonhankintatapahtumaa varten. Sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen koulutusvelvollisuuden vaatimuksesta johtuu, että tällaisen virkamiehen olisi erityisen tärkeä tiedostaa peitellyn tiedonhankinnan ja peitetoiminnan raja, jotta toimivaltuutta ei käytettäisi siten, että kysymys olisi tosiasiallisesti peitetoiminnasta. Koulutuksella voidaan myös vähentää tiedonhankinnan paljastumisen riskiä sekä edistää toiminnan tuloksellisuutta. Vielä peiteltyä tiedonhankintaa voimakkaammin nämä näkökohdat liittyvät peitetoimintaan ja valeostoon.

Toiminnan luonteeseen kuuluisi lisäksi ainoastaan väärien, harhauttavien tai peiteltyjen tietojen käyttäminen. Esimerkkinä voidaan mainita kuljetustoimintaa harjoittavan yhtiön haalareiden ja nimikyltin käyttäminen. Tällaista suojausta voitaisiin käyttää ainoastaan Puolustusvoimien tiedustelulaitoksen tehtävän salaamiseksi, toisin sanoen tiedonhankinnan paljastumisen estämiseksi. Tiedonhankinnan suojaaminen olisi mahdollista 80 §:n mukaisesti.

Pykälän 3 momentin mukaan peitelty tiedonhankinta ei olisi sallittua asunnossa edes asunnonhaltijan myötävaikutuksella.

22 §. *Peitellystä tiedonhankinnasta päättäminen.* Pykälän 1 momentin mukaan pääesikunnan tiedustelupäällikkö tai tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättäisi peitellystä tiedonhankinnasta. Kuten edellä 20 §:n yksityiskohtaisissa perusteluissa on todettu. tiedustelumenetelmien käyttöön erityisesti perehtyneellä sotilaslakimiehellä tai muulla virkamiehellä on korostuneesti velvollisuus tunnistaa se, onko tilanteessa kyseessä peitellyn tiedonhankinnan käyttö vai peitetoiminta.

Tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai virkamiehen koulutusvelvoitteen myötä päätöksen tekevällä taholla olisi erityiset tiedot peitellyn tiedonhankinnan ja peitetoiminnan rajasta, jotta toimivaltuutta ei käytettäisi siten, että kysymys olisi tosiasiallisesti peitetoiminnasta. Koulutuksella voitaisiin myös vähentää paljastumisen riskiä.

Pykälän 2 momentin mukaan päätös peitellystä tiedonhankinnasta olisi tehtävä kirjallisesti. Päätöksessä olisi mainittava: 1) toimenpide ja sen tavoite sekä toimenpiteen perusteena oleva tiedustelutehtävä, 2) toimenpiteen kohteena oleva henkilö tai henkilöryhmä, 3) tosiseikat, joihin peitellyn

tiedonhankinnan edellytykset ja kohdistaminen perustuvat, 4) peitellyn tiedonhankinnan suorittamista johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies, 5) toimenpiteen suunniteltu toteuttamisajankohta, 6) mahdolliset peitellyn tiedonhankinnan rajoitukset ja ehdot.

Kuten muidenkin tiedustelumenetelmien osalta, myös peiteltyä tiedonhankintaa koskevassa päätöksessä tulisi kertoa henkilöön tai henkilöryhmään kohdistuvan tiedonhankinnan taustalla olevat tosiseikat, joiden perusteella olisi ulkopuolisen tarkastelijan mahdollista tehdä tiedustelumenetelmän käytön edellytysten olemassaolosta omat johtopäätöksensä.

Toimenpiteellä tarkoitettaisiin varsinaista peitellyn tiedonhankinnan toimenpidettä, kuten esimerkiksi sitä, että kysymyksessä on toimiminen tarjoilijana tai lähettinä. Toimivaltuuden käytön osalta edellytettäisiin erikseen siitä vastaavan Puolustusvoimien tiedustelulaitoksen virkamiehen nimeämistä, jonka tehtävänä olisi huolehtia muun muassa siitä, ettei toiminnassa ole tosiasiallisesti kysymys peitetoiminnasta eikä taksikuskina toimiva peitemies ryhtyisi luomaan luottamuksellista suhdetta kuljetettavana olevaan.

Peitellyn tiedonhankinnan osalta ei edellytettäisi alkamis- ja päättymisajankohdan määrittelyä kellonaikatarkkuudella, koska kysymys on useimmiten yksittäisen toimenpiteen suorittamisesta ennakolta määräämättömänä ajankohtana. On mahdollista, että peitelty tiedonhankinta tapahtuu tiettynä päivänä tai tiettynä viikkona.

Peitellyn tiedonhankinnan osalta päätöksentekijä voisi asettaa rajoituksia ja ehtoja kuten muidenkin tiedustelumenetelmien käytön yhteydessä. Rajoitukset voisivat johtua esimerkiksi suhteellisuusperiaatteesta sekä tarkoituksenmukaisuus-, oikeusturva- ja työturvallisuusnäkökohdista.

Peitellyn tiedonhankinnan osalta päätöksentekijä voisi asettaa rajoituksia ja ehtoja, kuten muidenkin tiedustelumenetelmien käytön yhteydessä. Rajoitukset voisivat johtua esimerkiksi suhteellisuusperiaatteesta sekä tarkoituksenmukaisuus-, oikeusturva- ja työturvallisuusnäkökohdista.

Pykälän 3 momentin mukaan päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava. Tiedusteluoperaatiossa on mahdollista, että tiedonhankinnan kohde täsmentyy, jolloin tiedustelumenetelmän käyttö tulisi kohdistaa siihen henkilöön tai henkilöryhmään, josta on alun perinkin ollut tarkoitus hankkia tietoa. Tämä velvoittaisi toimenpiteestä vastaavan seuraamaan peitellyn tiedonhankinnan edellytysten olemassaoloa ja tiedonhankinnan tarpeellisuutta erityisesti silloin, kun päätöksentekohetki ja tiedonhankinnan toteuttaminen eroavat ajallisesti paljon toisistaan.

Pykälän 4 momentin mukaan jos toimenpide ei siedä viivytystä, 1 momentissa tarkoitettua päätöstä ei tarvitse laatia kirjallisesti ennen peiteltyä tiedonhankintaa. Päätös on kuitenkin laadittava kirjallisesti viipymättä toimenpiteen jälkeen.

Sotilastiedusteluviranomainen voisi tilanteen edellyttäessä ryhtyä kiireellisesti toteuttamaan peiteltyä tiedonhankintaa. Tämä ei poistaisi päätöksen kirjallisuusvaatimusta, vaan mahdollistaisi tiedustelumenetelmän käytön nopeassa tilanteessa. Päätös peitellystä tiedonhankinnasta olisi tehtävä kirjallisesti heti, kun se olisi mahdollista. Kiiretilanteessa tulisi huolehtia siitä, että toimenpiteen suorittajalle on tämän työturvallisuuden ja oikeusturvan kannalta kerrottu päätökseen kirjattavat tiedot suullisesti. Kiiretilanteessa korostuu päätöstä tekevän virkamiehen ammattitaito ja osaaminen.

23 §. *Tekninen kuuntelu.* Pykälän 1 momentin mukaan sotilastiedusteluviranomaisella olisi oikeus tietojen hankkimiseksi tiedustelutehtävän suorittamiseksi muualla kuin vakituiseen asumiseen käytettävässä tilassa suoritettavaan tekniseen kuunteluun. Tekninen kuuntelu eroaisi tarkkailusta siinä, että teknisessä kuuntelussa käytettäisiin paikkaan sijoitettuja teknisiä laitteita, menetelmiä tai ohjelmistoja.

Teknisellä kuuntelulla tarkoitettaisiin rikoslain 24 luvun 5 §:n estämättä tapahtuvaa tietyn henkilön sellaisen keskustelun tai viestin, joka ei ole ulkopuolisen tietoon tarkoitettu ja johon keskusteluun kuunteluja ei osallistu, kuuntelua, tallentamista ja muuta käsittelyä teknisellä laitteella, menetelmällä tai ohjelmistolla keskustelun tai viestin sisällön tai sen osapuolten toiminnan selvittämiseksi. Momentissa mainittaisiin kuuntelun ja tallentamisen ohella myös muunlainen keskustelun tai viestin käsittely sekä tekniikkaneutraalisti teknisen laitteen ohella myös menetelmät ja ohjelmistot.

Tekninen kuuntelu on liitännäinen usein suunnitelmalliseen tarkkailuun. Teknisellä kuuntelulla voidaan saada tietoa esimerkiksi siitä, milloin suunnitelmallisen tarkkailun kohteena oleva henkilö lähtee liikkeelle, jonka jälkeen suunnitelmallista tarkkailu voidaan taas aloittaa aktiivisesti.

Esimerkkinä voidaan mainita tilanne, jossa kaksi Suomessa olevaa vieraan valtion sotilastiedusteluorganisaation edustajaa tapaavat, Tilanteen kannalta voi olla tarpeen saada tieto siitä, mistä he keskustelevat. Tällöin Puolustusvoimien tiedustelulaitoksen virkamies voisi esimerkiksi älypuhelimella nauhoittaa keskustelun siihen itse lainkaan osallistumatta.

Teknisen kuuntelun tarkoituksena on hankkia tietoa ainoastaan tiedustelutehtävään liittyen. On kuitenkin todennäköistä, että tiedustelumenetelmän rikostorjuntatoimivaltuuksiin nähden laveampien kohdistamisedellytysten (henkilö, henkilöryhmä, tila tai muu paikka) takia myös muut kuin tiedustelutehtävän kannalta relevantit henkilöt joutuvat väistämättä kuuntelun kohteeksi. Tämän takia olisi välttämätöntä, että muun muassa tiedustelutehtävään liittymättömät tiedot hävitettäisiin välittömästi. Toisaalta sotilastiedustelun kannalta tilaan kohdistuvan tekninen kuuntelu voisi olla merkityksellistä myös sen selvittämiseksi, ettei tiettyä tilaa käytetä.

Tekninen kuuntelu kattaisi myös tilanteet, joissa teknisesti tarkkailtaisiin sähköpostin lähettämisen yhteydessä tapahtuvaa tietokonepäätteen näppäimistöä.

Tekninen kuuntelu olisi mahdollista, jos tiedonhankinta olisi kohdennettava vapautensa menettäneeseen. Vaikka sotilastiedustelulla ei ole toimivaltuutta ottaa kiinni henkilöitä, tilanne voisi tulla kyseeseen muiden viranomaisten kiinni ottamien henkilöiden kohdalla, kuten Tullin ja Rajavartiolaitoksen kiinni ottamien henkilöiden kohdalla voisi olla kyse.

Teknistä kuuntelua ei saisi kohdistaa vakituiseen asumiseen käytettävään tilaan. Merkitystä ei olisi sillä, mihin tekninen laite, menetelmä tai ohjelmisto asennetaan. Merkityksellistä olisi se mihin teknistä kuuntelua kohdistetaan.

Sotilastiedustelutoiminnassa erotuksena poliisilain 5 luvun 17 §:n teknisen kuuntelun käyttötilanteissa, olisi huomioitava myös se, ettei Puolustusvoimilla ole oikeutta ottaa kiinni henkilöä. Tästä johtuen sotilastiedustelutoiminnassa ei olisi tarvetta vapautensa menettäneen henkilön tekniseen kuunteluun normaalioloissa.

Teknisen kuuntelun määritelmässä määritettäisiin tiedonhankintakeinon suhde rikoslaissa kiellettyyn toimintaan. Rikoslain 24 luvun 5 §:n 1 momentissa säädetään rangaistavaksi salakuuntelu. Ilmaisu rikoslain estämättä tarkoittaisi sitä, että teknisen havainnoinnin yhteydessä ei syyllistytä salakuunteluun tai -katseluun, kunhan kyseistä tiedustelumenetelmää käytetään asianmukaisesti. Tämä tarkoittaa sitä, että päätös teknisen kuuntelun käyttämisestä on syntynyt oikeassa järjestyksessä ja että teknistä kuuntelua käytetään lainmukaisesti.

Teknistä kuuntelua voidaan toteuttaa reaaliaikaisesti tai passiivisesti. Reaaliaikaisessa teknisessä kuuntelussa olisi kiinnitettävä huomiota siihen, onko tiedustelumenetelmän käytön kohteena oleva henkilö tilassa vai ei sekä keskeytettävä tekninen kuuntelua sen ajaksi, jos tiedustelumenetelmän käytön kohteena oleva henkilö poistuu tilasta muuten kuin hetkellisesti. Passiivisessa teknisessä kuuntelussa edellä sanottu toteutettaisiin sotilastiedustelun viranomaisille asetettujen tallenteiden

tarkastamista sekä asiaankuulumattoman ja tarpeettoman tiedon hävittämistä koskevien velvollisuuksien kautta.

Teknisen kuuntelun määritelmää liittyy se, että esimerkiksi julkisessa tilassa käytävää kovaäänistä keskustelua koskeva tiedonhankinta ei edellytä tiedustelumenetelmien käyttöä. Sama koskee keskustelua, johon kuuntelija osallistuu. Teknistä kuuntelua ei olisi myöskään se, että kuuntelulaitteella seurataan epäillyn henkilön liikkumisen aiheuttamia ääniä. Teknistä kuuntelua olisi puolestaan se, että teknisellä laitteella kuunnellaan tai tallennetaan, mitä puhelinkeskustelun toinen osapuoli sanoo puhelimeen, kun kuuntelu kohdistuu puheen synnyttämiin ääniaaltoihin.

Tietyn henkilön kuuntelua teknisellä laitteella ei pidettäisi teknisenä kuunteluna, jos laite ei ole paikkaan sijoitettu. Näissä tapauksissa toimenpiteen kestosta riippuen kysymyksessä olisi tarkkailu tai suunnitelmallinen tarkkailu. Paikkaan sijoittamista koskeva vaatimus tarkoittaisi käytännössä sitä, että teknisen havainnoinnin toteuttaminen ei ole lyhytaikaista toimintaa. Paikkaan sijoitetulla tarkoitettaisiin esimerkiksi sitä, että laite, menetelmä tai ohjelmisto on kiinnitetty seinään, kattoon tai muuhun kiinnittämiseen soveltuvaan kohteeseen. Lisäksi tekniselle kuuntelulle sen määritelmästä johtuen olisi ominaista, että laite, menetelmä tai ohjelmisto seuraisi kohdetta yleensä ilman sotilastiedusteluviranomaisen samanaikaista havaintojen tekemistä ja paikallaoloa. Seurantalaitteen asentamisesta ja poisottamisesta säädettäisiin jäljempänä. Jos kysymys on sellaisesta kohdehenkilön seurannasta, jossa virkamies reaaliaikaisesti käyttää hallussaan olevaa laitetta kohdehenkilön havainnointiin, toimenpide olisi suunnitelmallista tarkkailua.

Pykälän 1 momentissa mainittaisiin kuuntelun ja tallentamisen ohella myös muunlainen keskustelun tai viestin käsittely. Tällä tarkoitettaisiin muun muassa sähköpostin lähettämisen yhteydessä tapahtuvaa tietokonepäätteen näppäimistön käytön teknistä tarkkailua, josta käytetään myös termiä näppäimistökuuntelu. Momentin määritelmäsäännöksessä todettaisiin nimenomaisesti, että teknisen havainnoinnin tavoitteena on myös keskustelun tai viestin sisällön selvittäminen. Varsinaisen merkityssisällön selvittämisen lisäksi tavoitteena voi olla keskustelun tai viestinnän osapuolten tunnistaminen taikka epäillyn henkilön toiminnan selvittäminen muuten.

Tässä yhteydessä on syytä kuitenkin korostaa sotilastiedustelussa sovellettavien periaatteiden merkitystä silloin, kun teknistä kuuntelua toteutetaan tavalla, joka ilman toimivaltuutta tarkoittaisi salakuunteluun tai -katseluun syyllistymistä.

Pykälän 2 momentissa säädettäisiin siitä, keihin ja mihin teknistä kuuntelua voitaisiin kohdentaa. Teknistä kuuntelua voitaisiin kohdistaa henkilöön tai henkilöryhmään, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Erittäin tärkeä merkitys -edellystä on kuvattu aiemmin 10 §:n yksityiskohtaisissa perusteluissa.

Tekninen kuuntelu voitaisiin esimerkiksi toteuttaa kohdistamalla se tosiasiallisesti tilaan tai paikkaan, johon kohdistuva kuuntelu on sallittua. Kysymys olisi siten niin sanotusta tilakuuntelusta. Momentin mukaisissa tilanteissa teknistä kuuntelua ei voitaisi kohdistaa esimerkiksi paljastumisriskin vuoksi jatkuvana seurantatoimenpiteenä, vaan ainoastaan tietyissä tiedustelutehtävän kannalta merkityksellisissä tiloissa ja paikoissa. Esimerkkinä voidaan mainita tilanne, jossa epäilty tiedustelun kannalta olennainen henkilö siirtyy yleiseltä paikalta varastotilaan. Tiedustelua toteuttava virkamies ei voi paljastumatta seurata henkilöä kyseiseen tilaan, vaan tekninen kuuntelu on toteutettava muulla tavoin. Käytännössä tämä tarkoittaa sitä, että kyseinen tila on varustettava kuuntelulaitteilla ennakkoon. Teknisellä kuuntelulla voidaan toisaalta saada tietoa myös siitä, ettei tiettyä tilaa tai muuta paikkaa käytetä tiedustelutehtävän kohteena olevaan toimintaan.

Teknistä kuuntelua voitaisiin kohdistaa henkilöön tai henkilöryhmään rikoslain 24 luvun 11 §:n mukaisessa kotirauhan suojaamassa tilassa, kunhan se ei ole vakituiseen asumiseen käytetty tila. Merkitystä ei olisi sillä, mihin tekninen laite, menetelmä tai ohjelmisto asennetaan.

Teknisen kuuntelun käyttämisessä vakituiseen asumiseen käytettävien tilojen rajaus tulisi määrittää tapauskohtaisesti. Merkitystä ei kuitenkaan olisi sillä, mihin tekninen laite, menetelmä tai ohjelmisto asennettaisiin. Merkityksellistä olisi se, mihin teknistä kuuntelua kohdistetaan.

24 §. *Teknisestä kuuntelusta päättäminen.* Pykälän 1 momentin mukaan tuomioistuin päättäisi vapautensa menettäneen henkilön teknisestä kuuntelusta. Jos asia ei sietäisi viivytystä, tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saisi päättää teknisestä kuuntelusta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia olisi saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta.

Kiiretilannepäätöksen mahdollistamista perustelee operatiivisen toiminnan luonne. Äkillisesti voi syntyä tilanne, jolloin tuomioistuimen lupaa ei ehdittäisi hakea ilman, että menetetään sotilastiedustelun kohteesta merkityksellinen tieto. Esimerkkinä voidaan mainita tilanne, jossa kaksi Suomessa olevaa vieraan valtion tiedusteluviraston virkamiestä tapaavat. Tilanteen kannalta voi olla tarpeen saada tieto mistä he keskustelevat. Tällöin sotilastiedustelun virkamies voisi esimerkiksi älypuhelimella nauhoittaa keskustelun siihen itse lainkaan osallistumatta.

Pykälän 2 momentin mukaan Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saisi tehdä päätöksen teknisestä kuuntelusta muussa kuin pykälän 1 momentissa tarkoitetuissa tapauksissa. Päätöksentekijä ja päätöksenteko tehtäisiin samalla tasolla kuin edellä 19 §:ssä säädetyssä suunnitelmallisessa tarkkailussa. Päätöksessä olisi vastaavasti osoitettava jokainen tiedustelutehtävän kohteena oleva henkilö tai henkilöryhmä riittävällä tarkkuudella.

Tietyissä tilanteissa teknisellä kuuntelulla saatettaisiin hankkia tietoa myös luottamuksellisen viestin suojaa nauttivasta viestinnästä. Viestintä liittyisi käytännössä kahden ihmisen väliseen keskusteluun. Puuttuminen luottamukselliseen viestintään ei olisi kuitenkaan yhtä vakavasti perusoikeuksiin puuttuvaa kuin telekuuntelussa, joten päätöksentekotasona voisi olla tiedustelumenetelmien käyttöön erityisesti perehtyneellä virkamiehellä.

Pykälän 2 momentin mukaan päätös tekniseen kuunteluun voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan. Päätöksen voimassaoloaika olisi pidempi, mitä esimerkiksi rikostorjunnasta on säädetty vastaavien toimivaltuuksien osalta. Tämä olisi perusteltua sotilastiedustelun tehtävien, tiedustelumenetelmien käytön perusteen ja käyttötarkoituksen takia. Tiedustelu on rikostorjuntaan verrattuna pidempikestoisempaa ja tiedustelutehtävät ennakkoon tarkoin suunniteltu. Tiedustelutehtävän tavoitteena voi olla esimerkiksi kerätä tietoa kohdevaltion asevoimien toiminnasta ja siihen liittyvistä seikoista. Jos tiedustelutehtävän kohde on merkittävä, sen kesto voisi olla hyvinkin pitkäaikainen. Esimerkiksi vieraan valtion aikeisiin kohdistuva tiedustelu voi käytännössä olla jatkuvaa. Tiedustelun tarkoituksena ei olisi yksittäisen rikoksen estäminen tai selvittäminen, vaan varhaisen vaiheen tiedon kerääminen kokonaiskuvan saamiseksi. Säännös mahdollistaisi ennakoivan ja pidempiaikaisemman tiedonhankinnan yhdellä lupapäätöksellä.

Tiedustelumenetelmiä ei saisi käyttää yksittäisten rikosten estämiseksi, paljastamiseksi tai selvittämiseksi eikä menetelmillä saatua tietoa olisi lähtökohtaisesti tarkoitus käyttää rikoksiin liittyen. Tästä pääsäännöstä olisi kuitenkin säädetty poikkeuksia 6 luvussa.

Säännöksessä tarkoitettu kuuden kuukauden aika ei kuitenkaan automaattisesti tarkoittaisi sitä, että lupa päätös tehtäisiin aina kuudeksi kuukaudeksi. Suhteellisuus- ja vähimmän haitan periaatteen mukaista harkintaa edellyttäisi säännöksessä oleva ilmaisu ”enintään kuudeksi kuukaudeksi kerrallaan”. Siksi päätöstä annettaessa tulisi harkita tiedustelumenetelmän käytön ajallisen keston tarpeellisuutta tapauskohtaisesti.

Pykälän 3 momentissa säädettäisiin asioista, jotka teknistä kuuntelua koskevassa päätöksessä olisi mainittava.

Momentin 1 kohdassa toimenpiteen perusteena olevalla tiedustelutehtävällä tarkoitettaisiin 13 §:ssä tarkoitettua tiedustelutehtävää, joka perustuisi 4 §:ssä oleviin sotilastiedustelun kohteisiin ja 16 §:ssä tarkoitettuun tietopyyntöön tai Puolustusvoimien toimeksiantoon. Tiedustelutehtävän tulisi olla tiedustelumenetelmän käytön perusteena. Lisäksi päätöksessä tulisi ilmetä toimenpiteen tavoite, mihin tiedustelumenetelmän käytöllä pyrittäisiin. Tavoite tulisi määritellä riittävällä tarkkuudella.

Momentin 2 kohdassa säädettäisiin edellytyksestä sisällyttää päätöksen tiedustelumenetelmän käytön kohde. Kohdan mukaan teknisen kuuntelun kohteena voisi olla henkilö tai henkilöryhmä. Päätöksessä tulisi osoittaa perustellusti, että tietty henkilö tai henkilöryhmä liittyy tiedustelutehtävään.

Lisäksi kohdan mukaan tekninen kuuntelu voisi kohdistua tilaan tai muuhun paikkaan. Tilalla tarkoitettaisiin seinillä ja katolla taikka vastaavilla rakenteilla rajattua paikkaa. Tila siis erotetaan jollakin rakenteellisella tavalla paikasta (yleinen tai yksityinen paikka). Muulla paikalla tarkoitettaisiin seinillä ja katolla taikka vastaavilla rakenteilla rajatun tilan ulkopuolista paikkaa, kuten esimerkiksi liikekiinteistön piha-aluetta.

Teknisen kuuntelun tarkoituksena olisi hankkia tietoa ainoastaan tiedustelutehtävään. On kuitenkin todennäköistä, että tiedustelumenetelmien rikostorjuntaa laveampien kohdistamisedellytysten (henkilö, henkilöryhmä, tila tai muu paikka) takia myös muut kuin sotilastiedustelun kannalta relevantit henkilöt joutuvat väistämättä kuuntelun kohteeksi. Tätä asetelmaa tasapainotettaisiin muun muassa ilmoitusvelvollisuutta ja -oikeutta koskevilla säännöksillä. Toisaalta tiedustelutehtävän kannalta voi olla merkitystä myös sen selvittämisellä, ettei tiettyä tilaa käytetä tiedustelutehtävän kohteena olevaan toimintaan.

Teknisen kuuntelun kohdistuessa muuhun paikkaan, kuin tilaan, niin luvassa ja päätöksessä olisi määriteltävä niin täsmällisesti kuin mahdollista, kuinka suurelle alueelle teknistä kuuntelua on tarkoitus kohdistaa. Teknisen kuuntelun kohteena oleva alue olisi mahdollisuuksien rajattava niin pieneksi kuin mahdollista.

Teknisen kuuntelun käyttämisessä rajaus vakituiseen asumiseen käytettävien tilojen ja muiden paikkojen välillä tulisi määritellä tapauskohtaisesti, kun harkitaan teknisen kuuntelun edellytysten täyttymistä. Tekniseen kuunteluun liittyisi tiedustelumenetelmästä päättävän arviointivelvollisuus, johon tarvittaessa liittyisi selonottovelvollisuus. Jos tila tai muu paikka kuuluisi vakituiseen asumiseen käytettävän tilan piiriin, niin tiedustelumenetelmää ei voitaisi käyttää. Tämä lähtökohta voitaisiin kumota vastakkaista asiantilaa koskevalla selvityksellä. Esimerkiksi toimistona käytettävää huoneistoa voidaan tosiasiallisesti käyttää asumiseen (esim. KKO 2009:54) ja toisaalta asuinhuoneistoa voidaankin tosiasiallisesti käyttää toimistona.

Momentin 3 kohta olisi päätöksenteon kannalta merkityksellinen. Kohdan mukaan vaatimukseen ja päätökseen tulisi sisällyttää ne tosiseikat, joihin teknisen kuuntelun edellytykset ja kohdistaminen perustuisivat. Tosiseikkojen esittäminen päätöksentekijälle velvoittaa esittämään ja perustelemaan ne tosiseikat, joiden perusteella päätöksentekijä voisi tehdä omat johtopäätöksensä edellytysten täyttymisestä. Mainituissa edellytyksissä olisi kyse 10 §:n tiedustelumenetelmien yleisistä edellytyksistä ja toimivaltuutta koskevassa 23 §:ssä mainituista edellytyksistä. Lisäksi päätöksessä olisi esitettävä riittävät tosiseikat tiedustelutehtävästä ja sen pohjana olevasta lain 4 §:ssä tarkoitetusta sotilastiedustelun kohteesta sekä 16 §:ssä tarkoitetusta tietopyynnöstä tai muusta toimeksiannosta. Suhteellisuusperiaatteen kannalta tärkeässä asemassa olisi erityisesti se, kuinka vakavasta toiminnan ilmenemismuodosta olisi kysymys.

Momentin 4 kohdan mukaan päätökseen olisi sisällytettävä teknistä kuuntelua koskevan päätöksen voimassaoloaika kellonajan tarkkuudella.

Momentin 5 kohdan mukaan päätöksessä olisi mainittava teknisen kuuntelun suorittamista johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies.

Momentin 6 kohdan mukaan vaatimukseen tai päätökseen tulisi sisällyttää mahdolliset teknisen kuuntelun rajoitukset ja ehdot. Päätöksessä voitaisiin asettaa tekniselle kuuntelulle rajoituksia ja käyttöehtoja.

25 §. *Tekninen katselu.* Pykälän 1 momentissa määriteltäisiin tekninen katselu. Sillä tarkoitettaisiin rikoslain 24 luvun 6 §:n estämättä tapahtuvaa tietyn henkilön tai henkilöryhmä taikka tilan tai muun paikan tarkkailua tai tallentamista kameralla tai muulla sellaisella paikkaan sijoitetulla teknisellä laitteella, menetelmällä tai ohjelmistolla.

Kuten tekninen kuuntelu, tekninen katselu liittyy myös olennaisesti suunnitelmallisen tarkkailun toteuttamiseen. Teknisellä katselulla voidaan saada tieto esimerkiksi siitä, milloin kohteena oleva henkilö lähtee liikkeelle, jonka jälkeen voidaan aloittaa suunnitelmallisen tarkkailu. Lisäksi tekninen katselu voisi tulla kyseeseen, kun tietolähteen tapaamisessa teknisellä katselulla hankittaisiin tietoa alueella liikkuvista henkilöistä, kuten toisen valtion tiedustelupalveluiden kiinnostuksesta tietolähdettä kohtaan. Teknisellä katselulla voidaan myös toteuttaa tiedonhankintaa, mikä ei olisi mahdollista tai turvallista esimerkiksi suunnitelmallisella tarkkailulla ilman, että sotilastiedusteluviranomaisen läsnäolo paljastuu.

Teknisen kuuntelun määritelmän tavoin myös teknisen katselun määritelmässä todettaisiin, että tekninen katselu kohdistuu tiettyyn henkilöön tai henkilöryhmään. Teknistä katselua voitaisiin kuitenkin kohdistaa myös tiettyyn tilaan tai muuhun paikkaan. Tekniikkaneutraalisti säännöksessä mainittaisiin erilaisten kameroiden lisäksi myös muut tekniset laitteet, menetelmät ja ohjelmistot. Tekninen katselu eroaisi tarkkailusta ja suunnitelmallisesta tarkkailusta siinä, että teknisessä katselussa käytettäisiin paikkaan sijoitettuja teknisiä laitteita, menetelmiä tai ohjelmistoja.

Teknisen kuuntelun määritelmän tavoin myös teknisen katselun määritelmässä määritettäisiin tiedustelumenetelmän suhde rikoslaissa kiellettyyn toimintaan. Rikoslain 24 luvun 6 §:n 1 momentin mukaan salakatseluun syyllistyy se, joka oikeudettomasti teknisellä laitteella katselee tai kuvaa 1) kotirauhan suojaamassa paikassa taikka käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa oleskelevaa henkilöä taikka 2) yleisöltä suljetussa 3 §:ssä (julkisrauhan rikkominen) tarkoitetussa rakennuksessa, huoneistossa tai aidatulla piha-alueella oleskelevaa henkilöä tämän yksityisyyttä loukaten. Momentissa oleva rikoslain viittaus tarkoittaisi sitä, että katselun yhteydessä ei syyllistytä salakatseluun, kunhan tiedustelumenetelmää käytetään asianmukaisesti. Tämä tarkoittaisi sitä, että päätös teknisen katselun käyttämisestä on syntynyt oikeassa järjestyksessä ja katselua käytetään lainmukaisesti.

Teknisen katselun kohdalla olisi huomioita sotilastiedustelua koskevat periaatteet. Erityisesti tämä koskisi rikoslain 24 luvun 6 §:n 1 momentin 1 kohdassa tarkoitettuja tiloja ja muita paikkoja. Suhteellisuusperiaatteen mukaisesti punninnassa on otettava huomioon tiedustelumenetelmän käytöstä aiheutuva oikeuksien, tässä tapauksessa kotirauhan ja yksityisyyden suojan loukkaaminen. Huomioon on lisäksi otettava sotilastiedustelutoimintaa ohjaavat yleiset periaatteet. Erityisesti käymälätiloihin, pukeutumistiloihin ja muihin vastaaviin tiloihin teknistä katselua ei tulisi kohdistaa ilman painavia perusteita.

Tekninen katselu voitaisiin toteuttaa myös muulla kuin viranomaisen laitteella. Tämä voi tapahtua esimerkiksi niin, että kaupungin hallitsema kameravalvontalaitteisto kohdistetaan sotilastiedusteluviranomaisen intressissä tiettyyn epäiltyyn henkilöön. Mikäli puolestaan kaupungin kameravalvon-

tajärjestelmästä vain toimitettaisiin sotilastiedusteluviranomaiselle mahdollisesti tiedustelutehtävää tukevaa kuvamateriaalia ja tallentaminen olisi tapahtunut muuten kuin sotilastiedusteluviranomaisen kontrolloimana ja intressissä, kysymys ei olisi teknisestä katselusta.

Paikkaan sijoittamista koskeva vaatimus tarkoittaisi käytännössä sitä, että teknisen katselun toteuttaminen ei ole lyhytaikaista toimintaa. Paikkaan sijoitetulla tarkoitettaisiin esimerkiksi sitä, että laite, menetelmä tai ohjelmisto on kiinnitetty seinään, kattoon tai muuhun kiinnittämiseen soveltuvaan kohteeseen. Lisäksi tekniselle havainnoinnille sen määritelmästä johtuen olisi ominaista, että laite, menetelmä tai ohjelmisto seuraisi kohdetta yleensä ilman sotilastiedusteluviranomaisen samanaikaista havaintojen tekemistä ja paikallaoloa. Seurantalaitteen asentamisesta ja poisottamisesta säädettäisiin jäljempänä. Jos kysymys on sellaisesta kohdehenkilön seurannasta, jossa virkamies reaaliaikaisesti käyttää hallussaan olevaa laitetta kohdehenkilön havainnointiin, toimenpide olisi tarkkailua tai suunnitelmallista tarkkailua.

Pykälän 2 momentin mukaan sotilastiedusteluviranomaisen virkamiehellä olisi oikeus tiedustelutehtävän suorittamiseksi vakituiseen asumiseen käytettävän tilan ulkopuolella olevan henkilön tekniseen katseluun. Tiedustelumenetelmää voitaisiin kohdistaa tilaan tai muuhun paikkaa, jossa tiedustelutehtävään liittyvä henkilön voidaan olettaa todennäköisesti oleskelevan tai käyvän.

Teknisen kuuntelun sääntelyn tavoin momentista ilmenisi, että teknisen katselun kohteena olisi tietty henkilö tai henkilöryhmä, mutta katselu voitaisiin toteuttaa kohdistamalla se tiettyyn tilaan, jolla on riittävän kiinteä yhteys mainittuun henkilöön tai henkilöryhmään. Tältä osin voidaan viitata siihen, mitä edellä 20 §:n perusteluissa on todettu teknisestä katselusta. Tilassa saattaa oleskella ja liikkua muitakin henkiöitä, kuin tiedustelutehtävän kohteena olevia. Näissä tilanteissa tiedustelutehtävän ulkopuolisia henkiöitä koskevat tiedot ja tallenteet olisi hävitettävä heti.

Teknistä katselua voitaisiin kohdistaa henkilöön tai henkilöryhmään rikoslain 24 luvun 11 §:n mukaisessa kotirauhan suojaamassa tilassa, kunhan se ei ole vakituiseen asumiseen käytetty tila. Merkitystä ei olisi sillä, mihin tekninen laite, menetelmä tai ohjelmisto asennetaan.

26 §. *Teknisestä katselusta päättäminen.* Teknistä kuuntelua vastaavasti vapautensa menettäneen teknisestä katselusta päättäisi tuomioistuin. Tämän ja kiirepäätöksen osalta voidaan viitata 24 §:n 1 momentin yksityiskohtaisiin perusteluihin.

Pykälän 2 momentin mukaan sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättäisi muusta kuin vapautensa menettäneen teknisestä katselusta.

Pykälän 3 momentin mukaan päätös voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan. Päätösharkintaan vaikuttavien seikkojen osalta voidaan viitata edellä 23 §:n 2 momentin yksityiskohtaisissa perusteluissa todettuun.

Pykälän 4 momentissa olisi lueteltuna päätöksen sisällöstä tavalla, joka vastaa edelle 24 §:n 3 momentin yksityiskohtaisissa perusteluissa todettua.

27 §. *Tekninen seuranta.* Pykälän 1 momentissa määriteltäisiin tekninen seuranta. Sillä tarkoitettaisiin esineen, aineen tai omaisuuden liikkumisen seurantaa siihen erikseen sijoitettavalla tai siinä jo olevalla radiolähettimelle tai muulla sellaisella teknisellä laitteella taikka menetelmällä tai ohjelmistolla. Tekninen seuranta on yksi tiedustelun perinteisimpiä menetelmiä, eikä sillä puututa yhtä merkittävästi kohteena olevan henkilön perus- ja ihmisoikeuksiin kuin henkilön teknisellä seurannalla, josta säädetään jäljempänä.

Momentin mukaan periaatteessa minkä tahansa esineen, aineen tai omaisuuden liikkumista voitaisiin seurata. Määritelmässä mainittaisiin liikkumisen seuranta erotuksena muista teknisen tarkkailun muodoista. Tämä sisältäisi luonnollisesti myös tiedon esineen, aineen tai omaisuuden sijainnista, kun se ei ole liikkeessä.

Tekninen seuranta olisi mahdollista toteuttaa tekniikkaneutraalisti erilaisilla teknisillä laitteilla, menetelmillä ja ohjelmistoilla. Siinä voitaisiin esimerkiksi käyttää hyödyksi esineen, aineen tai omaisuuden olemassa olevia teknisiin, kaupallisiin tai vastaaviin tarkoituksiin kehitettyjä ominaisuuksia tai kiinnittämällä esineeseen, aineeseen tai omaisuuteen paikantamisen mahdollistava tekninen laite tai asentaa salaa paikantamisen mahdollistava ohjelmisto. Esimerkkinä voidaan mainita moottoriajoneuvossa olevan paikannuslaitteen aktivoiminen salaa. Henkilöiden paikantamisessa voitaisiin käyttää esimerkiksi seurattavan henkilön vaatteisiin laitettavaa seurantalaitetta.

Pykälän 2 momentin mukaan teknisellä seurannalla olisi voitava olettaa saatavan tiedustelutehtävän kannalta tärkeää tietoa esimerkiksi yksittäisen henkilön liikkeistä tai henkilön havainnoinnin helpottamiseksi. Tieto teknisen seurannan kohteesta on voitu saada esimerkiksi muilla tiedustelun keinoilla.

Joissain tapauksissa sotilastiedustelu voisi saada tärkeitä tietoja tiedustelutehtävän suorittamiseksi esimerkiksi tietyn esineen liikkumisesta. Tilanteessa saatettaisiin tunnistaa jokin esimerkiksi sotilaalliseen toimintaan soveltuva esine, mutta vielä ei olisi selkeää, kuka henkilö esinettä käsittelisi. Teknisellä seurannalla voitaisiin seurata esineen liikkumista uuteen määränpäähän ja tämän jälkeen selvittää muilla tiedustelumenetelmillä, ketkä ovat esineestä kiinnostuneita.

Lisäksi teknistä seurantaa voitaisiin kohdistaa tiedustelutehtävään liittyvän henkilön oletettavasti hallussa olevaan tai käyttämään esineeseen, aineeseen tai omaisuuteen. Tällä pystyttäisiin hankkimaan tietoa suoraan tietyn henkilön liikkumisesta.

Pykälän 3 momentissa säädettäisiin erikseen henkilön teknisen seurannan edellytyksistä. Jos teknisen seurannan tarkoituksena olisi seurata henkilön liikkumista sijoittamalla seurantalaite hänen yllään oleviin vaatteisiin tai mukanaan olevaan esineeseen, saataisiin toimenpide suorittaa ainoastaan, jos toimenpiteen suorittamisella voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Tieto henkilö liittymisestä tiedustelutehtävään oltaisiin voitu saada muita tiedustelumenetelmiä käyttäen.

28 §. *Teknisestä seurannasta päättäminen.* Pykälän 1 momentin mukaan tuomioistuin päättäisi henkilön teknisestä seurannasta sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies virkamiehen vaatimuksesta. Jos asia ei siedä viivytystä, tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saisi päättää seurannasta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua tiedustelumenetelmän käytön aloittamisesta.

Jäljempänä säädettäisiin tilanteesta, jossa kiiremenettelyssä aloitetun henkilön teknisen seurannan edellytyksiä ei olisi tuomioistuimen harkinnan mukaan ollut. Tällöin tiedustelumenetelmän käyttö olisi lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot olisi heti hävitettävä.

Pykälän 2 momentin mukaan muusta kuin henkilön teknisestä seurannasta päättäisi sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

Pykälän 3 momentin mukaan lupa voitaisiin antaa ja päätös tehdä enintään kuudeksi kuukaudeksi kerrallaan. Säännös vastaisi tältä osin voimassa olevia muiden viranomaisten toimivaltuuksia.

Pykälän 4 momentissa säädettäisiin teknistä seurantaa koskevassa vaatimuksessa ja päätöksessä mainittavista tiedoista tavalla, joka vastaisi pääosin muita tiedustelumenetelmiä koskevissa vaatimuksissa ja päätöksissä mainittavia tietoja, kuten edellä 23 §:n yksityiskohtaisissa perusteluissa on todettu. Momentin 2 kohdassa olisi tarkemmin mainittava toimenpiteen kohteena oleva esine, aine tai omaisuus, jota seurattaisiin teknisesti.

29 §. *Tekninen laitetarkkailu.* Pykälän 1 momentissa määriteltäisiin tekninen laitetarkkailu. Teknisellä laitetarkkailulla tarkoitettaisiin esimerkiksi tietokoneen tai muun vastaavan teknisen laitteen taikka sen ohjelmiston toiminnan, sisältämien tietojen tai yksilöintitietojen muuta kuin yksinomaan aistinvaraista tarkkailua, tallentamista tai muuta käsittelyä tiedustelutehtävän kannalta tarpeellisen seikan selvittämiseksi. Tekninen laitetarkkailu kohdistuisi esimerkiksi teknisten laitteiden ja ohjelmistojen väliseen tiedonvaihtoon.

Teknisessä laitetarkkailussa ei olisi merkitystä sillä, missä laitetta käytettäisiin, sillä toimivaltuudella ei olisi selvittää laitteen sijainti paikan tapahtumia näkö- tai kuulohavainnoin. Teknistä laitetarkkailu ei ole tältä osin rinnastuisi edellä tarkoitettuihin toimivaltuuksiin.

Voimassa olevasta poliisilaista tai sen perusteluista ei ilmene kuin välillisesti, että säännöksessä mainitulla viestin sisällöllä tarkoitetaan nimenomaan viestin sisältöä telekuuntelun ja teknisen kuuntelun tarkoituksessa eli silloin, kun viestintä tapahtuu kahden ihmisen välillä reaaliaikaisesti tietokoneelta tai älypuhelimestä. Siten esimerkiksi kyseiselle laitteelle jo tallentuneet tai tallennetut asiakirjat, jotka eivät ole teknisen kuuntelun tai telekuuntelun reaaliaikaisessa yhteydessä, kuuluvat teknisen laitetarkkailun piiriin. Teknisellä laitetarkkailulla voitaisiinkin hankkia tietoa esimerkiksi tietojärjestelmään tallennetuista asiakirjoista. Asiakirjat eivät kuitenkaan saisi olla luottamuksellisen viestin suojan soveltamisalan piirissä, jota koskisivat muut tässä laissa säädetyt toimivaltuudet.

Teknisellä laitetarkkailulla voitaisiin hankkia tietoja esimerkiksi valtiollisen toimijan tiedustelutoiminnasta Suomessa.

Teknisellä laitetarkkailulla tarkkailtaisiin teknistä laitetta ja yleensä laitteen sisältämiä tiedustelutehtävään liittyvän henkilön siihen tallettamia tietoja. Tällaiset tiedot voisivat olla laitteeseen tallennetussa asiakirjassa. Teknisellä laitetarkkailulla voitaisiin seurata henkilön ja teknisen laitteen välistä vuorovaikutusta. Toimivaltuudella voitaisiin hankkia laitteen tai sen ohjelmiston yksilötietietoja sekä tietoa viestiin liittymättömästä signalointi- tai ohjausliikenteestä. Teknisellä laitetarkkailulla voitaisiin seurata henkilön ja teknisen laitteen välistä vuorovaikutusta menemättä viestin sisältöön. Eräs teknisen laitetarkkailun muoto olisi niin sanottu näppäimistökuuntelu, jonka tavoitteena on esimerkiksi selvittää verkkopalvelimen salasanan sisältö. Toimenpiteen tulisi olla luonteeltaan pääasiallisesti teknistä erotukseksi yksinomaan aistinvaraisesta, näkö- tai kuulohavainnoin tapahtuvasta tarkkailusta. Näppäimistökuuntelusta viestin sisällön selvittämiseksi on käsitelty edellä 23 §:n yksityiskohtaisissa perusteluissa.

Määritelmän mukaisesti mikä tahansa tekninen laite ei voisi olla teknisen laitetarkkailun kohteena, vaan laitteen tulisi olla tietokoneeseen rinnastettava, kuten esimerkiksi kulunvalvontajärjestelmä ja älypuhelimet.

Pykälän 2 momentissa säädettäisiin teknisen laitetarkkailun rajoituksista. Teknistä laitetarkkailua ei saisi kohdistaa henkilöiden väliseen viestiliikenteeseen eikä sillä saisi hankkia tietoa viestin sisällöstä tai välitystiedoista. Momentti selkeyttäisi linjanvetoa eri tiedustelumenetelmien välillä. Kuten edellä on jo todettu, esimerkiksi näppäimistökuuntelu viestin sisällön selvittämiseksi olisi teknistä kuuntelua. Teknisellä laitetarkkailulla ei saisi myöskään kiertää telekuuntelua tai televalvontaa kos-

kevien säännösten soveltamista. Jos teknisen laitetarkkailun aikana kävisi ilmi, että tarkkailu kohdistuu viestin sisältöön tai välitystietoihin, tiedustelumenetelmän käyttö olisi keskeytettävä niin pian kuin mahdollista sekä tallenteet ja tiedustelumenetelmällä saatuja tietoja koskevat muistiinpanot olisi heti hävitettävä myöhemmin säädetysti.

Teknisen laitetarkkailun luvan ohella toimivaltuutta käyttävällä virkamiehellä voisi olla samanaikaisesti myös muita tiedustelumenetelmiä, jos niiden käyttämisen edellytykset täyttyvät.

Edellä sanottu ei kuitenkaan tarkoittaisi sitä, ettei yksityisen viestin suojan ulkopuolella olevaan viestintään voitaisi puuttua. Jos viesti ei olisi yksityisen viestin suojan piirissä, voitaisiin tällaisen viestin sisällöstä ja tunnistamistiedoista hankkia tietoa. Jälkimmäinen tilanne tulisi kyseeseen etenkin tilanteissa, joissa teknistä laitetta käyttäisi esimerkiksi tunnistettu vieraan vallan sotilasviranomaisen edustaja.

Pykälän 3 momentissa säädettäisiin teknisen laitetarkkailun edellytyksistä. Teknisen laitetarkkailun edellytyksenä olisi, että sillä voitaisiin olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän suorittamiseksi. Puolustusvoimien tiedustelulaitos saisi kohdistaa tiedustelutehtävään liittyvän henkilön todennäköisesti käyttämään tietokoneeseen tai muuhun vastaavaan tekniseen laitteeseen taikka sen ohjelmiston toimintaan teknistä laitetarkkailua.

Momentin rajaus tiedustelutehtävään liittyvän henkilön käyttämiin laitteisiin merkitsisi sitä, että laitteiden ei tarvitse olla hänen omistamia tai muutoin hallitsemia. Kohteena voisi olla myös laite tai ohjelmisto, jota tiedustelumenetelmän käytön kohteena oleva henkilö ei vielä käytä, mutta tulee tulevaisuudessa käyttämään. Näyttökynnys laitteen ja epäillyn henkilön väliselle yhteydelle olisi korkea, mihin momentissa käytetty sana ”todennäköisesti” viittaisi. Jos tiedustelumenetelmän käytön yhteydessä havaittaisiin, että teknistä laitetta käyttää joku muu kuin mainittu henkilö, olisi toimenpide keskeytettävä sekä mahdolliset tallenteet ja toimenpiteellä saatuja tietoja koskevat muistiinpanot hävitettävä.

30 §. *Teknisestä laitetarkkailusta päättäminen.* Pykälän 1 momentin mukaan tuomioistuin päättäisi teknisestä laitetarkkailusta sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimiehen tai muun virkamiehen vaatimuksesta. Jos asia ei siedä viivytystä, sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saisi päättää seurannasta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua tiedustelumenetelmän käytön aloittamisesta.

Jäljempänä säädettäisiin tilanteesta, jossa kiiremenettelyssä aloitetun henkilön teknisen seurannan edellytyksiä ei olisi tuomioistuimen harkinnan mukaan ollut. Tällöin tiedustelumenetelmän käyttö olisi lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot olisi heti hävitettävä.

Pykälän 2 momentin mukaan lupa voitaisiin antaa ja päätös tehdä enintään kuudeksi kuukaudeksi kerrallaan. Säännös vastaisi tältä osin voimassa olevia muiden viranomaisten toimivaltuuksia. Kuuden kuukauden enimmäisaikaa on perusteltua aiempana.

Pykälän 3 momentissa olisi listattuna seikat, jotka olisi mainittava vaatimuksessa ja päätöksessä. Momentti vastaisi edellä säädettyjä tiedustelumenetelmien käytön vaatimuksia. Edellytyksiä on kuvattu tarkemmin edellä 23 §:n yksityiskohtaisissa perusteluissa.

31 §. *Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen.* Pykälän 1 momentin mukaan sotilastiedusteluviranomaisella olisi oikeus sijoittaa tekniseen havainnointiin käytettävä

laite, menetelmä tai ohjelmisto toimenpiteen kohteena olevaan esineeseen, aineeseen, omaisuuteen, tilaan tai muuhun paikkaan taikka tietojärjestelmään, jos tiedustelumenetelmän käyttö sitä edellyttää. Tiedustelumenetelmää käyttävällä virkamiehellä olisi tällöin oikeus laitteen, menetelmän tai ohjelmiston asentamiseksi, käyttöön ottamiseksi ja poistamiseksi salaa mennä edellä mainittuihin kohteisiin tai tietojärjestelmään sekä kiertää, purkaa tai muulla vastaavalla tavalla tilapäisesti ohittaa kohteiden tai tietojärjestelmän suojaus tai haitata sitä. Tämä ei kuitenkaan tarkoittaisi yrityksille velvoitteita laitteidensa tai tuotteidensa tietoturvan heikentämiseen tai rajoituksia salausteknologian käytölle.

Pykälässä ei olisi erityisiä vaatimuksia Puolustusvoimien tiedustelulaitoksen virkamiehelle, joka saisi pykälässä tarkoitetut toimet suorittaa. Tiedustelumenetelmien käyttäminen voi edellyttää laitteen, menetelmän tai ohjelmiston asentamisessa ja poisottamisessa teknisen asiantuntijan käyttämistä. Esimerkiksi eräiden kohteiden tai tietojärjestelmien suojaus voi edellyttää tilapäistä kiertämistä, pukamista tai ohittamista.

Jos tiedustelumenetelmän käyttöön tarvittaisiin tuomioistuimen lupa, olisi tiedustelumenetelmän käyttöä koskevassa päätöksessä annettava erikseen lupa laitteen, menetelmän tai ohjelmiston asentamiselle. Erillistä lupaa ei enää tarvittaisi laitteen, menetelmän tai ohjelmiston poistamiseen.

32 §. *Telekuuntelu.* Pykälässä säädettäisiin telekuuntelusta. Pykälän 1 momentin mukaan telekuuntelulla tarkoitettaisiin yleiseen viestintäverkkoon tai siihen liitetyn viestintäverkon kautta teleosoitteeseen tai telepäätelaitteeseen vastaanotettavan taikka siitä lähetetyn viestin kuuntelua, tallentamista ja muuta käsittelyä viestin sisällön ja siihen liittyvien tunnistamistietojen selvittämistä. Telekuuntelua saadaan kohdistaa vain siltä henkilöltä lähtöisin olevaan tai sellaiselle henkilölle tarkoitettuun viestiin, jolla on erittäin tärkeä merkitys tiedustelutehtävän kannalta.

Telekuuntelussa on kysymys nimenomaan yleisissä viestintäverkoissa välitettävänä olevien viestien telekuuntelusta.

Telekuuntelun kohdistaminen tapahtuisi viestintäverkon rajapinnan tietoon tai ominaisuuteen perustuen, jolla voidaan yhdistää tiettyyn käyttäjään tai tilaajaan, ja laitteeseen sisältyvä ja sitä myötä myös käyttäjään tai tilaajaan yhdistettävissä oleva tieto tai ominaisuus. Tällaisia tietoja voivat olla esimerkiksi sähköpostiosoite, IP-osoite, käyttäjätunnus ja salasana, profiili tai muu televerkkoon sisältyvä tieto, jonka avulla tele- tai datayhteyden osapuolet voidaan yksilöidä. Näin ollen myös puhelimen sarjanumero (IMEI-koodi) taikka muu päätelaitteen suoraan yksilöivä tai sen yksilöimiseen johtava tieto sisältyisi telekuuntelun määritelmän piiriin.

Viestillä tarkoitetaan tietoyhteiskuntakaaren mukaan viestintäverkossa osapuolten välillä tai vapaasti valikoituville vastaanottajille välitettävää puhelua, sähköpostiviestiä, tekstiviestiä, puheviestiä ja muuta vastaavaa sanomaa. Käsite kattaa lähes kaikenlaiset informaatiomuodot, mutta ei sisällä kuitenkaan puhtaasti viestiin liittymätöntä tietokoneiden välistä ohjaus- ja signalointiliikennettä. Telekuuntelutoimivaltuutta ei tarvittaisi kaikkien saataville toimitettavan verkkoviestin sisällön selvittämiseksi. Verkkoviestin tunnistamistiedot ovat kuitenkin luottamuksellisia, mikä vastaa niin ikään voimassa olevaa oikeutta. Telekuuntelu koskisi teleosoitteeseen tai telepäätelaitteeseen vastaanotettavaa tai siitä lähetettyä viestiä. Viesti olisi telekuuntelutoimivaltuudella saatavissa, kun se on viestintäverkossa välitettävänä siten, että viesti on ylittänyt esimerkiksi lähettäjän teleosoitteen muodostaman rajapinnan, jolloin sitä pidettäisiin lähetettynä, eikä se ole vielä saapuessaan vastaanottajalle ylittänyt vastaanottavan teleosoitteen rajapintaa, jolloin se olisi edelleen vastaanotettavana. Näin ollen esimerkiksi matkapuhelimeen saapunut tekstiviesti ei olisi tässä tarkoitetulla tavalla välitettävänä.

Telekuuntelutoimivaltuus kattaisi viestin välitystietojen hankkimisen. Käytännössä viesti ilman siihen liittyviä tunnistamistietoja (esimerkiksi lähettäjän ja vastaanottajan yksilöivä tieto) on merkityk-

setön. Tältä osin televalvonta sisältyisi telekuunteluun. Telekuuntelutoimivaltuudella ei kuitenkaan voitaisi esimerkiksi estää viestin perille menoa. Telekuuntelun yhteydessä saatavat tunnistamistiedot eivät myöskään sisältäisi telepäätelaitteen sijaintietoja. Tätä tarkoitettaisiin nimenomaisella maininnalla viestiin liittyvien tunnistamistietojen selvittämisestä. Jos myös sijaintitiedot ovat tarpeen, tulee hakea televalvontalupa. Momentissa todettaisiin nimenomaisesti, että telekuuntelua saadaan kohdistaa vain siltä henkilöltä lähtöisin olevaan tai sellaiselle henkilölle tarkoitettuun viestiin, joka on lähtöisin perustellusti tiedustelutehtävään liittyvältä henkilöltä tai jonka vastaanottajana on perustellusti tiedustelutehtävään liittyvältä henkilöltä ja saatavalla tiedolla on olennaista merkitystä tiedustelutehtävän kannalta. Tällä on tarkoitus korostaa sitä, ettei telekuuntelua saa kohdistaa kenenkään muun kuin mainitun henkilön viestintään. Hän voi tosin olla toistaiseksi nimeltään tuntematon henkilö, jonka perustellusti voidaan olevan olennainen tiedustelutehtävän kannalta. Tällöin hänet voidaan yksilöidä hänen hallussaan olevan tai hänen muuten oletettavasti käyttämän teleosoitteen tai telepäätelaitteen avulla. Erityisesti on kuitenkin huolehdittava siitä, että kuunteluluvan antaminen tuntemattomien henkilöiden käyttämiin teleosoitteisiin tai telepäätelaitteisiin ei tosiasiallisesti johda tiettyjen teleosoitteiden tai telepäätelaitteiden kuuntelemiseen siitä riippumatta, kuka niitä käyttää.

Kuten edellä on todettu 4 luvun yksityiskohtaisten perusteluiden johdantokappaleessa, telekuuntelutoimivaltuus saisi käyttää ainoastaan tiedonhankinnassa, jossa tiedustelutehtävä perustuisi sotilastiedustelun kohteeseen, joka olisi sotilaallista toimintaa tai aiheuttaisi Suomen kansalliselle turvallisuudelle vakavaa uhkaa. Lisäksi huomiota olisi kiinnitettävä siihen, onko tiedonhankinnan kohteena valtiollinen toimija vai muu toimija. Esimerkiksi 4 §:n 1 kohdan tarkoittama sotilaallinen toiminta ei nauti perustuslain 10 §:n 3 momentin suojaa, joten tällaiseen toimijaan kohdistetulla telekuuntelulla ei puututtaisi perusoikeussuojaan. Telekuuntelulla voitaisiin hankkia tietoa sotilaallisen toimijan palveluksessa olevasta henkilöstä tämän edustaessa sotilaallista toimijaa.

Vastaavasti 4 §:n 2 kohdassa sotilastiedustelun kohteeksi määriteltäisiin tiedon hankkiminen ulkomaisten tiedustelupalveluiden toiminnasta. Kuten edellä on todettu, valtiolliset toimijat eivät nauti perusoikeussuojaa, joten ulkomaisten tiedustelupalveluiden edustajatkaan eivät sitä nauti Suomessa.

Momentissa säädettäisiin nimenomaisesti, että telekuuntelua saadaan kohdistaa vain siltä henkilöltä lähtöisin olevaan tai sellaiselle henkilölle tarkoitettuun viestiin, jonka voidaan perustellusti olettaa liittyvän tiedustelutehtävään. Tällä korotettaisiin sitä, ettei telekuuntelua saa kohdistaa muun henkilön viestintään. Henkilö voi sinänsä olla sotilastiedusteluviranomaiselle tuntematon henkilö, jonka perustellusti voidaan epäillä esimerkiksi välittävän tietoja toisen valtion sotilastiedustelun käytettäväksi. Tällöin henkilö voidaan yksilöidä hänen hallussaan olevan tai hänen muuten oletettavasti käyttämän teleosoitteen tai telepäätelaitteen avulla. Erityisesti on kuitenkin huolehdittava siitä, että jos tuntematonta teleosoitetta tai päätelaitetta käyttäisi joku muu kuin tiedustelutehtävän kannalta merkityksellinen henkilö, hankitut tiedot olisi välittömästi hävitettävä, kun käy ilmi, ettei tiedustelumenetelmän käytön kohteena ollut tiedustelutehtävän kannalta olennainen henkilö.

Telekuuntelun kohteena oleva tietty teleosoite, telepäätelaite tai henkilö voi viestiä myös tiedustelutehtävän kohteena olevaan toimintaan liittymättömien henkilöiden kanssa. Jos telekuuntelua käytettäessä tiedonhankinnan kohteeksi joutuisi tällaista tiedustelutehtävään liittymätöntä viestintää, olisi tällainen viestintä hävitettävä välittömästi. Tiedon hävittämisestä säädettäisiin jäljempänä.

Pykälän 2 momentin mukaan telekuuntelua olisi mahdollista kohdistaa tiedustelumenetelmien yleisten edellytysten täyttyessä valtiolliseen toimijaan. Kuten aiemmin tässä esityksessä on todettu yleisperusteluissa, valtiollisen toimijan ei voida katsoa nauttivan perusoikeussuojaa. Näin ollen kahden valtiollisen toimijan välinen viestintä ei ole luottamuksellisen viestin salaisuuden piirissä. Huomion arvoista on se, että telekuuntelu saa kohdistua ainoastaan viestintää, joka tapahtuu valtiollisen toimijan sisäisesti tai valtiollisten toimijoiden välillä. Kaikki muu viestintä olisi hävitettävä,

kuten jäljempänä tässä esityksessä säädetään. Telekuuntelu olisi kohdistettava tiedustelutehtävän kannalta olennaiseen valtiollista toimijaa edustavaan henkilöön. Tämä edellytys tarkoittaisi sitä, että sotilastiedusteluviranomaisella on ennakolta käsitys siitä, että telekuuntelun kohteeksi joutuva henkilö edustaa valtiollista toimijaa.

Valtiollisen toimijan telekuuntelu voisi tulla kyseeseen esimerkiksi tilanteessa, jossa on tunnistettu vieraan vallan tiedustelupalvelua edustava henkilö.

Huomion arvoista on myös se, että tiedustelumenetelmien käytön kohde saattaa alussa näyttäytyä olemassa olevien tietojen nojalla muulta kuin valtiolliselta toimijalta, mutta tiedustelun edetessä saattaa käydä ilmi, että henkilö on esimerkiksi vieraan vallan tiedusteluorganisaation edustaja tai kohde on suoraan valtiollisen toimijan ohjauksessa.

Pykälän 3 momentissa säädettäisiin muuhun kuin valtiolliseen toimijaan kohdistuvasta telekuuntelusta. Telekuuntelun kohteena voisi olla tiedustelutehtävän kannalta olennainen henkilö, jos tiedon hankkiminen olisi erittäin tärkeä merkitys tietojen hankkimiseksi tiedustelutehtävän kannalta. Sotilastiedustelun kohteet pyrkivät salaamaan toimintansa todelliset tarkoitusperät ja toimimaan salassa. Tilanne voisi tulla kyseeseen esimerkiksi silloin, kun tietoja olisi hankittava vieraan vallan tiedustelutoiminnasta eikä tiedustelumenetelmän kohteena olevaa henkilöä tai henkilöryhmää voida tunnistaa valtiolliseksi toimijaksi.

33 §. *Tietojen hankkiminen telekuuntelun sijasta.* Pykälän 1 momentissa säädettäisiin eräistä telekuuntelun kaltaisista tiedonhankintakeinoista. Pykälän 1 momentin mukaan, jos on todennäköistä, että 32 §:ssä tarkoitettua viestiä ja siihen liittyviä välitystietoja ei ole enää saatavissa telekuuntelulla, sotilastiedusteluviranomaiselle voidaan antaa tiedustelutehtävän toteuttamiseksi lupa tietojen hankkimiseen teleyrityksen tai yhteisötilaajan hallusta 32 §:ssä säädetyillä edellytyksillä. Tiedustelumenetelmän edellytyksenä olisi myös, että sillä voidaan olettaa olevan erittäin tärkeä merkitys tiedustelutehtävän toteuttamiseksi.

Pykälässä olisi kyse tapauksista, joissa telekuuntelutoimivaltuudella saatava viesti on hävinnyt, mutta se on vielä teknisesti saatavissa teleyritykseltä tai yhteisötilaajalta. Sääntelyn tarkoituksen olisi myös estää telekuuntelun käyttöedellytyksien kiertäminen. Toimenpiteen käytölle asetettaisiin kynnykseksi todennäköisyys siitä, ettei viestiä ha siihen liittyviä välitystietoja ole enää saatavissa telekuuntelulla.

Momentin tilanteet tulisivat kyseeseen silloin, kun tiedetään, että ennen telekuuntelun aloittamista olisi olemassa jo tietoja, jotka olisivat käytettävissä tiedustelutehtävään. Edellytykset vastaisivat telekuuntelua.

Pykälän 2 momentin mukaan, jos tietojen hankkiminen kohdistetaan viestin sisällön selvittämiseksi telepäätelaitteeseen välittömästi yhteydessä olevaan viestin lähettämiseen ja vastaanottamiseen soveltuvaan henkilökohtaiseen tekniseen laitteeseen tai tällaisen laitteen ja telepäätelaitteen väliseen yhteyteen, sotilastiedusteluviranomaiselle voidaan antaa lupa tietojen hankkimiseen telekuuntelun sijasta, jos 32 §:ssä säädetyt edellytykset täyttyvät. Tämä estäisi sen, että telekuuntelun soveltamiskynnys muodostuisi tavanomaista alemmaksi silloin, kun kuuntelu voidaan toteuttaa kohdistamalla esimerkiksi teknistä havainnointia puhelun välityksessä käytettävään henkilökohtaiseen apulaitteeseen, kuten hands free -laitteeseen tai muuhun esimerkiksi matkapuhelimeen blue tooth -yhteydellä liitynnässä olevaan laitteeseen. Tiedustelumenetelmän käytön kohde voi edellä sanotussa tilanteessa perustellusti olettaa, että viestintä on yhtä luottamuksellista kuin puhuttaessa suoraan matkapuhelimeen.

Momentin mukaan tietojen hankkiminen telekuuntelun sijasta tehtäisiin viestin sisällön selvittämiseksi. Laitteen tulisi olla välittömässä yhteydessä tekniseen laitteeseen, mikä sulkisi ulkopuolelle

erilaiset siirrettävät tallennusvälineet. Momentin mukaisten laitteiden tulisikin olla nimenomaan viestin lähettämiseen ja vastaanottamiseen soveltuvia henkilökohtaisia apuvälineitä tai muita sellaisia teknisiä laitteita. Kyse olisi kuitenkin tekniikka neutraalista sääntelystä.

Momentin mukaan tiedonhankinta kohdistuisi tiedonhankinnan kohdistaminen henkilökohtaisen apuvälineen ja telepäätelaitteen väliseen yhteyteen. Tällöin tiedonhankinta ei kohdistuisi sinänsä apuvälineeseen vaan sen ja telepäätelaitteen väliseen radio- tai muuhun vastaavaan yhteyteen. Esimerkiksi matkapuhelimen kaiutin puhelu tai kovaäänisen puhelun kuuntelu ei olisi momentissa tarkoitettua tietojen hankkimista telekuuntelun sijasta.

34 §. *Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättäminen.* Pykälän 1 momentin mukaan päätöksen telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta tekisi tuomioistuin Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimiehen tai muun virkamiehen vaatimuksesta. Vaatimuksen käsittelystä tuomioistuimessa säädettäisiin jäljempänä 134 §:ssä.

Pykälän 2 momentin mukaan lupa telekuunteluun ja telekuuntelun sijasta toimitettavaan tietojen hankkimiseen voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan. Lupa-aika olisi pidempi, mitä voimassa olevassa lainsäädännössä, kuten poliisilain 5 luvussa tarkoitetun telekuuntelun osalta. Tämä olisi perusteltua sotilastiedustelun luonteen ja tehtävien, tiedustelumenetelmien käytön perusteen ja käyttötarkoituksen takia. Näitä on käsitelty aiemmin tässä esityksessä yleisperusteluissa.

Telekuuntelutoimivaltuudella voidaan saada yksittäisen henkilön toiminnasta erittäin tarkkaa ja laajasti tietoa. Tiedustelutoiminnassa telekuuntelulla hankittuja tietoja ei kuitenkaan saisi käyttää rikostorjunnassa. Tästä pääsäännöstä olisi kuitenkin poikkeuksena 6 luku, jossa olisi säädetty tarkasti tilanteet, joissa tiedustelumenetelmin hankitusta tiedosta saataisiin ilmoittaa sotilastiedustelun ulkopuolelle.

Kuten edellä on todettu teknisen kuuntelun osalta, tiedustelu on pitkäkestoista ja ennakkoon tarkoin suunniteltua toimintaa. Näin tarkoituksena ei olisi yksittäisen rikoksen estäminen tai selvittäminen, vaan varhaisen vaiheen tiedon kerääminen kokonaiskuvan saamiseksi. Säännös mahdollistaisi ennakoivan ja pidempiaikaisemman tiedonhankinnan yhdellä lupapäätöksellä.

Säännöksessä tarkoitettu kuuden kuukauden lupa-aika ei kuitenkaan automaattisesti tarkoittaisi sitä, että lupa voitaisiin aina hakea kuudeksi kuukaudeksi tai että se tulisi myöntää kuuden kuukauden määräajaksi. Harkittaessa luvan voimassaoloaikaa, erityistä huomiota olisi kiinnitettävä suhteellisuus- ja vähimmän haitan periaatteisiin. Siksi lupaa hakiessa sekä sitä myönnettäessä tulisi harkita tiedustelumenetelmän käytön ajallisen keston tarpeellisuutta tapauskohtaisesti.

Pykälän 3 momentissa säädettäisiin vaatimukseen ja päätökseen sisällytettävistä tiedoista.

Momentin 1 kohdassa toimenpiteen perusteena olevalla tiedustelutehtävällä tarkoitettaisiin 13 §:ssä tarkoitettua tiedustelutehtävää, joka perustuisi 4 §:ssä oleviin sotilastiedustelun kohteisiin ja 9 §:ssä tarkoitettuun tietopyyntöön tai muuhun toimeksiantoon. Tiedustelutehtävän tulisi olla tiedustelumenetelmän käytön perusteena. Lisäksi vaatimuksessa ja päätöksessä tulisi ilmetä toimenpiteen tavoite, mihin tiedustelumenetelmän käytöllä pyrittäisiin. Toimivaltuuden käytön tavoite tulisi määritellä riittävällä tarkkuudella.

Momentin 2 kohdassa säädettäisiin edellytyksestä sisällyttää vaatimukseen ja päätöksen tiedustelumenetelmän kohde, joka telekuuntelussa olisi teleosoite tai telepäätelaite taikka henkilö.

Kohdan mukaan telekuuntelun kohteena voisi olla myös henkilö. Kun telekuuntelulupa kohdistuisi henkilöön, lupa käsittäisi telekuunteluluvan kohteena olevan henkilön hallussa olevan tai hänen oletettavasti muuten käyttämän teleosoitteen tai telepäätelaitteen. Telekuuntelulupa ei olisi teleosoite- tai telepäätelaitekohtainen, vaan lupa käsittäisi kaikki luvan kohteena olevan henkilön hallussa olevat teleosoitteet ja telepäätelaitteet. Luvan hakijan tulisi pystyä osoittamaan, että tietty teleosoite tai telepäätelaite on luvan kohteena olevan henkilön hallussa tai että henkilö oletettavasti muuten käyttää teleosoitetta tai telepäätelaitetta. Henkilöön kohdistuvassa telekuuntelussa tiedonhankinta voisikin olla liitännäinen muihin tiedustelumenetelmiin, kuten teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimiseen. Henkilöön kohdistuvassa telekuuntelussa olisi huomioitava henkilön asema valtiollisena toimijana taikka muuna toimijana.

Momentin 3 kohta olisi päätöksenteon kannalta merkityksellinen. Kohdan mukaan vaatimukseen ja päätökseen tulisi sisällyttää ne tosiseikat, joihin telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen edellytykset ja kohdistaminen perustuisivat. Tosiseikkojen esittäminen tuomioistuimelle velvoittaa tiedusteluviranomaisen esittämään ja perustelemaan ne tosiseikat, joiden perusteella luvan tuomioistuin voisi tehdä tiedustelumenetelmän käytön edellytysten täyttymisestä omat johtopäätöksensä. Mainituissa edellytyksissä olisi kyse 10 §:n tiedustelumenetelmien yleisistä edellytyksistä ja toimivaltuutta koskevassa 32 §:ssä mainituista edellytyksistä. Lisäksi vaatimuksessa ja päätöksessä olisi esitettävä riittävät tosiseikat tiedustelutehtävästä ja sen pohjana olevasta lain 4 §:ssä tarkoitetusta sotilastiedustelun kohteesta sekä 16 §:ssä tarkoitetusta tietopyynnöstä tai muusta toimeksiannosta. Suhteellisuusperiaatteen kannalta tärkeässä asemassa olisi erityisesti se, kuinka vakavasta toiminnan ilmenemismuodosta olisi kysymys.

Lupaa haettaessa ja päätöstä perusteltaessa erityisen tärkeässä asemassa ovat edellä säädetyt periaatteet. Tältä osin olisi pystyttävä osoittamaan esimerkiksi kuinka vakavasta sotilastiedustelun kohteena olevan toiminnan ilmenemismuodosta olisi kysymys.

Momentin 4 kohdan mukaan vaatimukseen ja päätökseen olisi sisällytettävä telekuuntelua tai telekuuntelun sijasta toimitettavaa tietojen hankkimista koskevan luvan voimassaoloaika kellonajan tarkkuudella. Kellonajantarkkuutta ei edellytettäisi tietojen hankkimisessa telekuuntelun sijasta.

Momentin 5 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen suorittamista johtava ja valvova Puolustusvoimien tiedustelulaitoksen virkamies.

Momentin 6 kohdan mukaan vaatimukseen tai päätökseen tulisi sisällyttää mahdolliset telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen rajoitukset ja ehdot. Tuomioistuin voisi asettaa päätöksessään telekuuntelulle rajoituksia ja käyttöehtoja. Jos tällaisia rajoituksia ja ehtoja olisi tiedossa jo vaatimusta laadittaessa, vaatimuksen esittäjän tulisi harkita niiden kirjaamista vaatimukseen.

35 §. *Televalvonta.* Televalvonnalla tarkoitettaisiin välitystietojen hankkimista viestistä, joka on lähetetty viestintäverkkoon kytketystä teleosoitteesta tai telepäätelaitteesta taikka vastaanotettu tällaiseen osoitteeseen tai laitteeseen sekä teleosoitteen tai telepäätelaitteen sijaintitiedon hankkimista taikka osoitteen tai laitteen käytön tilapäistä estämistä.

Tunnistamistiedolla tarkoitetaan tilaajaan tai käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

Tietoyhteiskuntakaaren 134 §:n mukaan viestiin liittyvät välitystiedot ovat luottamuksellisia, jollei laissa toisin säädetä. Viesti ei ole luottamuksellinen, jos se on saatettu yleisesti vastaanotettavaksi. Verkkoviestin eli radioaaltojen, sähköisen viestintäverkon tai muun vastaavan teknisen järjestelyn avulla yleisön saataville toimitetun tiedon, mielipiteen tai muun viestin tunnistamistietojen luovutta-

misesta säädetään puolestaan sananvapauden käyttämisestä joukkoviestinnässä annetun lain 17 §:ssä.

Välitystietojen käytössä on yleensä kysymys viestinnän osapuolen selvittämisestä.

Välitystietoihin voi kuulua tietoja, jotka viittaavat muun muassa viestinnän reititykseen, kestoon, ajankohtaan tai siirrettävän tiedon määrään, käytettyyn protokollaan, lähettäjän tai vastaanottajan päätelaitteen sijaintiin tietyn tukiaseman alueella, lähettävään tai vastaanottavaan verkkoon ja yhteyden alkuun, loppuun tai kestoon. Tiedot voivat myös koskea muotoa, jossa viesti välitetään verkossa. Olennaista on, että näiden tietojen tulee olla yhdistettävissä tilaajaan tai käyttäjään. Esimerkiksi sähköpostiviestin tunnistamistietoja ovat viestin otsikkotiedot, jotka koskevat lähettäjää, vastaanottajaa, reittitietoja ja aikamerkintöjä. Tunnistamistiedon käsitteen kannalta on huomattava, että tilaaja, johon tunnistamistieto voidaan yhdistää, voi olla luonnollisen henkilön lisäksi myös oikeushenkilö. Lisäksi on huomattava, että televalvonnan avulla on mahdollisuus saada tunnistamistietoja televiesteistä, mutta oikeus saada tunnistamistietoja ei merkitse oikeutta televalvontaan.

Televalvonnan piiriin kuuluisi myös teleosoitteen ja telepäätelaitteen sijaintitiedon hankkiminen.

Sotilastiedustelu voisi hankkia tietoja esimerkiksi tiedustelutehtävän kohteena olevan henkilön liikkeistä ja siitä kenen kanssa kohteena olevan henkilö viestii. Viestin sisällöstä ei voitaisi hankkia tietoja tällä toimivaltuudella.

Määritelmän rajoittuminen viestiä koskeviin tietoihin tarkoittaisi sitä, että viestiin liittymätön tietokoneiden välinen ohjausliikenne ei olisi luottamuksellisen viestinnän suojan piirissä. Ohjausliikenteellä tarkoitetaan tiedonsiirtoon, eli siihen, että tieto siirtyy tietyltä tekniseltä laitteelta tietylle tarkoitetulle tekniselle laitteelle, internet-verkossa liittyviä tietoja.

Pykälän 2 momentin mukaan, vastaavasti kuin telekuuntelun osalta, sotilastiedusteluviranomaiselle voitaisiin antaa lupa tiedustelutehtävän kannalta olennaisen valtiollisen toimijan käyttämän teleosoitteen tai telepäätelaitteen televalvontaan. Kuten telekuuntelun yksityiskohtaisista perusteluista käy ilmi, valtiolliset toimijat eivät nauti samantasoista perusoikeussuojaa kuin yksityiset ihmiset.

Vastaavasti, kuten telekuuntelussa, pykälän 3 momentissa televalvontaa olisi mahdollista kohdistaa muuhun kuin valtiolliseen toimijaan. Televalvontaa voitaisiin näissä tapauksissa käyttää tiukemmin edellytyksin, eli jos televalvonnalla voitaisiin olettaa olevan erittäin tärkeä merkitys tiedon hankkimiseksi tiedustelutehtävän kannalta.

36 §. *Televalvonnasta päättäminen.* Pykälän 1 momentin mukaan päätöksen televalvonnasta tekisi tuomioistuin sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta. Jos televalvontaa koskeva asia ei siedä viivytystä, sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saisi päättää televalvonnasta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia olisi saatettava tuomioistuimen ratkaistavaksi heti, kun se olisi mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta.

Jos kiireellisessä tilanteessa tehdyn päätöksen yhteydessä tuomioistuin katsoo, että edellytyksiä toimenpiteelle ei ole ollut, tiedustelumenetelmän käyttö olisi lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot olisi heti hävitettävä.

Kiirepäätösasia tulisi saattaa tuomioistuimen käsiteltäväksi siitä huolimatta, että televalvonnan käyttäminen lopetetaan 24 tunnin kuluessa sen käytön aloittamisesta. Muuten hyvin lyhytaikaisella tiedonhankinnalla voitaisiin kiertää päätöksentekomenettelylle annettavia vaatimuksia. Asian saat-

taminen tällaisissakin tapauksissa tuomioistuimen käsiteltäväksi edistää toimimista lainmukaisesti. Tämä koskisi muitakin tilanteita, joissa Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies voi väliaikaisesti päättää tiedustelumenetelmän käytöstä.

Pykälän 2 momentin mukaan sotilastiedusteluviranomainen saisi tietojen hankkimiseksi tiedustelutehtävän kohdistaa televalvontaa henkilön suostumuksella tämän hallinnassa olevaan teleosoitteeseen tai telepäätelaitteeseen. Momentissa säädettäisiin suostumukseen perustuvasta televalvonnasta, jos sillä voidaan olettaa saatavan tietoja tiedustelutehtävään. Esimerkiksi, jos henkilö joutuu osaksi tiedustelutehtävää tietämättään olevansa vieraan vallan tiedustelupalvelun tietojen välittäjä ja sotilastiedusteluviranomaiselle tämä käy ilmi, voisi sotilastiedusteluviranomainen ryhtyä henkilön kanssa yhteistyöhön asian selvittämiseksi ja henkilö voisi antaa suostumuksensa oman telepäätelaitteensa tai teleosoitteensa televalvontaan.

Teleosoitteen tai telepäätelaitteen hallinnalla tarkoitettaisiin tosiasiallista hallintaa. Näin ollen esimerkiksi työnantaja ei voisi antaa suostumusta työntekijän käytössä olevan matkapuhelimen televalvontaan. Myöskään satunnainen toisen henkilön matkapuhelimen käyttäminen ei voisi oikeuttaa suostumuksen antamiseen matkapuhelimen omistajana viestinnän osalta. Suostumus tulisi antaa kirjallisessa muodossa. Kiireellisissä tilanteissa suostumus voitaisiin kuitenkin antaa suullisesti, mutta se tulisi vahvistaa kirjallisesti niin pian kuin mahdollista (HE 224/2010 vp., s. 99–100).

Loukatun suostumusta koskevan opin mukaisesti jokainen voisi pätevästi antaa suostumuksensa hallinnassaan olevan teleosoitteen tai telepäätelaitteen televalvontaan, jos suostumus on annettu vapaaehtoisesti ennen toimenpiteeseen ryhtymistä ja ymmärtäen sen merkitys. Suostumuksen tulee olla aidosti vapaaehtoinen. Sen saamiseksi Puolustusvoimien tiedustelulaitoksen puolelta ei saa käyttää taivuttelua tai muuta vastaavaa johdattelua. Puolustusvoimien tiedustelulaitos voi tuoda esiin mahdollisuuden käyttää suostumusperusteista televalvontaa, mutta johtopäätösten tekeminen tiedonhankintakeinon käytöstä on aina jätettävä asianomaiselle henkilölle (HE 224/2010 vp., s. 99–100).

Pykälän 3 momentin mukaan pääesikunnan tiedustelupäällikkö tai tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättäisi 2 momentissa tarkoitetusta televalvonnasta.

Sotilastiedustelua koskevissa asioissa suostumusperäistä televalvontaa koskeva päätösvalta olisi aina pääesikunnan tiedustelupäälliköllä tai Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtyneellä sotilaslakimiehellä tai muulla virkamiehellä. Jotta mainituilla virkamiehellä olisi itsenäinen päätösvalta asiassa, niin tämän tulisi olla tiedustelumenetelmien käyttöön erityisesti perehtynyt tai koulutettu. Koulutuksen järjestämisvastuu olisi Puolustusvoimilla. Esimerkiksi Puolustusvoimien rikostorjuntaa hoitavat virkamiehet ovat osallistuneet poliisihallinnossa järjestettyihin niin sanottuihin STEK-POV -koulutuksiin. Koulutusta voitaisiin järjestää yhteistyössä suojelupoliisin kanssa tai sitä voitaisiin hankkia kansainvälisiltä yhteistyötahoilta. Puolustusvoimilla on jo nykyisin tiettyjen esitettävien tiedustelumenetelmien käytöstä ja koulutuksesta pitkäaikaista kokemusta, kun taas suojelupoliisilla on pidempiaikainen kokemus yleisellä alueella toteutettavasta ja muiden kuin Puolustusvoimien käyttämien salaisten tiedonhankintakeinojen ja salaisten pakkokeinojen käytöstä. Lisäksi Puolustusvoimien olisi järjestettävä ja huolehdittava sisäisestikin Puolustusvoimien tiedusteluun liittyvien virkamiesten riittävästä koulutuksesta.

Perehtyneisyys tiedustelumenetelmien käyttöön voisi tulla myös muuta kautta kuin nimenomaisella koulutuksella. Etenkin toiminnan alkuvaiheessa määrämuotoista koulutusta ei olisi saatavilla. Perehtyneisyys olisikin voitu saavuttaa esimerkiksi rikostorjunnan tehtävien kautta tai muilla keinoin. Viime kädessä vastuun siitä, että virkamies on riittävän perehtynyt tehtäviensä hoitamiseen, kantaa viranomaisen johtajat.

Pykälän 4 momentin mukaan lupa tai päätös voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan. Se voitaisiin antaa myös päätöstä edeltänyttä tiettyä ajanjaksoa koskien, joka voisi olla kuutta kuukautta pidempi. Edeltänyttä aikaa koskevat tiedot ovat teleyrityksen säilyttämiä tietoja, joiden säilyttämisestä ja säilyttämisajoista säädetään tietoyhteiskuntakaaren 157 §:ssä. Säilyttämisaika on enimmillään 12 kuukautta. Näin ollen takautuvaa televalvontaa koskeva lupa voitaisiin antaa korkeintaan 12 kuukauden ajalta.

Takautuvassa televalvonnassa olisi tarkkaan harkittava, minkä pituista ajanjaksoa lupa voisi koskea. Tiedustelutarkoituksessa takautuvalla televalvonnalla voitaisiin saada erittäin laajasti tietoja siitä, keiden kanssa tietty taho on ollut yhteyksissä.

Pykälän 5 momentissa säädettäisiin asioista, jotka televalvontaa koskevassa vaatimuksessa ja päätöksessä olisi mainittava. Tämän osalta voidaan viitata 32 §:n 3 momentin yksityiskohtaisissa perusteluissa esitettyyn.

37 §. *Tukiasematietojen hankkiminen.* Pykälän 1 momentissa tukiasematietojen hankkimisella tarkoitettaisiin tiedon hankkimista tietyn tukiaseman kautta tukiasemaan kirjautuneista tai kirjautuvista telepäätelaitteista ja teleosoitteista. Tukiasematietojen hankkiminen sotilastiedustelussa kohdistuisi ennalta määräämättömään joukkoon teleosoitteita ja telepäätelaitteita, kuten matkaviestimiä. Toimivaltuus oikeuttaa tiedon saamiseen vain matkaviestimen sijainnista tiettynä hetkenä, mutta sitä vastoin ei siitä, onko matkaviestimellä otettu yhteyttä toiseen matkaviestimeen. Toimivaltuuden käytöllä voitaisiin selvittää niin tukiasemaan jo aiemmin kirjautuneet telepäätelaitteet ja tukiasemat kuin luvan voimassa olon aikana tiettyyn tukiasemaan kirjautuvat teleosoitteet ja telepäätelaiteet. Tiedustelumenetelmällä voitaisiin hankkia tietoja tietyn telepäätelaitteen ja teleosoitteen liikkeistä. Kyseessä ei olisi yhtä merkittävällä tavalla perusoikeuksien suojaan puuttuvasta keinosta kuin telekuuntelu ja tiedustelumenetelmä rinnastuisi tekniseen seurantaan.

Pykälän 2 momentin mukaan sotilastiedusteluviranomaiselle voidaan antaa lupa tukiasematietojen hankkimiseen, jos sillä voidaan tiedustelumenetelmien käytön yleisten edellytysten täyttyessä saada tarpeellisia tietoja tiedustelutehtävän kannalta olennaisessa tilassa tai alueella liikkuvista ihmisistä. Tiedustelutehtävän suorittamisen kannalta voidaan saada olennaisia tietoja hankkimalla tietoja tietyllä siitä, keitä tietyllä alueella tai tilassa liikkuu. Tukiasematietojen hankkiminen olisi tässä tarkoituksessa tehokas tapa. Teleosoitteen ja telepäätelaiteet kirjautumistiedoista ei kuitenkaan suoraan saada tietoa yksittäisten henkilöiden liikkumisesta tietyllä alueella, vaan teleosoitteiden ja telepäätelaitteiden tiedot on erikseen muilla keinoin liitettävä yksittäiseen henkilöön.

38 §. *Tukiasematietojen hankkimisesta päättäminen.* Pykälän 1 momentin mukaan tuomioistuin päättäisi tukiasematietojen hankkimisesta sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisen koulutetun virkamiehen vaatimuksesta. Jos asia ei siedä viivytystä sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää tukiasematietojen hankkimisesta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kutienkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta.

Tukiasematietojen hankkiminen merkitsee televalvontaa vähäisempään puuttumista perusoikeuksiin ja ei puuttuisi luottamuksellisen viestinnän suojan alaan. Jos kiireellisessä tilanteessa on tehty päätös tukiasematietojen hankkimisesta ja tuomioistuin katsoo, että edellytyksiä toimenpiteelle ei ole ollut, tiedustelumenetelmän käyttö olisi lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot olisi heti hävitettävä. Rikosperusteisiin vastaaviin toimivaltuuksiin nähden tiedustelumenetelmällä saatua tietoa ei saisi käyttää ylimääräisenä tietona.

Pykälän 2 momentin mukaan lupa annettaisiin tietyksi ajanjaksoksi. Sotilastiedustelussa lupa voitaisiin ulottaa koskemaan muutakin kuin tietyn tapahtuman kannalta merkityksellistä aikaa, sillä

tiedustelulle tyypillistä saattaisi olla pidempiaikainen tiedonhankinta. Olennaista on se, että tietojen merkitys pystytään perustelemaan. Esimerkkinä voitaisiin mainita tilanne, jossa on tarve selvittää tietyn alueen tai paikan läheisyydessä tietyn tukiaseman kautta telejärjestelmään kirjautuneet teleosoitteet ja telepäätelaitteet sekä se, ovatko tietyt tiedustelumenetelmän käytön kohteena olevat tahot liikkuneet tällä alueella ja kuinka usein.

Tukiasematietojen hankkimisessa ei olisi yhtä merkittävästä puuttumisesta perusoikeussuojaan kuin esimerkiksi telekuuntelussa. Tiettyyn tukiasemaan kohdistuva lupa ei vielä itsessään tarkoita sitä, että sotilastiedustelun kohteena oleva telepäätelaite tai teleosoite tulisi siihen kirjautumaan, vaan tilannetta voidaan pitää osittain myös tukiasemaan kirjautuvien telepäätelaitteiden ja teleosoitteiden tarkkailutyyppisestä tilanteesta.

Pykälän 3 momentissa säädettäisiin asioista, jotka tukiasematietojen hankkimista koskevassa vaatimuksessa ja päätöksessä olisi mainittava. Tämän osalta voidaan viitata pääosin 32 §:n 3 momentin yksityiskohtaisissa perusteluissa esitettyyn. Koska tukiasematietojen hankkiminen ei olisi sidottu erityisesti keneenkään tiettyyn henkilöön vaan tiedustelutehtävän kannalta merkitykselliseen ajankohtaan ja paikkaan, riittäisi vaatimuksessa tai päätöksessä ainoastaan tiedustelutehtävän tosiseikkojen mainitseminen. Vaatimuksessa ja päätöksessä pitäisi perustella se, miksi tukiasematietojen hankkimisen tulisi koskea tiettyä ajanjaksoa ja mitä tukiaseman tietojen hankkimisella pyrittäisiin selvittämään. Suhteellisuusperiaatteen valossa ajanjakso ei voisi olla kuutta kuukautta pidempi kuin erittäin poikkeuksellisessa tapauksessa.

Momentin 3 kohtaa tulisi soveltaa siten, että kysymyksessä ovat tosiseikat, joiden perusteella tukiaseman alueen ja esimerkiksi siellä mahdollisesti liikkuvien tiettyjen henkilöiden voitaisiin katsoa olevan olennaisia tiedustelutehtävän kannalta.

39 §. *Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen.* Pykälän 1 momentin mukaan sotilastiedusteluviranomainen saisi hankkia tiedustelutehtävän suorittamiseksi telepäätelaitteen tai teleosoitteen yksilöintitiedot. Yksilöintitietojen hankkimiseen käytettäisiin sotilastiedusteluviranomaisen käyttämää teknistä laitetta. Toimivaltuudella hankittaisiin tiedustelutehtävän kannalta olennaisen henkilön, tilan tai alueen osalta voidaan hankkia teleliittymän tai telepäätelaiteen yksilöiviä tietoja viranomaisen itse käyttämän teknisen laitteen avulla ilman, että on tarpeen kytkeä operaattoreita mukaan viranomaisten tiedonhankintaan.

Hankittavat tiedot eivät koskisi telepäätelaiteen sijaintitietojen hankkimista, vaan toimivaltuudella hankittaisiin telepäätelaitteen yksilöintiin tarvittavat tiedot, kuten puhelimen IMEI-koodi tai IP-osoite. Tietoja ei hankittaisi siitä, missä henkilö milloinkin sijaitsee, vaan hänen hallussaan olevan tai hänen oletettavasti käyttämänsä telepäätelaitteen tai teleliittymän yksilöintiin tarvittavista tiedoista. Hankittuja tietoja voitaisiin käyttää esimerkiksi muiden tiedustelumenetelmien kohdistamisessa.

Säännös ei antaisi sotilastiedusteluviranomaiselle oikeutta pykälässä tarkoitetun teknisen laitteen muuhun käyttöön kuin yksittäisen telepäätelaitteen tai teleosoitteen yksilöintitietojen hankkimiseen.

Sotilastiedusteluviranomainen saisi käyttää tietojen hankkimiseksi ainoastaan sellaista teknistä laitetta, jota voidaan käyttää vain teleosoitteen ja telepäätelaitteen yksilöimiseen. Erotuksena poliisitoiminnassa, sotilastiedustelun kohdalla ei olisi tarvetta sille, että ulkopuolinen virasto tarkastaisi teknisen laitteen ominaisuuksia. Tarkastukset suorittaisi hallinnonalan yleistä valvontaa suorittava puolustusministeriö sekä tiedustelun ulkopuolista valvontaa suorittava taho.

Pykälän 2 momentin mukaan teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisesta päättäisi sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

40 §. *Peitetoiminta.* Pykälän 1 momentissa määriteltäisiin peitetoiminta. Peitetoiminnalla tarkoitettaisiin, erotuksena esimerkiksi tarkkailuun, kaikkea vuorovaikutuksessa tapahtuvaa tiedonhankintaa, jossa esimerkiksi henkilön tai henkilöryhmän luottamuksen saavuttamiseksi tai tiedonhankinnan salaamiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja.

Tiedustelutoiminnalle on tyypillistä sen suunnitelmallisuus ja pitkäjänteisyys. Peitetoiminta voisi tarkoittaa pitkäaikaista kanssakäymistä, luottamussuhteen rakentamista tai soluttautumista kohteena olevaan yhteisöön.

Erotuksen voimassa oleviin rikosperusteisiin toimivaltuuksiin nähden, peitetoiminta voisi kohdistua myös henkilöryhmään.

Soluttautumisen kohteen voisi olla myös sellainen henkilöryhmä, jonka taustalla olevasta toiminnasta olisi tarkoitus hankkia tietoa. Kyse voisi olla kohdehenkilöryhmän toimintaa ohjaavasta tai siihen vaikuttavasta henkilöryhmästä tai organisaatiosta, kuten esimerkiksi ulkomaan sotilastiedustelupalvelun toiminnasta, jolla pyritään niin sanotun hybridivaikuttamisen kautta vaikuttamaan Suomen kansallisiin intresseihin.

Kohteena olevaa henkilöä tai henkilöryhmää ei olisi tarve nimetä tai yksilöidä esimerkiksi fyysisiltä ominaisuuksiltaan, vaan riittävää on, että henkilö tai henkilöryhmä voidaan yksilöidä esimerkiksi hänen toimintansa tai heidän toiminnan kautta.

Peitetoiminnan toteuttaminen vaatii tiedustelumenetelmänä laajaa resursointia ja pitkäjänteistä kouluttautumista esimerkiksi tietyn yhteiskunnan tai yhteisön toimintatavoista ja käytännöistä.

Peitetoiminnasta olisi erotettava itsenäisenä toimivaltuutena sotilastiedustelun suojaamisesta, josta säädettäisiin jäljempänä 81 §:ssä. Tiedustelun suojaaminen voisi kuitenkin tulla peitetoiminnankin yhteydessä kyseeseen, kun peitehenkilöllisyydelle luodaan tarvittava taustainformaatio ja taustatiedot.

Pykälän 2 momentissa säädettäisiin tilanteista, joissa sotilastiedusteluviranomainen voisi käyttää peitetoimintaa. Sotilastiedusteluviranomainen saisi käyttää tiedustelutehtävässä peitetoimintaa, jos se olisi välttämätöntä tietojen saamiseksi tiedustelutehtävän kannalta.

Lisäedellytyksenä olisi, että tiedonhankintaa on tiedustelutehtävän kohteena olevan toiminnan suunnitelmallisuuden, järjestäytyneisyyden taikka ennakoitavissa olevan jatkuvuuden vuoksi pidettävä tarpeellisena. Peitetoiminnan käyttäminen olisi mahdollista järjestäytyneeseen toimintaan liittyen. Järjestäytyneeseen toimintaan liittyy usein myös suunnitelmallisuus. Suunnitelmallisuuden mainitseminen säännöksessä tarkoittaisi myös sitä, että menetelmää olisi mahdollista kohdistaa jatkossakin esimerkiksi saman yksittäisen toimijan suunnitelmalliseen toimintaan.

Peitetoiminnassa sotilastiedusteluviranomaisella olisi oltava ennakkokäsitys siitä, keneen tai keihin taikka mihin toimintaan peitetoiminta kohdistetaan.

Poikkeuksena voimassa olevassa lainsäädännössä tarkoitetusta peitetoiminnasta, esitettävä säännös mahdollistaisi peitetoiminnan käyttämisen myös henkilöryhmää koskevassa tiedonhankinnassa.

Soluttautuminen olisi mahdollista kohdentaa myös sellaiseen henkilöryhmään, jonka taustalla olevasta toiminnasta olisi tarkoitus hankkia tietoa. Kyse voisi olla kohdehenkilöryhmän toimintaa ohjaavasta tai siihen vaikuttavasta henkilöryhmästä tai organisaatiosta, kuten esimerkiksi ulkomaan tiedustelupalvelun toiminnasta, jolla pyritään hybridivaikuttamaan Suomen kansallisiin intresseihin.

Tiedustelumenetelmän käyttöä rajaa vakituiseen asumiseen käytettävät tilat. Peitetoimintavaltuus ei oikeuttaisi menemään vakituiseen asumiseen käytettävään tilaan. Toisaalta pykälän 3 momentin mukaan peitetoimintaa suorittavalla henkilöllä tulisi olla oikeus paljastumisen estämiseksi mennä asuntoon, loma-asuntoon ja muuhun asumiseen tarkoitettuun tilaan, kuten hotellihuoneeseen, telttaan, asuntovaunuun ja asuttavaan alukseen, sekä asuntalojen porraskäytäviin ja asukkaiden yksityisaluetta oleville pihoille käyttämällä hyväkseen luotua peitettä. Peitetoimintaa suorittava Puolustusvoimien tiedustelulaitoksen virkamies ei useinkaan voisi edes paljastumatta kieltäytyä tällaisessa tilanteessa esimerkiksi hotellihuoneeseen menosta. Peitetoiminnassa tulisi kuitenkin pyrkiä välttämään sellaista tilannetta, että peitetoiminta ajautuisi vakituiseen asumiseen käytettävään tilaan. Tämä edellyttäisi peitetoiminnan täsmällistä suunnittelua.

Pykälän 4 momentin mukaan peitetoimintaa voitaisiin suorittaa myös tietoverkoissa. Tietoverkoissa tapahtuvalle ihmisten väliselle vuorovaikutukselle on jo muutoin sinänsä tyypillistä, ettei toisen osapuolen henkilöllisyyttä aina tiedetä varmuudella. Tietoverkoissa tapahtuvassa peitetoiminnassa olisikin arvioitava, minkä tyyppisiä toimia Puolustusvoimien tiedustelulaitoksen virkamies toteuttaisi. Tietoverkoissa tapahtuva peitetoiminta olisi mahdollista, jos sillä voitaisiin olettaa olevan erittäin tärkeä merkitys tiedustelutehtävän kannalta.

Tietoverkoissa tapahtuva peitetoimintaa on toteuttamisen osalta huomattavasti kevyempää ja turvallisempaa kuin normaali peitetoiminta. Tietoverkoissa tapahtuvasta peitetoiminta voidaankin katsoa olevan tällä hetkellä pääasiallinen toimivaltuus peitetoiminnan osalta.

Tietoverkoissa tapahtuvassa peitetoiminnassa olisi otettava huomioon esimerkiksi tilanteet, joissa rekisteröitymisessä tiettyyn palveluun vaadittaisiin niin sanottua vahvaa sähköistä tunnistetta, josta on säädetty vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009). Vahvan sähköisen tunnisteen käyttäminen vaatii peitetoiminnalle tyypillisiä valmistelutoimia ja tietoverkoissa toimiminen tapahtuisi ulkoisesti vahvaa ulkoista luottamusta herättävien tunnisteiden avulla. Pelkästään rekisteröityminen kaikille avoimelle keskustelufoorumille nimimerkillä ja keskustelufoorumilla käytävän keskustelun seuraamista ei voitaisi katsoa peitetoiminnaksi, sillä peitetoiminnalle tyypillinen luottamuksellisen suhteen saavuttaminen ja väärien, harhauttavien tai peiteltyjen tietojen käyttäminen eivät täyttyisi näissä tapauksissa. Pelkkä rekisteröityminen väärillä tiedoilla olisi katsottava peitellyksi tiedonhankinnaksi, jos esimerkiksi yleisellä keskustelupalstalla ei olisi tarkoitus aktiivisesti keskustella yksittäisten henkilöiden kanssa.

Tietoverkoissa tapahtuvassa peitetoiminnassa sotilastiedusteluviranomaisella tulisi olla ennakkotieto esimerkiksi siitä, millä keskustelufoorumilla tiedustelutehtävän kannalta olennainen henkilö tai henkilöryhmä toimii tai mitä viestintäkanavaa esimerkiksi tiedustelutehtävän kannalta olennainen henkilö käyttää ennen kuin peitetoiminnan tarkoittamaa luottamuksellisen suhteen rakentaminen voidaan aloittaa.

41 §. *Peitetoimintaa koskeva esitys ja suunnitelma.* Pykälän mukaan peitetoimintaa koskevassa esityksessä olisi mainittava 1) toimenpiteen esittäjä, 2) tiedonhankinnan kohteena oleva henkilö tai henkilöryhmä riittävästi yksilöitynä, 3) toimenpiteen perusteena oleva uhka ja toimenpiteen tavoite riittävästi yksilöitynä, 4) peitetoiminnan tavoite, 5) peitetoiminnan tarpeellisuus, 6) muut peitetoiminnan edellytysten arviointia varten tarvittavat tiedot.

42 §. *Peitetoiminnasta päättäminen.* Pykälän 1 momentin mukaan pääesikunnan tiedustelupäällikkö päättäisi 40 §:ssä tarkoitetusta peitetoiminnasta. Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättäisi tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

Pykälän 2 momentin mukaan peitetoimintaa koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Pykälän 3 momentin mukaan päätös peitetoiminnasta on tehtävä kirjallisesti. Päätöksessä on mainittava: 1) toimenpiteen esittäjä, 2) peitetoiminnan toteuttamisesta vastaava tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies, 3) tunnistetiedot peitetoiminnan suorittavista virkamiehistä, 4) toimenpiteen perusteena oleva tiedustelutehtävän ja toimenpiteen tavoite riittävästi yksilöitynä, 5) tiedonhankinnan kohteena oleva henkilö tai henkilöryhmä riittävästi yksilöitynä, 6) tosiseikat, joihin peitetoiminnan edellytykset ja kohdistaminen perustuvat, 7) peitetoiminnan tavoite ja toteuttamissuunnitelma, 8) päätöksen voimassaoloaika ja 9) peitetoiminnan mahdolliset rajoitukset ja ehdot.

Pykälän 3 momentin 3 kohdassa tarkoitettavilla tunnistetiedoilla tarkoitetaan tietoja, joilla peitetoimintaa suorittava virkamies pystytään peitetoiminnan aikana ja sen jälkeen tunnistamaan.

Pykälän 4 momentin mukaan päätöstä olisi olosuhteiden muuttuessa tarvittaessa tarkistettava. Peitetoiminnan lopettamisesta on tehtävä kirjallinen päätös.

43 §. *Tietolähdetoiminta.* Pykälän 1 momentti sisältäisi tietolähdetoiminnan määritelmän. Tietolähdetoiminnalla tarkoitettaisiin muuta kuin satunnaista luottamuksellista, sotilastiedustelulle merkityksellisten tietojen vastaanottamista ja yhteydenpitoa suomalaisen viranomaisen ulkopuolisen henkilön kanssa (tietolähde). Tietolähde toiminta on yksi henkilötiedustelun keskeisimpiä tiedonhankintakeino.

Yksittäisten tietojen antajat eivät olisi määritelmässä tarkoitettuja tietolähteitä minkä lisäksi määritelmän ulkopuolelle jäisivät virkamiehet. Tietolähteen ohjattua käyttöä ei olisi se, että tietolähde kertoo oma-aloitteisesti sotilastiedusteluviranomaiselle tätä oletettavasti kiinnostavista seikoista, joita viranomainen harkintansa mukaan hyödyntää. Ohjatulle toiminnalle on luonteenomaista, että tietolähteen antamat tiedot hankitaan tiedustelutehtävän kohteesta kohteen tietämättä.

Tietolähdetoiminnasta olisi erotettava tilanteet, joissa henkilö muuten avustaisi sotilastiedustelua. Henkilö voisi antaa tukea esimerkiksi luovuttamalla tilan sotilastiedusteluviranomaisen käyttöön tiedustelumenetelmän käytön ajaksi taikka antamalla perustamansa yrityksen tunnisteet Puolustusvoimien tiedustelulaitoksen käytettäväksi tiedustelutehtävässä. Tätä toimintaa ei voida pitää tietolähdetoimintana. Koska henkilön antama tuki sotilastiedustelulle perustuisi esimerkiksi tämän määräysvaltaan kuuluvasta vapaudesta käyttää omaisuuttaan haluamallaan tavalla, jolloin tällainen toiminta ei edellyttäisi erillistä sääntelyä. Henkilön tulisi antaa vapaaehtoinen suostumuksensa sotilastiedusteluviranomaisen avustamiseen. Sotilastiedusteluviranomaisen virkamies voisi tuoda esille mahdollisuuden sotilastiedustelun avustamiseen, mutta henkilön tulisi itse tehdä johtopäätöksensä avustamiseen ryhtymisestä.

Lähtökohtana tiedustelumenetelmien käytössä on, ettei niitä saa kohdistaa vakituiseen asumiseen käytettävään tilaan. Tietolähdetoiminnassa on kuitenkin muihin tiedustelutoimivaltuuksiin nähden erilainen tilanne, sillä poliisimies ei ole toteuttamassa tiedonhankintaa. Näin ollen tietolähteen toiminta ei myöskään olisi muutoin kuin tietolähdettä ohjattaessa sotilastiedusteluviranomaisen kontrollissa. Tästä syystä tietolähteen kanssa asioivan sotilastiedusteluviranomaisen virkamiehen tulisi kertoa tietolähteelle edellä mainittu rajoite eikä tietolähteelle saisi edes välillisesti antaa sellaista tehtävää, jossa hän voisi ajautua tilanteeseen, jolloin pyydetyt tiedot tulisi hankkia vakituiseen asumiseen käytettävässä tilassa.

Pykälän 2 momentissa säädettäisiin tietolähteen ohjatun käytön edellytyksistä. Momentin mukaan sotilastiedusteluviranomainen saisi pyytää tähän tarkoitukseen hyväksyttyä, henkilökohtaisilta ominaisuuksilta sopivaa, rekisteröityä ja tiedonhankintaan suostunutta tietolähdettä hankkimaan 1 momentissa tarkoitettuja tietoja.

Momentissa tarkoitetun suostumuksen tulisi aina olla aidosti vapaaehtoinen. Suhde sotilastiedusteluviranomaisen virkamiehen ja tietolähteen välillä ei saa muodostua epäasialliseksi esimerkiksi niin, että virkamies painostaa tietolähdettä tiedonhankintaan lupaamalla etuja, joita ei voida voimassa olevan lainsäädännön perusteella antaa. Epäasiallinen riippuvuussuhde saattaa syntyä myös silloin, kun tietolähteestä muodostuu sotilastiedusteluviranomaiselle liian tärkeä muut tiedonhankintakeinot ohittava keino.

Maininta tietolähteen henkilökohtaisista ominaisuuksista liittyisi siihen, että tietolähteellä saattaa olla epäasiallisia syitä tietolähteenä toimimiseen. Näitä voivat olla esimerkiksi taloudellisen hyödyn tai muun edun tavoittelu ja kosto. Ohjattua tietolähdetoimintaa käynnistettäessä olisikin selvitettävä se, missä tarkoituksessa ja miksi tietolähde lähtee mukaan ohjattuun toimintaan.

Pykälän 3 momentissa säädettäisiin tietolähteen ohjatun käytön rajoituksista ja tiedonhankinnan toteuttamisesta muutenkin. Tietolähteen ohjatussa käytössä tietoja ei saisi pyytää hankittavaksi sellaisella tavalla, joka edellyttäisi viranomaiselle kuuluvien toimivaltuuksien käyttöä tai joka vaarantaisi tietolähteen tai muun henkilön hengen tai terveyden. Ennen tietolähteen ohjattua käyttöä tietolähteelle olisi tehtävä selkoa hänen oikeuksistaan ja velvollisuuksistaan sekä erityisesti hänelle lain mukaan sallitusta ja kielletystä toiminnasta. Tietolähteen turvallisuudesta olisi tarpeen mukaan huolehdittava tiedonhankinnan aikana ja sen jälkeen.

Muu henkilö kuin virkamies ei voi käyttää viranomaisten toimivaltuuksia, ellei asiasta ole nimenomaisesti säädetty. Tietolähteelle ei ehdoteta annettavaksi oikeuksia perusoikeuksien ydinalueelle kohdistuvien toimivaltuuksien käyttöön. Tästäkin lähtökohdasta on selvää, että tietolähdettä ei voida käyttää viranomaisille annettujen toimivaltuuksien käyttöä koskevien rajoitusten kiertämiseen. Esimerkiksi vakituiseen asumiseen kohdistuvien rajoitusten kiertäminen tietolähdettä käyttämällä ei olisi sallittua. Sama koskisi myös esimerkiksi teknistä kuuntelua ja teknistä katselua. Puolustusvoimien tiedustelulaitos ei voisi varustaa tietolähdettä kuuntelun tai katselun mahdollistavilla laitteilla. Momentti noudattaisi EIT:n ratkaisukäytäntöä (esimerkiksi Allan v. Yhdistynyt kuningaskunta).

Sallittua tietolähdetoiminnassa olisi kuitenkin se, että tietolähde suhteidensa johdosta liikkuu sotilastiedustelun kohteiden parissa ja tapaa entuudestaan tuntemiaan henkilöitä sekä keskustelee heidän kanssaan. Sallittua tiedonhankintaa olisi myös esimerkiksi yhteyden muodostaminen peitteellä toimivan Puolustusvoimien tiedustelulaitoksen virkamiehen ja tiedustelutehtävän kohteena olevaa toimintaa harjoittavan organisaation välille. Tietolähde voisi välittää myös tietoja ja toimia rajoitetusti vaikkapa tulkkina. Tätä toimintamahdollisuutta rajoittaisi kuitenkin se, ettei Puolustusvoimien tiedustelulaitoksen virkamiehen tai tietolähteen toiminta saa johtaa siihen, että tietolähde toiminnallaan syyllistyisi rikokseen. Rikosprovokaation välttämiseen liittyy se, että välihenkilöitä käyttäessään sotilastiedusteluviranomaisen on lähtökohtaisesti toimittava passiivisesti niin, että tällainen henkilö ei tietolähdetoiminnassa syyllisty rikoksiin (EIT:n ratkaisut esimerkiksi Vanyan v. Venäjä ja Ramanauskas v. Liettua).

Sotilastiedusteluviranomainen ei voisi antaa tietolähteelle tehtävää, joka vaarantaa tietolähteen hengen tai terveyden. Vaara voi kohdistua myös tietolähteen läheisiin, mikä on tietolähdetoiminnan järjestämisessä otettava huomioon. Riippuu tapauksesta, onko tiedonhankinnan aikana ja sen jälkeen huolehdittava tietolähteen turvallisuudesta ja missä määrin. Tietolähteen erityisestä suojaamisesta säädettäisiin jäljempänä.

44 §. *Tietolähdettä koskevien tietojen käsittely ja palkkion maksu.* Pykälän 1 momentissa säädettäisiin, että tietolähdettä koskevat tiedot voitaisiin tallettaa henkilörekisteriin.

Pykälän 2 momentin mukaan rekisteröidylle tietolähteelle voitaisiin maksaa palkkio. Perustellusta syystä palkkio voitaisiin maksaa myös rekisteröimättömälle tietolähteelle. Lisäksi momentissa todettaisiin, että palkkion veronalaisuudesta säädetään erikseen.

45 §. *Tietolähteen ohjatusta käytöstä päättäminen.* Pykälän 1 momentin mukaan pääesikunnan tiedustelupäällikkö päättäisi tietolähteen ohjatusta käytöstä. Päätöksentekotaso vastaisi rikosperusteista tietolähdetoimintaa.

Pykälän 2 momentin mukaan tietolähteen ohjattua käyttöä koskeva päätös voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan.

Pykälän 3 momentissa säädettäisiin tietolähteen ohjattua käyttöä ja suojaamista koskevassa päätöksessä mainittavista asioista. Momentin mukaan päätös olisi tehtävä kirjallisesti. Päätöksessä olisi mainittava 1) toimenpiteen esittäjä, 2) tiedustelutehtävän toteuttamisesta vastaava Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti koulutettu virkamies, 3) tunnistetiedot tietolähteestä, 4) toimenpiteen perusteena olevat seikat, 5) tiedonhankinnan tai suojaamisen tavoite ja toteuttamissuunnitelma, 6) päätöksen voimassaoloaika ja 7) mahdolliset tietolähteen käyttämisen ja suojaamisen rajoitukset ja ehdot.

Pykälän 4 momentin mukaan päätöstä olisi olosuhteiden muuttuessa tarvittaessa tarkistettava. Tietolähteen ohjatun käytön ja suojaamisen lopettamisesta olisi tehtävä kirjallinen päätös.

46 §. *Tietolähteen turvaaminen.* Pykälässä säädettäisiin tietolähteen turvaamisesta. Sotilastiedusteluviranomaisella on lähtökohtaisesti velvollisuus huolehtia tietolähteidensä turvallisuudesta tarpeen mukaan tiedonhankinnan aikana ja sen jälkeen. Tietolähteen turvaamistoimivaltuus ei kuitenkaan korvaisi todistajansuojeluohjelmasta annetussa laissa (88/2015) tarkoitettua todistajansuojeluohjelmaa. Jos tietolähdettä olisi tarpeen suojella pidempiaikaisesti ja häneen kohdistuisi vakava hengen tai terveyden uhka eikä uhkaa voitaisi tehokkaasti torjua muilla toimenpiteillä, niin olisi perusteltua harkita tietolähteen kohdalla todistajansuojeluohjelman käynnistämistä.

Pykälän 1 momentin mukaan sotilastiedusteluviranomainen voisi tietolähteen suostumuksella valvoa tämän asuntoa tai muuta tietolähteen asumiseen käyttämää tilaa tai muuta paikkaa ja sen välitöntä lähiympäristöä kameran tai muun paikkaa sijoitetun teknisen laitteen, menetelmän tai ohjelmiston avulla, jos se olisi tarpeen tietolähteen henkeä tai terveyttä uhkaavan vaaran torjumiseksi. Tietolähteen turvaamisesta ei tarvitsisi ilmoittaa sivullisille.

Momentissa mahdollistettaisiin erilaisten tietolähteen turvaamiseksi tarpeellisten turvajärjestelmien, kuten esimerkiksi valvontakameroiden ja liiketunnistimien asentamisen suojelun tarpeessa olevan tietolähteen asuntoon ja sen välittömään lähiympäristöön. Muulla tietolähteen asumiseen käyttämällä tilalla tarkoitettaisiin esimerkiksi hotellihuoneita sekä muita kyseisellä hetkellä tietolähteen asuttamaa tilaa.

Toisin kuin teknisessä katselussa, valvonta ei tapahtuisi kohteen tietämättä eikä tiedonhankintatarkoituksessa. Valvonnan tarkoituksena olisi sen sijaan tietolähteen turvaaminen, mutta välillisesti tietolähteen turvaamiseen liittyisi myös tiedonhankintatarkoitus esimerkiksi siitä, keitä alueella liikkuisi.

Valvontaa ei saisi suorittaa, ellei se olisi tarpeen tietolähteen henkeä ja terveyttä uhkaavan vaaran torjumiseksi. Tällä tarkoitettaisiin sitä, että tietolähteen henkeen ja terveyteen kohdistuisi ainakin potentiaalinen vaara.

Säännös koskisi myös tilanteita, joissa suojeltavan kotiin tai sen välittömään lähiympäristöön asennetut laitteet ulottuisivat jonkun toisen kotirauhan suojaamalle alueelle, joskaan ei sen ydinalueelle. Tällainen tilanne voisi olla kerrostalossa, jossa turvakamera kuvaisi myös taloyhtiön asukkaiden yhteistä rappukäytävää tai rivitalossa, jolloin kuvaaminen saattaisi ulottua myös yhteisille piha-alueille.

Tietolähteen turvaaminen edellyttäisi, ettei kamera- ja muusta valvonnasta tiedoteta sivullisille paljastumisriskin välttämiseksi ja tietolähteen hengen tai terveyden suojaamiseksi.

Pykälän 2 momentin mukaan tietolähteen turvaamisen edellytyksenä on lisäksi se, että tietolähde olisi henkilökohtaisilta ominaisuuksiltaan sopiva. Tällä tarkoitettaisiin sitä, että tietolähde on tosiasiallisesti turvaamisen tarpeessa ja että tietolähde myös haluaa tulla turvatuksi. Tietolähde ei saisi olla esimerkiksi itsetuhoinen tai muuten vaarantaa tiedustelutoimintaa.

Pykälän 3 momentin mukaan valvonta olisi lopetettava viipymättä, jos se ei olisi enää tarpeen tietolähteen henkeä tai terveyttä uhkaavan vaaran torjumiseksi. Tämä tarkoittaisi sitä, että kun tietolähteen turvaamiselle ei olisi enää perustetta olemassa, niin turvaamistoimet tulisi lopettaa välittömästi.

Pykälän 4 momentin mukaan edellä 1 momentissa tarkoitetussa valvonnassa kertyneet tallenteet olisi hävitettävä heti sen jälkeen, kun niitä ei tarvittaisi tietolähteen turvaamiseen. Jos niitä olisi kuitenkin tarpeen säilyttää asiaan osallisen oikeusturvaan liittyvistä syistä, tallenteet saataisiin säilyttää ja niitä saataisiin käyttää tässä tarkoituksessa. Tällöin tallenteet olisi hävitettävä, kun asia olisi lainvoimaisesti ratkaistu tai jätetty sillensä.

Tallenteita ei saisi säilyttää ja käyttää muuhun kuin säännöksessä mainittuun tarkoitukseen. Kysymys, näissä tapauksissa saattaisi olla siitä, että tietolähteeseen on kohdistettu välivaltaan ja viranomainen puuttuu välittömästi toimintaan. Mikäli tässä tilanteessa viranomaista vastaan nostettaisiin syyte, tietolähteen turvaamisessa syntyneitä tallenteita voitaisiin käyttää syyttömyyttä tai syyllisyyttä osoittavana selvityksenä. Näissä tapauksissa tallenteita saatettaisiin tarvita rikosasian tai vahingonkorvausasian käsittelyn yhteydessä. Koska kyse on turvaamistoimivaltuudesta eikä tiedustelumenetelmän käytöstä, niin kyse ei olisi tiedustelumenetelmällä saadun tiedon käyttämisestä rikosprosessissa, vaan tallenteet olisivat syntyneet eri tarkoituksessa. Rikos- ja vahingonkorvauskäsittely saattaisi kuitenkin edellyttää suljettua käsittelyä.

47 §. *Valeosto.* Pykälän 1 momentin mukaan valeostolla tarkoitettaisiin sotilastiedusteluviranomaisen tekemää esineen, aineen, omaisuuden tai palvelun ostotarjousta tai ostoa, jonka tavoitteena on saada sotilastiedusteluviranomaisen haltuun tai löytää tiedustelutehtävään liittyvä esine, aine, omaisuus tai tieto.

Valeosto voisi tulla kyseeseen esimerkiksi väärien asiakirjojen valmistamisessa käytettävästä materiaalista, jota vieraan valtion tiedustelupalvelu saattaisi käyttää. Toisaalta kyse voisi olla yhteiskunnan elintärkeiden toimintojen vahingoittamiseen mahdollisesti käytettävästä ohjelmistosta tai sen valmistamisesta, jolla voitaisiin suorittaa vakava tietoverkkohyökkäys yhteiskunnan elintärkeisiin toimintoihin. Sotilastiedusteluviranomainen voisi tässä tapauksessa hankkia tällaisesta toimijasta tietoa tekemällä ostotarjouksen tällaisen ohjelmiston valmistamisesta tai hankkia näytteen tällaisesta ohjelmistosta.

Tarkoituksena olisi myös hankkia tietoja tiettyyn myyjään yhteydessä olevista tahoista. Valeoston kautta voitaisiin päästä lähelle tiettyä tiedustelutehtävään liittyvää myyjää ja tätä kautta voitaisiin myös saada tietoa siitä, ketkä hankkivat esimerkiksi tietyltä myyjältä palveluita ja tarvikkeita.

Yksinomaan yleisön saataville toimitetusta myyntitarjouksesta tehtävästä valeostosta säädettäisiin 47 §:n 1 momentissa sen johdosta, että päätöksenteko silloin poikkeaisi pääsäännöstä. Valeosto on kuitenkin erotettava tiedustelujen tekeminen yleisesti saatavilla olevan ilmoituksen perusteella.

Valeoston yhteydessä olisi mahdollista myös tehdä valmistelevia toimenpiteitä, kuten esimerkiksi valeoston kohteena olevan tavaran varastoiminen tai siirtäminen ennen varsinaista ostotarjousta tai ostoa, jolloin tällainen toimenpide voisi muodostaa myös osan vastikkeesta.

Pykälän 2 momentissa säädettäisiin valeoston edellytyksistä. Sotilastiedustelun viranomainen saisi tehdä valeoston, jos sen tekeminen olisi välttämätöntä tietojen saamiseksi tiedustelutehtävän kannalta.

Pykälän 3 momentin mukaan valeoston toteuttaja saisi tehdä vain sellaista tiedonhankintaa, joka on välttämätöntä valeoston toteuttamiseksi. Valeosto olisi toteuttava siten, ettei se saa kohteena olevaa tai muuta henkilöä tekemään rikosta, jota hän ei muuten tekisi.

Valeostoa ei ole usein mahdollista tehdä, jollei sitä edellä tiedonhankinta- ja kauppaneuvotteluvaihe sekä luonteva kaupantekotilaisuudesta irtautumisen vaihe. Ennen valeostoa on pystyttävä varmistumaan siitä, että valeoston kohteena oleva esine, aine, omaisuus tai palvelu on kohteena olevan henkilön hallinnassa, jolloin voidaan sulkea pois rikosprovokaation vaaraa. Näiden seikkojen vuoksi momentissa todettaisiin nimenomaisesti, että valeoston toteuttaja saa tehdä vain sellaista tiedonhankintaa, joka on välttämätöntä valeoston toteuttamiseksi. Valeostona koskevalla toimivaltuudella ei saisi kiertää esimerkiksi peitetoimintavaltuutta tekemällä pelkästään tiedonhankintaa varsinaiseen valeostoon pyrkimättä.

Momentissa mainittaisiin nimenomaisesti velvollisuudesta toteuttaa valeosto siten, ettei se saa kohteena olevaa tai muuta henkilöä tekemään rikosta, jota hän ei muuten tekisi. Jos valeoston toteuttamiseksi jouduttaisiin käyttämään jotakin sivullista henkilöä esimerkiksi yhteyden muodostamiseksi valeostajan ja valeoston kohteena olevan henkilön välille, olisi varmistuttava siitä, ettei valeosto saa aikaan sitä, että sivullinen tekisi yhteyttä muodostaessaan rikoksen. Toisaalta sotilastiedustelun viranomaisen selonottovelvollisuus ei voisi olla kovin ankara, koska valeostotapahtumaan nähden etäisten henkilöiden toiminta on usein sotilastiedustelun viranomaisten vaikutusmahdollisuuksien ulkopuolella. Luonnollisesti kysymyksessä oleva kielto koskisi ennen kaikkea sitä henkilöä, jolle ostotarjous tehdään tai jolta ostetaan.

Pykälän 4 momentissa mainittaisiin, että valeosto asunnossa on sallittua vain, jos sisäänkäynti tai oleskelu tapahtuu asuntoa käyttävän aktiivisella myötävaikutuksella. Puheena olevan sääntely olisi oikeusturvasyistä perusteltua, koska valeosto voidaan toteuttaa myös asunnossa. Sääntely olisi perusteltua säätää yhdenmukaisesti peitetoimintaa koskevan vastaavanlaisen vaatimuksen kanssa.

48 §. *Valeostosta päättäminen.* Pykälän 1 momentin mukaan pääesikunnan tiedustelupäällikkö päättäisi valeostosta. Yksinomaan yleisön saataville toimitetusta myyntitarjouksesta tehtävästä valeostosta saa päättää myös tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies. Yleisön saataville toimitetusta myyntitarjouksesta tehtävässä valeostossa rikos provokaatioriski on lähtökohtaisesti vähäinen, jolloin myös päätöksentekotaso voisi alla matalampi.

Pykälän 2 momentin mukaan valeostoa koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Pykälän 3 momentin mukaan päätös valeostosta on tehtävä kirjallisesti. Päätöksessä on mainittava: 1) toimenpiteen perusteena oleva uhka ja toimenpiteen tavoite, 2) valeoston kohteena oleva henkilö, 3) tosiseikat, joihin valeoston edellytykset ja kohdistaminen perustuvat, 4) valeoston kohteena oleva esine, aine, omaisuus tai palvelu, 5) valeoston tarkoitus, 6) päätöksen voimassaoloaika, 7) valeoston suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies, 8) mahdolliset valeoston rajoitukset ja ehdot.

Valeoston tuloksellisuusodotus (3 kohta) liittyisi asetettavaan todennäköisyyden vaatimukseen. 46 §:n mukaan valeoston tulisi olla välttämätöntä tiedon saamiseksi tiedustelutehtävän kannalta.

Valeosto voisi kohdistua myös niin sanotusti vilpittömässä mielessä toimivaan henkilöön. Valeosto voisi nykyiseen tapaan kohdistua myös muuhun kuin myyjänä olevaan henkilöön. Esimerkiksi tehokas tiedonhankkiminen vieraan vallan sotilastiedustelupalvelun toiminnasta edellyttää, että sotilastiedustelun viranomaiset kykenevät saamaan riittävästi tietoa vieraan vallan sotilastiedustelupalvelun toiminnasta, maksuyhteyksistä sekä taustalla toimivasta organisaatiosta ja sen johdosta. Tällaisessa tilanteessa valeosto voisi olla tarpeen kohdistaa esimerkiksi edellä kuvatun tahon kauppakumppaniin.

49 §. *Valeoston toteuttamista koskeva suunnitelma.* Pykälän 1 momentin mukaan valeoston toteuttamisesta olisi laadittava kirjallinen suunnitelma, jos se on tarpeen toiminnan laajuuden tai muun vastaavan syyn vuoksi. Pykälän 2 momentin mukaan valeoston toteuttamista koskevaa suunnitelmaa olisi olosuhteiden muuttuessa tarvittaessa tarkistettava. Avataan suunnitelma, kuka tekee jne.

Erillinen valeoston toteuttamista koskeva suunnitelma voi olla tarpeen erityisesti toimintaan sisältyvien riskien torjumiseksi.

50 §. *Valeoston toteuttamista koskeva päätös.* Pykälän 1 momentin mukaan päätös valeoston toteuttamisesta olisi tehtävä kirjallisesti. Päätöksen tekee valeoston toteuttamisesta vastaava tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies. Valeoston käyttäminen olisi siis kaksivaiheinen. Valeoston käytännön toteuttaminen vaatii ensi päätöksen valeostosta, jonka jälkeen olisi tehtävä erillinen päätös valeostotapahtumasta, kun tilaisuus valeostolle tulee mahdolliseksi.

Pykälän 2 momentin mukaan päätöksessä olisi mainittava: 1) valeoston päättänyt tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies; 2) tunnistetiedot valeoston suorittavista sotilastiedusteluviranomaisten virkamiehistä; 3) selvitys siitä, miten on varmistuttu, että valeosto ei saa sen kohteena olevaa tai muuta henkilöä tekemään rikosta, jota hän ei muuten tekisi; 4) mahdolliset valeoston rajoitukset ja ehdot.

Pykälän 3 momentin mukaan, jos toimenpide ei siedä viivytystä, 2 momentissa tarkoitettua päätöstä ei tarvitsisi laatia kirjallisesti ennen valeostoa. Päätös olisi kuitenkin laadittava kirjallisesti viipymättä valeoston jälkeen.

Pykälän 4 momentin mukaan valeoston toteuttamista koskevaa päätöstä olisi olosuhteiden muuttuessa tarvittaessa tarkistettava.

51 §. *Paikkatiedustelu.* Pykälässä säädettäisiin täysin uudesta tiedonhankintatoimivaltuudesta, paikkatiedustelusta. Pykälän 1 momentin mukaan paikkatiedustelulla tarkoitettaisiin paikassa toimitettavaa tiedustelua esineen, omaisuuden, asiakirjan, tiedon tai seikan löytämiseksi. Momentissa tarkoitettu paikka vastaisi pakkokeinolain 8 luvun 1 §:n 4 momentissa tarkoitettua paikkaa, mikä kävisi ilmi pykälän 2 momentissa olevasta rajauksesta.

Paikkatiedustelu toteutettaisiin lähtökohtaisesti salaa niin, ettei paikan omistaja, haltija tai muu henkilö tietäisi sotilastiedusteluviranomaisen käyvän siellä. Tätä ilmentäisi välillisesti myös tiedustelumenetelmän nimi, paikkatiedustelu.

Paikkatiedustelun kohteena voisi olla esimerkiksi suljettu kulkuneuvo (kuten auto), jota ei käytetä asumiseen. Esineen tai asiakirjan löytämiseksi ja jäljentämiseksi auton tavaratilaan tai hansikaslokeroon kohdistuva salaa toimitettava etsintä olisi tyyppiesimerkki paikkatiedustelusta. Muina esimerkkeinä paikkatiedustelun piiriin kuuluvista paikoista voidaan mainita myymälät, virastot, kahvilat ja liiketilojen huoneet.

Tiedustelussa tiedon välittämiseenkin tarvitaan toisinaan useita välikäsiä, ja voi olla tarpeen selvittää, kuka tiedon välittää eteenpäin. Tiedustelutoiminnassa on melko yleistä käyttää esimerkiksi kätköjä ja postilaatikoita, joissa tietoa voidaan piilottaa erilaisiin paikkoihin. Lähetyksen toimittaja ja vastaanottaja eivät tapaa toisiaan ja kiinnijäämisen riski pienenee. Sotilastiedustelun kannalta on erittäin tärkeää pystyä kohdistamaan tiedonhankintaa mainitunlaisiin paikkoihin salaa ja jäljentää esimerkiksi ulkomaan sotilasorganisaatioiden sisäistä ja ulkoista viestintää.

Pykälän viittaus paikkaan olisi yläkäsite, joka käsittää tilat ja muut paikat. Viimeksi mainittuja olisivat lähinnä ulkoalueet. Viittauksella tilaan tarkoitettaisiin seinin ja usein myös katolla rajattuja paikkoja.

Pykälän 2 momentissa olisi lueteltuna paikat, joihin paikkatiedustelua ei saisi kohdistaa. Vakituiseen asumiseen käytettävä tila mainittaisiin erikseen pykälän 3 momentissa.

Momentin kiellon piirissä olisivat erityisesti sellaisten tilojen paikkatiedustelu, jossa voisi olla jonkin muun lain perusteella erityisen salassapitovelvollisuuden alaista tietoa. Tilojen korostunut liityntä salassapitovelvollisuuteen tai -oikeuteen todettaisiin ilmaisulla ”tiedustelua sellaisessa tilassa, jossa tiedustelun kohteeksi on syytä olettaa joutuvan tietoa”. Ilmaisu tarkoittaisi sitä, että paikkaan kohdistuvan tiedonhankinnan määrittäminen paikkatiedustelun kieltojen alaan ei riippuisi kategorisesti siitä, mihin tarkoitukseen kyseessä olevaa paikkaa yleensä tai pääasiallisesti käytetään. Paikkatiedustelun alaan saattaisi mennä esimerkiksi asianajajan asunto, jos hän tekee töitä siellä tai jos siellä muuten on hänen työhönsä liittyviä asiakirjoja. Toisaalta asianajotoimistoon kohdistuva paikkatiedustelu saatettaisiin rajata siten, että tietoon ei ilmeisesti tule salassa pidettäviä tietoja. Koska tarkoituksena on tältä osin suojata salassapitovelvollisuutta tai -oikeutta eikä tiettyjä tiloja, paikkatiedustelun kohteena olevan tilan määrittely jäisi pakostakin jossakin määrin avoimeksi ja paikkatiedustelupäätöksen valmistelussa tehtävän huolellisen harkinnan yhteydessä yksityistapauksellisesti määritettäväksi.

Momentissa kiellettäisiin paikkatiedustelu tilassa, jossa tiedustelun kohteeksi on syytä olettaa joutuvan tietoa, josta oikeudenkäymiskaaren 17 luvun 23 §:n 1 momentissa tarkoitettu henkilö ei saa todistaa oikeudenkäynnissä tai josta mainitun luvun 24 §:n 2 tai 3 momentissa tarkoitettu henkilö saa kieltäytyä kertomasta. Mainitun säännöksen tiloja olisivat esimerkiksi virkamiesten työhuoneet, lääkärin vastaanottotilat ja asianajotoimistot. Oikeudenkäymiskaaren 17 luvun 24 §:n 2 ja 3 momentin ja siinä viitatun sananvapauden käyttämisestä joukkoviestinnässä annetun lain perusteella kohdan soveltamisalaan kuuluvia tiloja yleensä olisivat esimerkiksi toimittajien asunnot sekä lehtien ja kirjojen toimitusten ja kustantamojen toimitilat ja niiden palveluksessa olevien henkilöiden asunnot.

Ilmaisu ”tiedustelun kohteeksi on syytä olettaa joutuvan tietoa” tarkoittaa sitä, että tiedonhankinnan arvioiminen paikkatiedusteluksi on tietyn kynnyksen takana. Tämä kynnys riippuisi siitä, onko kysymyksessä salassapitoon velvollisen tai oikeutetun työhuone, liiketila tai muu vastaava ammatinharjoittamispaikka vai onko kysymyksessä muu tila. Jos kysymys on ammatinharjoittamispaikasta ja jos tiedustelun kohteena ovat paikassa olevat asiakirjat ja tiedot, lähtökohtana olisi etsinnän katsominen paikkatiedustelun käyttöalan ulkopuolelle. Muiden tilojen osalta tulisi olla nimenomaista tietoa siitä, että sieltä saattaa löytyä kysymyksessä olevaa tietoa. Kuten edellä on viitattu, kumpienkin paikkojen kohdalla vaikuttaisi se, mitä paikkatiedustelupäätöksen perusteella paikasta etsitään ja mitä siellä tutkitaan. Lisäksi kynnykseen saattaisi vaikuttaa se, minkälaisen henkilön salassapitovelvollisuudesta tai -oikeudesta on kysymys. Esimerkiksi virkamiehillä ei välttämättä ole työhuoneessaan samassa määrin salassa pidettävää tietoa kuin asianajajalla.

Jos alkuperäinen arvio tilojen luonteesta osoittautuisi vääräksi, paikkatiedustelun lähtökohtia olisi arvioitava uudelleen ja paikkatiedustelu keskeytettävä välittömästi.

Pykälän 3 momentissa olisi paikkatiedustelun erityiset edellytykset. Paikkatiedustelua ei saisi kohdistaa vakituiseen asumiseen käytettävään tilaan. Lisäksi erityisenä edellytyksenä olisi se, että paikkatiedustelulla voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Tätä edellytystä on kuvattu tarkemmin aiemmin yksityiskohtaisissa perusteluissa.

52 §. *Paikkatiedustelusta päättäminen.* Pykälän 1 momentin mukaan tuomioistuin päättäisi paikkatiedustelusta, kun se kohdistuu paikkaan, johon ei ole yleistä pääsyä tai johon yleinen pääsy siihen on rajoitettu tai estetty paikkatiedustelun toimittamisajankohtana, tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimiehen tai muun virkamiehen vaatimuksesta.

Vaikka paikkatiedustelulla ei puututa kotirauhan suojan ydinalueelle, niin päätöksentekotoimivallan osoittaminen tuomioistuimelle 1 momentissa tarkoitetuissa tapauksissa on perusteltua paikkatiedustelun vaivihkaisen luonteen johdosta. Paikkatiedustelussa ei noudatettaisi kotietsintämenettelyä. Tällöin tiedonhankinnan kohteella ei ole mahdollisuuksia kontrolloida viranomaisen toimintaa samalla tavalla kuin esimerkiksi pakkokeinolain 8 luvun 1 §:n 4 momentissa tarkoitetussa paikanetsinnässä.

Pykälän 2 momentin mukaan, jos 1 momentissa tarkoitettu asia ei siedä viivytystä, pääesikunnan tiedustelupäällikkö tai tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saisi päättää paikkatiedustelusta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia olisi saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta.

Jos kiireellisessä tilanteessa tehdyssä päätöksessä tuomioistuin katsoisi, että edellytyksiä toimenpiteelle ei ole ollut, tiedustelumenetelmän käyttö olisi lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot olisi heti hävitettävä. Hävittämisvelvollisuudesta näissä tapauksissa säädettäisiin jäljempänä.

Pykälän 3 momentin mukaan pääesikunnan tiedustelupäällikkö tai tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättäisi muusta kuin 1 momentissa tarkoitetusta paikkatiedustelusta.

Momentin alaan kuuluisivat sellaiset paikat, joihin on yleinen pääsy ja joihin yleistä pääsyä ei ole rajoitettu tai estetty paikkatiedustelun toimittamisajankohtana. Sama koskisi paikkatiedustelua, jonka kohteena olisi kulkuneuvo.

Pykälän 4 momentin mukaan lupa voitaisiin antaa ja päätös tehdä enintään kuukaudeksi kerrallaan.

Paikkatiedustelu on tiedustelumenetelmä, jonka tarkoituksena on löytää tiedustelutehtävän kannalta tietoa, jolla voidaan olettaa olevan erittäin tärkeä merkitys tiedustelutehtävän kannalta. Tiedustelun luonteeseen kuuluu se, että tietyssä paikassa ilmenisi tarvetta käydä useammin kuin kerran. Tällaiset tilanteet perustelevat pidempää lupa-aikaa. Mainittakoon esimerkkinä tilanne, jossa olisi tarpeen paikkatiedustelun yhteydessä jäljentää tiedustelutehtävän kannalta merkityksellisiä asiakirjoja useammin kuin kerran.

Pykälän 5 momentin mukaan paikkatiedustelu koskevassa vaatimuksessa tai päätöksessä olisi riittävällä tarkkuudella yksilöitävä: 1) toimenpiteen perusteena oleva uhka ja toimenpiteen tavoite, 2) paikkatiedustelun kohteena oleva paikka, 3) ne seikat, joiden perusteella paikkatiedustelun edellytysten katsotaan olevan olemassa, 4) mahdollisuuksien mukaan se, mitä paikkatiedustelulla pyritään löytämään, 5) mahdolliset paikkatiedustelun rajoitukset.

Pykälän 6 momentin mukaan asian kiireellisyyden sitä edellyttäessä paikkatiedustelua koskeva päätös saataisiin kirjata paikkatiedustelun toimittamisen jälkeen.

Pykälän 7 momentin mukaan paikkatiedustelussa ei saisi hankkia pakkokeinolain 8 luvun 1 §:n 3 momentissa tarkoitettua tietoa. Jos paikkatiedustelussa ilmenisi, että tiedustelu on kohdistunut sellaiseen tietoon, olisi tiedustelu siltä osin heti lopetettava ja tietoa koskevat muistiinpanot ja jäljennökset heti hävitettävä.

Viittauksella tiedustelun siltä osin heti lopettamiseen tarkoitettaisiin sitä, ettei paikkatiedustelua muilta osin olisi tarpeen lopettaa.

53 §. *Jäljentäminen.* Pykälän mukaan sotilastiedusteluviranomainen olisi sotilastiedustelussa oikeus jäljentää asiakirja tai muu esine käyttämällä teknistä laitetta tietojen hankkimiseksi tiedustelutehtävään.

Tietojen hankkiminen tiedustelutehtävään edellyttäisi mahdollisuutta asiakirjojen jäljentämiseen. Tiedonhankinta ei ole luontevaa, jos virkamies joutuisi muistinvaraisesti kirjaamaan esimerkiksi paikkatiedustelussa tiedustelutehtävän kannalta merkityksellisten asiakirjojen sisällön paikkatiedustelun jälkeen.

Asiakirja tai muu esine tulisi pääsääntöisesti jäljentää ilman haltuunottamista tiedusteluoperaation paljastumisriskin takia.

Asiakirja voitaisiin käytännössä jäljentää ottamalla siitä valokuva tai skannaamalla asiakirja esimerkiksi puhelimeen asennetulla skannausohjelmalla. Muun esineen jäljentämisellä tarkoitettaisiin esimerkiksi tilannetta, jossa olisi tarpeen jäljentää esine käyttämällä 3D-skanneria.

54 §. *Jäljentämiskiellot.* Sotilastiedustelulainsäädännön yhteydessä on huomioitava se, ettei tiedustelumenetelmillä hankittua tietoa ole lähtökohtaisesti tarkoitus käyttää rikosprosessissa todisteena. Jäljentämiskielloilla ei olisi vastaavanlaista merkitystä tiedustelutoiminnassa kuin mitä rikosprosessuaalisia toimivaltuuksia käytettäessä on. Jäljentämiskieltoja ei myöskään ole mahdollista soveltaa yhteneväisesti vastaavien takavarikoimis- ja jäljentämiskieltojen sekä todistelua koskevien säännösten kanssa.

Pykälän 1 momentin mukaan asiakirjaa tai muuta 1 momentissa tarkoitettua kohdetta ei saisi jäljentää, jos se sisältää tietoa, josta oikeudenkäymiskaaren 17 luvun 10–14, 16, 20 tai 21 §:n nojalla on velvollisuus tai oikeus kieltäytyä todistamasta.

Sääntely vastaisi tältä osin pakkokeinolain 7 luvun 3 §:n 1 momentissa säädettyjä jäljentämiskieltoja.

Pykälän 2 momentin mukaan jos salassapitovelvollisuus tai -oikeus perustuu oikeudenkäymiskaaren 17 luvun 11 §:n 2 tai 3 momenttiin tai 13, 14, 16 tai 20 §:ään, edellytyksenä kiellolle 1 momentissa säädetyn lisäksi olisi, että kohde on mainitussa lainkohdassa tarkoitetun henkilön tai häneen mainitun luvun 22 §:n 2 momentissa tarkoitetussa suhteessa olevan henkilön hallussa taikka sen hallussa, jonka hyväksi salassapitovelvollisuus tai -oikeus on säädetty.

Sääntely vastaisi tältä osin pakkokeinolain 7 luvun 3 §:n 2 momentissa säädettyjä jäljentämiskieltoja. Kielto on voimassa vain, milloin asiakirja on momentissa mainitun henkilön hallussa tai sen hallussa, jonka hyväksi vaitiolovelvollisuus on säädetty. Tiedustelutoiminnan luonteesta johtuen kyseinen säännös ei tulisi usein sovellettavaksi.

Pykälän 3 momentin mukaan jäljentämiskieltoa ei kuitenkaan olisi, jos: 1) oikeudenkäymiskaaren 17 luvun 11 §:n 2 tai 3 momentissa, 12 §:n 1 tai 2 momentissa, 13 §:n 1 tai 3 momentissa, 14 §:n 1 momentissa taikka 16 §:n 1 momentissa tarkoitettu henkilö, jonka hyväksi salassapitovelvollisuus on säädetty, suostuu jäljentämiseen, 2) oikeudenkäymiskaaren 17 luvun 20 §:n 1 momentissa tarkoitettu henkilö suostuu jäljentämiseen.

Sääntely vastaisi pakkokeinolain 7 luvun 3 §:n 3 momentissa säädettyjä jäljentämiskieltoja. Tiedustelutoiminnan luonteesta johtuen kyseinen säännös tulisi harvoin sovellettavaksi.

55 §. *Telekuunteluun, televalvontaan ja tukiasematietoihin liittyvät jäljentämiskiellot.* Pykälän 1 momentin mukaan tietoyhteiskuntakaaren 3 §:n 27 kohdassa tarkoitetun teleyrityksen (teleyritys) tai mainitun lain 3 §:n 36 kohdassa tarkoitetun yhteisötilaajan (yhteisötilaaja) hallusta ei saa jäljentää asiakirjaa tai dataa, joka sisältää tämän lain 5 luvun 5 §:n 1 momentissa tarkoitettuun viestiin liittyviä tietoja taikka mainitun luvun 8 §:n 1 momentissa tarkoitettuja tunnistamistietoja tai 11 §:n 1 momentissa tarkoitettuja tukiasematietoja.

Pykälän 2 momentin mukaan poikkeuksesta 1 momentissa tarkoitettuun takavarikoimiskieltoon säädettäisiin 5 §:ssä. Tällä tarkoitettaisiin tietojen hankkimista telekuuntelun sijasta.

56 §. *Lähetyksen jäljentäminen.* Pykälän mukaan kirje tai muu vastaava lähetys saataisiin ennen sen saapumista vastaanottajalle jäljentää, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tiedustelutehtävän kannalta ja tiedot liittyvät toimintaan, joka vakavasti uhkaa maanpuolustusta tai kansallista turvallisuutta. Kirjeen osalta olisi huomioitava, että kirje kuuluu luottamuksellisen viestin salaisuuden alaan.

Pykälä vastaisi pakkokeinolain 7 luvun 5 §:ään. Erona olisi, ettei lähetyksen jäljentämisestä tarvitsisi ilmoittaa lähetyksen vastanottajalle, vaan kyseessä olisi vastaanottajalta salaa tehtävä toimenpide.

57 §. *Lähetyksen pysäyttäminen jäljentämistä varten.* Pykälän 1 momentin mukaan jos olisi syytä olettaa, että kirje tai muu vastaava lähetys, joka voidaan jäljentää, on tulossa postitoimistoon, rautateiden liikennepaikkaan tai lähetysten kuljetusta ammatikseen liikennöinnin yhteydessä tai muuten harjoittavan toimipaikkaan taikka on jo siellä, tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa määrätä lähetyksen pidettäväksi postitoimistossa, liikennepaikassa tai toimipaikassa, kunnes jäljentäminen on ehditty suorittaa.

Momentin sääntely perustuisi pääosin pakkokeinolain 7 luvun 6 §:n 1 momentin sääntelyyn. Tavaraliikenteen osalta edellytyksenä on, että on olemassa kiinteä toimipaikka, josta lähetys voidaan noutaa tai joka huolehtii sen toimittamisesta vastaanottajalle. Tällaisena toimipaikkana voidaan pitää esimerkiksi yhden logistiikka-alan yritystoimintaa harjoittavan konttoria, milloin sieltä käsin hoidetaan saapuvaa rahtia koskevia asioita ja pidetään yhteyttä sen vastaanottajiin.

Pykälän 2 momentin mukaan edellä 1 momentissa tarkoitettu määräys annettaisiin enintään kuukauden määräajaksi, joka alkaa siitä, kun postitoimiston, liikennepaikan tai toimipaikan esimies on saanut tiedon määräyksestä. Lähetystä ei saisi ilman 1 momentissa tarkoitetun virkamiehen lupaa luovuttaa muulle kuin hänelle tai hänen määräämälleen henkilölle.

Määräajan asettaminen ei voisi olla kuukautta pidempi, koska määräyksellä asetetaan toimipaikan henkilöstölle ylimääräinen velvoite valvoa saapuvia lähetyksiä. Määräys voitaisiin antaa uudelleen edellisen määräajan loputtua.

Pykälän 3 momentin mukaan postitoimiston, liikennepaikan tai toimipaikan esimiehen olisi heti ilmoitettava määräyksen antajalle lähetyksen saapumisesta. Tämän on ilman aiheetonta viivytystä päätettävä jäljentämisestä.

Jos saapuvaa lähetystä ei ole voitu tarkoin yksilöidä ja määräyksen antajan tai hänen edustajansa saapuessa toimipaikkaan esimerkiksi kirjekuoressa olevan lähettäjän nimen tai käsialan perusteella on selvää, että kysymyksessä ei voi olla jäljennettävä lähetys, sitä ei saa avata eikä tutkia, vaan se on viipymättä toimitettava eteenpäin.

58 §. *Jäljentämisestä päättäminen.* Pykälän mukaan tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättäisi jäljentämisestä. Kyseisiin virkamieheen liittyvä koulutuksen vaatimus johtuu siitä, että olisi erityisen tärkeää tiedostaa rajapinnat jäljentämisen ja muiden tiedustelumenetelmien, kuten teknisen laitetarkkailun välillä. Näihin liittyisivät olennaisesti jäljentämiskieltojen hallitseminen. Koulutuksella voidaan myös vähentää tiedonhankinnan paljastumisen riskiä sekä edistää toiminnan tuloksellisuutta.

Pykälän 2 momentissa säädettäisiin kiirepäätöksentekomenettelystä. Muu kuin tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies voisi yksittäistapauksessa päättää jäljennöksen ottamisesta itsenäisesti. Asia olisi kuitenkin saatettava 24 tunnin sisällä pykälän 1 momentissa tarkoitetun sotilaslakimiehen tai virkamiehen ratkaistavaksi.

59 §. *Jäljentämisen kirjaaminen ja jäljennöksen hävittäminen.* Pykälän mukaan asiakirjan tai muun kohteen jäljentämisestä olisi ilman aiheetonta viivytystä laadittava pöytäkirja. Siinä olisi riittävästi mainittava jäljentämisen tarkoitus, selostettava jäljentämiseen johtanut menettely sekä yksilöitä jäljentämisen kohde.

Pykälän 2 momentin mukaan tarpeettomaksi osoittautuva, jäljennös olisi hävitettävä. Pykälässä ei säädettäisi hävittämisen ajankohdasta. Lähtökohtana olisi, että jäljennös hävitetään heti, kun havaitaan, ettei se ole tarpeen tiedustelutehtävän kannalta. Jäljennöksen hävittämisestä tulisi tehdä merkintä.

60 §. *Radiosignaalitiedustelu.* Pykälän 1 momentissa säädettäisiin radiosignaalitiedustelusta, jonka avulla sotilastiedusteluviranomainen voisi hankkia tietoa radiotaajuisista sähkömagneettisista aalloista. Radiosignaalitiedustelua voitaisiin kohdistaa laajasti eri sotilaskohteiden käyttämään viestintään.

Sähkömagneettisia aaltoja eli radioaaltoja käytetään esimerkiksi asevoimien viestinnässä laajalti. Valtioiden hallitsemista taajuusalueista on usein varattu tietyt taajuudet pelkästään asevoimien käyttöön, eikä näillä taajuusalueilla tapahtuvan viestinnän voida katsoa nauttivan yksityisen viestin suojasta.

Radiosignaalitiedustelu kattaa signaalitiedustelun osa-alueista radioteknisen viestitiedustelun sekä elektronisen mittaustiedustelun. Viestitiedustelu kohdistuu tyypillisesti vieraan vallan viranomaisten sisäiseen viestiliikenteeseen tai esimerkiksi suomalaiselle rauhaturvajoukolle uhkaa aiheuttavan joukon viestiliikenteeseen.

Lisäksi eri tekniset laitteet ja järjestelmät voivat viestiä keskenään radioaalloilla ilman, että kyseessä on kahden ihmisen välinen viestintä. Kyse voi olla esimerkiksi kahden laitteen välisestä tietojen vaihdosta, mikä ei sisällä viestiksi katsottavaa tietoa, kuten ohjuksen ohjautuminen annettuun maaliinsa tai asejärjestelmän ohjaaminen kauempana olevasta ohjauskeskuksesta. Kyseessä voi olla myös muu radioaaltoihin perustuva toiminta, kuten lentokoneiden ja ohjusten liikkuminen sekä näiden liikkeen mittaaminen.

Radiosignaalitiedustelu kattaisi elektronisen mittaustiedustelun, jolla tarkoitetaan muiden kuin viestintää sisältävien signaalien etsimistä, sieppaamista, paikantamista, tallentamista sekä näin kerätyn tiedon analysointia. Näitä ovat esimerkiksi tutkasignaalit, korkeusmittaussignaalit ja muut vastaavat signaalit.

Radiosignaalitiedustelussa voi toiminnan luonteesta johtuen tiedustelun kohteeksi joutua myös radiosignaaleja, jotka sisältävät luottamuksellisen viestin suojan alaan kuuluvaan viestintää. Jos näin kävisi, olisi tällaiset tiedot hävitettävä välittömästi, kuten esimerkiksi telekuunteluun liittyvien ylimääräisten tietojen kohdallakin on tilanne. Tällaisen tiedon hävittämisestä säädetään jäljempänä.

Pykälän 2 momentissa olisi erikseen säädetty radiosignaalitiedustelun kohdistumisesta Suomen rajan ulkopuolella olevaan kohteeseen. Jos kohde siirtyisi Suomen rajan sisäpuolelle, voitaisiin siihen puuttua ja sitä seurata muun muassa aluevalvontalain toimivaltuuksin ja muilla tiedustelumenetelmillä.

Pykälän 3 momentissa säädettäisiin informatiivisesti siitä, ettei radiosignaalitiedustelua ei saisi kohdistaa henkilöiden väliseen luottamukselliseen viestintään Suomen alueella. Radiosignaalitiedustelussa toiminnan kohteena ovat radioaallot, jotka saattavat kulkea pitkiäkin matkoja eikä niitä ole tarkoitettu kahden henkilön väliseksi luottamukselliseksi viestinnäksi. Suomen rajan sisäpuolella sotilastiedusteluviranomaisella olisi käytössää henkilötiedustelun toimivaltuudet, joilla tilanteen niin vaatiessa voitaisiin puuttua kahden henkilön väliseen luottamukselliseen viestintään.

61 §. *Radiosignaalitiedustelusta päättäminen.* Pykälän mukaan päätöksen radiosignaalitiedustelusta tekisi pääesikunnan tiedustelupäällikkö. Radiosignaalitiedustelun luonteesta johtuen toiminnassa ei olisi tarpeen säätää päätöksen voimassaoloaikaa.

Lisäksi radiosignaalitiedustelu on pitkäkestoista ja laajasti vieraan vallan asevoimien toimintakenttää kohdistuvaa, minkä takia olisi perusteluta, ettei radiosignaalitiedustelulle olisi säädetty päätöksen voimassaoloaikaa.

62 §. *Ulkomaan tietojärjestelmätiedustelu.* Pykälässä säädettäisiin ulkomaan tietojärjestelmätiedustelusta. 1 momentin mukaan sotilastiedusteluviranomainen voisi tunkeutua Suomen rajan ulkopuolella olevaan tietojärjestelmään ja -verkkoon tiedonhankintatarkoituksessa Suomesta käsin. Tiedonhankinta tapahtuisi tietoteknisin menetelmin.

Erotuksena edellä säädetyistä teknisestä laitetarkkailun, teknisen kuuntelun, telekuuntelun ja televalvonnan toimivaltuuksista ulkomaan tietojärjestelmätiedustelussa olisi kyse laajasta ja pitkäkestoisesta tiedonhankinnasta ulkomaisista tietojärjestelmistä ja -verkoista. Ulkomaan tietojärjestelmätiedustelussa olisi kuitenkin samoja tiedonhankinnassa käytettäviä elementtejä kuin edellä mainituissa henkilötiedustelun toimivaltuuksissa, kuten näppäimistökuuntelu, tietoteknisellä menetelmällä teknisen laitteen ja ihmisen välisen vuorovaikutuksen tarkkailu sekä viestintäjärjestelmien kuuntelu. Toiminnasta olisi kuitenkin tarkoituksenmukaista säätää yhtenä kokonaisuutena.

Tietojärjestelmätiedustelu olisi kohteen osalta tekniikkaneutraali, eli tietojärjestelmätiedustelu voisi kohdistua tietokoneen lisäksi myös muuhun vastaavaan tekniseen laitteeseen. Olennaista olisi se, että laitteella käsitellään tietoja, joilla voi olla merkitystä sotilastiedustelun tiedonhankinnan kannalta.

Toimivaltuus olisi myös kohdeneutraali ja sen kohteena voisivat olla esimerkiksi tietojärjestelmään tallennettujen asiakirjojen sisältämät tiedot ja lähetetyt viestit.

Säädettävästä toimivaltuudesta ei aiheutuisi suomalaisille yksityisille toimijoille velvoitetta asentaa ohjelmistoihin ja laitteistoihin niin sanottuja takaportteja eikä yksityiset toimijat olisi velvollisia luovuttamaan salausavaimia.

Tietojärjestelmätiedustelussa ei olisi kyse hyökkäyksellisestä toiminnasta, jonka tarkoituksena olisi puuttua kohdejärjestelmän toiminnallisuuteen, vaan kyse olisi tietojärjestelmän sisältämien, tietojärjestelmään tallennettavien ja tietojärjestelmällä tuotettavien tietojen hankinnasta. Operaatioihin voi kuitenkin liittyä ulkopoliittisia näkökohtia, jotka vaativat tarkkaa harkintaa.

Kansainvälisoikeudellisessa keskustelussa tehdään yleensä ero yhtäältä tiedonhankintaa palvelevien tietojärjestelmäoperaatioiden ja toisaalta haitallisten verkkohyökkäysten kesken. Erilaisia näkemyksiä on esitetty siitä, voidaanko tiedonhankinta tai jopa pelkkä läsnäolo toisen valtion tietojärjestelmissä ymmärtää suvereenisuuden loukkaukseksi. Valtiot voivat kuitenkin suvereniteettinsa perusteella reagoida katsomallaan tavalla paljastuneeseen tiedonhankintaan.

Pykälän 2 momentin mukaan Puolustusvoimien tiedustelulaitos saa kohdistaa tietojärjestelmään ulkomaan tietojärjestelmätiedustelua, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Momentti rajaisi niitä kohteita, joidenka tietojärjestelmistä voitaisiin hankkia tietoa ja missä tilanteissa. Sotilastiedusteluviranomainen ei voisi laskea vapaasti liikkeelle esimerkiksi tietojärjestelmään takaportin luovia haittaohjelmia ja käyttää näitä satunnaisiin tietojärjestelmiin luotuja takaportteja vapaasti tiedonhankinnassaan.

Pykälän 3 momentissa olisi erillinen kielto hankkia tietojärjestelmä tiedustelulla tietoja henkilöiden välisestä luottamuksellisesta viestistä. Tämä tarkoittaisi esimerkiksi sitä, että ulkomaan tietojärjestelmätiedustelu on kohdennuttava järjestelmässä oleviin tietoihin pois lukien viestit, jotka nauttivat luottamuksellisen viestin suojaa. Toisaalta kohteena olevan tietojärjestelmän viesteistä voisi hankkia viestejä, jos ne olisivat valtiollisen toimijan toiminnassaan käyttämiä viestejä.

63 §. *Ulkomaan tietojärjestelmätiedustelusta päättäminen.* Pykälän 1 momentissa säädettäisiin päätöksenteosta tietojärjestelmätiedustelussa tilanteessa, joka ei sisällä ulko- ja turvallisuuspoliittisesti merkittäviä liityntöjä. Tietoliikennetiedustelun käyttämisestä tiedonhankinnassa päättäisi Puolustusvoimien tiedustelupäällikkö. Pääesikunnan tiedustelupäällikön olisi otettava huomioon lain 1 luvussa tarkoitetut periaatteet päätöksenteossaan ja arvioitava tiedonhankintakeinon oikeasuhtaisuus saatavaan tietoon nähden.

Riittävän yhteiskunnallisen hyväksyttävyyden varmistamiseksi tällaisissa tilanteissa Puolustusvoimien tiedustelupäällikön olisi tilanteen arvioituaan vietävä ennen ulkomaan tietojärjestelmätiedusteluoperaation aloittamista koskevaa päätöstään asia tiedustelun koordinaatioryhmän käsiteltäväksi. Arvion tarpeesta käsitellä asiaa yhteen sovittavasta 17 §:ssä tarkoitettujen viranomaisten kesken tekisi pääesikunnan tiedustelupäällikkö.

Pykälän 2 momentin mukaan puolustusministeriö olisi pidettävä tietoisena käynnissä olevasta tietojärjestelmätiedustelusta. Puolustusministeriö voisi harkintansa mukaan informoida muita keskeisiä ulko- ja turvallisuuspoliittisia merkittäviä toimijoita, kuten ulkoministeriä ja tasavallan presidenttiä.

64 §. *Ulkomailla tapahtuvasta sotilastiedustelusta päättäminen.* Pykälässä säädettäisiin henkilötiedustelun menetelmien käytöstä Suomen rajan ulkopuolella. Pykälässä tarkoitettua toimintaa koskevassa päätöksenteossa olisi otettava huomioon ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteisen kokouksen valmistelevasti käsittelemät sotilastiedustelun suuntaviivat. Ulkomailla tapahtuva tiedustelumenetelmiä käytettäessä olisi huomioitava myös aiemmin 17 §:ssä tarkoitettu tiedustelutoiminnan yhteensovittaminen.

Pykälän 1 momentin mukaan päätöksen ulkomaan henkilötiedustelusta tekisi pääesikunnan tiedustelupäällikkö. Tiedustelupäällikkö voisi viedä etenkin ulko- ja turvallisuuspoliittisesti merkittävän yksittäisen asian tarvittaessa tiedustelun koordinaatioryhmän käsiteltäväksi.

Pykälän 2 momentin mukaan päätös olisi tehtävä kirjallisesti. Ulkomaan henkilötiedustelussa poliittinen ulottuvuus korostuu suhteessa kohdemaahan, mutta myös silloin, kun toimitaan yhteistyössä kolmannen valtion kanssa tai tiedustelumenetelmiä käytetään kolmannen valtion alueelta käsin. Tiedustelun mahdolliset vaikutukset ja riskit olisi arvioitava ulkomaan henkilötiedustelua koskevassa päätöksessä tarkoin.

Pykälän 3 momentin mukaan tämän lain 55, 76, 77, 85, 86, 126 ja 127 §:n säännöksiä ei sovellettaisi 1 momentissa tarkoitettuun sotilastiedusteluun ja tiedustelumenetelmän käyttöön. Edellä tarkoitettujen säännösten lisäksi ulkomailla tapahtuvaan sotilastiedusteluun ja tiedustelumenetelmän käyttöön ei sovellettaisi, mitä vakituiseen asumiseen kohdistuvista tiedustelumenetelmien käytön rajoituksista säädettäisiin tiedustelumenetelmiä koskevissa säännöksissä.

5 luku. Tiedonhankinta tietoliikenteestä

65 §. *Soveltamisala.* Pykälän mukaan luvussa säädettäisiin tietoliikennetiedustelusta. Lisäksi pykälässä määriteltäisiin tietoliikennetiedustelu.

Pykälän määritelmän mukaan tietoliikennetiedustelulla tarkoitettaisiin Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen kohdistuvaa teknistä tiedonhankintaa. Määritelmän olennaisia elementtejä olisivat ensinnäkin se, että tietoliikennetiedustelu kohdistuu Suomen rajan ylittävään tietoliikenteeseen, toiseksi se, että rajan ylittyminen tapahtuu viestintäverkossa.

Tietoliikenteen Suomen rajan ylittymisellä tarkoitettaisiin sitä, että tietoliikenne tosiasiassa ylittää valtakunnanrajan siirtymällä suomalaisesta viestintäverkosta ulkomaiseen viestintäverkkoon tai päinvastoin. Tietoliikennetiedustelu toteutettaisiin tekniseesti lähellä niitä pisteitä, joissa Suomen viestintäverkko ja ulkomainen kiinteä verkko tai satelliittiverkko kytkeytyisi toisiinsa ja tietoliikenteen valtakunnanrajan ylittyminen tapahtuisi.

Suomen sisäiseksi tarkoitettu tietoliikenne voi internetin luonteesta johtuen sattumanvaraisesti reitittyä ulkomaisen viestintäverkon kautta, kuuluisi tällainen tietoliikenne sinänsä määritelmän mukaisesti tietoliikennetiedustelun piiriin. Sen varmistamiseksi, että tietoliikennetiedustelulla ei tästä huolimatta hankittaisi tietoja asialliselta luonteeltaan kotimaisesta viestinnästä, asiasta säädettäisiin jäljempänä kotimaista viestintää koskevasta tiedustelukiellosta, jonka mukaan tietoliikennetiedustelua ei muun muassa saisi kohdistaa viestiin, jonka lähettäjä ja vastaanottaja olisivat Suomessa.

Tiedustelu kokonaisuudessaan on toimintaa, jossa pyritään ennakoimaan tulevia tapahtumia ja tunnistamaan Suomeen kohdistuvia sotilastiedustelun tehtävien mukaisia uhkia mahdollisimman varhaisessa vaiheessa. Tiedustelun kohteen muodostavat ennen kaikkea vieraan vallan organisaatiot ja niiden toimijat. Tietoliikennetiedustelu on osa sotilastiedustelun kokonaisuutta ja sotilastiedustelun toteuttamaa tiedustelua. Suomen alueella liikkuvasta tietoliikenteestä kerättäisiin automatisoidusti ja tallennettaisiin lupaehtojen mukaisessa viestintäverkon osassa, kuten esimerkiksi tietoliikennekaapelin kuiduissa, liikkuvaa tietoliikennettä hakuehtojen mukaisesti. Erotuksena ulkomaan tietojärjestelmätiedustelusta, tietoliikennetiedustelu tapahtuisi Suomen alueella ja se kohdistuisi Suomen alueella liikkuvaan Suomen rajan ylittävään tietoliikenteeseen. Tietoliikennetiedustelun kohteena olevan viestinnän sekä lähettäjä ja vastaanottaja eivät ole viestinnän tapahtumisen aikana Suomen alueella, vaan tietoliikenteen reitittämisen takia viestintä käy hetkellisesti Suomen rajan sisäpuolella. Tietoliikennetiedustelussa etsittäisiin kohdennetusti suuresta määrästä tietoa tiedustelutehtävien kannalta olennaisia tietoja.

Tietoliikennetiedustelun avulla sotilastiedustelun kohteesta voitaisiin saada laajasti tietoja. Tietoliikennetiedustelulla tietoja voitaisiin saada puheluista, sähköpostiviesteistä, pikaviestinnästä ja muista vastaavista viestintäkanavista ja -menetelmistä. Sotilastiedustelun kannalta olennaisia tietoja voi välittää kuka tahansa sotilastiedustelun kohdeorganisaatiossa. Kokonaisuudessa tietoliikennetiedustelulla hankittavat tiedot voivat muodostaa esimerkiksi tiedon tiedustelutehtävän kohteen sijainnista, liikkumisesta, kokoonpanosta ja sekä sotilastiedustelun kohteisiin liittyvistä organisaatioista, kuten esimerkiksi vieraanvaltion sotilasorganisaatioita tukevat toimijat, voidaan saada tietoja.

Tietoliikennetiedustelun kohdentamisessa luvan mukaisesta viestintäverkon osasto, esimerkiksi kuidusta, ohjattaisiin tietoliikennettä edelleen sotilastiedustelulle, jolla olisi oikeus kerätä ja tallentaa sotilastiedusteluviranomaisen käsittelyä varten tuomioistuimen luvassa määriteltyjen hakuehtojen mukaisia viestejä. Hakuehdot eivät saisi kohdistua viestien sisältöön keräys- ja tallennusvaiheessa. Vasta viestien käsittelyssä sotilastiedusteluviranomainen voisi käsitellä viestien sisältöä ja muita viesteihin liittyviä tietoja.

Sotilastiedusteluviranomainen ei voisi käsitellä muuta tietoliikennettä kuin sitä, joka on tallennettu tuomioistuimen antaman luvan perusteella. Muu kuin tuomioistuimen luvassa tarkoitettujen hakuehtojen mukainen tietoliikenne ja viestit poistetaan automaattisessa keräämisessä ja tallentamisessa tiedustelun ja tietoliikennetiedustelun prosessista. Hakuehtoluokkia ja hakuehtoja vastaamatonta tietoliikennettä ei voitaisi palauttaa jälkikäteen tiedusteluviranomaisen käytettäväksi. Tietoliikennetiedustelu liittyy aina tiettyyn tiedustelutehtävään ja sitä voitaisiin käyttää ainoastaan tuomioistuimen luvassa myönnetyn ajanjakson aikana.

Tietoliikennetiedustelun tarkoituksena on kerätä olennaisia tietoja tiedustelutehtävän kohteen tietoliikenteestä, eikä tarkoituksena olisi kerätä esimerkiksi yksittäisiin henkilöihin liittyvien välitystietojen kautta laajempaa profiilia henkilön käyttäytymisestä.

Tietoliikennetiedustelu voisi kohdistua myös pilvipalveluun tallennettaviin tietoihin. Tietoliikennetiedustelun keskeisenä käyttötarkoituksena on hankkia tietoja sotilastiedustelun kohteista sekä tunnistaa niiden taustalla olevia henkilöitä. Pilvipalveluun tallentamiseen kohdistettavalla tietoliikennetiedustelulla on samankaltainen merkitys kuin muullakin tietoliikennetiedustelulla tämän tarkoituksen toteuttamisen kannalta. Pilvipalveluun tallentamista käytetään tosiasiassa laajasti hyväksi esimerkiksi vakoiluun liittyvässä toiminnassa. Esimerkiksi valtiollinen kybervakoilu toteutetaan yleensä siten, että vakoilussa käytettävä haittaohjelma tallentaa anastamansa tiedot ulkomailla sijaitsevaan pilvipalvelun serverille. Jos pilvipalveluliikenteeseen liitettäisiin tiedustelukielto ja tietojen hävittämiskielto, ei tietoliikennetiedustelua voitaisi käyttää tällaisen toiminnan havaitsemiseen ja estämiseen. Lisäksi useat pikaviestinpalvelut käyttävät viestinnän välittämiseen pilvipalveluita.

Pilvipalveluun kohdistuvaa hakuehtoa saisi käyttää samoin perustein kuin muita hakuehtoja, eli jos tuomioistuin hyväksyisi sen käytön päätöksessään. Pilvipalveluun tallentamista koskevan hakuehdon tulisi aina perustua johonkin riittävän konkreettiseen sotilastiedustelun kohteeseen, jota koskevat tosiseikat Puolustusvoimien tiedustelulaitos olisi velvoitettu antamaan tuomioistuimelle esittämässään lupavaatimuksessa.

Tietoliikennetiedusteluun sisältyisi myös viestinnän teknisten tietojen käsittely, jolla tarkoitettaisiin viestintäverkoissa kulkevien viestien muita kuin sisältöön liittyviä tietoja. Tällaisia tietoja ovat muun muassa viestin välitystiedot.

Lisäksi tietoliikennetiedustelussa voitaisiin hankkia tietoja teknisen laitteen tai päätelaitteen sijainnista.

66 §. *Teknisten tietojen käsittely.* Pykälässä säädettäisiin Puolustusvoimien tiedustelulaitoksen oikeudesta kerätä ja tallentaa sekä automaattisen tietojenkäsittelyn avulla käsitellä tilastollista ana-

lyysiä varten viestintäverkon tietoliikenteestä tietoliikenteeseen liittyviä teknisiä tietoja tietoliikennetiedustelun kehittämiseksi ja viestintäverkon osan tarkemmaksi kohdentamiseksi. Tekniset tiedot kohdistuvat yhteyksiä käyttäviin ja viestintää välittäviin teleyrityksiin ja tiedonsiirtäjiin sekä muihin organisaatioihin, kuten suoratoistopalveluihin. Hankituilla tiedoilla olisi merkitystä kohdistettaessa tietoliikennetiedustelua jäljempänä 68 ja 70 §:ssä säädetysti.

Viestinnän tekniset tiedot eivät koskisi viestin sisältöä, vaan viestinnän teknisten tietojen avulla tietoliikennetiedustelu voitaisiin kohdistaan paremmin vain niihin viestintäverkon osiin, joissa liikkuisi tiedustelutehtävän kannalta olennaista viestintää. Teknisiä tietoja analysoimalla voitaisiin hankkia tarkempia tietoja tietoliikennetiedustelun lupahakemukselle.

Viestinnän teknisillä tiedoilla tarkoitettaisiin muun muassa viestien välitystietoja. Tietoliikenteen tekniset tiedot on määritelty aiemmin tämän lain 9 §:n 6 kohdassa. Muita viestinnän teknisiä tietoja voivat olla BGP-reititystiedot (Border Gateway Protocol), yhteyskäytäntöosoitealueet (IP-osoitealueet) ja autonomisen järjestelmän numero (AS-numero).

Viestinnän teknisten tietojen käsittelyssä pyritään selvittämään, mitä viestintäverkon osaa pitkin tietyn toimijan tai tietyltä maantieteelliseltä alueelta tuleva viestintä kulkee. Tämä voisi tapahtua esimerkiksi hankkimalla ensin julkisesti saatavilla olevista tiedoista viestinnän BGP-reitityksestä, josta voidaan nähdä kaikki ne autonomisten järjestelmien omistajat, joidenka kautta viestintä on tullut tiettyyn pisteeseen.

Autonomisten järjestelmien omistajat ovat tyypillisesti operaattoreita ja muita suurempia toimijoita, joidenka vastattavana on tiettyjen IP-osoitealueiden reitittämiskokonaisuus. Autonomiset järjestelmät yksilöidään niin sanotulla AS-numerolla. AS-numero voi olla lähinnä teleyrityksillä paikallisesta teleyrityksestä maailmanlaajuisiin tietoliikenteen välittäjiin, ICT-palveluiden tarjoajilla sekä isoilla, globaaleilla yrityksillä. AS-numeroiden kautta pystytään yksilöimään tietyt IP-osoitealueet, joita AS-numeron haltija hallinnoi ja jakaa asiakkailleen edelleen käytettäväksi.

IP-osoitealueiden perusteella voidaan tunnistaa liikenteestä tiedustelutehtävän kannalta olennaisia toimijoita ja tietty alue, josta tietoliikenne tulee.

Kerätyistä ja tallennetuista viestinnän teknisistä tiedoista tehtäisiin tilastollinen analyysi automaattisella tietojenkäsittelyllä. Tilastollisen analyysin perusteella viestinnän kerääminen ja tallentaminen voidaan kohdentaa paremmin fyysisesti ainoastaan siihen osaan viestintäverkkoa, jossa oletettavasti liikkuu tiedustelutehtävän kannalta olennaista viestintää.

Lisäksi tilastollisella analyysillä voitaisiin saada tarkempia tietoja viestinnän keräämistä ja tallentamista koskevalle lupahakemukselle.

Pykälän 1 momentin mukaisesti teknisten tietojen kerääminen ja tallentaminen tapahtuisi hetkellisesti. Hetkellisellä keräämisellä ja tallentamisella tarkoitettaisiin hyvin lyhyttä ajanjaksoa, käytännössä kyse olisi muutamista sekunneista, jonka aikana keräämisen ja tallentamisen kohteeksi joutuisivat satunnaiset IP-paketit. IP-paketeista ei selvitettäisi viestin sisältöä vaan ainoastaan IP-paketin tekniset tiedot. IP-paketeista voidaan saada tietoja tietoliikenteen kulkureitistä.

Viestinnän teknisten tietojen tilastollisen analyysin tarkoituksena on selvittää, liikkuuko tietyltä maantieteelliseltä alueelta tai tietyn toimijan tietoliikennettä tietyssä viestintäverkon osassa. Sotilastiedusteluviranomainen ei saisi käyttää kerättyjä ja tallennettuja viestinnän teknisiä tietoja muuhun tarkoitukseen kuin automaattisella tietojenkäsitellyllä tapahtuvaan tilastolliseen analyysiin. Automaattinen tietotekninen tilastollinen analyysi tehtäisiin välittömästi teknisten tietojen keräämisen ja tallentamisen jälkeen, jonka jälkeen analyysin pohjana olleet tiedot tuhottaisiin välittömästi. Soti-

lastiedusteluviranomaisella ei olisi pääsyä yksittäisiin viestinnän teknisiin tietoihin eikä sotilastiedusteluviranomainen voisi siten selvittää viestinnän osapuolena olevaa luonnollista henkilöä.

Teknisten tietojen käsittelyllä pystyttäisiin myös hankkimaan tarvittavia tietoja tietoliikenteessä tapahtuvista muutoksista. Tietoliikenteen liikkumisessa viestintäverkossa voi tapahtua varsin lyhyelläkin aikavälillä muutoksia muun muassa viestinnän reitittämisessä, teknologioissa sekä tietoliikennekaapeleissa tapahtuvien muutosten johdosta. Jotta tietoliikennetiedustelu voitaisiin kohdistaa mahdollisimman tarkasti fyysisesti ja teknisesti, sotilastiedusteluvirnaomaisella olisi oltava mahdollisimman ajantasainen tieto kohdentamiseen vaikuttavista teknisistä seikoista, kuten viestien BGP-reitityksestä ja tiettyjen toimijoiden, kuten suoratoistopalveluiden, käyttämistä viestintäverkon osista.

Viestinnän teknisten tietojen tilastollisella analyysillä ei voitaisi selvittää viestinnän osapuolena olevaa luonnollista henkilöä tai viestin sisältöä.

Puolustusvoimien tiedustelulaitos suorittaa suojelupoliisille tietoliikennetiedustelun teknisen toteuttamisen suojelupoliisin erillisen toimeksiannon perusteella. Suojelupoliisi voisi antaa teknisten tietojen hankkimista koskevan toimeksiannon Puolustusvoimien tiedustelulaitokselle, joka tässä tapauksessa hankkisi tarvittavan luvan ja suorittaisi teknisten tietojen tilastollisen analyysin sekä toimittaisi analyysin suojelupoliisin käyttöön. Tietoliikennetiedustelun teknisestä toteuttamisesta suojelupoliisille säädettäisiin jäljempänä.

Pykälän 2 momentissa säädettäisiin kiellosta tuottaa viestinnän teknisten tietojen pohjalta tilastollinen analyysi tai muuta tietoa, josta voitaisiin tunnistaa yksittäisiä luonnollisia henkilöitä. Kiellon tarkoituksena on myös estää henkilöihin kohdistuvan tietoliikennetiedustelutoimivaltuuden kiertäminen. Tilastollisen analyysin tarkoituksena on tuottaa tietoa siitä, missä viestintäverkon osassa liikkuu tietystä tiedustelutehtävän kannalta olennaisesta kohteesta lähtevää tai sinne tulevaa tietoliikennettä. Tilastollisen analyysin tarkoituksena olisi tietoliikennetiedustelun kohdentaminen fyysisesti ja teknisesti mahdollisimman tarkasti ainoastaan siihen osaan viestintäverkossa liikkuvasta tietoliikenteestä, joka on tiedustelutehtävän kannalta olennaista. Fyysisellä ja teknisellä kohdentamisella pystyttäisiin rajaamaan pois suuri osa viestintäverkoissa liikkuvasta tietoliikenteestä, jolla ei olisi sotilastiedustelun tehtävien kannalta merkitystä.

Pykälän 3 momentissa olisi teknisten tietojen hävittämisvelvollisuus. Teknisten tietojen käsittelyssä käytettäviä teknisiä tietoja ei saisi tallentaa sotilastiedustelulle myöhempää käyttöä varten. Teknisten tietojen käsittelyssä olisi tarkoituksena tuottaa tilastollinen analyysi, jonka jälkeen analyysin pohjana olleet tiedot olisi välittömästi hävitettävä eikä niitä voitaisi jälkikäteen käyttää tiedustelutehtävän suorittamiseksi.

67 §. *Teknisten tietojen käsittelystä päättäminen*. Pykälän 1 momentin mukaan teknisten tietojen keräämisestä päättäisi tuomioistuin tiedustelumenetelmien käyttöön perehtyneen Puolustusvoimien tiedustelulaitoksen virkamiehen vaatimuksesta. Menettelystä tuomioistuimessa säädettäisiin jäljempänä.

Pykälän 2 momentin mukaan teknisten tietojen käsittelyä koskevan luvan enimmäisvoimassaoloaika olisi kolme kuukautta. Luvan voimassaoloaikaan vaikuttaisi se, miten teknisten tietojen kerääminen toteutettaisiin; teknisten tietojen kerääminen voidaan toteuttaa ottamalla teknisen analyysin kohteeksi lyhyt aikainen näyte tietyssä viestintäverkon osassa liikkuvasta tietoliikenteestä, jolloin perusteltua olisi lyhyempi luvan voimassaoloaika, tai ottamalla tietyssä viestintäverkon osassa liikkuvista IP-paketeista esimerkiksi joka kymmenestuhannes paketti, jolloin luvan voimassaoloaika voisi olla pidempi.

Ensimmäisessä vaihtoehdossa luvan voimassaolon aikana sotilastiedusteluviranomainen voisi useampaan otteeseen hetkellisesti kerätä ja tallentaa viestintäverkossa liikkuvan viestinnän teknisiä tietoja ja tuottaa niistä automaattisella tietojen käsittelyllä tilastollisen analyysin. Tässä tapauksessa olisi luonnollista, että luvan voimassaoloaika olisi lyhyempi, koska teknisen analyysin kohteeksi joutuisi laajemmin tietoliikennettä, vaikka kyseessä olisikin hetkellinen tietojen kerääminen ja tallentaminen. Jälkimmäisessä vaihtoehdossa luvan voimassaoloaika voisi olla pidempi, koska kyseessä olisi satunnaisten IP-pakettien ottaminen tekniseen analyysiin. Tässä vaihtoehdossa tietoliikennettä ei joutuisi tiettynä ajanhetkenä teknisen analyysin kohteeksi yhtä laajalti kuin ensimmäisessä vaihtoehdossa, mikä perustelisi pidempää luvan voimassaoloaikaa.

Pykälän 3 momentin 1 kohdan mukaan lupahakemuksessa olisi ilmoitettava maantieteellinen alue, jolta tulevan tai jolle menevään tietoliikenteeseen liittyvää viestintäverkon osaa selvitettäisiin. Maantieteellinen alue voisi olla tarpeen mukaan laaja alue, jossa esimerkiksi tiedetään olevan sotilaallista toimintaa, tai tietty rakennus, jonka tiedetään liittyvän tiedustelutehtävään.

Momentin 2 kohdan mukaan sotilastiedusteluviranomaisen olisi ilmoitettava ne viestintäverkon osat, kuten tietoliikennekaapelin kuitu, kuidun aallonpituus tai muu tarkempi tiedonsiirron taso, joista tietoliikenteen teknisiä tietoja kerättäisiin. Jotta viestintäverkon kokonaisuudesta löytyisit tiedustelun kannalta olennainen osa, olisi teknisten tietojen keräämistä ja tallentamista voitava kohdistaa useampaan kuin viestintäverkon osaan samalla luvalla.

Momentin 3 kohdan mukaan lupahakemuksessa olisi ilmoitettava tiedonsiirtäjät, jotka pystyisivät avustamaan luvan mukaisten tietojen hankkimisessa. Sotilastiedusteluviranomaisella saattaisi olla ennakkotieto siitä, kenen hallinnassa olevaan viestintäverkon osaan tietyltä maantieteelliseltä alueelta peräisin oleva tietoliikenne kulkeutuu. Esimerkiksi tällaisen tiedon perusteella tietty teleoperaattori voitaisiin määrätä avustamaan sotilastiedusteluviranomaista. Teleoperaattorin avustamisvelvollisuudesta säädettäisiin jäljempänä.

Momentin 4 kohdassa teknisten tietojen keräämiseen olisi nimettävä viestinnän teknisten tietojen käsittelyä valvova ja johtava tiedustelumenetelmien käyttöön erityisesti perehtynyt Puolustusvoimien tiedustelulaitoksen virkamies. Valvova ja johtava virkamies toimisi tehtävässä virkavastuulla. Teknisten tietojen keräämistä, tallentamista ja käsittelyä valvoisi tiedustelun valvontaviranomainen, jonka tehtävistä säädettäisiin erillisessä laissa.

Momentin 5 kohdan mukaan lupahakemuksessa olisi esitettävä suunnitelma siitä, miten, milloin ja minkä pituisissa ajanjaksoissa teknisten tietojen kerääminen ja tallentaminen toteutettaisiin. Suunnitelmassa olisi esitettävä se, minkälaista keinoa teknisessä analyysissä käytettäisiin. Pykälän tarkoittama teknisten tietojen käsittely voitaisiin toteuttaa ottamalla lyhyt kestoisia, sekunnista muutaman, näytteitä kaikesta tietyssä viestintäverkon osassa liikkuvasta tietoliikenteestä tai ottamalla satunnaisesti esimerkiksi joka kymmenestuhannes IP-paketti viestintäverkon osassa liikkuvasta tietoliikenteestä.

Suunnitelmassa olisi kuvattava, millä edellä kuvatulla keinoilla teknisiä tietoja hankittaisiin. Koska teknisten tietojen käsittely tietoliikenteestä voisi tapahtua hetkellisesti, olisi tarkoituksen mukaista, että sotilastiedusteluviranomainen voisi luvan voimassaoloajan kerätä ja tallentaa teknisiä tietoja useamman kerran. Suunnitelmassa olisi ilmoitettava myös se, kuinka monesti teknisiä tietoja olisi tarkoitus hankkia luvan voimassaolon aikana.

Vaihtoehtoisesti suunnitelmassa olisi ilmoitettava se, miten satunnainen IP-pakettien kerääminen toteutettaisiin.

68 §. *Valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu.* Pykälässä säädettäisiin Puolustusvoimien tiedustelulaitoksen toimivaltuudesta kerätä, tallentaa ja käsitellä valtiollisen toimijan

viestintää sekä sen edellytyksistä. Pykälässä tarkoitettu valtiollinen toimija olisi erityinen kohde verrattuna muuhun tietoliikennetiedusteluun.

Voimassa olevan tulkinnan mukaan valtio ja muut julkisyhteisöt jäävät perusoikeussuojan ulkopuolelle (HE 309/1993 vp. ja PeVL 9/2015 vp.), jolloin myöskään valtion harjoittaman viestinnän ei voida katsoa nauttivan peruslaillista luottamuksellisen viestin salaisuuden suojaa.

Jos tietoliikenteen kerääminen voitaisiin kohdistaa pelkästään vieraan valtion tietoliikenteeseen, siihen voitaisiin kohdistaa myös viestin sisältöä kuvaavaa tietoa. Hakuehtona voisi olla viestin sisällöstä löytyvä merkkijono, esimerkiksi luonnollisen kielen sana tai lause.

Vieraan valtion tietoliikennettä koskevan poikkeuksen soveltaminen tulisi kyseeseen vain niissä tapauksissa, joissa tiedustelujärjestelmään ohjautuva tietoliikennevirtaan ei voisi päätyä luottamuksellisen viestinnän suojaa nauttivaa tietoliikennettä. Käytännössä tämä edellyttäisi, että se viestintäverkon osa, johon tuomioistuimen antama lupa koskee ja johon hakuehdot kohdistuvat, olisi varattu valtiollista tietoliikennettä varten. Vieraan valtion tietoliikennettä koskevan poikkeuksen käyttö olisi siten käytännössä kapea.

Luottamuksellisen viestin suojan ala kattaa niin viestin lähettäjän kuin sen vastaanottajan; kysymyksessä on viestinnän molempien osapuolten perusoikeus (HE 309/1993 vp.). Tästä johtuen valtiolliseen toimijaan kohdistuvassa tietoliikenteen tiedustelussa tiedustelun kohteeksi voisi päätyä myös viestintää, jossa vastaanottajana tai lähettäjänä olisi muu kuin valtiollinen toimija. Tällainen tietoliikenne olisi hävitettävä välittömästi esitetyn 74 §:n mukaisesti, kun tietoliikenteen luonne on käynyt ilmi. Pykälässä säädettyjen edellytysten lisäksi toimivaltuuden käytön edellytyksiä harkittaessa olisikin otettava huomioon myös sotilastiedustelutoiminnan yleiset periaatteet, joista olisi säädetty aiemmin tässä laissa sekä viranomaisia lähtökohtaisesti koskeva perus- ja ihmisoikeuksien kunnioittaminen.

Valtiollisen toimijan tietoliikenteeseen kohdistuvan tiedustelun edellytyksenä olisi tiedustelun yleisenä edellytyksenä oleva tuloksellisuusvaatimus. Toimivaltuutta voitaisiin käyttää, jos sillä voidaan olettaa saatavan tietoja tiedustelutehtävän kannalta.

Pykälän 1 momentin mukaista tietoliikennetiedustelua olisi mahdollista käyttää valtiollisen tietoliikenteen tiedustelun. Tietoliikenteen tiedustelu käsittäisi tietoliikenteen keräämisen, tallentamisen ja käsittelyn tiedonhankinta tarkoituksessa.

Valtiollisen toimijan tietoliikenteen tiedustelussa ensimmäisessä vaiheessa tiedustelulle ohjatusta tietoliikenteestä etsittäisiin tiedustelutehtävän kannalta olennaisia tietoja tuomioistuimen myöntämässä luvassa määritellystä viestinverkon osasta. Tuomioistuimen luvasta säädettäisiin jäljempänä.

Pykälän 1 momentin tilanteissa kerääminen tapahtuisi automaattisen tietojen käsittelyn avulla, joka perustuisi hakuehtojen käyttöön. Tällä tehtäisiin eroa muihin viestintäverkossa liikkuvaan tietoliikenteeseen kohdistuvien tiedonhankintakeinojen, ennen kaikkea 4 luvussa säädettäviin telekuunteluun ja televalvontaan samoin kuin poliisi- ja pakkokeinolaeissa säänneltyjen telekuuntelun ja televalvonnan välille. Telekuuntelu kohdistetaan täsmällisesti johonkin sellaiseen telepäätelaitteeseen tai teleosoitteeseen, jonka yksilöintitiedot ovat selvillä tiedonhankinnan alkaessa taikka henkilöön, joka on etukäteen tiedossa. Tietoliikennetiedustelussa ei olisi kyse mihinkään ennakkoon yksilöitävissä olevaan telepäätelaitteeseen tai teleosoitteeseen kohdistuvasta tiedonhankinnasta, vaan automatisoiduin menetelmin tapahtuvasta tietoliikenteen seulonnasta tiettyyn tiedustelutehtävään liittyvien tietojen löytämiseksi. Käytännössä valtiolliseen toimijan tietoliikenteeseen kohdistuvassa tiedustelussa kerääminen toteutettaisiin tunnistamalla tietty viestintäverkon osa, jossa valtiollisen toimijan tietoliikenne kulkee ja tarvittaessa vertailemalla tietoliikennettä hakuehdoiksi kutsut-

taviin ennakkoon asetettuihin kriteereihin. Tietoliikennetiedustelun yhtenä tarkoituksena olisi myös tunnistaa yksittäisiä telepäätelaitteita ja teleosoitteita telekuuntelun tai televalvonnan toteuttamisen mahdollistamiseksi.

Momentin viimeisen virkkeen mukaan tietojen hankkiminen valtiollisen toimijan tietoliikenteestä perustuisi hakuehtojen käyttöön. Hakuehdot on tarkemmin kuvattu 70 §:n yksityiskohtaisissa perusteluissa.

Hakuehtoihin perustuva kerääminen kohdistuisi vain tietyssä osassa viestintäverkkoa kulkevaan tietoliikenteeseen. Tämän viestintäverkon osa olisi määritelty 69 §:n mukaisessa tuomioistuimen lupapäätöksessä, tai poikkeuksellisissa tilanteissa, pääesikunnan tiedustelupäällikön väliaikaisessa kiirepäätöksessä. Kyseisessä viestintäverkon osassa kulkeva tietoliikennevirta ohjattaisiin kulkemaan myös tiedustelujärjestelmän kautta, jolloin tiedustelujärjestelmä keräisi ja tallentaisi järjestelmään ennakkoon syötettyjen hakuehtojen mukaisen tietoliikenteen. Kerääminen ja tallentaminen tapahtuisivat automaattisella tietojenkäsittelyllä, mistä johtuen kukaan luonnollinen henkilö ei näkisi tiedustelujärjestelmän läpi kulkenutta tietoliikennettä. Ainoastaan hakuehtoja vastaava liikenne tallentuisi järjestelmään niin, että sotilastiedusteluviranomaisen virkamies voisi sitä käsitellä.

Puolustusvoimien tiedustelulaitoksella ei olisi oikeutta tai mahdollisuutta tallentaa muuta viestintää kuin sitä, joka vastaa tuomioistuimen myöntämässä luvassa tarkoitettuja hakuehtoja. Sotilastiedusteluviranomaisella ei myöskään olisi mahdollisuutta jälkikäteen palauttaa tai tarkastella tietoja, jotka eivät ole vastanneet tuomioistuimen myöntämän luvan mukaisia ehtoja. Tietoliikennetiedustelua käyttävä viranomainen ei saisi missään tilanteessa pääsyä muuhun kuin hakuehtojen mukaiseen tietoliikenteeseen.

Puolustusvoimien ensisijainen tehtävänä on puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdan mukaan Suomen sotilaallinen puolustaminen. Sotilaallisen uhkan muodostavat keskeisimmin vieraat valtiot. Pykälän mukaan tietoliikennetiedustelua voitaisiin käyttää vieraan valtion viestinnän tiedusteluun. Vieraan valtion viestinnästä voidaan saada olennaista tietoa vieraan valtion suunnitelmista ja toimintakyvystä, jotka vaikuttavat suoraan Suomea vastaan kohdistuvaan uhkaan ja siihen varautumiseen. Tehokkaan tiedustelun kautta sotilastiedusteluviranomainen pystyy muodostamaan ennakkovaroituksen Suomea kohtaan kohdistuvasta sotilaallisesta uhkasta ja siihen varautumisesta.

Pykälän 2 momentin mukaan Puolustusvoimien tiedustelulaitoksella olisi mahdollisuus käsitellä automaattisen tietojenkäsittelyn avulla hankittuja tietoja automaattisesti ja manuaalisesti. Tässä vaiheessa Puolustusvoimien tiedustelulaitoksen virkamies pääsisi käsittelemään kerättyä tietoliikennettä ja viestien sisältöä tiedustelutehtävän kannalta olennaisia tietoja analysoimiseksi.

Tiedon analysointivaiheessa automaattisella käsittelyllä tarkoitettaisiin sellaista kerätyn tiedon analysointia, joka toteutetaan automaattisen tietojen käsittelyn eli teknisen tietojärjestelmän avulla. Suurin osa kerätyn tiedon analysoinnista toteutettaisiin käytännössä automaattisesti. Automaattisen käsittelyn tarkoituksena olisi esimerkiksi kohdistaa kerättyyn tietoon sellaisia hakuja, joiden avulla voitaisiin edelleen supistaa manuaalisen käsittelyn kohteeksi otettavan tiedon määrää. Tietojärjestelmän avulla suoritettavat analysointi ja haut voisivat koskea niin kerättyyn tietoon sisältyviä välitystietoja ja muita ohjaustietoja kuin tällaisen tiedon merkityksellistä sisältöä.

Kerättyjä ja tallennettuja tietoja voitaisiin käsitellä myös aistinvaraisesti luonnollisen henkilön toimesta. Koska tällaisessa käsittelyssä samoin kuin edellä automaattisessa käsittelyssä saataisiin selvittää viestin välitystiedot ja viestin sisältö, kuuluisi aistinvaraiseen käsittelyyn esimerkiksi se, että Puolustusvoimien tiedustelulaitoksen palveluksessa oleva virkamies lukisi käsiteltävänä olevan viestin tekstisisällön, tarkastelisi sen kuvaliitteitä, kuuntelisi ääntä tai antaisi viestisisällön syötteeksi ohjelmistolle, jolle lähettäjä on sen tarkoittanut, seuratakseen ohjelmiston suoritusta.

Jos viestin käsittelyn aikana kävisi ilmi, että käsittelyn kohteena olevasta tiedosta ei saataisi tiedustelutehtävän kannalta olennaista tietoa taikka viesti olisi luottamuksellisen viestin suojan piirissä, tulisi se viipymättä hävittää hävittämistä koskevien säännösten perusteella.

Suomen alueelle sijoittuneille toimijoille ei aseteta velvollisuutta asentaa salaukseen käytettäviin ohjelmistoihin niin sanottuja takaportteja eikä toimijoita velvoiteta luovuttamaan salausavaimia tai muuntoinkaan rajoiteta salausteknologian käyttöä.

Pykälän 3 momentissa säädettäisiin nimenomainen kielto käyttää Suomessa oleskelevan henkilön hallussa olevaa tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja valtiollisen toimijan tietoliikenteeseen kohdistuvassa tiedustelussa. Pykälässä tarkoitetut sotilastiedustelun kohteiden aiheuttama uhka tulee Suomen rajojen ulkopuolelta. Uhkan aiheuttajat ovat lisäksi organisatorisesti järjestäytyneitä suuria toimijoita.

69 §. *Valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta päättäminen.* Valtio ja muut julkisyhteisöt jäävät perusoikeussuojan ulkopuolelle (HE 309/1993 vp. ja PeVL 9/2015 vp.). Koska esimerkiksi vieraan valtion sotilasorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa, voitaisiin valtiollisen toimijan viestinnän keräämisestä, tallentamisesta ja käsittelystä päättää lievemmin edellytyksin kuin muun toimijan viestinnän keräämisestä, tallentamisesta ja käsittelystä.

Pykälän 1 momentin mukaan oikeudesta kohdistaa tiedustelua 68 §:ssä tarkoitetun valtiollisen toimijan tietoliikenteeseen päättäisi pääesikunnan tiedustelupäällikön vaatimuksesta Helsingin käräjäoikeus.

Momentin kahdessa viimeisessä virkkeessä säädettäisiin kiiremenettelystä asiassa, joka ei siedä viivytystä. Päätöksen voisi tehdä pääesikunnan tiedustelupäällikkö siihen asti, kunnes tuomioistuin olisi ratkaissut luvan myöntämistä koskevan vaatimuksen. Valtiollisen toimijan viestinnän keräämisessä, tallentamisessa ja käsittelyssä saattaisi tulla vastaan tilanteita, joissa valtiolliseen toimijaan kohdistuva viestinnän kerääminen, tallentaminen ja käsittely olisi voitava aloittaa välittömästi yllättävästi saadun tiedon tai nopeasti muuttuvan toimintaympäristön takia. Vaatimus tuomioistuimelle olisi esitettävä 24 tunnin sisällä toimivaltuuden käytön aloittamisesta.

Lupa voitaisiin antaa pykälän 2 momentin mukaisesta enintään kuudeksi kuukaudeksi kerrallaan.

Pykälän 3 momentissa säädettäisiin lupahakemuksessa esitettävistä tiedoista. Momentin 1 kohdan mukaan lupahakemuksessa olisi esitettävä tiedustelutehtävä, jota varten valtiollisen toimijan tietoliikenteeseen kohdistettaisiin tietojen hankkimista. Tiedusetelutehtävän kuvauksessa yksilöitäisiin suurempi kokonaisuus, jota varten tietojen hankkiminen tietystä valtiollisesta toimijasta olisi tarpeen. Tiedustelutehtävää on kuvattu edellä 13 §:n yksityiskohtaisissa perusteluissa.

Momentin 2 kohdan mukaan hakemuksessa olisi ilmoitettava hakuehdot tai hakuehtojen luokat, joiden perusteella viestintää kerättäisiin, tallennettaisiin ja käsiteltäisiin. Hakuehtojen tai hakuehtojen luokkien perusteella suuresta määrästä tietoliikennettä etsittäisiin tiedustelutehtävän kannalta olennaiset tiedot. Jotta tietoliikennetiedustelu olisi riittävän kohdennettua, käytettävien hakuehtojen tulisi olla riittävän tarkkoja, jottei tietoliikenteen manuaaliseen käsittelyyn joutuisi tiedustelutehtävän kannalta tarpeetonta tietoa.

Haluehdot kuvailisivat tiedonhankinnan kohdetta. Valtiolliset toimijat ovat kooltaan isoja organisaatioita. Edellä sanotusta johtuen tiedustelutehtävän kohteeseen liittyy lukuisa määrä välitystietoja, joidenka perusteella tiedustelutehtävän kohteesta hankittaisiin tietoa. Lupahakemuksessa esitettävät hakuehdoissa esitettäisiin hakuehtojen ryhmät, joidenka perusteella tietoliikennetiedustelua kohdennettaisiin. Ryhmät sisältäisivät tarkemmat välitystiedot, jotka kohdistuisivat tiettyyn tieduste-

lutehtävän kannalta olennaiseen organisaatioon, kuten tiettyä uutta asejärjestelmää kehittävään organisaatioon.

Momentin 2 kohdan mukaan valitut hakuehdot tai hakuehtojen luokat olisi myös perusteltava vaatimuksessa. Perusteluissa kerrottaisiin tarkemmin, mihin kohteeseen ja miten valituilla hakuehdoilla tai hakuehtojen luokilla tiedustelutehtävän kannalta olennainen viestintä saataisiin kerättyä ja tallennettua 3 kohdassa tarkoitetusta viestintäverkon osasta.

Koska valtiollinen toimija ei nauti luottamuksellisen viestin suojaa, hakuehtona voitaisiin käyttää myös viestin sisältöä kuvaavia tietoja. Valtiolliseen toimijan tietoliikenteeseen kohdistuvassa tiedustelussa saattaisi kuitenkin olla tarpeellista käyttää hakuehtoja tietoliikenteen suuren määrän takia tai sen takia, että tietoliikenteestä saadaan jo tässä vaiheessa karsittua pois viestintä, joka liikkuisi valtiollisen toimijan tietoliikenteessä, mutta olisi sisällöltään luottamuksellisen viestin suojan alassa.

Momentin 3 kohdan mukaan hakemuksessa olisi ilmoitettava ne Suomen rajan ylittävät viestintäverkon osat, kuten kaapeleiden kuidut, joista viestintää kerättäisiin ja tallennettaisiin. Esimerkiksi yksittäiseen kuituun kohdistetulla tietoliikennetiedustelulla rajataan ulos merkittävä osa Suomen rajan ylittävästä tietoliikenteestä, mikä osaltaan myös tehostaa ja kohdentaa tietoliikennetiedustelua asianmukaisella tavalla.

Lisäksi hakemuksessa olisi perusteltava, miksi juuri valitusta viestintäverkon osasta saataisiin tiedustelutehtävän kannalta olennaisen valtiollisen toimijan viestintää kerättyä ja tallennettua.

Momentin 4 kohdan mukaan lupahakemuksessa olisi nimettävä ne tiedonsiirtäjät, joiden olisi avustettava valtiollisen toimijan tietoliikenteen tiedustelussa. Avustava tiedonsiirtäjä olisi mahdollista esittää lupahakemuksessa teknisten tietojen ja muun yhteistyön perusteella. Tiedonsiirtäjät pystyisivät avustamaan liitynnän tekemisessä tiettyyn hallinnoimansa viestintäverkon osaan, kuten kuituun, asianmukaisimmin ja mahdollisimman vähän häiriötä muulle viestintäverkon toiminnalle aiheuttaen.

Tiedonsiirtäjän avustamisvelvollisuudesta säädettäisiin erikseen jäljempänä.

Momentin 5 kohdan mukaan lupahakemuksessa olisi ilmoitettava luvan voimassaoloaika kellonajan tarkkuudella. Kuten muidenkin tiedustelumenetelmien kohdalla, hankittuja tietoja olisi kokoajan arvioitava ja keskeytettävä, kun tiedustelutehtävän kannalta olennaiset tiedot olisi hankittu. Lisäksi luvan voimassaolon osalta voidaan viitata edellä 20 §:n yksityiskohtaisissa perusteluissa todettuun.

Momentin 6 kohdan mukaan luvan mukaiselle tietoliikennetiedustelulle olisi nimettävä sen suorittamista johtava ja valvova sotilastiedusteluviranomaisen virkamies.

Momentin 7 kohdan mukaan valtiollisen toimijan tietoliikenteen tiedustelulle voitaisiin asettaa muita ehtoja ja rajoituksia.

70 §. *Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu.* Pykälässä säädettäisiin muun kuin valtiollisen toimijan tietoliikenteen tiedustelusta sekä toimivaltuuden käytön edellytyksistä. Pykälässä säädettyjen edellytysten lisäksi toimivaltuuden käytön edellytyksiä harkittaessa olisi otettava huomioon myös tiedustelutoiminnan yleiset periaatteet.

Muulla kuin valtiollisella toimijalla tarkoitettaisiin tiedustelutehtävän kohteita, joita ei voida katsoa vieraan valtion tai sellaiseen rinnastuvaksi toimijaksi. Toimijan asemaa arvioitaessa huomiota kiin-

nitettäisiin toimijaan, toimijan organisaatioon, toimijan käytettävissä oleviin resursseihin ja ennen kaikkea siihen, liittyisikö toimija sotilastiedustelun kohteeseen.

Edellä tarkoitettuja muita kuin valtiollisia toimijoita voisivat olla esimerkiksi aseteknologiaa kehittävät yritykset ja joukko-osastoja tukevat muut kuin sotilaalliset organisaatiot. Sotilastiedustelu voisi saada lisäksi olennaista tietoa myös lukuisista aseteollisuuteen liittyvistä organisaatioista.

Erotuksena 68 §:ssä säädetystä valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta, pykälän tarkoittamissa tilanteissa tietoliikenteen tiedustelulle asetettaisiin tiukemmat edellytykset. Tiedustelu tapahtuisi teknisesti samalla tavalla hakuehtojen perusteella kuin 68 §:n perusteluissa on kuvattu, mutta tiukemmilla vaatimuksilla.

Pykälän 1 momentin mukaan muun kuin valtiollisen toimijan tietoliikenteen tiedustelua voitaisiin käyttää tiedustelutehtävän kannalta olennaisen muun kuin valtiollisen toimijan tietoliikenteen tiedusteluun, jos tietoliikenteeseen kohdistuvan tiedustelun voidaan olettaa olevan välttämätöntä tiedon saamiseksi tiedustelutehtävän kannalta.

Tietoliikennetiedustelulle asetettaisiin tältä osin tiukempi edellytys kuin edellä 4 luvussa säädettäväksi ehdotetuille luottamuksellisen viestin salaisuuden suojaan puuttuville tiedustelumenetelmille tai edellä 68 §:ssä tarkoitetulle valtiollisen toimijan tietoliikenteeseen kohdistuvalle tiedustelulle. Syynä tähän on Euroopan ihmisoikeustuomioistuimen ratkaisu Szabo & Vissy v. Unkari, jonka mukaan ihmisoikeussopimuksen 8 artiklan mukaista "välttämätön demokraattisessa yhteiskunnassa" -edellytystä on tulkittava tietoliikennetiedustelun kaltaisen kehityksen kärkeä edustavan valvontateknologian yhteydessä siten, että se edellyttää "ehdotonta välttämättömyyttä" (strict necessity) kahdessakin suhteessa. Menetelmän käytön tulee olla yleisellä tasolla ehdottoman välttämätön demokraattisten instituutioiden suojaamiseksi. Toiseksi menetelmän käytön tulee yksittäisen tiedusteluoperaation yhteydessä olla ehdottoman välttämätöntä olennaisen tärkeän tiedon (vital information) saamiseksi.

Tietoliikennetiedustelun käytölle ehdotetulla välttämättömyysedellytyksellä tarkoitettaisiin viimesijaisuutta eli käytännössä sitä, että tietojen hankkiminen muulla keinolla kuin tietoliikennetiedustelulla ei ole mahdollista tai esimerkiksi vaatisi oleellisesti enemmän voimavaroja tai viivästyttäisi tiedonhankintaa kohtuuttomasti. Pakkokeinolain uudistamista koskevan hallituksen esityksen (HE 222/2010 vp, s. 316) välttämättömyysarvioinnille asettamaa kriteeristöä noudatellen selvitystä muiden tiedustelumenetelmien tosiasiallisesta käytöstä tai niiden yrittämisestä ei kuitenkaan edellytettäisi, koska silloin jouduttaisiin suorittamaan kalliita ja turhiakin yksityiselämän suojaan ulottuvia toimenpiteitä. Välttämättömyys voisi perustua kokonaisarviointiin siitä, että muut keinot tulisivat olemaan esimerkiksi tuloksettomia tai tiedonhankintaan soveltumattomia ilman, että niiden käyttöä olisi tullut konkreettisesti yrittää. Esimerkiksi Suomen rajan ulkopuolella olevan toimijan viestiliikenteen seuraaminen ei välttämättä ole mahdollista muilla tiedustelumenetelmillä, koska tiedustelun kohteen viestintää ei voitaisi seurata riittävän huomaamattomasti tai viestintää ei pystyttäisi keräämään ja tallentamaan riittävän nopeassa tahdissa.

Vaikka tietojen hankkiminen sinänsä olisikin mahdollista muuta tiedustelumenetelmää käyttäen, toisen tiedustelumenetelmän käyttäminen ei välttämättä olisi perusteltua sotilastiedustelun käytössä olevien rahallisten tai henkilöstö resurssien kannalta. Säännöksen soveltaminen edellyttäisikin vertailua yhtäältä 4 luvussa säädettäväksi ehdotettujen tiedustelumenetelmien, erityisesti telekuuntelun ja televalvonnan, sekä toisaalta tietoliikennetiedustelun välillä. Koska telekuuntelun ja televalvonnan käyttö pääsääntöisesti voidaan kohdentaa tarkemmin kuin tietoliikennetiedustelun käyttö, sisältää telekuuntelun ja -valvonnan käyttö myös vähäisemmän mahdollisuuden, että sivullisten viestintä tulee tiedustelun piiriin. Näin ollen, jos telekuuntelun tai -valvonnan käyttö ei yksittäistapauksessa olisi mahdotonta tai huomattavan vaikeaa, tulisi niitä käyttää ensisijaisina keinoina suhteessa tietoliikennetiedusteluun.

Lisäksi tietojen hankkiminen muilla keinoin saattaisi olla erityisen vaarallista tiedusteluoperaation toteuttajan kannalta. Tiedusteluoperaation toteuttaminen kotimaasta on huomattavasti turvallisempaa kuin vieraan valtion alueella toteutettava tiedustelu.

Välttämättömyysedellytykseen ei olisi säännöstasolla liitetty vaatimusta, että tietoliikennetiedustelulla saatavan tiedon olisi oltava olennaisen tärkeää. Tämä johtuu siitä, että tiedon olennaisen tärkeyden arvottaminen on tiedustelussa vaikeampaa kuin esimerkiksi rikostorjunnassa, jossa estettävänä, paljastettavana tai selvitettävänä on jokin konkreettinen teko.

Tiedustelussa ja erityisesti tietoliikennetiedustelussa ei kuitenkaan olisi kyse ainoastaan välittömien vaarojen torjumisesta, vaan myös pidempiaikaisesta tiedonhankinnasta kansallista turvallisuutta vakavasti vaarantavista toiminnoista. Tietoliikennetiedustelu voisi olla välttämätön esimerkiksi sellaisen tiedon hankkimiseksi, joka seuraavassa vaiheessa mahdollistaa jonkin tämän lain 4 luvussa tarkoitetun tiedustelumenetelmän käytön, mutta jonka ei vielä yksinään voida katsoa olevan välttämätön uhkan torjumisen mahdollistavan tiedon saamiseksi. Sotilastiedustelu olisi useista toisiaan täydentävistä tiedustelumenetelmistä muodostuva kokonaisuus, jonka puitteissa on erittäin vaikea ennakkoon arvottaa ja osoittaa kullakin yksittäisillä menetelmällä saatavan tiedon merkitys tiedonhankinnan kohteena olevaa toimintaa koskevan kokonaiskäsityksen kannalta.

Muuhun kuin valtiolliseen toimijaan kohdistuvassa viestinnän kerääminen ja tallentaminen eivät saisi pykälän 2 momentin mukaan tapahtua Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöivän tiedon perusteella. Sotilastiedustelun kohteet eivät olisi yksittäisiä henkilöitä Suomessa oleskelevia henkilöitä. Muun kuin valtiollisen toimijan viestinnän kerääminen ja tallentaminen kohdistuu suuriin toimijoihin, jotka toimivan Suomen rajan ulkopuolella. Tietoja yksittäisen Suomessa oleskelevan henkilön telepäätelaiteesta tai käyttämästä teleosoitteesta voitaisiin tarvittaessa hankkia 4 luvussa tarkoitetuilla toimivaltuuksilla. Esimerkiksi suomalaisessa verkossa olevaan matkapuhelimeen kohdistuva tiedonhankinta pystyttäisiin kohdistamaan 4 luvussa säädettäväksi ehdotettavilla tiedustelumenetelmillä, jolloin vaikutukset sivullisten tietoliikenteeseen pystyttäisiin minimoimaan.

Pykälän 3 momentissa säädettäisiin nimenomaisesta kiellosta, ettei tietoliikenteen tiedustelu saisi tapahtua viestin sisällön perusteella. Tietoliikenteen kerääminen ja tallentaminen saisivat tapahtua ainoastaan luvan mukaisten hakuehtojen tai hakuehtojen luokkien perusteella, jotka kohdistuisivat viestintään liittyviin muihin tietoihin kuin veistin sisällössä oleviin tietoihin.

Edellä sanotusta poikkeuksena olisivat kuitenkin haittaohjelman sisältöä ja ominaisuutta kuvaavat tiedot. Tiedustelutoiminnan pääasiallisena tehtävänä ei olisi tietoturvan parantaminen, mutta tietoliikennetiedustelun yhteydessä voitaisiin yksityisyyden suojaa vaarantamatta saada tiedustelutehtävän yhteydessä tietoa tietoverkoissa liikkuvista haittaohjelmista. Teknisiä verkkohyökkäyksiä on yleensä tehokkainta tunnistaa mahdollisimman lähellä potentiaalista hyökkäyksen kohdejärjestelmää ja järjestelmän omien ylläpitäjien toimesta. On kuitenkin tilanteita, joissa mahdollisia kohteita on paljon tai potentiaalisten kohdejärjestelmien ylläpito on ulkoistettu jollekin sellaiselle ilmaiselle taholle, ettei yksityiskohtaista tietoa torjuntaindikaattoreista ole mahdollista luovuttaa asettamatta kansallista turvallisuutta vaaraan. Tällöin tieto hyökkäyksistä tai valmistelevista toimenpiteistä voitaisiin hankkia tietoliikennetiedustelulla. Momentissa tarkoitetut haittaohjelmat olisivat korkealle kehittyneitä, joiden kehittämisen taustalla on usein valtiollinen toimija ja toiminnan taustalla ovat valtiolliset intressit, Suomen valtioon kohdistuvan vakoilun lisäksi myös teollisuuteen ja elinkeinoelämään liittyvien etujen tavoittelu. Suomalaisten organisaatioiden omasta tietoturvasta huolehtiminen jäisi edelleen organisaation itsensä huolehdittavaksi. Tietoja haittaohjelmista voitaisiin antaa yhteiskunnan eri toimijoille 75 §:ssä säädetyllä tavalla.

Toteutuneen tietoturvaloukkauksen jälkeen poikkeamaa voidaan pyrkiä tunnistamaan haittaohjelman tai haitallisen käsken aiheuttaman liikennevirran omaisuusjoukon perusteella. Sen sijaan tor-

junta ennalta ei useinkaan ole mahdollista pelkkien tietoliikenteen otsikkotietojen tai liikennevirran ominaispiirteiden nojalla, sillä tunkeutumista ennakoiva tietoliikenne pyrkii naamioitumaan tavanomaiseksi viestinnäksi. Siksi haitallisen tietokoneohjelman tai käsken sisältävälle liikenteelle säädettäisiin sisältöhaun mahdollistava poikkeus.

Haitallisuus tarkoittaisi tässä teknisen tietoturvallisuuden vaarantumista eli tietokoneohjelmaa tai käskyä, joka pyrkii anastamaan tietoa, muuttamaan tietoa oikeudetta tai haittaamaan kohdejärjestelmän toimintaa. Kohdejärjestelmäksi katsottaisiin mikä tahansa digitaalinen järjestelmä, myös itse verkko eli tietoliikennettä ohjaavat verkkolaitteet sekä reaalimaailman prosesseja ohjaavat laitteet. Koska hakuehtona ei olisi luonnollisen kielen sana, vaan jokin tekninen merkkijono, vaatimus automaattiseen vertailuun päätyvän tietoliikenteen rajaukselle ei olisi yhtä tiukka kuin muuten tietoliikenteen tiedustelussa edellytettäisiin.

Pykälän 4 momentissa säädettäisiin mahdollisuudesta käsitellä automaattisesti ja manuaalisesti 1 momentissa tarkoitettuja automatisoidusti hankittua tietoliikennettä. Manuaalisessa käsittelyssä viestien sisällöstä hankittaisiin tiedustelutehtävän kannalta olennaisia tietoja.

Automaattisessa ja aistin varaisessa käsittelyssä saataisiin selvittää viestin välitys- ja paikkatiedot sekä viestin sisältö. Viestin sisällön mainitsemisella tuotaisiin julki se, että selvittämisen piiriin voivat kuulua kaikki sellaiset tiedot, jotka nauttivat luottamuksellisen viestin salaisuuden suojaa. Edellä mainittujen luottamuksellisen viestin salaisuuden suojaa nauttivien tietojen ohella automaattisessa ja manuaalisessa käsittelyssä saataisiin ilman erillistä säännöstason mainintaa selvittää myös sellaiset tietoliikenteen ohjaamiseen liittyvät tiedot, jotka eivät kuulu luottamuksellisen viestin salaisuuden piiriin.

Suomen alueelle sijoittuneille toimijoille ei aseteta velvollisuutta asentaa salaukseen käytettäviin ohjelmistoihin niin sanottuja takaportteja eikä toimijoita velvoiteta luovuttamaan salausavaimia.

71 §. *Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta päättäminen.* Pykälän 1 momentin mukaan vaatimuksen tuomioistuimelle tekisi pääesikunnan tiedustelupäällikkö. Momentin kahdessa viimeisessä virkkeessä säädettäisiin muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvan tiedustelussa kiireellisessä tilanteessa. Päätöksen näissä tilanteissa tekisi pääesikunnan tiedustelupäällikkö.

Tietoliikennetiedustelussa saattaisi tulla vastaan tilanteita, joissa olisi pystyttävä reagoimaan nopeasti esimerkiksi sen takia, että tiedustelutehtävän kohteeseen liittyvät hakuehdot ja muut olennaisesti kohdistamiseen liittyvät tiedot, kuten reititystiedot, muuttuvat. Lisäksi tietoliikennetiedustelun aikana saattaisi tulla vastaan tilanteita, joissa uuden saadun tiedon pohjalta voitaisiin saada merkittäviä tiedustelutehtävään liittyviä olennaisia tietoja, mutta voimassa oleva lupa ei tällaista tiedonhankintaa kattaisi.

Pääesikunnan tiedustelupäällikön tekemän päätöksen jälkeen asia olisi saatettava tuomioistuimen käsiteltäväksi heti, kun se olisi mahdollista, kuitenkin viimeistään 24 tunnin kuluttua kiireellisen tietoliikennetiedustelun aloittamisesta. Tuomioistuimen arvioitua päätöksen edellytykset, lupa voitaisiin antaa tai tuomioistuin voisi hylätä vaatimuksen. Kiiretilanteessa käynnistetyt tiedustelumenetelmän käytön lopettamisesta säädettäisiin jäljempänä.

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

Pykälän 3 momentissa säädettäisiin vaatimuksessa ja päätöksessä esitettävistä tiedoista.

Momentin 1 kohdan mukaan lupahakemuksessa olisi esitettävä tiedustelutehtävä, jota varten muun kuin valtiollisen toimijan tietoliikennettä tiedusteltaisiin. Tiedustelutehtävän kuvauksessa yk-

silöitäisiin suurempi kokonaisuus, jota varten tietojen hankkiminen tietystä muun kuin valtiollisen toimijan tietoliikenteestä olisi tarpeen.

Momentin 2 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava kohdetta koskevat tosiseikat, jotka antava aiheen olettaa muun kuin valtiollisen toimijan liittyvän tiedustelutehtävään. Sotilastiedusteluviranomaisen olisi tuomioistuimelle esittämässään vaatimuksessa näin ollen tehtävä riittävän tarkkaan selkoa sen konkreettisen toiminnan luonteesta, josta tietoliikennetiedustelulla olisi tarkoitus hankkia tietoa. Vaatimuksessa annettavat tiedot voisivat koskea esimerkiksi sitä, kuinka toiminnasta on saatu tieto, kuinka toiminta on toistaiseksi ilmennyt, kuinka toiminnan oletetaan kehittyvän, mikä taho tai ketkä henkilöt ovat toiminnan taustalla ja miltä osin ja millä tavalla toiminta liittyy tiedustelutehtävään. Luvan myöntäminen edellyttäisi, että tuomioistuin Puolustusvoimien tiedustelulaitoksen esittämien seikkojen perusteella vakuuttuisi vaatimuksen kohteena olevan konkreettisen toiminnan liittymisestä tiedustelutehtävään. Vaatimuksen esittäjän olisi näin osoitettava, että konkreettinen toiminta siitä tiedossa olevien tosiseikkojen perusteella vastaa viime kädessä sitä tai niitä sotilastiedustelun kohteita, joka tai jotka olisi tullut yksilöidä vaatimuksen tai päätöksen 1 kohdassa.

Momentin 3 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava tosiseikat, joihin tietoliikennetiedustelun käytön edellytykset perustuvat. Muun kuin valtiollisen toimijan tietoliikenteen tiedustelun edellytyksistä ehdotetaan säädettäväksi 70 §:ssä. Vaatimuksessa ja päätöksessä olisi ensinnäkin perusteltava 70 §:n 1 momentissa tietoliikennetiedustelun yleiseksi edellytykseksi asetettavaksi ehdotettu toiminnan tuloksellisuus. Puolustusvoimien tiedustelulaitoksen olisi vaatimuksessaan tehtävä selkoa niistä seikoista, joiden perusteella tietoliikennetiedustelulla voidaan ylipäätään olettaa saatavan tietoja siitä tiedustelutehtävän kannalta olennaisesta toimijasta, jota vaatimus koskee. Lisäksi kohdan mukaan vaatimuksessa olisi tehtävä selkoa edellytykseksi asetetusta välttämättömyyden täyttymisestä. Vaatimuksessa ja samoin tuomioistuimen päätöksessä olisi näin ollen tehtävä selkoa siitä, miksi niitä tietoja, jotka tietoliikennetiedustelulla olisi kyseisessä tapauksessa tarkoitus hankkia, ei voitaisi hankkia muulla tavalla, tai miksi niiden hankkiminen muulla tavalla olisi oleellisesti vaikeampaa tai vaarallisempaa. Vaatimuksessa olisi esitettävä arvio siitä, miksi juuri tietoliikennetiedustelulla tietojen hankkiminen olisivat käsillä olevassa tilanteessa muita tiedustelumenetelmiä parempi keino hankkia tiedustelutehtävän kohteena olevia tietoja.

Momentin 4 kohdan mukaan vaatimuksessa ja päätöksessä ilmoitettava hakuehdot tai hakuehtojen luokat, joiden perusteella tietoliikennettä hankittaisiin sekä perustelut niille. Hakuehtojen tai hakuehtojen luokkien perusteella suuresta määrästä tietoliikennettä etsittäisiin tiedustelutehtävän kannalta olennaiset tiedot. Jotta tietoliikennetiedustelu olisi riittävän kohdennettua, käytettävien hakuehtojen tulisi olla riittävän tarkkoja, jottei viestinnän käsittelyyn joutuisi tiedustelutehtävän kannalta tarpeetonta tietoa.

Hakuehdot kuvailisivat tiedonhankinnan kohdetta ja kohdistuisivat kohteen viestinnän siihen osaan, joka ei ole viestin sisältöä. Näitä tietoja ovat esimerkiksi viestin välitystiedot ja muut tekniset tiedot. Hakuehtoina voisivat olla esimerkiksi AS-numerot, IP-osoitealueet sekä domain-nimet.

Pääsäännön mukaan hakuehto ei saisi kuvata viestin sisältöä, jolloin hakuehdoksi ei voisi asettaa viestivien henkilöiden käyttämiä ilmaisuja. Sisällön ja ohjaustiedon käsitteet edellyttävät internetverkossa enemmän määrittelyä ja avaamista kuin vanhoissa puhelinverkoissa, sillä sisällön ja otsikkotiedon raja voi vaihdella suuresti riippuen siitä, millä verkkoliikenteen toimintaa kuvaava OSI-viitemallin kerroksella asiaa tarkastellaan. Asiasta on kaksi tulkintaa. Molemmissa niiden soveltamisesta aiheutuvat perusoikeusvaikutukset eroavat toisistaan merkittävästi.

Jos sisältö erotetaan ohjaustiedosta kuljetuskerroksen perusteella, ohjaustietoa on ainoastaan se tieto, jolla viestin ohjataan verkossa. Kuljetuskerrokselta tarkasteltuna hakuehtona voisi siten olla vain laitteiden verkko-osoite, sillä esimerkiksi sähköpostiosoite kuljetetaan kuljetuskerroksen tieto-

liikennepaketin hyötykuorman sisällä. Tiedustelua ei tällöin voitaisi rajata hakuehdolla esimerkiksi yksittäiseen sähköpostiosoitteeseen (esimerkiksi: xx.xxx@sähköposti.com). Manuaaliseen virkamiehen toteuttamaan sisältöanalyysin piiriin jouduttaisiin ottamaan kaikki palvelimen gmail.com sähköpostiliikenne. Kuljetuskerroksella tapahtuva haku olisi toisaalta varsin suoraviivainen. Yhdenkään tietoliikennepaketin hyötykuormaa ei avata, vaan kerääminen ja tallentaminen tapahtuvat otsikkokenttien perusteella.

Jos taas sisältö erotetaan ohjaustiedosta sovelluskerroksen perusteella, ohjaustietojen joukkoon kuuluu myös se tieto, jonka perusteella viesti ohjataan tarkasti oikealle vastaanottajalle vastaanottavan laitteen viestintäohjelmistossa. Sovelluskerrokselta tarkasteltuna siten sähköpostipalvelinten ja Suomen välisestä tietoliikenteestä voitaisiin hakuehdolla seuloa sisältöanalyysiin tarkasti vain osoitteen (xx.xxx@säköposti.com) tietoliikenne, muu palvelimen liikenne jätettäisiin keräämisen ja tallentamisen ulkopuolelle. Toisaalta sovelluskerroksen otsikkotiedon analysointi edellyttää sitä, että valitus tietoliikennevirran kuljetuskerroksen pakettien hyötykuorma joudutaan avaamaan teknisellä analysaattorilla, jotta sovelluskerroksen otsikkotietoa voidaan verrata hakuehtoon.

Tietoliikennetiedustelussa käytetty tulkinta sisällön ja teknisten tietojen erosta olisi lähempänä OSI-viitemallin sovelluskerroksen tulkintaa kuin kuljetuskerroksen tulkintaa. Tällöin sisältöanalyysiin päätyvän aineiston haku pystyttäisiin kohdentamaan merkittävästi tarkemmin, jolloin tiedustelusta aiheutuva perusoikeusvaikutus olisi pienempi.

Raja ei kuitenkaan ole luonteeltaan suoraviivaisen tietotekninen, vaan tulkinnan ohjenuorana tulisi pitää hakuehdoksi valitun merkkijonon tarkoitusta tietoliikennevirrassa: Esiintyykö se tietovirrassa ohjaamassa viestisisältöä vai onko se tarkoitettu semanttiseksi sanomasisällöksi lähettäjältä vastaanottajalle. Rajaa voidaan havainnollistaa sähköpostiviestin "Aihe:"-kentällä. Sähköpostiviestin Aihe-kenttä näytetään sovelluksissa otsikkotietojen seassa. Jos lähettäjä on tarkoittanut sen sanomaksi viestin vastaanottavalle henkilölle, sitä ei voida pitää ohjaustietona, vaan semanttisena sisältönä. Tietoliikennetiedustelussa käytettäviä hakuehtoja voisivat olla kaikki sellaiset tiedot, joita käytetään ohjaamaan tai dokumentoimaan viestin kulkua viestijärjestelmässä, kun taas sisältöä olisi kaikki sellainen tieto, jonka lähettäjä on tarkoittanut vastaanottajalle. Kyseeseen tulisivat siten osoitteet, sosiaalisen median palveluiden käyttäjätunnukset kuin myös teleosoitteet. Hakuehto voisi myös olla rakenteinen siten, että se muodostuisi joukosta ohjaustietoja, esimerkiksi IP-osoitteen, kohdeportin ja jonkin kuljetuskerroksen tunnisteen yhdistelmästä.

Tiedustelutehtävän kohteeseen saattaa liittyä lukuisa määrä välitystietoja, joidenka perusteella tiedustelutehtävän kohteena olevan kohteen tietoliikennettä kerättäisiin.

Vaatimuksessa voitaisiin esittää myös hakuehtojen luokat, joidenka perusteella tietoliikenteen erottelu tapahtuisi. Hakuehtojen luokilla ei hakuehdoista poiketen viitattaisi sellaisiin yksittäisiin teknisiin tietoihin, joita voidaan sellaisinaan käyttää tietoliikennevirtaan kohdistettavan automatisoidun seulonnan vertailuehtoina. Hakuehtojen luokalla tarkoitettaisiin tarkkarajaista suullista kuvausta tiedustelutehtävän kannalta relevanteista hakuehdoista. Hakuehtojen luokat sisältäisivät tiedustelutehtävän useita tietoja, joidenka perusteella viestinnän kerääminen ja tallentaminen tapahtuisi. Hakuehtojen luokista sotilastiedusteluviranomainen voisi valita tiedustelutehtävän edessä parhaiten olennaisimman viestinnän löytävät hakuehdot, jotka kohdistuisivat esimerkiksi uutta asejärjestelmää kehittävään organisaatioon.

Hakuehtojen luokkaa voitaisiin käyttää tilanteessa, jossa samaan tarkkarajaisesti määriteltävissä olevaan kokonaisuuteen kuuluu joukko keskenään samantyyppisiä hakuehtoja, joista vain osa on tietoliikennetiedustelun käynnistyessä tiedossa. Sen sijaan, että tietoliikennetiedustelulla saadun uuden tiedon myötä käynnistettäisiin aina uusi lupamenettely, voitaisiin hakea lupa hakuehdoista muodostuvan joukon suulliselle kuvaukselle, jolloin uuden tiedon perusteella luotavat uudet yksittäiset hakuehdot kuuluisivat aiemmin haetun luvan piiriin. Hakuehtojen luokkana voisi olla esimer-

kiksi tietyn vaatimuksessa yksilöidyn henkilöryhmän viestiyhteydet yleisesti. Ryhmään kuuluvia henkilöitä yhdistävänä tekijänä voisi olla esimerkiksi jäsenyys tietyssä lupavaatimuksessa yksilöidyssä sotilaallisesti organisoituneessa ryhmittymässä taikka toimiminen tietyssä työtehtävässä sellaisessa vierasta valtiota edustavassa sotilaallisessa organisaatiossa.

Kun tietoliikennetiedustelun avulla saataisiin yksitellen tietoon ryhmään kuuluvien henkilöiden käyttämiä teleosoiteavaruuksia ja muita ulkomaisia teleosoitteita, niitä voitaisiin käyttää hakuehtoina. Tiedustelun kuluessa laajoista, suuren teleosoitemäärän kattavista, hakuehdoista voitaisiin siten tietoliikennetiedustelulla hankittavan tiedon nojalla siirtyä tarkempiin hakuehtoihin sekä lisäksi alkuperäisen osoitejoukon ulkopuolelta paljastuviin uusiin hakuehtoihin. Tiedustelutehtävän kohteen luonteen vuoksi olisi välttämätöntä saada uudet hakuehdot tiedustelun piiriin välittömästi. Jotta tietyn henkilöryhmän viestiyhteydet voisivat tulla hyväksytyksi hakuehtojen luokkana, edellytettäisiin, että henkilöryhmän jäsenyyden perusteet olisi määritelty vaatimuksessa riittävän tarkasti, että ryhmän olisi osoitettu olevan tiedustelutehtävän kohteena, ja että ryhmää koskeva vaatimus muutenkin täyttäisi tietoliikennetiedustelun edellytykset.

Sallittuna hakuehtojen luokkana voisi tulla kyseeseen myös tietoliikenneyhteydet tietyn hakemuksessa yksilöidyn rajatun maantieteellisen alueen ja Suomen välillä. Kyseinen maantieteellinen alue voisi olla esimerkiksi tietyn sotilasjoukko-osaston komentopaikka, josta sen muun tiedustelutiedon perusteella tiedetään ohjaavan toisen valtion alueella toimivia sotilaita. Jotta tiettyyn maantieteelliseen alueeseen liittyvät viestiyhteydet voisivat tulla hyväksytyksi hakuehtojen luokkana, olisi Puolustusvoimien tiedustelulaitoksen kyettävä osoittamaan kyseisen rajatun maantieteellisen alueen merkitys tiedustelutehtävän kannalta. Sen olisi tarpeen mukaan myös yksilöitävä ne rajaukset, joiden puitteissa konkreettiset hakuehdot muodostetaan, jotta tiedustelu ei kohdistuisi kyseiseltä maantieteelliseltä alueelta sinänsä lähtöisin olevaan mutta tiedustelutehtävän kannalta sivulliseen tietoliikenteeseen.

Edelleen hakuehtojen luokkina voisivat tulla kyseeseen esimerkiksi sellaiset lupahakemuksessa ennakkoon yksilöimättömät haittaohjelmakoodit, joita tietyn vieraan valtion tietty tiedustelupalvelu käyttää kybervakoilussaan, tai sellaiset lupahakemuksessa ennakkoon yksilöimättömät verkko-osoitteet, joita kyseinen tiedustelupalvelu käyttää kybervakoilunsa välikappaleena. Jos haittaohjelmakoodit tai verkko-osoitteet yksilöitäisiin vaatimuksessa, olisi niissä kyse hakuehdoista eikä niiden luokista. Tarve vaatia lupaa kybervakoilussa käytettäviin haittaohjelmakoodeihin ja verkko-osoitteisiin yleisemmin johtuu siitä, että koodit ja osoitteet saattavat tietoliikennetiedustelun meneillään ollessa muuttua tai niistä saatetaan tietoliikennetiedustelussa saada uutta tietoa. Haittaohjelmaa kybervakoilussaan käyttävä tiedustelupalvelu saattaa esimerkiksi muuntaa ohjelman koodia siten, ettei se enää vastaa alkuperäistä, jolloin myöskään sellainen yksittäinen hakuehto, jonka käyttöön tuomioistuin on myöntänyt luvan, ei sitä enää tunnista. Jos lupa voitaisiin vaatia ja saada vaatimuksessa mainitun tiedustelupalvelun käyttämiin haittaohjelmakoodeihin yleisesti (hakuehtojen luokka), voitaisiin tietoliikennetiedustelu ilman keskeytystä suunnata muunnettuun koodiin.

Vastaavasti, jos lupa tietoliikennetiedusteluun voitaisiin vaatia ainoastaan yksittäiseen kybervakoilun välikappaleena käytettävään verkko-osoitteeseen (hakuehto), seuraisi tästä, että tietoliikennetiedustelu jouduttaisiin keskeyttämään, jos vakoilua harjoittava taho ohjaa liikenteen uudelle reitille. Keskeytyksetön tietoliikennetiedustelu edellyttäisi sitä, että lupa olisi vaadittu ja saatu vaatimuksessa mainitun tiedustelupalvelun kybervakoilunsa välikappaleen käyttämiin verkko-osoitteisiin yleisesti (hakuehtojen luokka).

Niitä tietoja, jotka tulisivat kyseeseen sallittuina hakuehtojen luokkina, on mahdoton määritellä ennakkoon tyhjentävästi. Näin ollen sen selkeyttäminen, mikä toisistaan liittyvistä tiedoista koostuva joukko olisi riittävän täsmällinen tullakseen kyseeseen hakuehtojen luokkana, ehdotetaan jätettäväksi tuomioistuinkäytännön varaan. Hyväksyessään tietyn hakuehtojen luokan käytön tuomiois-

tuin voisi asettaa käytölle sellaisia rajoituksia ja tarkempia ehtoja kuin jäljempänä tämän momentin kohdassa 9 ehdotetaan.

Koska hakuehtojen luokkaa koskevassa tuomioistuimen lupahyväksynnässä olisi kyse siitä, että Puolustusvoimien tiedustelulaitokselle annettaisiin rajattu oikeus muotoilla tietoliikennetiedustelussa käytettävät konkreettiset hakuehdot itse, olisi toimintaan tältä osin tarve kohdistaa erityisen tarkkaa valvontaa. Valvonnan kohteena olisi se, että konkreettisten hakuehtojen määrittäminen tapahtuu tuomioistuimen päätöksessään hyväksymän hakuehtojen luokan puitteissa. Tiedustelutoiminnan valvonnasta säädettäisiin erillislaissa. Käytännössä hakuehtojen luokkien sisällä tapahtuvaa hakuehtojen tarkentamista valvoisi ensisijaisesti muun kuin valtiollisen toimijan tietoliikenteen tiedustelua johtava ja valvoja tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies.

Lupavaatimuksessa ja päätöksessä olisi mainittava myös perustelut tietoliikennetiedustelussa käytettäviksi aiotuille hakuehdoille tai hakuehtojen luokille. Tietoliikenteen tiedustelussa käytettävät hakuehdot olisivat pääsääntöisesti teknisiä tietoja, joiden liityntä tietoliikennetiedustelun kohteena olevaan toimintaan ei välttämättä näytä ilmeiseltä. Vaatimuksen esittäjän tulisi näin ollen perustella tuomioistuimelle, mikä on hakuehdon ja tiedustelutehtävän välinen yhteys, miksi hakuehdon käytöllä oletetaan saatavan tietoa kyseisestä toiminnasta ja minkälaista tietoa hakuehdon käytön avulla todennäköisesti saadaan. Jos hakuehtona esimerkiksi olisi IP-osoiteavaruus, tulisi Puolustusvoimien tiedustelulaitoksen tehdä selkoa siitä, millä perusteilla tiedustelutehtävään liittyvää tietoliikennettä oletetaan olevan kyseisessä IP-osoiteavaruudessa ja minkälaista tämä liikenne siinä tapauksessa olisi. Jos vaatimus koskisi hakuehtojen luokkaa, tulisi Puolustusvoimien tiedustelulaitoksen vastaavalla tavalla perustella se, mikä on valitun hakuehtojen luokan ja tietoliikennetiedustelulla selvitettävän tiedustelutehtävää koskevan toiminnan yhteys, miten tekniset hakuehdot on tarkoitus muodostaa hakuehtojen luokan puitteissa ja minkälaista tietoa muodostettavien hakuehtojen avulla on tarkoitus hankkia.

Momentin 5 kohdan mukaan vaatimuksessa ja päätöksessä olisi ilmoitettava ne Suomen rajan ylittävät viestintäverkon osat, kuten kaapeleiden kuidut, joihin tietoliikennetiedustelua kohdennettaisiin. Esimerkiksi yksittäiseen kuituun kohdistetulla tietoliikennetiedustelulla rajataan ulos merkittävä osa Suomen rajan ylittävästä tietoliikenteestä, mikä osaltaan myös tehostaa ja kohdentaa tietoliikennetiedustelua asianmukaisella tavalla.

Hakuehtojen avulla toteutettava tietoliikenteen kerääminen ei voisi koskea koko viestintäverkkoa, vaan tietoliikenteen kerääminen saisi kussakin tilanteessa koskea mahdollisimman suppeaa osaa siitä. Puolustusvoimien tiedustelulaitoksen velvollisuutena olisi lupavaatimuksessaan määritellä mahdollisimman täsmällisesti ne tietoliikennekaapelit tai, mikäli mahdollista, ne kuidut tai aallonpituudet, joissa liikkuvaan tietoliikenteeseen tietoliikennetiedustelussa käytettäviä hakuehtoja käytettäisiin. Vaatimuksessa ja päätöksessä edellytetty tieto viestintäverkon osasta selvitettäisiin tapauksesta riippuen joko edellä 66 §:ssä säädettäväksi ehdotetulla tietoliikenteen teknisten tietojen käsittelyllä tai 94 §:ssä tiedonsiirtäjille säädettäväksi ehdotetun avustamisvelvollisuuden avulla. Yleisimmin viestintäverkon osan selvittämisessä käytettäisiin edellä mainittujen selvittämiskeinojen yhdistelmää.

Viestintäverkon osan tunnistamisessa 66 §:ssä säädettävällä teknisten tietojen käsittely ja tiedonsiirtäjän tiedonantovelvollisuus olisivat liitännäisiä. Jos tietoliikennetiedustelua kohdennettaisiin valtiolliseen toimijaan 68 §:ssä tarkoitetusti, eli tiedustelua kohdennettaisiin staattiseen tietoliikenteeseen, edellyttäisi tämä tietojen saamista tiedonsiirtäjältä alkutilanteessa, jotta tietoliikennetiedustelua voitaisiin käytätä mahdollisimman kohdennetusti ja rationaalisesti. Muun kuin 68 §:ssä tarkoitetun tietoliikenteen reitittymisessä tiedonsiirtäjältä saadut tiedot olisi voitava todentaa tietoliikenteen teknisten tietojen käsittelyn avulla. Lisäksi tällä toiminnalla voitaisiin saada sellaista uutta tietoa, jota tiedonsiirtäjällä ei olisi hallussaan ja jota voitaisiin käyttää tietyn tietoliikenteen poissuljennassa. Poissulkevan tiedon käyttö mahdollistaisi sen, että myöhemmässä vaiheessa toteutetta-

vaa tietoliikennetiedustelun hakuehtoperusteista tiedonhankintaa ei kohdistettaisi laajempaan osaan tietoverkkoa kuin on välttämätöntä.

Vaatimuksessa ja päätöksessä olisi mainittava perustelut sille viestintäverkon osalle, johon tietoliikennetiedustelu kohdistettaisiin. Puolustusvoimien tiedustelulaitoksen olisi tehdä vaatimuksessaan selkoa siitä, miksi ja millä perusteilla tiedusteluntehtävän kohteena olevaan toimintaan liittyvän tietoliikenteen voidaan olettaa kulkevan siinä tietoverkon osassa, jota vaatimus koskee.

Momentin 6 kohdan mukaan vaatimuksessa ja päätöksessä olisi ilmoitettava tietoliikennetiedustelua koskevan luvan voimassaoloaika kellonajan tarkkuudella. Kuten muidenkin tiedustelumenetelmien kohdalla, hankittuja tietoja olisi koko ajan arvioitava ja tiedustelu olisi keskeytettävä, kun tietoliikennetiedustelun tavoite olisi saavutettu.

Momentin 7 kohdan mukaan luvan mukaiselle tietoliikennetiedustelulle olisi mainittava sen suorittamista johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt Puolustusvoimien tiedustelulaitoksen virkamies. Johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies valvoisi ensimmäisenä myös edellä kohdassa 3 tarkoitettujen hakuehtojen käyttöä ja hakuehtojen luokkien sisällä tapahtuvaa hakuehtojen tarkentamista.

Momentin 8 kohdan mukaan vaatimuksessa ja päätöksessä olisi esitettävä myös tietoliikennetiedustelun rajoitukset ja ehdot. Tuomioistuin voisi asettaa päätöksessään tietoliikennetiedustelulle rajoituksia ja ehtoja. Jos Tällaisia rajoituksia ja ehtoja olisi tiedossa jo vaatimusta laadittaessa, niin ne olisi syytä kirjata jo vaatimukseen. Rajoituksia ja ehtoja voitaisiin asettaa esimerkiksi sille, kuinka Puolustusvoimien tiedustelulaitos saa muodostaa hakuehtoja niiden hakuehtojen luokkien puitteissa, joihin tuomioistuin myöntää luvan.

72 §. *Tietoliikennetiedustelun edellyttämän kytkennän toteuttaminen.* Pykälän mukaan 67, 69 ja 71 §:ssä tarkoitetun luvan mukaisen liitynnän Suomen rajan ylittävän kaapelin yksittäiseen kuituun tekisi kytkennän suorittaja tuomioistuimen luvassa osoitetun tiedonsiirtäjän avustuksella. Täytäntöönpano tarkoittaisi sitä, että kytkennän suorittaja ohjaisi tiedonsiirtäjän hallinnoimasta viestintäverkon osasta luvan mukaisessa fyysisessä liitynnässä kulkevan tietoliikenteen edelleen Puolustusvoimien tiedustelulaitokselle. Kytkennän suorittaja myös varmistaisi, että Puolustusvoimien tiedustelulaitoksella olisi pääsy koko luvan voimassaolon ajan ainoastaan 67, 69 ja 71 §:ssä tarkoitetun luvan mukaiseen viestintäverkon osaan eikä Puolustusvoimien tiedustelulaitos pääsisi käyttämään muissa yhteyksissä, kuten kuiduissa tai aallonpituuksissa, liikkuvaa tietoliikennettä tiedustelussaan.

Pykälän 2 momentin mukaan kytkennän suorittaja luovuttaisi edelleen luvan mukaisessa viestintäverkon osassa liikkuvan tietoliikenteen edelleen Puolustusvoimien tiedustelulaitokselle. Sotilastiedusteluviranomaisella ei näin olisi suoraa pääsyä muussa viestintäverkon osassa liikkuvaan viestintään.

73 §. *Tietoliikennetiedustelun tekninen toteuttaminen suojelupoliisin puolesta.* Sotilastiedusteluviranomaisella on Suomessa tarvittava osaaminen ja resurssit tietoliikennetiedustelun tekniseen toteuttamiseen. Suojelupoliisilla olisi tarve tietoliikennetiedustelulla hankitulle tiedolle. Resurssien tehokkaan käytön näkökulmasta ei ole kuitenkaan tarkoituksen mukaista, että usealla eri viranomaisella olisi tekninen valmius tietoliikennetiedustelun toteuttamiseen. Pykälän 1 momentin mukaan viestinnän keräämisen tietoliikenteestä toteuttaisi puolustushallinnon ulkopuoliselle toimijallekin sotilastiedusteluviranomainen.

Pykälän 1 momentin 1 kohdassa tietoliikennetiedustelun teknisellä toteuttamisella suojelupoliisille tarkoitettaisiin teknisten tietojen hankkimista tietoliikennetiedustelun kohdentamiseksi. Sotilastiedusteluviranomainen voisi hankkia tietoliikennetiedustelun asianmukaiseksi toteuttamiseksi tekni-

siä tietoja tietoliikenteestä teknisen analyysin tekemiseksi, kuten edellä 68 §:ssä säädetään. Näitä teknisiä tietoja voitaisiin hankkia myös suojelupoliisin pyynnöstä suojelupoliisin tarvitseman tietoliikennetiedustelun toteuttamiseksi. Tässä tilanteessa Puolustusvoimien tiedustelulaitos hankkisi myös tuomioistuimen luvan suojelupoliisin puolesta. Teknisten tietojen käsittelyssä ei ole kyse tuomioistuimen harkintaa edellyttävästä luvan hankkimisesta. Kyse on teknisten tietojen hankkimisesta tietoliikenteeseen kohdistuvan tiedustelun asianmukaiseksi kohdentamiseksi eikä teknisten tietojen käsittelyllä hankittaisi tietoja viestien sisällöstä. Tuomioistuimen harkinta rajoittuisi siihen, miten teknisiä tietoja käsiteltäisiin ja luvan voimassaoloaikaan.

Momentin 2 kohdan mukaan teknisellä toteuttamisella tarkoitettaisiin myös tietojen hankkimista suojelupoliisin hankkiman tuomioistuimen luvan mukaisesti. Puolustusvoimien tiedustelulaitos toimisi tietoliikennetiedustelun teknisenä toteuttajana suojelupoliisille. Näissä tapauksissa Puolustusvoimien tiedustelulaitos hankkisi suojelupoliisin saaman tuomioistuimen luvan mukaisen tietoliikenteen luvassa tarkoitetusta viestintäverkon osasta ja luovuttaisi sen edelleen käsittelemättömänä suojelupoliisille.

Tietoliikennetiedustelussa kukin viranomainen olisi vastuussa muuhun kuin tietoliikenteen teknisiin tietoihin kohdistuvasta tietoliikennetiedustelussa tarvittavan luvan hakemisesta toimivaltaiselta tuomioistuimelta. Teknisessä toteuttamisessa suojelupoliisille Puolustusvoimien tiedustelulaitos ainoastaan hankkisi tietoliikenteestä lupaehtojen mukaiset tiedot toiselle viranomaiselle. Hankitut tiedot luovutettaisiin suojelupoliisille, joka käsittelisi hankittuja tietoja omien tehtäviensä mukaisesti.

Pykälän 3 momentissa olisi viittaussäännös tietoliikennetiedustelusta siviilitiedustelussa annettuun lakiin. Suojelupoliisille toteuttavasta tietoliikennetiedustelusta säädettäisiin lain 10 §:ssä.

Pykälän 4 momentin mukaan Puolustusvoimien tiedustelulaitoksella ei olisi pääsyä suojelupoliisille tietoliikennetiedustelulla hankittuihin tietoliikenteeseen eikä se voisi niihin jälkikäteen palata. Tämä ei kuitenkaan koskisi tietoliikenteen teknisten tietojen perusteella tehtyä teknistä analyysia suojelupoliisin toimeksiannon perusteella. Tietoliikennetiedustelun asianmukainen kohdentaminen vaatisi ajantasaista tietoa tietoliikenteen reitittymisestä internetverkossa. Reitittymisessä voi tapahtua nopeasti muutoksia, joten tiedusteluviranomaisten toiminnan kannalta olisi tarkoituksen mukaista, että tiedusteluviranomaisilla olisi käytössään mahdollisimman laaja ja ajantasainen kuva tietoliikenteen liikkumisesta.

74 §. *Tietojen hävittäminen.* Pykälässä säädettäisiin tietojen hävittämisvelvollisuudesta. Pykälän 1 kohdan mukaan viestintäverkosta kerätty ja tallennettu viestintä olisi hävitettävä, jos käy ilmi, että viestinnän kumpikin osapuoli oli viestinnän tapahtumisen aikaan Suomessa.

Momentin 2 kohdan mukaan viestintä olisi hävitettävä välittömästi, jos viestinnän lähettäjä tai vastaanottajalla on oikeus tai velvollisuus kieltäytyä todistamasta oikeudenkäymiskaaren 17 luvun 13–16 §:n tai 20 §:n nojalla. Viitatuissa pykälissä säädetään oikeudenkäyntiasiamiehen tai -avustajan taikka tulkin, lääkärin tai muun terveydenhuollon ammattihenkilön, uskonnonvapauslaissa (453/2003) tarkoitetun rekisteröidyn uskonnollisen yhdyskunnan papin tai muun vastaavassa asemassa olevan henkilön ja sananvapauden käyttämisestä joukkoviestinnässä annetussa laissa (460/2003) tarkoitetun yleisön saataville toimitetun viestin laatijan taikka julkaisijan tai ohjelmatoiminnan harjoittajan oikeudesta kieltäytyä todistamasta. Oikeudenkäymiskaaren 17 luvun 15 §:ssä säädetään, että tuomioistuin voi velvoittaa henkilön, jota velvollisuus tai oikeus kieltäytyä todistamasta koskee, todistamaan, jos se, jonka hyväksi salassapitovelvollisuus on säädetty, on kuollut.

75 §. *Haitallista tietokoneohjelmaa koskevien tietojen luovuttaminen yrityksille ja yhteisöille.* Pykälän mukaan haitallista tietokoneohjelmaa tai käskyä koskevia tietoja voitaisiin luovuttaa yrityksille ja yhteisöille, jos tietojen luovuttaminen on tarpeen maanpuolustuksen turvaamiseksi, kansallisen turvallisuuden suojaamiseksi taikka yrityksen tai yhteisön etujen turvaamiseksi. Lisäksi Puolustus-

voimien tiedustelulaitos voisi luovuttaa haitallista tietokoneohjelmaa koskevia tietoja toimivaltaiselle viranomaiselle, kuten Viestintävirastolle.

Suomessa valtion ja yhteiskunnan puolustukseen ja sen kehittämiseen osallistuu lukuisa määrä yrityksiä ja muita yhteisöjä, jotka myös tuottavat valtion turvallisuuteen ja yhteiskunnan elintärkeitä toimintoihin liittyviä palveluita. Näiden palveluiden jatkuvuuden takaamiseksi olisi tärkeää, että tietoliikennetiedustelulla saatuja tietoja kehittyneistä haitallisista tietokoneohjelmista tai käskyistä voitaisiin antaa myös yrityksille ja yhteisöille.

Tietoliikennetiedustelun yhtenä tarkoituksena olisi parantaa yhteiskunnan suojaa teknisesti edistyneitä tietoverkkohyökkäyksiä, esimerkiksi kybervakoilua, vastaan. Tietoliikennetiedustelun voidaan arvioida tuottavan runsaasti havaintoja ja tietoa tietoverkkohyökkäyksissä käytettävistä haitallisista tietokoneohjelmista ja -käskyistä. Kun edistyneet tietoverkkohyökkäykset voivat kohdistua paitsi viranomaisiin myös yrityksiin ja yhteisöihin, olisi suomalaisen yhteiskunnan kokonaissuojautumisen kannalta tärkeää, että hyökkäyksissä käytettäviä haittaohjelmia koskevia tietoja voitaisiin mahdollisimman laajasti luovuttaa hyökkäysten potentiaalisille kohteille. Tällaisten tietojen luovuttamisoikeudesta säätämällä voitaisiin osaltaan turvata yritysten ja yhteisöjen mahdollisuuksia ryhtyä sellaisiin toimenpiteisiin tietoturvastaan huolehtimiseksi, joista säädetään tietoyhteiskuntakaaren 272 §:ssä. Kyseisen säännöksen mukaiset toimenpiteet voivat pitää sisällään muun muassa viestin sisällön automaattisen selvittämisen, viestinen välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen sekä tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä.

Teknisiä verkkohyökkäyksiä on yleensä tehokkainta tunnistaa mahdollisimman lähellä potentiaalista hyökkäyksen kohdejärjestelmää ja järjestelmän omien ylläpitäjien toimesta. On kuitenkin tilanteita, joissa mahdollisia kohteita on paljon tai potentiaalisten kohdejärjestelmien ylläpito on ulkoistettu jollekin sellaiselle ulkomaiselle taholle, ettei yksityiskohtaista tietoa torjuntaindikaattoreista ole mahdollista luovuttaa asettamatta kansallista turvallisuutta vaaraan. Tällöin tieto hyökkäyksistä tai valmistelevista toimenpiteistä voitaisiin hankkia tietoliikennetiedustelulla.

Toteutuneen tietoturvaloukkauksen jälkeen, poikkeamaa voidaan pyrkiä tunnistamaan haittaohjelman tai haitallisen käskyn aiheuttaman liikennevirran ominaisuusjoukon perusteella. Sen sijaan torjunta ennalta ei useinkaan ole mahdollista pelkkien tietoliikenteen otsikkotietojen tai liikennevirran ominaispiirteiden nojalla, sillä tunkeutumista ennakoiva tietoliikenne pyrkii naamioitumaan tavanomaiseksi viestinnäksi. Siksi haitallisen tietokoneohjelman tai käskyn sisältävälle liikenteelle säädettäisiin sisältöhaun mahdollistava poikkeus.

Haitallisuus tarkoittaisi tässä teknisen tietoturvallisuuden vaarantumista eli tietokoneohjelmaa tai käskyä, joka pyrkii anastamaan tietoa, muuttamaan tietoa oikeudetta tai haittaamaan kohdejärjestelmän toimintaa. Kohdejärjestelmäksi katsottaisiin mikä tahansa digitaalinen järjestelmä, myös itse verkko eli tietoliikennettä ohjaavat verkkolaitteet sekä reaalimaailman prosesseja ohjaavat laitteet. Koska hakuehtona ei olisi luonnollisen kielen sana, vaan jokin tekninen merkkijono, vaatimus automaattiseen vertailuun päätyvän tietoliikenteen rajaukselle ei olisi yhtä tiukka kuin valtiollisen viestinnän semanttiseen sisältöön kohdistuvassa sisältöhaussa.

Säännöksen mukaan haitallisia tietokoneohjelmia ja -käskyjä koskevat tiedot saataisiin luovuttaa salassapitosäännösten estämättä. Tällaiset tiedot voisivat ilmeisesti olla salassa pidettäviä lähinnä viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 24 §:n 1 momentin 7 kohdan tai 9 kohdan perusteella. Ensiksi mainitun lainkohdan mukaan salassa pidettäviä ovat muun muassa tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat ja niiden toteuttamiseen vaikuttavat asiakirjat, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna turvajärjestelyjen tarkoituksen toteutumista. Haitallista tietokoneohjelmaa tai -käskyä koskevan tiedon julkiseksi tuleminen saattaisi ainakin joissain tapauksissa vaarantaa turvajärjestelyjen tarkoituksen toteutumisen, koska haitta-

ohjelmaa tai -käskyä käyttävä taho tiedon julkiseksi tulemisen myötä voisi tehdä johtopäätöksiä viranomaisten kyvykkyydestä havaita ja torjua hyökkäyksiä. Tämä puolestaan voisi johtaa siihen, että haittaohjelmaa tai -käskyä muutetaan tai edelleen kehitetään entistä vaikeammin havaittavaan suuntaan. Koska muunneltua haittaohjelmaa olisi mahdollista käyttää myös sellaiseen toimintaan, joka suoraan vaarantaa valtion turvallisuuden, saattaa salassapitoperusteena tulla kyseeseen myös viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 9 kohta. Kyseisen lainkohdan mukaan salassa pidettäviä ovat suojelupoliisin ja muiden viranomaisten asiakirjat, jotka koskevat valtion turvallisuuden ylläpitämistä, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna valtion turvallisuutta. Vaikka haittaohjelmaa koskevan tiedon julkistaminen vaarantaisi edellä mainittuja etuja, ei tiedon luovuttaminen tietoverkkohyökkäyksen kohteena olevalle yksittäiselle organisaatiolle niitä välttämättä vaarantaisi. Jos näin on, voitaisiin tieto luovuttaa kohdeorganisaatiolle kansallisen turvallisuuden suojaamiseksi tai kohdeorganisaation etujen turvaamiseksi.

Säännös olisi luonteeltaan salliva eikä velvoittava. Tiedon luovuttamista koskeva päätöksenteko perustuisi tapauskohtaiseen harkintaan ja intressipunnintaan. Joissain tilanteissa maanpuolustukseen tai kansalliseen turvallisuuteen liittyvät syyt voivat estää tiedon luovuttamisen, vaikka tiedon saaminen sinänsä olisi yrityksen tai yhteisön kannalta tarpeen, jotta se voisi turvata etunsa. Säännöksen tarkoituksena ei olisi siirtää vastuuta yritysten ja yhteisöjen tietoturvasta huolehtimisesta suojelupoliisille, vaan mahdollistaa se, että suojelupoliisi osaltaan tukee yritysten ja yhteisöjen toimenpiteitä tietoverkkohyökkäyksiltä suojautumiseksi.

Haitallista tietokoneohjelmaa tai -käskyä koskevan tiedon luovuttamiselle olisi kolme vaihtoehtoista perustetta: maanpuolustuksen turvaaminen, kansallisen turvallisuuden suojaaminen ja yrityksen tai yhteisön etu. Perusteet tiedon luovuttamiselle voisivat yhtyä tapauksissa, joissa kyse on esimerkiksi yhteiskunnan elintärkeän infrastruktuurin ylläpitämisen tai koko kansantalouden kannalta merkittävästä yrityksestä tai yhteisöstä. Perusteiden vaihtoehtoisuudesta seuraisi kuitenkin, että tieto voitaisiin harkinnan rajoissa luovuttaa siihen katsomatta, onko yrityksellä tai yhteisöllä tällaista merkitystä vai ei.

Tietojen luovuttaminen toimivaltaiselle viranomaiselle tulisi kyseeseen silloin, kun haitallista tietokoneohjelmaa tai -käskyä koskevalla tiedolla olisi laajempi merkitys yhteiskunnan kannalta. Tieto tällaisissa tilanteissa olisi parhaiten levitettävissä viranomaisten, kuten Viestintäviraston, välityksellä. Näin myös voitaisiin taata se, ettei tiedustelutoiminta vaarantuisi.

6 luku. Tiedustelutietojen ilmoittaminen eräissä tilanteissa

Sotilastiedustelutoiminnassa tiedonhankinta on laaja-alaista ja sillä hankitaan tietoja Suomea koskevasta ulkoisesta merkittävästä uhkasta. Yleistoimivalta rikosten ennalta estämisessä, selvittämisessä ja tutkimisessa on poliisilla. Sotilastiedusteltutoiminnan ensisijaisena tarkoituksena ei ole hankkia tietoja rikosten estämiseksi taikka tiedon hankkiminen rikosten valmistelusta tai suunnittelusta.

Sotilastiedustelun kohteena on toiminta, joka ei ole välttämättä rikollista toimintaa tai ei koskaan sellaiseksi muutu. Sotilastiedustelu voi kohdistua tietyn sinänsä laillisen toiminnan tarkoituksen ja taustojen selvittämiseen, kuten tiettyjen sotilaskohteiden läheisyydessä tapahtunut kiinteistökauppa.

Lisäksi sotilastiedusteluviranomaisen olisi hävitettävä kaikki tiedustelutehtävään liittymätön ylimääräinen tieto. Tämän takia sotilastiedustelussa ei lähtökohtaisesti synny tietoa tai tallenteita, jotka olisivat käytettävissä rikoksen tutkimisessa, syytteeseen saattamisessa tai rikosprosessissa.

Sotilastiedustelutehtävän suorittamisen aikana saatettaisiin joutua tilanteisiin, joissa itse tiedustelutehtävään liittymättömästi tiedustelutehtävää suorittava havaitsee tai hänen tietoon tulee tapahtu-

nut, tapahtumassa oleva tai suunniteltu rikos, josta esimerkiksi jokaisella Suomen lainkäyttöpiirissä saattaa olla ilmoitusvelvollisuus. Koska sotilastiedustelun lainmukaisena tehtävänä olisi hankkia ainoastaan tietyssä lain tarkkaan rajaamassa sotilaallisessa tarkoituksessa, tietojen ilmoittaminen muuhun käyttöön olisi oltava tarkoin rajattua ja vain tietyn kynnyksen ylittävissä tilanteissa. Tietyissä tilanteissa sotilastiedusteluviranomaiselle säädettäisiinkin velvollisuus ilmoittaa havaitsemansa tarpeelliset tiedot toimivaltaiselle esitutkintaviranomaiselle.

76 §. *Ilmoitus rikosepäilystä.* Pykälän 1 momentin mukaan sotilastiedusteluviranomaisen olisi viivytyksettä ilmoitettava toimivaltaiselle esitutkintaviranomaiselle, jos tiedustelumenetelmän käytön aika ilmenee, että on syytä epäillä rikoslain 15 luvun 10 §:ssä tarkoitettu rikos. Viranomaisista esitutkinnassa säädetään esitutkintalain (805/2011) 2 luvun 1 §:ssä.

Momentissa viitattu rikoslain 15 luvun 10 §:ssä kriminalisoidaan törkeä rikoksen ilmoittamatta jättäminen. Sitomalla sotilastiedusteluviranomaisen ilmoittamisvelvollisuus rikoslain 15 luvun 10 §:ään sotilastiedusteluviranomaiselle asetettaisiin velvollisuus ilmoitta niin sanotuista ylitörkeistä rikoksista. Ylitörkeistä rikoksista säädetty vähimmäisrangaistus on kuusi vuotta vankeutta.

Viivytyksettömyyden vaatimus sallii käytännössä enintään kolmen päivän reagointiajan. Pykälässä tarkoitettuja rikoksia ovat muun muassa murha ja ihmiskauppa. Edellä tarkoitettuja rikoksia voidaan pitää rikoksen selvittämisintressiltään ja rikosvastuun toteuttamisintressiltään niin suurina, ettei niiden kohdalla olisi hyväksyttävää jättää harkinnanvaraiseksi ilmoituksen antamista esitutkintaviranomaiselle.

Momentissa tarpeellisilla tiedoilla tarkoitetaan sotilastiedusteluviranomaisen havaintotietoja, joilla voidaan olettaa olevan merkitystä esitutkinnan käynnistämisen kannalta. Koska sotilastiedustelutoiminnassa ei olisi tarkoitus hankkia tietoja rikoksista käyttämällä tässä laissa säädettyjä toimivaltuuksia, ei sotilastiedusteluviranomaisella ole mahdollisuutta luovuttaa tiedustelutehtävän aikana syntynyttä aineistoa tai materiaalia esitutkintaviranomaiselle. Vaikka rikokseen liittyvää tietoa olisikin syntynyt tiedustelutehtävän suorittamisessa, olisi sotilastiedusteluviranomaisen hävitettävä tällainen tiedustelutehtävään liittymätön tieto välittömästi, kun se käy ilmi. Ylimääräisen tiedon hävittämisestä säädettäisiin jäljempänä.

Pykälän 2 momentissa säädettäisiin harkinnanvaraisesta ilmoituksesta esitutkintaviranomaiselle. Momentissa asetetaan lähtökohdaksi teot, joista säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta. Ilmoitus niistä rikoksista, joista säädetty enimmäisrangaistus ei ylitä kolmen vuoden rajaa, olisi aina jätettävä rikoksen selvittämisen tarkoituksessa esitutkintaviranomaiselle ilmoittamatta.

Hankinnassa tulisi suhteuttaa toisiinsa yhtäältä tiedustelutoiminnan turvaaminen, sotilastiedustelun tarkoitus hankkia tietoja sotilastiedustelun tehtävän toteuttamiseksi sekä hengen ja terveyden sekä yhteiskunnan suojaamiseen liittyviä seikkoja. Lisäksi harkinnassa olisi otettava huomioon ilmoittamisen erittäin tärkeä merkitys.

Ottaen huomioon yhtäältä 1 momentissa säädettäväksi ehdotettava ilmoitusvelvollisuus ja toisaalta tästä momentista johtuva ilmoituskielto, sotilastiedusteluviranomaiselle jäisi vähintään kolmen vuoden ja enintään kuuden vuoden seuraamusuhkaa kantavien rikosten osalta harkinnanvaraa siitä, ilmoitetaanko tällaisesta rikoksesta esitutkintaviranomaiselle vai ei.

Pykälän 3 momentin mukaan ilmoituksen tekisi tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies. Pykälän tarkoittamissa tilanteissa olisi kyse jo tapahtuneesta rikoksesta tai epäilystä. Tästä johtuen tarkoituksen mukaista olisi se, että tieto voitaisiin ilmoittaa mahdollisimman nopeasti esitutkintaviranomaiselle. Tiedustelumenetelmien käyttöön erityisesti

perehtyneillä sotilaslakimiehillä ja muilla virkamiehillä voidaan katsoa olevan riittävä osaaminen sen arvioimiseen, onko kyseessä jo tapahtunut rikos vai ei.

77 §. *Ilmoittaminen eräissä tapauksissa.* Pykälän 1 momentin mukaan sotilastiedusteluviranomaisen olisi viipymättä ilmoitettava toimivaltaiselle viranomaiselle, jos tiedustelumenetelmän käytön aikana ilmenee rikoslain 15 luvun 10 §:ssä tarkoitettu vielä estettävissä oleva rikos. Rikostorjuntaviranomaisella tarkoitettaisiin viranomaisia, joille olisi säädetty rikostorjuntatehtävä, eli poliisi, Puolustusvoimat, rajavartiolaitos ja tulli. Ilmoitus olisi tehtävä ilman aiheetonta viivytystä.

Edelleen pykälän 2 momentin mukaan tiedustelumenetelmän käytöllä saatua tietoa saisi ilmoittaa sellaisen rikoksen estämiseksi, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta. Sotilastiedusteluviranomainen saisi siis luovuttaa tietoa tiedustelumenetelmän käytön yhteydessä ilmenevistä ja vielä estettävissä olevista rikoksista rikostorjuntaviranomaiselle edellyttäen, että teosta seuraava rangaistusuhka on vähintään kaksi vuotta vankeutta. Tämän rangaistusuhkan alittavia tekoja koskisi ilmoituskielto. Rikostorjuntaviranomaiselle ilmoitettava tieto voi liittyä paitsi rikoksen estämiseen, myös sen paljastamiseen, esitutkinnan aloittamiskynnyksen selvittämiseen tai esitutkinnan suuntaamiseen.

Pykälän 3 momentin mukaan tiedustelumenetelmän käytöllä saatua tietoa saisi aina ilmaista syyttömyyttä tukevaksi selvitykseksi sekä hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi.

Kun otetaan huomioon tiedustelumenetelmällä hankitun tiedon käyttötarkoitus näissä tapauksissa, mitään lisäedellytyksiä tiedon käytölle ei ehdoteta asetettavaksi. Esitutkinnan tasapuolisuusperiaatteen sekä jokaiselle kuuluvan oikeuden oikeudenmukaiseen oikeudenkäyntiin ja henkilökohtaiseen vapauteen kannalta on selvää, että mitä suurempi vaara henkilölle on joutua pidätetyksi, vangituksi tai muun rikosoikeudellisen seuraamuksen kohteeksi virheellisin perustein, sitä vakavammin pyyntöön saada syyttömyyttä tukevaa selvitystä on suhtauduttava. Samoihin seikkoihin olisi viran puolesta kiinnitettävä huomiota myös silloin, kun sotilastiedusteluviranomainen harkitsee oma-aloitteista tiedon ilmoittamista syyttömän tueksi. Epäillyn pyyntö syyttömyyttä tukevan selvityksen saamiseksi tulisi käytännössä ohjata esimerkiksi syyttäjän kautta esitutkintaviranomaiselle, joka puolestaan kanavoisi pyynnön sotilastiedusteluviranomaiselle.

Sotilastiedusteluviranomaisen oma-aloitteinen tiedon ilmoittaminen syyttömän tueksi voisi tulla kyseeseen tilanteessa, jossa 78 §:n mukaisissa tilanteissa viranomainen ilmoittaisi sotilastiedusteluviranomaiselle esitutkinnan aloittamisesta tai rikostorjuntaan ryhtymisestä.

Momentissa tarkoitetun vaaran tai vahingon ei välttämättä tulisi liittyä rikokseen tai olla vielä rikokseksi kehittymässä, vaan kysymys saattaisi olla esimerkiksi onnettomuuden estämisestä tai yritykseen suuntautuvan laajan tietoverkkohyökkäyksen estämisestä.

Pykälän 4 momentin mukaan tiedon ilmoittamisesta päättäisi pääesikunnan tiedustelupäällikkö. Koska pykälän tarkoittamissa tilanteissa on kyse rikoksen estämisestä, jonka osalta rajanveto tiedustelutoiminnan ja rikostorjunnan välillä saattaa joissain tilanteissa olla tulkinnanvarainen, ilmoituksen antaminen voisi vaarantaa tietyissä tilanteissa tiedustelutoiminnan tai käynnissä olevan rikostorjunnan. Pääesikunnan päällikkö pystyisi parhaiten punnitsemaan eri näkökohtia liittyen rikostorjuntaan ilmoittamisesta.

Lisäsi pääesikunnan tiedustelupäällikkö pystyisi harkitsemaan etenkin 3 momentin tilanteissa sen, miten tieto esimerkiksi huomattavan varallisuusvahingon estämisestä olisi tarkoituksen mukaisinta luovuttaa.

78 §. *Ilmoitus esitutkinnan tai rikostorjunnan aloittamisesta.* Pykälän mukaan, jos esitutkintaviranomainen käynnistää esitutkinnan tai ryhtyy esitutkintatoimenpiteen käyttämiseen taikka rikostorjuntaviranomainen ryhtyy käyttämään poliisilain 5 luvussa tarkoitettuja salaisia tiedonhankintakeinoja tässä luvussa tarkoitetun ilmoituksen perustella, esitutkintaviranomaisen tai rikostorjuntaviranomaisen olisi riittävän ajoissa ennen esitutkinnan käynnistämistä, esitutkintatoimenpiteen käyttämiseen ryhtymistä tai salaisen tiedonhankintatoimenpiteen käynnistämiseen ryhtymistä ilmoitettava siitä sotilastiedusteluviranomaiselle. Pykälän tarkoituksena olisi varmistaa, että sotilastiedusteluviranomaisella säilyy tilannekuva siitä, minkälaisiin toimiin esitutkintaviranomaiset tai poliisi ovat ryhtyneet sotilastiedusteluviranomaisen niille antaman ilmoituksen perusteella. Näin varmistettaisiin myös se, että samalla tehtäväkentällä toimivat viranomaiset eivät vaikeuttaisi toistensa tehtävien hoitamista.

79 §. *Ilmoittaminen tuomioistuimen luvasta.* Pykälän mukaan sotilastiedusteluviranomaisen olisi annettava tieto lain 3 ja 4 luvun nojalla annetuista tuomioistuimen luvista tiedustelun valvontaviranomaiselle. Tiedustelutoiminnan luonteen vuoksi sekä tuomioistuimen tehtävän takia ei voida pitää tarkoituksen mukaisena, että tuomioistuin tekisi ilmoituksen tiedustelun valvontaviranomaiselle myönnetystä luvasta.

Ilmoitus olisi myös merkittävässä osassa toteutettaessa valvontaa. Valvontaviranomaisella olisi oltava ajantasainen tieto siitä, minkä tyyppisiä toimivaltuuksia sotilastiedusteluviranomainen käyttäisi milloinkin ja mihin sotilastiedusteluviranomaisen toimintaan liittyen tarkastuskäyntejä voitaisiin tehdä.

7 luku. Sotilastiedustelun suojaaminen ja turvaaminen, tietojen hävittäminen sekä tiedustelusta ilmoittaminen

80 §. *Sotilastiedustelun suojaaminen.* Pykälässä säädettäisiin sotilastiedustelun paljastumisen estämisestä. Tiedustelutehtävän suorittaminen ja tiedonhankinta, käytettävät keinot ja menetelmät on kyettävä tarvittaessa suojaamaan niiden paljastumisen estämiseksi.

Pykälän 1 momentin mukaan tiedonhankinnassa voitaisiin käyttää vääriä, harhauttavia tai peiteltyjä tietoja tiedustelutehtävän ja toimivaltuuksien käytön suojaamiseksi.

Tiedustelun suojaaminen voisi tapahtua myös tietoverkoissa, esimerkiksi erilaisten palveluiden hankinnan yhteydessä. Rekisteröityminen tiettyyn sähköiseen palveluun ja palveluiden hankkiminen saattaa edellyttää niin sanottua vahvaa sähköistä tunnistamista. Vahvan sähköinen tunniste voisi edellyttää väärien, harhauttavien tai peiteltyjen tietojen käyttöä tunnisteen saamiseksi.

Pykälän kattaisi myös tiedustelumenetelmistä tietolähteen suojaamisen tietolähteen tiedonhankinnan paljastumisen estämiseksi. Tietolähteen suojaamisessa olisi kysymys tietolähteen käytettäväksi annettavista väärien, harhauttavien tai peiteltyjen tietojen tai rekisterimerkintöjen taikka väärien asiakirjojen käytettäväksi antamisesta.

Rekisterimerkinnät voisivat olla esimerkiksi toista henkilöllisyyttä tukevia. Paljastumisriskin välttämiseksi on tärkeää, että suojeltavan toista henkilöllisyyttä tukeva tarina on mahdollisimman uskottava ja aukoton. Tilapäinen peitehenkilöllisyys ei olisi jäljitettävissä suojeltavan varsinaiseen henkilöllisyyteen, koska suojeltavan oikeus henkilöllisyys olisi lähtökohtaisesti vain Puolustusvoimien tiedustelulaitoksen tietyn virkamiehen ja pääesikunnan tiedustelupäällikön tiedossa. Kysymys ei olisi siten henkilöllisyyden vaihtamisesta, sillä suojeltavan henkilöllisyys pysyisi voimassa, vaikka suojeltava siirtyisi käyttämään peitehenkilöllisyyttä. Suojeltava voisi jälleen ottaa oikean henkilöllisyytensä käyttöönsä suojelutarpeen päätyttyä. Säännös mahdollistaisi peitehenkilöllisyyttä tukevien rekisterimerkintöjen ja asiakirjojen tekemisen esimerkiksi väestötietojärjestelmään. Säännöksen

nojalla voitaisiin tehdä tarvittavia rekisterimerkintöjä myös suojeltavan oikean henkilöllisyyden tietoihin.

Tietolähteen suojaaminen voisi tulla kyseeseen esimerkiksi tilanteessa, jossa tietolähteen pitäisi huomaamattomasti päästä liikkumaan valtion rajan yli ja tiedossa olisi, että tietolähteeseen saattaisi kohdistua konkreettinen hengen tai terveyden vaara.

Tietolähteen suojaamisessa olisi kiinnitettävä huomiota tietolähteen turvallisuuteen liittyvään opastukseen, kuten tiettyjen paikkojen välttämiseen sekä sosiaalisessa mediassa käyttäytymiseen, jotta hänen todellinen henkilöllisyytensä ei paljastuisi sivullisille. Yleiseen varovaisuuteen sisältyisi käytännössä se, että suojattava ei osallistu rikolliseen toimintaan. Tietolähteen suojaamisella ei olisi vaikutusta rikosoikeudellisen vastuun toteutumiseen, mistä syystä rikolliseen toimintaan osallistuminen saattaisi käytännössä tehdä suojelemisen mahdottomaksi, koska tällöin suojeltava joutuisi esiintymään varsinaisella henkilöllisyydellään.

Toimivalta merkintöjen tekemiseen olisi sotilastiedusteluviranomaisella, joskin merkinnät tehtäisiin käytännössä yhteistyössä asianosaisten rekisterinpitäjien kanssa rekisterin systematiikan ja teknisten ratkaisujen antamissa rajoissa. Ratkaisulla ei saatettaisi yksittäistä virkailijaa vaaraa ja toisaalta varmistettaisiin, että esimerkiksi suojattavan tietolähteen henkilötiedot ovat mahdollisimman pienen joukon tiedossa. Säännös ei mahdollistaisi merkintöjen tekemistä Puolustusvoimien tiedustelulaitoksen suorayhteydellä. Tietolähteen osalta keskeisin rekisteri olisi käytännössä väestötietojärjestelmä, joskin merkintöjä voidaan joutua tekemään muidenkin viranomaisten tai yksityisten toimijoiden rekistereihin. Kustakin yksittäisestä toimenpiteestä tulisi sopia erikseen. Käytännön yhteistyömuodot jäisivät turvallisuussyistä soveltamiskäytännössä kehitettäviksi.

Tietolähteen suojaamisen toteuttaminen onnistuneesti edellyttää käytännössä, että suojeltava tietää, mitä turvallisuusseikkoja hänen on itse jokapäiväisessä arjessaan otettava huomioon. Suunnitelmassa olisikin huomioita, miten suojeltava voi itse käyttäytymisellään myötävaikuttaa oman turvallisuutensa ylläpitämiseen. Tämä on tärkeää jo siksikin, että suojaaminen voitaisiin myös myöhemmin päättää. Tietolähteen suojaaminen voitaisiin myös päättää, jos suojattava omalla varomattomalla käyttäytymisellään tekee oman suojelunsa käytännössä mahdottomaksi.

Tietolähteen suojaamista koskevassa suunnitelmassa olisi myös huolehdittava suojattavan tavoitettavuuden käytännön toteuttamisesta. Tietolähteen peitehenkilöllisyyttä ei voida paljastaa ulkopuolisille. Suojattavalle tietolähteelle ei myöskään saa koitua perusteetonta hyötyä esimerkiksi siten, että suojattavaan kohdistuvien saatavien perintä estyisi.

Tietolähteen osalta tietyissä tapauksissa voitaisiin myös turvautua todistajansuojeluohjelmaan, josta säädetään todistajansuojeluohjelmasta annetussa laissa.

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

81 §. *Sotilastiedustelun suojaamisesta päättäminen.* Pykälän 1 momentin mukaan päätöksen tiedustelun suojaamisessa käytettävästä rekisterimerkinnästä tekisi pääesikunnan tiedustelupäällikkö.

Pykälän 2 momentin mukaan muusta tiedustelun suojaamisesta päätöksen tekisi tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

Pykälän 3 momentin mukaan pääesikunnan tiedustelupäällikkö vastaisi luetteloon tehdyistä rekisterimerkinnöistä ja valmistetuista asiakirjoista, valvottava niiden käyttöä sekä huolehdittava rekisterimerkintöjen oikaisemisesta. Tarkoituksen mukaisinta olisi, että viranomainen, joka päättää asia-

kirjojen valmistamisesta ja rekisterimerkintöjen tekemisestä, vastaa myös niitä koskevan luettelointi-, valvonta- ja oikaisuvelvoitteen täyttämisestä. Rekisterimerkinnän oikaisu olisi tehtävä, kun rekisterimerkintää ei enää tarvittaisi tiedustelun suojaamiseksi.

82 §. *Tiedustelumenetelmää käyttävän virkamiehen turvaaminen.* Pykälän 1 momentin mukaan tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää, että tiedustelumenetelmää käyttävä virkamies varustetaan kuuntelun ja katselun mahdollistavalla teknisellä laitteella, jos varustaminen on perusteltua hänen turvallisuutensa varmistamiseksi. Momentti koskisi niin sanottua turvakuuntelua ja -katselua. Salakuuntelua koskevan rangaistussäännöksen perusteella omien keskustelujen nauhoittaminen salaa ei ole rangaistavaa. Momentissa tarkoitettu laitteen käyttäminen ei muutenkaan olisi sellaista oikeudetonta toimintaa, jonka perusteella voisi seurata rangaistusvastuu salakuuntelusta tai salakatselusta. Turvakuuntelu ja -katselu saataisiin kohdistaa ainoastaan peitetoimintaa tai valeostoa toteuttavan poliisimiehen kanssa vuorovaikutuksessa oleviin henkilöihin. Ilmaisu ”kuuntelun ja katselun” tarkoittaisi sitä, että tapauksesta riippuen voitaisiin käyttää joko kuuntelun tai katselun mahdollistavaa laitetta taikka sekä kuuntelun että katselun mahdollistavaa laitetta.

Pykälän 2 momentin mukaan kuuntelu ja katselu saataisiin tallentaa. Tallenteet olisi hävitettävä heti sen jälkeen, kun niitä ei tarvita virkamiehen turvaamiseen. Jos niitä olisi kuitenkin tarpeen säilyttää asiaan osallisen oikeusturvaan liittyvistä syistä, tallenteet saataisiin säilyttää ja niitä saataisiin käyttää tässä tarkoituksessa. Tällöin tallenteet olisi hävitettävä, kun asia on lainvoimaisesti ratkaistu tai jätetty sillensä.

Momentti sisältäisi turvakuuntelu- ja katselutallenteiden säilyttämis- ja hyödyntämisrajoitukset. Tallenteita ei saisi säilyttää ja käyttää muuhun kuin säännöksessä mainittuun tarkoitukseen. Kysymys näissä tapauksissa saattaisi olla esimerkiksi siitä, että sotilastiedusteluviranomaisen virkamieheen on kohdistettu väkivaltaa tai että hän joutunut käyttämään väkivaltaa taikka että tiedustelumenetelmän käytön yhteydessä on jollekin aiheutunut vahinkoa. Näissä tapauksissa tallenteita saatettaisiin tarvita rikosasian tai vahingonkorvausasian käsittelyn yhteydessä.

83 §. *Tiedustelutietojen hävittäminen.* Säännöksen mukaan tiedustelumenetelmillä hankitut tiedot olisi hävitettävä sen jälkeen, kun on käynyt ilmi, ettei tietoa tarvita sotilastiedusteluviranomaisen tehtävien hoitamiseksi. Momentti koskisi kaikkea tiedustelumenetelmillä saatua tietoa. Sotilastiedustelun tehtävään liittymätön tieto tulisi hävittää pikaisesti. Tiedon luonteesta johtuen tulisi käydä nopeasti selville se, että sitä joko tarvitaan tai että se olisi hävitettävä. Tiedon säilyttäminen tulisi olla aina perusteltavissa sotilastiedustelun tehtäviin liittyen.

84 §. *Tiedustelutehtävään liittymättömän tiedon käyttäminen.* Pykälässä säädettäisiin tiedustelutehtävään liittymättömän tiedon käyttämisestä käynnissä olevassa toisessa tiedustelutehtävässä tai tulevaisuudessa alkavassa tiedustelutehtävässä. Tällaista tietoa voisi käyttää tilanteissa, joissa tietoa olisi saatu hankkia samalla tiedustelumenetelmällä kuin tiedustelutehtävään liittymätön tieto olisi hankittu. Jos hankittu tieto olisi hankittu tuomioistuimen lupaa edellyttämällä tiedustelumenetelmällä, tiedon käyttäminen edellyttäisi tuomioistuimen harkintaa.

Tiedustelutehtävään liittymättömän tiedon käyttämisestä päättäisi aina se taho, joka saisi tehdä päätöksen tiedustelumenetelmän käytöstä. Jos hankittu tieto olisi saatu esimerkiksi tuomioistuimen lupaa edellyttävällä tiedustelumenetelmällä, voitaisiin tällaista tietoa käyttää ainoastaan tuomioistuimen luvalla.

Tiedustelutehtävään liittymättömän tiedon säilyttämisessä olisi aina huomioitava tiedon hävittämistä koskeva sääntely ja henkilötietojen käsittelyä koskeva sääntely.

Pykälän 2 momentissa säädettäisiin informatiivisesti tiedosta, jota käytettäisiin 6 luvun tilanteissa. 6 luvussa säädetyissä tilanteissa on kyse tiedosta, joka ei liity tiedustelutehtävän suorittamiseen. Tiedustelutehtävän suorittamisen aikana saattaa kuitenkin tulla vastaan tilanteita, joissa on tapahtunut rikos tai käy ilmi, että rikokseen tullaan syyllistymään jollain todennäköisyydellä. Nämä olisivat tietoja, joita olisi arvioitava 6 luvun ilmoittamisvelvollisuuden ja -oikeuden nojalla.

85 §. *Tiedustelumenetelmän käytön lopettaminen kiiretilanteessa ja sillä saadun tiedon hävittäminen.* Pykälässä säädettäisiin kiireellisessä tilanteessa pääesikunnan tiedustelupäällikön, tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen päätöksen perusteella aloitetun lain 24, 26, 28, 30, 36, 38, 52, 58, 69 tai 71 §:ssä tarkoitetuissa tilanteissa saadun tiedon hävittämisestä, jos tuomioistuin tai muu päätöksentekijä olisi katsonut, ettei edellytyksiä tiedustelumenetelmän käytön aloittamiselle ole ollut. Tiedustelumenetelmän käyttö olisi lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot olisi hävitettävä välittömästi.

86 §. *Tiedonhankinnasta ilmoittaminen.* Pykälän 1 momentin mukaan telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta, suunnitelmallisesta tarkkailusta, peitellystä tiedonhankinnasta ja teknisestä tarkkailusta olisi viipymättä ilmoitettava tiedonhankinnan kohteelle kirjallisesti sen jälkeen, kun tiedonhankinnan tarkoitus on saavutettu ja toimenpiteen kohteena on henkilö.

Pykälässä kytkettäisiin velvollisuus ilmoittaa tiedustelun kohteelle momentissa tarkoitetun tiedustelumenetelmän käytöstä lähtökohtaisesti siihen ajankohtaan, kun tällainen tiedonhankinta on lopetettu. Vasta tämän hetken jälkeen tehtävä ilmoitus ei vaaranna käynnissä olevaa tiedonhankintaa. Ilmoitusvelvollisuus ehdotetaan sidottavaksi toiseksi siihen ajankohtaan, kun käynnissä olevan tiedonhankinnan jatkoksi valmisteltu tai suunniteltu tiedonhankinta on saatu päätettyä. Tiedonhankinnasta tulisi näin ollen ilmoittaa kohteelle viipymättä sen jälkeen, kun käynnissä olevan tai tulevan tiedusteluoperaation turvaaminen ei ole enää tarpeen.

Velvollisuus tehdä ilmoitus kohteelle kattaisi kaikki tässä momentissa tarkoitetut tiedustelumenetelmät. Tuntemattomaksi jääneelle ilmoitusta ei voitaisi luonnollisesti tehdä.

Ilmoitusvelvollisuuden piiriin kuuluisivat varsinaiset tiedonhankinnan kohteena olevat henkilöt, joiden osalta vaatimus tai päätös tiedonhankintakeinon käyttämisestä olisi tehty. Ilmoituksen tulisi olla sillä tavoin yksilöity, että kohde voi tarvittaessa pyrkiä selvittämään häneen kohdistetun tiedustelumenetelmän tai tietoliikennetiedustelun käytön perusteita.

Ilmoituksessa olisi mainittava esimerkiksi se, mistä tiedustelumenetelmästä on kysymys, sekä se, missä ja milloin sitä on käytetty. Taktisia ja teknisiä toteutustapaa koskevia yksityiskohtia ei tarvitsisi paljastaa. Ilmoitus voitaisiin tehdä kohteelle esimerkiksi kirjeitse viimeiseen tiedossa olevaan osoitteeseen. Silloin, kun tiedonhankinta on perustunut tuomioistuimen lupaan, kohteelle ilmoittamisesta olisi samalla annettava tieto myös tuomioistuimelle.

Silloin, kun tiedustelumenetelmän käyttö on tosiasiallisesti lopetettu ennen luvan tai päätöksen voimassaolon päättymistä, eikä uutta lupaa ole haettua tai jatkopäätöstä tehty, tulisi ilmoitus kohteelle tehdä tosiasiallisesta lopettamishetkestä. Siinä tapauksessa, että tiedonhankintaa jatkettaisiin jatkoluvan tai -päätöksen nojalla, tulisi ilmoitus tehdä joko tiedonhankinnan tosiasiallisesta lopettamisesta taikka uuden luvan tai päätöksen voimassaoloajan päättymisestä. Päätösten voimassaolon välillä voidaan hyväksyä muutaman päivän katkoksia, jotta tiedonhankintaa voidaan pitää yhdenjaksoisena.

Pykälän 2 momentissa säädettäisiin muuhun kuin valtiollisen toimijan tietoliikenteen tiedustelusta ilmoittamisesta. Yleisperusteluista ilmenevällä tavalla Euroopan ihmisoikeustuomioistuin on lukui-

sissa ratkaisuissaan ottanut kantaa kysymykseen siitä, tuleeko ja missä tilanteissa tiedonhankinnan kohdehenkilöllä olla oikeus saada viranomaiselta tieto häneen kohdistetusta tiedonhankintatoimenpiteestä. EIT on ratkaisukäytännössään korostanut, että tiedonhankinnan kohdehenkilön on voitava valittaa tai kannella tiedonhankintatoimenpiteestä. Valitus- tai kantelumahdollisuuden käytön edellytyksenä on yleensä se, että henkilö saa viranomaiselta tiedon häneen kohdistetusta tiedonhankinnasta sen jälkeen kun tiedonhankintakeinon käyttö on päättynyt. EIT:n ratkaisukäytännön mukaan tästä ei kuitenkaan seuraa, että ilmoitus on tehtävä välittömästi tiedonhankinnan päätyttyä. Uhka, josta tiedustelumenetelmän avulla on hankittu tietoja, voi jatkua vuosia tai jopa vuosikymmeniä, jolloin ilmoituksen tekemistä on turvallisuusviranomaisten toiminnan suojaamiseksi välttämätöntä lykätä vastaavasti. Oikeussuojakeinon käytön mahdollistamiseksi ilmoitus olisi kuitenkin tehtävä sen jälkeen, kun ilmoittamatta jättämiselle ei enää ole yksilöllistä perustetta. Kuitenkin myös järjestelmä, joka ei edellytä kohdehenkilölle ilmoittamista, voi olla sopusoinnussa ihmisoikeussopimuksen kanssa. Tällöin kanteluoikeus on tullut kansallisessa lainsäädännössä säätää niin yleiseksi, että kuka hyvänsä saa kannella pelkästään sen perusteella, että epäilee viranomaisten puuttuneen luottamuksellisen viestintänsä nauttimaan suojaan (Kennedy v. Yhdistynyt Kuningaskunta). Ehdotettavassa pykälässä velvollisuus ilmoittaa tietoliikennetiedustelusta rajattaisiin sellaisiin tapauksiin, joissa tietoliikennetiedustelun voidaan katsoa puuttuneen luottamuksellisen viestin salaisuuteen verrattain syvällisesti. Pykälän mukaisen rajatun ilmoittamisvelvollisuuden vastapainoksi tiedustelutoiminnan valvontaa koskevassa laissa (/) säädettäisiin yleisestä oikeudesta kannella tiedustelun oikeudelliselle valvontaviranomaiselle. EIT:n ratkaisukäytännössä suppeampaa ilmoittamisvelvollisuutta on pidetty hyväksyttävä, jos taho, joka kokee joutuneensa ilman perustetta tulleensa tiedustelutoimenpiteen kohteeksi, voi laajasta kannella tai muuten saattaa asiansa tutkittavaksi tiedustelusta ulkopuoliselle viranomaiselle.

Tallennettua viestintään saataisiin käsitellä automaattisesti ja manuaalisesti. Näin kerätyn tiedon jatkokäsittelyssä puolestaan saataisiin selvittää viestin välitystiedot, sijaintitiedot ja viestin sisältö. Nyt kyseessä olevassa momentissa edellytettäisiin kohteelle ilmoittamista silloin, kun tiedon manuaalinen jatkokäsittely olisi kohdistunut luottamuksellisen viestin sisältöön. Ilmoittamisvelvollisuuden olemassaolo edellyttäisi lisäksi, että manuaalinen käsittely olisi kohdistunut Suomessa olevan henkilön luottamuksellisen viestin sisältöön. Muualla kuin Suomessa olevan henkilön luottamuksellisen viestin sisällön manuaalisesta käsittelystä ei sitä vastoin olisi ilmoittamisvelvollisuutta jo yksin siitä syystä, että tämä olisi usein mahdotonta esimerkiksi kohteen oikeaa henkilöllisyyttä koskevan epätietoisuuden vuoksi tai koska henkilöllisyydeltään sinänsä tunnistetun kohteen olinpaikka ei ole tiedossa tai kohtuullisella työllä selvitettävissä.

Muuhun kuin valtiolliseen toimijaan kohdistuvan tietoliikennetiedustelun, jossa selvitetään luottamuksellisen viestin sisältö, voidaan katsoa sekä teknisessä mielessä että perusoikeuspuuttumisen syvyyden puolesta läheisesti rinnastuvan telekuunteluun. Siksi ehdotetaan, että velvollisuudet ilmoittaa edellä mainitusta kahdesta menetelmästä säädettäisiin yhdenmukaisesti.

Momentin mukaan velvollisuutta ilmoittaa tietoliikennetiedustelusta ei kuitenkaan olisi, jos tietoliikennetiedustelulla saatu tieto olisi hävitetty lain 74 §:n perusteella. Kyse olisi poikkeuksesta siihen, mitä ensimmäisessä virkkeessä olisi säädetty. Näin ollen, jos viestinnän käsittelyssä olisi selvitetty tietyn Suomessa olevan henkilön viestin sisältö, mutta samassa yhteydessä olisi havaittu heti hävitettävästä tiedosta, ja tuo heti hävitettävä tieto olisi velvollisuuden mukaisesti viipymättä hävitetty, ei velvollisuutta ilmoittamiseen olisi. Velvollisuutta ilmoittaa tietoliikennetiedustelu ei tällaisissa tapauksissa voida pitää perusteltuna, sillä sen henkilön tiedot, jolle ilmoitus olisi muuten tehtävä, olisi hävitetty tiedusteluviranomaisen hallusta.

Pykälän 3 momentin kohteelle ilmoittamisesta olisi samalla annettava kirjallisesti tieto luvan myöntäneelle tuomioistuimelle. Lupaa edellyttävän tiedustelumenetelmän kohteelle ilmoittaminen olisi siten saatettava myös Helsingin käräjäoikeuden tietoon.

Pykälän 4 momentin mukaan tuomioistuin voisi pääesikunnan tiedustelupäällikön taikka tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta päättää, että 1 momentissa tarkoitettua ilmoitusta kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedonhankinnan turvaamiseksi, Suomen sotilaallisen maanpuolustuksen, kansallisen turvallisuuden tai valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saataisiin tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä sotilaallisen maanpuolustuksen, kansallisen turvallisuuden tai valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi.

Ilmoitusta tiedonhankinnan kohteelle saataisiin lykätä tai se saataisiin jättää kokonaankin tekemättä, jos se on perusteltua valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Uuden lykkäyksen myöntäminen tulisi olla poikkeuksellista. Toistuvan ilmoittamisen lykkäämisen sijaan tulisi hakea kokonaan ilmoittamatta jättämistä, jos edellytykset ovat olemassa, koska esimerkiksi kymmenen vuoden kuluttua tehtävällä ilmoituksella ei käytännössä ole merkitystä kohteelle. Mikäli tuomioistuin ei myöntäisi lykkäystä tai päättäisi kokonaan ilmoittamatta jättämisestä, saisi vaatimuksen esittäjä kannella päätöksestä Helsingin hovioikeudelle siten kuin aiemmin tässä luvussa säädetään. Kohteella ei olisi oikeutta saada tietoa tiedonhankinnan käytöstä kantelua käsiteltäessä, ellei asian ratkaiseva tuomioistuin toisin määräisi.

Pykälän 5 momentin mukaan, jos tiedonhankinnan kohteen henkilöllisyys ei ole tiedossa 1- 2 tai 3 momentissa tarkoitetun määräajan tai lykkäyksen päättyessä, tiedonhankintakeinon käytöstä ei olisi ilmoitettava kirjallisesti hänelle ilman aiheetonta viivytystä henkilöllisyyden selvittyä.

Pykälän 6 momentin mukaan peitetoiminnasta, valeostosta, tietolähteen ohjatusta käytöstä tai paikkatiedustelusta ei olisi velvollisuutta ilmoittaa tiedonhankinnan kohteelle.

Sotilastiedustelussa ei hankittaisi tietoja rikostorjuntaan tai esitutkintaan. Mikäli tällaisia tietoja tulisi sotilastiedusteluviranomaiselle, tietoja voitaisiin antaa aiemmin 6 luvussa säädetyn menettelyn mukaisesti.

Pykälän 7 momentissa olisi viittaussäännös tuomioistuinmenettelyyn.

8 luku. Puolustusvoimien muun virkamiehen ja asevelvollisten osallistuminen sotilastiedusteluun sekä kansainvälinen toiminta

87 §. *Puolustusvoimien muun virkamiehen osallistuminen sotilastiedusteluun.* Pykälässä säädettäisiin Puolustusvoimien muun kuin sotilastiedusteluviranomaisen virkamiehen käyttämisestä sotilastiedustelussa. Puolustusvoimien joukko-osastoissa on yksiköitä, joissa palvelevat virkamiehet on koulutettu Puolustusvoimien rikostorjunnan salaisten tiedon hankintakeinojen käyttöön. Koska sotilastiedustelussa käytettäisiin samankaltaisia tiedonhankintatoimivaltuuksia, resurssien asianmukaisen käytön takia myös näitä virkamiehiä olisi voitava käyttää tilanteen niin vaatiessa.

Pykälän mukaan nämä virkamiehet olisivat aina tiedustelumenetelmiä käyttäessään sen sotilastiedusteluviranomaisen johdon ja valvonnan alaisena, jonka tiedustelutehtävän suorittamisessa pykälän tarkoittamia muita virkamiehiä käytettäisiin.

88 §. *Asevelvollisuuslain mukaisessa palveluksessa olevan reserviläisen toimivaltuudet.* Myös asevelvollisuuslain mukaisessa palveluksessa olevia reserviläisiä olisi tarvittaessa voitava käyttää tiedustelutoiminnassa. Yhteiskunnallisen tilanteen kehittyminen kohti poikkeusolojen toimivaltuuksien käyttöönotto on pitkä kestoinen prosessi, jonka aikana tietyssä tilanteessa sotilastiedusteluviranomainen saattaisi joutua hankkimaan korostetusti paljon tiedustelutietoa tilanteen kehittymisestä. Pykälän tarkoittamassa toiminnassa ei saisi käyttää varusmiespalvelustaan suorittavia asevel-

vollisia, mikä johtuisi siitä, että varusmiespalveluksen tarkoitus ei kata pykälässä tarkoittamien tehtävien suorittamista. Tämän lisäksi on huomattava, että varusmiespalvelustaan suorittavien koulutus on vielä kesken, eikä heillä ole vielä edellytyksiä suorittaa pykälässä tarkoitettuja tehtäviä.

Asevelvollisuuslain mukaisessa varusmiespalveluksessa olevien osalta on otettava huomioon heidän käyttämisensä valmiuden kohottamisessa. Näissä tilanteissa on kuitenkin otettava huomioon näiden tiedolliset ja taidolliset valmiudet erilaisten tehtävien hoitamiseen. Tämä voi tarkoittaa esimerkiksi sitä, kuinka pitkälle varusmies on ehtinyt päästä koulutuksessaan. Sotilastiedustelun tehtäviä suorittamaan kutsuttu reserviläinen saisi käyttää tässä laissa tarkoitettuja toimivaltuuksia ainoastaan sotilastiedustelun palveluksessa olevan virkamiehen ohjauksessa ja valvonnassa. Näin ollen merkittävää julkisen vallan käyttöä ei siirtyisi pykälän tarkoittamissa tilanteissa muille kuin virkamiehille.

Asevelvollisuuslain mukaisessa palveluksessa olevia reserviläisiä koskisivat samat salassapitovelvoitteet kuin heitä ohjaavia ja valvovia virkamiehiäkin, kuten jäljempänä säädettäisiin.

Pykälän 1 momentin mukaan riittävän koulutuksen saanut reserviläinen voisi avustaa sotilastiedusteluviranomaista ulkomaan tietojärjestelmätiedustelussa, tietoliikennetiedustelun kohdentamisessa ja radiosignaalitiedustelussa. Reserviläisen riittävää koulutusta arvioitaessa olisi otettava huomioon reserviläisen tiedolliset ja taidolliset valmiudet sekä se, miten pitkä aika reserviläisen saamasta koulutuksesta on ehtinyt kulua.

Tietojärjestelmätiedustelussa reserviläisen käyttäminen olisi mahdollista esimerkiksi tietojärjestelmän suojauksen ja suojauksen purkamisen mahdollistavien tietoteknisten menetelmien kehittämisessä. Itse ulkomaan tietojärjestelmätiedustelun käyttäminen olisi kuitenkin tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen käytettävissä. Kyseisen toimivaltuuden käytöllä voi olla merkittäviä vaikutuksia, joten sen käyttäminen olisi mahdollista ainoastaan sotilastiedusteluviranomaisen virkamiehelle.

Reserviläistä voitaisiin käyttää myös tietoliikennetiedustelun kohdentamisessa avustamiseen. Kyseisissä tapauksissa reserviläinen voisi käyttää hyväkseen lähinnä tietoliikenteen teknisiä tietoja ja tilastollista analyysiä, joidenka perusteella reserviläinen voisi avustaa tiedustelumenetelmien käyttöön erityisesti koulutettua virkamiestä tunnistamaan olennaiset viestintäverkon osat, joista tietoliikenteen kerääminen ja tallentaminen olisi tarkoituksen mukaisinta ja parhaiten kohdennetusti toteutettavissa. Avustavia tehtäviä suorittava reserviläinen ei saisi käsiteltäväkseen tietoliikennetiedustelussa hankittavia tietoja, kuten luottamuksellisten viestien sisältöä.

Vastaavasti kuin tietoliikennetiedustelun kohdentamisessa avustamisessa, radiosignaalistiedustelussa avustaminen kohdistuisi tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen ohjauksen ja valvonnan alaisena radiosignaalitiedustelun tekniseen toteuttamiseen, kuten radiosignaalien keräämiseen, olennaisten radiosignaalien tunnistamiseen, radiosignaalitiedustelun kohdentamiseen sekä salauksen purkuun.

Pykälän 2 momentissa säädettäisiin nopeutetussa menettelyssä kertausharjoitukseen määrätyn reserviläisen toimivaltuuksista. Nopeutetun kertausharjoituksen tilanteissa on kyse asevelvollisuuslain 32 §:n 4 momentin menettelystä. Tasavallan presidentti voi Puolustusvoimain komentajan esittelystä määrätä Suomen turvallisuusympäristössä ilmenevän välttämättömän tarpeen sitä edellyttäessä reserviin kuuluvia asevelvollisia kertausharjoitukseen sotilaallisen valmiuden joustavaksi kohottamiseksi. Turvallisuusympäristössä ilmenevä tarve voisi liittyä esimerkiksi Suomen lähialueella järjestettävään epätavanomaiseen sotilaalliseen harjoitukseen tai muuhun luonteeltaan uhkaavaksi kehittyvään tilanteeseen.

Pykälässä nimenomaisesti mainitut tiedustelumenetelmät ovat luonteeltaan sellaisia, joihin asevelvolliset ovat voineet saada riittävän koulutuksen ja perehtyneisyyden varusmiespalveluksen ja kertausharjoitusten perusteella eivätkä ne puutu luottamuksellisen viestin salaisuuden piiriin.

Pykälän 3 momentissa säädettäisiin puolustusvoimista annetun lain 47 §:n perusteella Puolustusvoimien palveluksesta eronneen kertausharjoituksessa olevan henkilön toimivaltuuksista. Edellä tarkoitetun pykälän nojalla eroamaan joutunut henkilö voi olla vielä tarpeellinen sotilastiedustelutoiminnassa ja hänelle on saattanut kertyä merkittävää osaamista sotilastiedusteluviranomaisen palveluksessa ollessaan. Tietyissä tilanteissa tätä osaamista saattaisi olla tarpeen käyttää vielä senkin jälkeen, kun henkilö on joutunut eroamaan sotilastiedusteluviranomaisen palveluksesta. Kyseeseen tulisivat ainoastaan ne henkilöt, joiden on lain nojalla erottava sotilastiedusteluviranomaisen palveluksesta.

Pykälän 4 momentin mukaan pykälässä tarkoitettu reserviläinen saisi käyttää toimivaltuuksia ainoastaan tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa.

89 §. *Reserviläisen osallistuminen kansainväliseen toimintaan.* Pykälässä säädettäisiin reserviläisen käyttämisestä kansainvälisissä tehtävissä. Pykälän tarkoittamat tilanteet eivät olisi 12 §:ssä säädettyjä sotilastiedusteluviranomaisen Suomen rajan ulkopuolella suorittamia tiedusteluoperaatioita vaan ne perustuisivat joko Suomen tekemään päätökseen antaa apua toiselle valtiolle tai Suomen sotilaallisesta kriisinhallinnasta annetun lain mukaiseen päätökseen osallistua sotilaalliseen kriisinhallintaoperaatioon. Edellä tarkoitetussa kansainvälisessä toiminnassa on tyypillistä, että osana kansallista tai monikansallista joukkoa toimii tiedusteluyksiköitä tai tiedustelu-upseereita, jotka toimivat pääasiassa operaatiota johtavan organisaation määräysten ja ohjeistuksen mukaisesti. Tiedusteluyksiköiden ja tiedustelu-upseereiden tehtävänä on tuottaa suomalaisten joukkojen toiminta-alueen toimintaympäristötietoisuutta kansallisen päätöksenteon sekä joukkojen omasuojan ja toiminnan suunnittelun tueksi.

Pykälän 1 momentin mukaan kansainvälisen avun antamisessa tai kriisinhallintaoperaation yhteydessä toimivan tiedusteluyksikön johtajana voisi toimia puolustusvoimista annetun lain 47 §:n mukaisesti sotilastiedustelunviranomaisen palveluksesta eroamaan joutunut tiedustelumenetelmien käyttöön erityisesti perehtynyt Puolustusvoimien palvelussuhteeseen otettu. Puolustusvoimista annetun lain 47 §:n mukaan sotilastiedusteluviranomaisen palveluksessa oleva henkilö saattaa joutua eroamaan sotilasvirasta jo 55-vuotiaana. Tämän jälkeen henkilö siirtyisi reserviin. Reserviläinen voidaan kuitenkin ottaa sotilaallisesta kriisinhallinnasta annetun lain mukaiseen palvelussuhteeseen tai HE 94/2016 tarkoittamaan palvelussuhteeseen kansainvälisessä avunantamisessa. Koska pykälässä tarkoitetuilla henkilöillä olisi tarvittava tiedustelutoimialan osaaminen, voitaisiin heitä käyttää kansainvälisessä toiminnassa tiedusteluyksikön johtajana ja hän voisi tehdä päätöksen 4 luvussa tarkoitettujen tiedustelumenetelmien käyttämisestä.

Pykälän 2 momentin mukaan myös muita reserviläisiä voitaisiin käyttää kasainvälisen avun antamiseen liittyvän operaation tai sotilaallisen kriisinhallintaoperaation yhteydessä toimivassa tiedusteluyksikössä. Näissä tehtävissä Puolustusvoimien palvelussuhteessa olevan henkilö saisi käyttää tiedusteluyksikön johtajan ohjauksessa ja valvonnassa 4 luvussa tarkoitettuja toimivaltuuksia.

Pykälän 3 momentin mukaan päätöksen pykälässä tarkoitetun henkilön osallistumisesta tekisi pääesikunnan tiedustelupäällikkö. Päätöksellä tarkoitettaisiin tiettyjen henkilöiden osallistumista kansainväliseen toimintaan, ei päätöstä osallistua kansainväliseen avun antamiseen tai sotilaalliseen kriisinhallintaoperaatioon. Koska kyseessä olisivat aina tiedustelumenetelmien käyttöön erityisesti perehtyneet reserviläiset, pääesikunnan tiedustelupäälliköllä olisi vastuu siitä, että kansainväliseen toimintaan osallistuvat reserviläiset olisivat riittävän perehtyneitä toimimaan puheena olevassa tehtävässä.

90 §. *Asevelvollisuuslain mukaisessa palveluksessa olevan virkavastuu.* Asevelvollisuuslain mukaisessa palveluksessa olevaan, joka käyttäisi 88 tai 89 §:ssä tarkoitettua toimivaltaa, sovellettaisiin rikosoikeudellista virkavastuuta koskevia säännöksiä.

91 §. *Asevelvollisuuslain mukaisessa palveluksessa olevan vahingonkorvausvastuu.* Edellä 89 §:ssä tarkoitetun tehtävän yhteydessä aiheutuneesta vahingosta vastaisi valtio sen mukaan kuin vahingonkorvauslaissa (412/1974) säädetään.

Pykälän 2 momentin mukaan edellä 89 §:ssä tarkoitettua tehtävää suorittavan korvausvastuuseen sovellettaisiin vahingonkorvauslain 4 luvun säännöksiä asevelvollisen korvausvastuusta.

Vahingonkorvauslain 3 luvun säännösten perusteella työnantaja on velvollinen korvaamaan vahingon, jonka työntekijä virheellään tai laiminlyönnillään työssään kolmannelle aiheuttaa (1 §:n 1 momentti). Jos joku suorittaa viranomaisen määräyksestä laissa määrättyä tehtävää olematta itsenäinen yrittäjä ja tätä tehtävää suorittaessaan virheellään tai laiminlyönnillään aiheuttaa vahinkoa, on se, jonka lukuun tehtävä suoritetaan, velvollinen korvaamaan vahingon (1 §:n 3 momentti). Varusmiestä on pidetty julkisoikeudellisessa oikeussuhteessa olevana työnsuorittajana, josta julkisyhteisö voi joutua vahingonkorvausvastuuseen.

Asevelvollisuuslain nojalla annetun tai muun vastaavan määräyksen perusteella valtion palveluksessa olevalla henkilöllä on vahingonkorvauslain 4 luvun 2 §:n 2 momentin mukaan sama vastuu kuin virkamiehellä ja työntekijällä. Sotilas on velvollinen korvaamaan vahingosta määrän, joka harkitaan kohtuulliseksi ottamalla huomioon vahingon suuruus, teon laatu, vahingon aiheuttajan asema, vahingon kärsineen tarve sekä muut olosuhteet. Erityisasemassa ovat pykälän 3 momentin mukaan ne sotilaat, jotka ovat tuottaneet vahingon ollessaan vastuussa sotaväen aluksesta tai ilma-aluksesta.

Edellä sanottu merkitsee myös mahdollisuutta vahingonkorvauksen sovitteluun huomioon ottaen muun muassa vahingon suuruus, teon laatu ja vahingon aiheuttajan asema. Jos hänen viakseen jää vain lievä tuottamus, ei vahingonkorvausta tuomita. Tahallisen rikoksen ollessa kyseessä pääsääntönä on täyden korvauksen tuomitseminen. Valtion oikeus regressioon vahingonaiheuttajalta on 4 luvun 3 §:n mukaan niin ikään rajoitettu.

Valtion isännänvastuun ulottaminen myös 88 ja 89 §:ssä tarkoitetuissa tehtävissä oleviin henkilöihin edellyttää säännöksen ottamista tähän lakiin. Vahingonkorvauslakia ei näin ollen tarvitsisi muuttaa.

9 luku. Ilmaisukielto, yksityisiä yhteisöjä koskevat velvollisuudet ja oikeudet sekä tietojen saanti eräiltä tahoilta

92 §. *Ilmaisukielto.* Pykälän 1 momentin mukaan sivullinen, joka olisi auttanut sotilastiedusteluviranomaista tiedustelutehtävän toteuttamisessa, ei saisi ilmaista tiedustelutehtävään liittyvää tietoa tai seikkaa. Edellytyksenä on, että sivullinen on avustanut sotilastiedusteluviranomaista tehtävänsä tai asemansa johdosta tai häntä on pyydetty avustamaan tiedustelutehtävän toteuttamisessa. Tilanteissa ei olisi kyse sotilastiedustelussa saatujen tietojen ilmaisemisesta sivullisille, vaan tavoitteena on huolehtia siitä, ettei tiedustelu paljastu liian varhaisessa vaiheessa. Lisäksi tavoitteena olisi suojata sotilastiedustelun salassa pidettäviä taktisia ja teknisiä menetelmiä.

Esimerkkinä momentin tarkoittamasta tilanteesta voitaisiin mainita asunto-osakeyhtiön huollosta vastaavaa huoltoyhtiön edustaja, jota pyydetään avaamaan taloyhtiön yhteisten tilojen lukituksia teknisen havainnoinnin laitteen asentamiseksi. Sotilastiedustelutoiminta olisi kuitenkin aina lähtökohtaisesti pyrittävä suorittamaan niin, ettei sen paljastumisvaaraa ole.

Pykälän 2 momentin mukaan rangaistus ilmaisukiellon rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teosta muualla laissa säädetä ankarampaa rangaistusta.

93 §. *Teleyrityksen avustamisvelvollisuus.* Pykälän 1 momentin mukaan teleyrityksen olisi tehtävä ilman aiheetonta viivytystä televerkkoon telekuuntelun ja televalvonnan edellyttämät kytkennät sekä annettava poliisiviranomaisen käyttöön telekuuntelun toimeenpanoa varten tarpeelliset tiedot, välineet ja henkilöstö. Sama koskisi myös niitä tilanteita, joissa telekuuntelu tai televalvonta toteutetaan sotilastiedusteluviranomaisen toimesta teknisellä laitteella. Teleyrityksen olisi lisäksi annettava sotilastiedusteluviranomaisen käyttöön hallussaan olevat telekuuntelun tai televalvonnan toimeenpanoa varten tarpeelliset tiedot. Telekuuntelu ja televalvonta voitaisiin toteuttaa myös sotilastiedusteluviranomaisen omilla laitteilla.

Voimassa olevien toimivaltasäännösten mukaan poliisilla on oikeus käyttää telekuuntelua ja televalvontaa. Sotilastiedustelussa käytettäisiinkin samaa teknistä ratkaisua ja järjestelmää, mitä poliisi käyttää. Tämä tarkoittaisi sitä, ettei toista vastaavaa telekuuntelun ja televalvonnan mahdollistavaa järjestelmää tarvitsisi rakentaa ainoastaan sotilastiedusteluviranomaisen toimivaltuuksia varten.

Pykälän mukaan teleyrityksen olisi annettava sotilastiedusteluviranomaisen käyttöön telekuuntelun ja televalvonnan toimeenpanoa varten tarpeelliset tiedot, välineet ja henkilöstö. Pykälä vastaisi asiallisesti poliisilain 5 luvun 61 §:n 1 momenttia.

94 §. *Tiedonsiirtäjän avustamisvelvollisuus.* Pykälässä säädettäisiin tiedonsiirtäjän avustamisvelvollisuudesta. Avustamisvelvollisuus koostuisi liityntäpisteen toteuttamisesta sekä sellaisten tiedonsiirtäjän hallussa olevien tietojen antamisesta Puolustusvoimien tiedustelulaitokselle, joilla olisi merkitystä tietyn Suomen rajan ylittävän viestintäverkon osan tunnistamisessa.

Pykälän 1 momentissa säädettäisiin tiedonsiirtäjän myötävaikuttamisvelvollisuudesta. Momentin mukaan tiedonsiirtäjän olisi yhteistyössä Puolustusvoimien tiedustelulaitoksen kanssa velvollisuus myötävaikuttaa tietoliikennetiedustelun edellyttämien liityntäpisteiden toteuttamiseen Puolustusvoimien tiedustelulaitokselle. Lisäksi tiedonsiirtäjällä olisi oikeus osallistua liityntäpisteiden toteuttamisen edellyttämiin toimenpiteisiin. Liityntäpisteen tarkoituksena on mahdollistaa Puolustusvoimien tiedustelulaitoksen pääsy tuomioistuimen luvan mukaiseen tiedonsiirtäjän Suomen rajan ylittävään tietoliikenneyhteyteen.

Myötävaikuttamisella tarkoitettaisiin yhteistyötä liityntäpisteen toteuttamisessa. Käytännössä tämä tarkoittaisin Puolustusvoimien tiedustelulaitoksen ja tiedonsiirtäjän suunnitelmaa siitä, miten liityntäpiste olisi tarkoituksenmukaisinta teknisesti toteuttaa. Lisäksi tiedonsiirtäjällä olisi oikeus osallistua liityntäpisteen edellyttämiin toimenpiteisiin.

Liityntäpisteellä tarkoitettaisiin teknistä ratkaisua, johon tehdystä liitynnästä Puolustusvoimien tiedustelulaitokselle voitaisiin ohjata tuomioistuimen luvassa tarkoitetussa Suomen rajan ylittävässä viestintäverkon osassa kulkeva tietoliikenne. Liityntää hallinnoisi kytkennänsuorittaja.

Liityntäpiste olisi tarkoituksen mukaisinta toteuttaa mahdollisimman lähellä sitä tiedonsiirtäjän omistamaa tai hallinnoimaa viestintäverkon osaa, joka ylittää Suomen rajan. Käytännössä tämä ei aina ole tarkoituksen mukaista, joten tiedonsiirtäjän myötävaikutuksella liityntäpiste voitaisiin toteuttaa myös muussa tarkoituksen mukaisessa kohdassa tiedonsiirtäjän omistamaa tai hallitsemaa viestintäverkkoa.

Momentin tarkoittama myötävaikuttaminen ja yhteistyö olisi liityntäpisteen toteuttamisen lähtökohtana ja Puolustusvoimien tiedustelulaitoksen olisi ensisijaisesti tunnistettava tiedonsiirtäjä ja oltava yhteydessä tähän liityntäpisteen toteuttamisen osalta.

Pykälän 2 momentissa säädetyissä tilanteissa olisi kyse tilanteista, joissa liityntäpistettä ei voitaisi toteuttaa tiedonsiirtäjän myötävaikutuksella ja osallistumisella. Kyseessä olisi poikkeus 1 momentin säännöksestä. Käytännössä tilanne tulisi vastaan silloin, kun Puolustusvoimien tiedustelulaitoksen yrityksistä huolimatta tiedonsiirtäjä ei ryhtyisi aktiivisiin toimenpiteisiin liityntäpisteen toteuttamiseksi.

Lisäksi säännöksen alaan kuuluisivat tilanteet, joissa Puolustusvoimien tiedustelulaitoksen aktiivisista yrityksistä huolimatta tiedonsiirtäjää ei pystytä tavoittamaan.

Pykälän 3 momentissa säädettäisiin tiedonsiirtäjän velvollisuudesta antaa Puolustusvoimien tiedustelulaitokselle sellaiset halussaan olevat tiedot, jotka ovat tarpeen viestintäverkon osan yksilöimiseksi tietoliikennetiedustelun käyttöä koskevaa lupavaatimusta ja -päätöstä varten. Velvollisuus liittyy tietoliikennetiedustelun tuomioistuimen lupia koskevan 67 §:n 3 momentin 2 kohtaan, 69 §:n 3 momentin 3 kohtaan sekä 71 §:n 3 momentin 5 kohtaan, jonka mukaan Puolustusvoimien tiedustelulaitoksen olisi tuomioistuimelle esittämässään lupavaatimuksessaan yksilöitävä se viestintäverkon osa, jossa kulkevaan tietoliikenteeseen tietoliikennetiedustelun automaattisia hakuehtoja verrattaisiin. Jotta viestintäverkon osa voitaisiin lupavaatimusta varten yksilöidä, olisi välttämätöntä, että Puolustusvoimien tiedustelulaitos saisi yksilöintiä edistäviä tietoja niiltä tahoilta, joilla sellaisia liiketoimintaansa liittyvistä syistä on hallussaan. Tietojen antamisvelvollisuudesta säätämällä voitaisiin ehkäistä se, että hakuperusteinen vertailu tulisi kohdistumaan tietoliikenteeseen laajemmin kuin on välttämätöntä sotilastiedustelun tarkoituksen mukaisesti. Jos tiedonsiirtäjän hallussa olevat tiedot osoittaisivat, että tiedonhankinnan kohteena oleva toimintaa koskeva tietoliikenne ei voi liikkua jossain tietyssä viestintäverkon osassa esimerkiksi sen vuoksi, että se on varattu jonkin tietoliikennetiedustelun kohteena olevan toiminnan kannalta epäolennaisen asiakasorganisaation käyttöön, ei tuo viestintäverkon osa voisi olla tietoliikennetiedustelua koskevan lupavaatimuksen piirissä.

Momentin tarkoittamat tietoliikennetiedustelun kohdentamiseksi tarpeelliset tiedot koskisivat ennen kaikkea sitä, mitkä asiakasorganisaatiot ovat varanneet tiedonsiirtäjältä siirtokapasiteettia käyttöönsä ja mitä tiedonsiirtäjän hallitsemia rajan ylittävän viestintäverkon osia tällaiset varaukset koskevat. Momentti velvoittaisi tiedonsiirtäjän antamaan tietoja myös muista mahdollisista seikoista, jotka vaikuttavat tietoliikenteen reitittymistodennäköisyyteen sen ylittäessä Suomen rajan tiedonsiirtäjän omistamassa tai muuten hallitsemassa viestintäverkon osassa. On syytä korostaa, että momentti velvoittaisi tiedonsiirtäjän antamaan tietoja vain siltä kapasiteettia varanneista asiakasorganisaatioista, ei sen sijaan viestintätapahtumien osapuolena olevista kuluttaja-asiakkaistaan. Pykälä ei muutenkaan perustaisi Puolustusvoimien tiedustelulaitokselle oikeutta hankkia tai saada tietoja yksittäisistä viestintätapahtumista tai sellaisten osapuolina olevista henkilöistä.

Momentin säännös velvoittaisi tiedonsiirtäjän antamaan Puolustusvoimien tiedustelulaitokselle sellaiset tiedot, jotka ovat tietoliikennetiedustelun kohdentamiseksi tarpeellisia. Tietojen tarpeellisuutta koskeva vaatimus sisältäisi sen, että tiedonsiirtäjän olisi annettava Puolustusvoimien tiedustelulaitokselle kaikki sellaiset tiedot, joilla voi olla merkitystä tietoliikennetiedustelun mahdollisimman tarkan kohdentamisen kannalta. Toiselta puolen tietojen tarpeellisuudelle asettavasta vaatimuksesta seuraisi, ettei tiedonsiirtäjä olisi velvoitettu antamaan Puolustusvoimien tiedustelulaitokselle mitään sellaisia hallussaan olevia tietoja, joilla ei voi olla merkitystä kohdentamisen kannalta. Lisäksi säännöksen nojalla tiedonsiirtäjä ei olisi velvollinen Puolustusvoimien tiedustelulaitoksen vaatimuksesta luomaan kohdentamisen kannalta merkityksellisiä raportteja tai hankkimaan muuta tietoa, mitä sillä ei olisi jo muuten hallussa tai mitä tiedonsiirtäjä ei liiketoimintaansa liittyen muuten tuottaisi.

Tiedonsiirtäjän velvollisuus antaa tietoja koskisi ainoastaan sellaisia tietoja, jotka sillä valmiiksi on hallussaan. Säädettäväksi ehdotettava tietojenantovelvollisuus ei näin ollen velvoittaisi tiedonsiirtä-

jiä hankkimaan tai keräämään Puolustusvoimien tiedustelulaitokselle varten sellaisia uusia tietoja, jotka sinänsä voisivat olla tarpeen tietoliikennetiedustelun kohdentamiseksi.

Avustamisvelvollisuus edellyttäisi Puolustusvoimien tiedustelulaitoksen yksilöityä pyyntöä. Pyynnössä Puolustusvoimien tiedustelulaitoksen olisi esitettävä ne tiedot, joiden perusteella tiedonsiirtäjä voisi arvioida, mitkä sen hallussa olevat tiedot voisivat olla tarpeen Tietyn Suomen rajan ylittävän viestintäverkon osan määrittelemiseksi. Pyyntö ei voisi koskea epäämäräistä rajoittamatonta tietojoukkoa, vaan Puolustusvoimien tiedustelulaitoksen olisi pyynnössä rajattava tilannetta, jota koskevia tietoja tiedonsiirtäjän olisi annettava avustamisvelvollisuuden nojalla.

95 §. *Korvaus teleyritykselle.* Pykälän 1 momentissa säädettäisiin, että teleyrityksellä on oikeus saada valtion varoista korvaus tässä luvussa tarkoitetusta viranomaisten avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista, kuten tietoyhteiskuntakaaren 299 §:ssä säädetään. Kustannusten korvaamisesta päättäisi Puolustusvoimat.

96 §. *Korvaus tiedonsiirtäjälle.* Pykälässä säädettäisiin tiedonsiirtäjälle tietojen antamisesta aiheutuneiden kustannusten korvaamisesta sekä korvauspäätöksen tekijästä.

Pykälän momentin mukaan tiedonsiirtäjällä olisi oikeus saada valtion varoista korvaus 95 §:ssä tarkoitetusta avustamisesta aiheutuneista välittömistä kustannuksista. Momentissa tarkoitettuja välittömät kustannukset olisivat pääasiassa työvoimakustannuksia. Välittömiä kustannuksia voisivat myös olla tietoja koostettaessa hyödynnettävien teknisten laitteistojen ynnä muiden apuvälineiden käytöstä aiheutuvat kustannukset. Korvauksen maksamisesta päättäisi Puolustusvoimien tiedustelulaitos. Puolustusvoimien tiedustelulaitos ratkaisisi näin ollen sen, mitkä kustannukset ovat välittömiä ja tulevat korvattavaksi. Puolustusvoimien tiedustelulaitos myös määrittäisi korvauksen suuruuden.

Pykälä kattaisi myös tietoliikennetiedustelun teknisestä toteuttamisesta suojelupoliisin puolesta aiheutuvat kustannukset. Näissäkin tapauksissa Puolustusvoimien tiedustelulaitos määrittäisi sen, mitkä kustannukset tulisivat korvattavaksi.

97 §. *Muutoksenhaku korvauspäätökseen.* Pykälässä säädettäisiin muutoksenhausta teleyritykselle tai tiedonsiirtäjälle maksettavaan korvaukseen. Muutosta voisi hakea vaatimalla oikaisua sotilastiedusteluviranomaisen tekemään päätökseen päätöksen tekijältä.

Pykälän 2 momentin mukaan oikaisuvaatimukseen tehtyyn päätökseen voisi hakea muutosta valittamalla siitä hallinto-oikeuteen siten kuin hallinlainkäyttölaissa (586/1996) säädetään.

Pykälän 3 momentin mukaan hallinto-oikeuden päätöksestä saisi valittaa korkeimpaan hallinto-oikeuteen, jos korkein hallinto-oikeus antaa valitusluvan.

Pykälän 4 momentin mukaan Viestintävirastolle olisi annettava tilaisuus tulla kuullut asian hallinto-oikeuskäsittelyssä.

98 §. *Kytkennän suorittamisen maksullisuus.* Pykälän mukaan kytkennän suorittaja voisi periä kytkennän suorittamisesta maksuja Puolustusvoimien tiedustelulaitokselta. Maksujen suuruus ei kuitenkaan saisi ylittää suoritteen tuottamisesta kytkennän suorittajalle aiheutuvien kokonaiskustannusten määrää (omaskustannusarvo). Omakustannusarvoa laskettaessa lähtökohtana voitaisiin käyttää esimerkiksi valtion maksuperustelain (150/1992) 6 §:n 1 momentissa tarkoitetun omakustannusarvon laskentaperusteita.

Maksujen suorittaminen olisi tarkoituksen mukaista osoittaa Puolustusvoimien tiedustelulaitokselle, joka toimii tietoliikennetiedustelun teknisenä toteuttajan myös suojelupoliisille. Suojelupoliisin on

toimitettava saamansa tuomioistuimen lupa Puolustusvoimien tiedustelulaitokselle, joka toteuttaa tietoliikennetiedustelun teknisen tietojen hankinnan ja toimittaa keräämänsä materiaalin käsittelemättömänä suojelupoliisille. Prosessin osana Puolustusvoimien tiedustelulaitoksen olisi ilmoitettava kytkennän suorittajalle ne Suomen rajan ylittävät viestintäverkon osat, joista tietoliikennettä hankittaisiin.

99 §. *Teleyrityksen säilyttämien tietojen käyttäminen.* Pykälässä säädettäisiin teleyrityksen velvollisuudesta säilyttää tietoyhteiskuntakaaren 157 §:n 1 momentissa tarkoitetut tiedot myös sotilastiedustelua varten.

100 §. *Tietojen saanti yksityiseltä yhteisöltä tai henkilöltä.* Pykälän 1 momentin mukaan sotilastiedusteluviranomaisella olisi tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimies tai muun virkamiehen pyynnöstä oikeus saada rikoksen estämiseksi tai selvittämiseksi tarvittavia tietoja yhteisön jäsentä, tilintarkastajaa, toimitusjohtajaa, hallituksen jäsentä tai työntekijää velvoittavan yritys-, pankki- tai vakuutussalaisuuden estämättä sellaisia tietoja, joiden yksittäistapauksessa voitaisiin olettaa olevan tarpeen 4 §:ssä tarkoitetun toiminnan selvittämisessä ja joilla voidaan olettaa olevan merkitystä: 1) sotilastiedustelun kohteena olevan henkilön tai oikeushenkilön tunnistamiseksi, 2) tiedustelumenetelmän käytön kohdentamiseksi tiettyyn henkilöön, tai 3) henkilön tai oikeushenkilön taloudellisen toiminnan selvittämiseksi.

Momentti vastaisi tarkoitukseltaan hyvin pitkälle, mitä poliisilain 4 luvun 3 §:n 1 momentissa säädetään. Tässä yhteydessä tietopyynnön kohteena ei kuitenkaan olisi rikoksen estäminen tai selvittäminen, vaan tietopyyntö olisi sidottu edellä 4 §:ssä tarkoitettuihin sotilastiedustelun kohteisiin. Tämän takia pykälässä mainittaisiin, että tietopyynnön kohteena olevilla tietojen voitaisiin olettaa olevan tarpeen 4 §:ssä tarkoitetun toiminnan selvittämisessä.

Toiminnan selvittämistä koskevalla ilmaisulla ei tarkoitettaisi rikoksen selvittämistä esitutkintalain mukaisessa merkityksessä, vaan kyse olisi yksilöidyn sotilastiedustelun kohteena olevan toiminnan selvittämisestä. Selvittämisellä tarkoitettaisiin siten tietojen kokoamista keräämällä tietoa eri lähteistä ja pykälässä tarkoitettu tietopyyntö olisi yksi keino kerätä sotilastiedustelun kohteista merkityksellistä tietoa.

Momentti sisältäisi tuloksellisuusodotukseen rinnastettavat edellytykset. Tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen olisi otettava edellytykset huomioon harkitessaan tietopyyntöä. Vaikka tietopyynnön esittäjällä ei olisi tiedon luovuttajaa kohtaan perusteluvelvollisuutta, hänen tulisi perustaa tietopyyntöään koskeva harkintansa objektiivisiin seikkoihin ja kirjata se asiasta, jotta tietopyynnön asianmukaisuus olisi laillisuusvalvonnan keinoin mahdollista jälkikäteen varmentaa.

Säännöksen tarkoituksena olisi mahdollistaa yksityiselle taholle tiedon luovuttaminen ilman, että tämä syyllistyisi rangaistavaksi säädettyyn tekoon. Yritys-, pankki- ja vakuutussalaisuuden alaisen tiedon luovuttaja voisi luovuttaessaan sotilastiedusteluviranomaiselle tiedon olla vakuuttunut, että hän toimisi sallitulla tavalla.

Pankkisalaisuudesta säädetään luottolaitostoiminnasta annetun lain (610/2014) 14 §:ssä ja vakuutussalaisuudesta vakuutusyhtiölain (521/2008) 30 luvun 1 §:ssä. Yrityssalaisuus on rikoslain 30 luvun 11 §:ssä määritelty niin, että sillä tarkoitetaan liike- tai ammattisalaisuutta taikka muuta vastaavaa elinkeinotoimintaa koskevaa tietoa, jonka elinkeinonharjoittaja pitää salassa ja jonka ilmaiseminen olisi omiaan aiheuttamaan taloudellista vahinkoa joko hänelle tai toiselle elinkeinonharjoittajalle, joka on uskonut tiedon hänelle. Merkityksellistä kuitenkin on, että puheena oleva säännös oikeuttaisi edellä kerrotun vaitiolovelvollisuuden piiriin kuuluvan tiedon luovutuksen sotilastiedusteluviranomaiselle.

Yrityksillä on runsaasti yrityssalaisuuden piiriin kuuluvia omalle elinkeinotoiminnalleen merkityksellisiä tietoja, kuten tuotekehitystietoja. Pykälän perusteella yrityksellä ei olisi velvollisuutta luovuttaa sotilastiedusteluviranomaiselle yrityssalaisuuden ytimeen kuuluvia tietoja, vaan tietopyynnössä olisi lähtökohtaisesti kyse asiakas-, työntekijä- tai muussa taloudellisessa suhteessa olevien tahojen yksilöivistä tiedoista.

Tietopyynnön yksittäistapauksellisuutta olisi arvioitava tiedonhankinnan kohteena olevan sotilastiedustelun kohteen kannalta. Näin ollen yksittäistapauksellisuus ei rajoittaisi tietopyyntöjen määrää saman sotilastiedustelun kohteena olevan toiminnan kohdalla. Yksittäistapauksellisuus voisi tarkoittaa tarvittaessa useampia tietopyyntöjä kyseistä toimintaa.

Pyynnön kohteena olevilla tiedoilla tulisi 1 kohdan mukaan perustellusti voida olettaa merkitystä sotilastiedustelun kohteena olevan henkilön tai oikeushenkilön tunnistamiseksi. Tällä tarkoitettaisiin sitä, että sotilastiedustelun kohteena oleva henkilö voitaisiin saatavilla tiedoilla oletettavasti tunnistaa tai tämän toimintaa muutoin selvittää esimerkiksi hotellien majoituslistan tai laivan matkustajalistan perusteella. Pykälän 2 kohdan mukaan pyynnön perusteena voisi olla tiedustelumenetelmän käytön kohdentaminen tiettyyn henkilöön. Tämä tarkoittaisi esimerkiksi pyynnön osoittamista vähittäismyyntiliikkeelle koskien pre paid -liittymän ostoa ja sen ostajaa. Pykälän 2 kohta koskettaisi muun muassa pankkitiedusteluja sekä muita luottolaitoksille tai rahavälitystoimijoille tehtäviä tietopyyntöjä.

Pykälän 2 momentin mukaan sotilastiedusteluviranomaisella olisi pyynnöstä yksittäistapauksessa oikeus saada teleyritykseltä ja yhteisötilaajalta yhteystiedot sellaisesta teleosoitteesta, jota ei mainita julkisessa luettelossa, taikka teleosoitteen tai telepäätelaitteen yksilöivät tiedot, jos tiedot ovat tarpeen sotilastiedusteluviranomaisen tiedustelutehtävän suorittamiseksi. Sotilastiedusteluviranomaisella olisi vastaavasti oikeus saada postitoimintaa harjoittavalta yhteisöltä jakeluosoitetietoja.

Sääntely vastaisi asiallisesti poliisilain 4 luvun 3 §:ää. Kyseessä olisi sellainen tiedustelutoimintaan liittyvä tavanomainen toimenpide, joka ei edellyttäisi sotilaslakimiehen tai tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen pyyntöä.

10 luku. Sotilastiedustelun tietojärjestelmä ja muut henkilörekisterit

Lakiehdotuksen 10 lukua sovellettaisiin sotilastiedusteluviranomaisen laissa säädettyjen tehtävien suorittamiseksi tarpeellisten henkilötietojen käsittelyyn. Lisäksi luvussa säädettäisiin sotilastiedusteluviranomaisen oikeudesta saada rekistereistä ja muista tietojärjestelmistä henkilötietoja sille laissa säädettyjen tehtävien suorittamiseksi, rekisteritietojen käsittelystä ja luovuttamisesta.

Yleinen tietosuoja-asetus korvaa vuoden 1995 henkilötietodirektiivin (95/46/EY) ja sen kansalliseksi täytäntöön panemiseksi annetun henkilötietolain (523/1999) säännökset niiltä osin kuin henkilötietojen käsittely kuuluu asetuksen soveltamisalaan. Oikeusministeriössä on vireillä lainsäädäntöhanke henkilötietojen suojaa koskevan kansallisen lainsäädännön tarkistamiseksi. Hankkeessa arvioidaan henkilötietolain toimivuus henkilötietojen käsittelyä sääntelevänä yleislakina ja erityissäännösten tarpeellisuus ja merkitys. Oikeusministeriö on tammikuussa 2017 asettanut työryhmän, jonka tehtävänä on laatia ehdotus tietosuojadirektiivin kansallista täytäntöönpanoa koskevaksi yleiseksi lainsäädännöksi samoin kuin ehdotukset direktiivin edellyttämistä muutoksista oikeusministeriön hallinnonalan lainsäädäntöön. Työryhmän tulee myös selvittää, voidaanko yleistä lainsäädäntöä soveltaa sellaiseen toimintaan, joka jää tietosuojadirektiivin ja tietosuoja-asetuksen soveltamisalan ulkopuolelle, mutta jonka sääntely on perusteltua sovittaa yhteen turvallisuusviranomaisia koskevan muun sääntelyn kanssa.

Myös eri ministeriöiden hallinnonaloille kuuluvat säännökset on saatettava tietosuoja-asetuksen mukaisiksi asetuksen mahdollistaman kansallisen liikkumavaran puitteissa. Puolustusministeriö on

elokuussa 2016 asettanut työyöryhmän, jonka tehtävänä on selvittää henkilötietojen käsittelyä puolustushallinnossa koskevan lainsäädännön muutostarpeet ja valmistella ehdotus tarvittaviksi säädösmuutoksiksi. Sotilastiedustelun henkilörekistereitä koskevat säännökset sovitetaan yhteen edellä mainittujen vireillä olevien säädöshankkeiden kanssa.

101 §. *Sotilastiedustelun tietojärjestelmä.* Pykälässä säädettäisiin sähköisestä sotilastiedustelun tietojärjestelmästä. Rekisterissä voisi myös manuaalisia osia, kuten kortistoja. Poikkeusolojen sekä normaaliolojen vakavien häiriötilanteiden varalta tai tietoturvasyistä olisi tarkoituksenmukaista, että sotilastiedustelun tietojärjestelmä ei olisi yksinomaan sähköisen tietojärjestelmän varassa vaan sitä kyettäisiin tarvittaessa käyttämään osin myös manuaalisesti.

Pykälän 1 momentissa säädettäisiin sotilastiedustelun tietojärjestelmän käyttötarkoituksesta ja rekisterinpitäjästä. Sotilastiedustelun tietojärjestelmä olisi sotilastiedusteluviranomaisten eli pääesikunnan ja Puolustusvoimien tiedustelulaitoksen käyttöön tarkoitettu pysyvä henkilörekisteri, jonka rekisterinpitäjä olisi pääesikunta.

Tietojärjestelmästä olisi 2 momentin mukaan käytävä ilmi tiedon tallettaja. Tämä olisi tarpeen esimerkiksi henkilöstön vaihtuvuuden ja tiedon jäljitettävyyden vuoksi.

102 §. *Sotilastiedustelun tietojärjestelmän tietosisältö.* Pykälässä säädettäisiin tietojärjestelmään talletettavista henkilötiedoista. Henkilötietolain 3 §:n 1 momentin 1 kohdan mukaan henkilötiedolla tarkoitetaan kaikenlaista luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

Termien ”käsitellä” ja ”yhdistää” katsottaisiin pitävän sisällään myös tietojen keräämisen ja tallettamisen, sekä talletetun tiedon analysoinnin. Henkilöä koskevia tietoja sotilastiedustelun tietojärjestelmässä saisi käsitellä ja yhdistää vain silloin kun se olisi tarpeen sotilastiedusteluviranomaisen tässä laissa säädetyn tehtävän suorittamiseksi.

Tietojärjestelmän yhtenä käyttötarkoituksena olisi järjestelmään talletettujen tietojen yhdistäminen sekä sen pohjalta mahdollisesti tehtävä arviointi. Silloin esimerkiksi tieto, joka ei yksinään olisi henkilötietolaissa tarkoitettu henkilötieto, voisi yhdistettynä muuhun tietoon muuttua sellaiseksi.

Tietojärjestelmään voitaisiin tallentaa myös muita kuin henkilötietoja.

Pykälän 2 momentti sisältäisi tyhjentävän luetteloa tietojärjestelmään talletettavista henkilötiedoista. Tiedot on ryhmitelty kymmeneen pääryhmään. Asianmukaisilla ja riittävillä pohjatiedoilla kyettäisiin kohdentamaan esimerkiksi salaisten tiedustelumenetelmien käyttö oikein.

Pykälän 2 momentin 2 kohdassa tarkoitettuja muita tunnistetietoja 1 kohdassa tarkoitetun henkilötunnuksen lisäksi olisivat esimerkiksi henkilön nimi, syntymäaika, sukupuoli, äidinkieli, henkilöä koskevat ääni- ja kuvatallenteet kuten valokuvat, tieto henkilön kuolemasta tai kuolleeksi julistamisesta ja henkilön fyysisiin ominaisuuksiin perustuvat tunnistetiedot kuten tuntomerkit, pituus, paino tai silmien väri. Henkilön nimillä tarkoitettaisiin väestörekisteriin merkittyä sukunimeä ja etunimiä, entisiä etu- ja sukunimiä ja puhuttelunimiä.

Pykälä 2 momentin 3 kohdassa tarkoitettuja kansalaisuutta koskevia tietoja olisivat henkilön kansalaisuus, entinen kansalaisuus, kansalaisuudettomuus ja kansallisuus. Perhesuhteita koskevilla tiedoilla tarkoitettaisiin siviilisäätyä, perhesuhteita, ulkomaalaisen henkilön vanhempien nimiä ja osoitteita. Asuinpaikkatietoja olisivat kotikunta- ja kotipaikkatiedot.

Pykälän 2 momentin 5 kohdassa tarkoitettuja koulutusta ja ammattia koskevia tietoja olisivat myös tiedot työ- ja palvelushistoriasta. Pykälän 2 momentin 6 kohdassa tarkoitettuja yhteystietoja olisivat osoite, puhelinnumero ja muut yhteystiedot.

Matkustamiseen liittyvät tarpeelliset tietoja olisivat matkustusasiakirjan tiedot ja muut maahantuloon ja rajanylittämiseen liittyvät tarpeelliset tiedot kuten esimerkiksi jäljempänä 110 §:ssä tarkoitetut lentoliikenteen matkustajatiedot.

Muita henkilön tai oikeushenkilön yksilöimiseksi tai hänen turvallisuutensa kannalta tarpeellisia tietoa voisivat olla viranomaisen antama asiakasnumero, henkilöä koskevat hänen oman turvallisuutensa tai Puolustusvoimien työturvallisuuden kannalta välttämättömät tiedot ja oikeushenkilön yksilöimiseksi tarpeelliset tiedot.

Viranomaisen antamalla asiakasnumerolla tarkoitettaisiin esimerkiksi ulkomaalaisen henkilön tunnistamiseksi Maahanmuuttoviraston tietojärjestelmän antamaa, rekisteriin talletetuille ulkomaalaisille henkilölle annettua asiakasnumeroa, jolla Suomen viranomaiset yksilöivät kyseisen henkilön.

Rekisteriin voitaisiin tallentaa myös henkilöä koskevat hänen oman turvallisuuden tai Puolustusvoimien työturvallisuuden kannalta välttämättömät tiedot, joiden etsintä eri viranomaisten rekistereistä on hankalaa tai epävarmaa ja jotka kuvaavat kohteen tai henkilön vaarallisuutta tai arvaamattomuutta.

Sen mukaisia henkilötietoja ovat tiedot jotka kuvaavat tai on tarkoitettu kuvaamaan rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta taikka henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä. Henkilön vaarallisuus työturvallisuusriskinä voi ilmetä aggressiivisuutena tai käsittää vaarallisen tai helposti tarttuvan taudin.

Henkilön omaa turvallisuutta taas palvelevat tiedot sairauksista, joiden oireet muistuttavat esimerkiksi humalatilaa tai sairaudet, jotka edellyttävät säännöllistä tai kohtauksissa vaadittavaa lääkitystä. Puolustusvoimilla ei olisi tämän pykälän nojalla oikeutta pyytää terveydentilatietoja esimerkiksi lääkintäviranomaisilta, vaan tiedot kirjattaisiin, kun ne tulevat esiin henkilön itsensä kertomana tai tehtävän yhteydessä.

Pykälän 2 momentin 9 kohdassa tarkoitettuja tunnistamistiedot määriteltäisiin edellä 9 §:n 7 kohdassa. Tunnistamistiedot olisivat sellaisia viestiä koskevia tietoja kuten esimerkiksi IP-osoitteita, jotka voitaisiin Pykälä 2 momentin 3 kohdassa tarkoitettuja yhdistää viestintäpalvelun tilaajaan tai käyttäjään.

Sotilastiedusteluviranomaisella olisi tarvetta tallentaa rekisteriin myös muita tietoja henkilön toiminnasta tai käyttäytymisestä. Sellaisia voisivat olla esimerkiksi tiedot henkilön yleisistä elämäntavoista, harrastuksista ja muista kiinnostuksen kohteista.

Rekisterissä olisi lisäksi 3 momentin mukaisesti tietoja henkilön tai yrityksen luotettavuuden selvittämisestä. Tällä tarkoitettaisiin tietoja turvallisuusselvityksistä annetussa laissa (726/2014) tarkoitetusta pääesikunnan tekemästä perusmuotoisesta turvallisuusselvityksestä taikka laajasta tai suppeasta turvallisuusselvityksestä, selvityksen kohteena olevan henkilön tunnistetietoja sekä mainitun selvityksen antamisaikaa.

103 §. *Sotilastiedustelun tietojärjestelmän käyttöoikeus*. Tietojärjestelmää saisivat käyttää sotilastiedustelun virkamiehet, jotka on määrätty hoitamaan tässä laissa tarkoitettuja tiedustelutehtäviä.

Käyttöoikeus voitaisiin sotilastiedusteluviranomaisen oman päätöksen perusteella antaa myös asevelvollisuuslain nojalla palvelustaan suorittavalle asevelvolliselle eli kertausharjoituksessa ole-

valle reserviläiselle tai varusmiehelle niin normaalioloissa, normaaliolojen vakavissa häiriötilanteissa kuin poikkeusoloissa. Tietojärjestelmän käyttö ja tietojen käsittely tapahtuisivat kuitenkin aina virkamiehen johdon ja valvonnan alaisena. Asevelvollisten osallistumisesta sotilastiedusteluun sekä siihen liittyvästä virkavastuusta ja vaitiolovelvollisuudesta säädettäisiin 8 luvussa.

104 §. *Tilapäiset henkilörekisterit.* Tiedustelutehtävissä olevien virkamiesten käyttöön voitaisiin perustaa automaattisen tietojenkäsittelyn avulla tai manuaalisesti ylläpidettäviä tilapäisiä henkilörekistereitä. Tilapäiset henkilörekisterit olisi tarkoitettu tiettyjen yksittäisten tiedustelutehtävien tai tehtäväkokonaisuuksien yhteydessä perustettaviksi väliaikaisiksi rekistereiksi. Kyse olisi siis lyhyempiaikaisesta tietojen yhdistelemisestä, analysoinnista tai muusta käsittelystä eikä tietojen säännönmukainen tallentaminen sotilastiedustelun tietojärjestelmään olisi tarkoituksenmukaista.

Jos tehtävän aikana kävisi ilmi, että tietojen käsittely tai säilyttäminen olisi tarpeen pitempiaikaisesti, talletettaisiin tiedot sotilastiedustelun tietojärjestelmään 101 §:ssä säädetyin edellytyksin. Pykälä vastaisi pääosin eri viranomaisten tilapäisiä henkilörekistereitä koskevaa voimassaolevaa sääntelyä.

Pykälän 2 momentissa säädettäisiin tilapäisen henkilörekisterin käyttötarkoituksesta, rekisteriin talletettavista tiedoista sekä rekisterin käyttöoikeudesta Tilapäisessä henkilörekisterissä saisi käsitellä vain tiedustelutehtävän tai tehtäväkokonaisuuden suorittamiseksi välttämättömiä henkilötietoja. Tilapäisen henkilörekisterin käyttöoikeus olisi niillä virkamiehillä, joiden käyttöön rekisteri on perustettu. Kuten 101 §:ssä tarkoitetusta sotilastiedustelun tietojärjestelmästä, myös tilapäisestä henkilörekisteristä tulisi käydä ilmi tiedon tallettaja.

Pykälän 3 momentissa säädettäisiin tilapäisen henkilörekisterin rekisterinpitäjästä. Valtakunnallisen tilapäisen henkilörekisterin rekisterinpitäjä olisi pääesikunta. Jos kyse ei olisi valtakunnallisesta tilapäisestä henkilörekisteristä, olisi rekisterinpitäjänä toiminnasta vastaava Puolustusvoimien hallintoyksikkö.

Tilapäisen henkilörekisterin perustamisesta päättäisi pykälän 4 momentin mukaan valtakunnallisen rekisterin osalta pääesikunta ja muun kuin valtakunnallisen tilapäisen henkilörekisterin osalta toiminnasta vastaava hallintoyksikkö. Rekisterin perustamisesta tehtäisiin kirjallinen päätös. Valtakunnallisessa käytössä olevien tilapäisten henkilörekisterien osalta rekisterin perustamista koskevasta päätöksestä ja sen olennaisesta muuttamisesta olisi ilmoitettava viimeistään kuukautta ennen rekisterin perustamista tai muuttamista tietosuojavaltuutetulle. Perustamispäätöksessä olisi mainittava henkilörekisterin käyttötarkoitus.

105 §. *Arkaluonteisten tietojen käsittely*. Myös henkilötietolain 11 §:ssä tarkoitettuja arkaluonteisia henkilötietoja voitaisiin käsitellä sotilastiedustelun tietojärjestelmässä ja muussa tässä luvussa säädetyssä henkilörekisterissä tietyin rajoituksin. Arkaluonteiset henkilötiedot olisi poistettava tietojärjestelmästä välittömästi, kun niiden käsittely ei olisi enää tehtävän kannalta välttämätöntä.

Pykälässä säädettäisiin tässä laissa tarkoitettuihin henkilörekistereihin sisältyvien arkaluonteisten henkilötietojen käsittelystä. Arkaluonteisten tietojen käsittely on henkilötietolain 11 §:n mukaan lähtökohtaisesti kielletty. Henkilötietolain 12 §:n mukaan käsittelykielto ei kuitenkaan estä esimerkiksi tietojen käsittelyä, josta säädetään laissa tai joka johtuu välittömästä rekisterinpitäjälle säädetystä tehtävästä.

Ehdotettu pykälä vastaisi pääpiirteissään arkaluonteisten tietojen käsittelyä koskevaa henkilötietojen käsittelytä poliisitoimessa annetun lain (761/2003) 10 §:ää.

Henkilötietolain 11 §:n mukaan arkaluonteisina tietoina pidetään henkilötietoja, jotka kuvaavat tai on tarkoitettu kuvaamaan rotua tai etnistä alkuperää, henkilön yhteiskunnallista, poliittista tai us-

konnollista vakaumusta tai ammattiliittoon kuulumista, rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta, henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia, henkilön seksuaalista suuntautumista tai käyttäytymistä taikka henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.

Ehdotetun pykälän mukaan rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta koskevan henkilötietolain 11 §:n 3 kohdassa tarkoitetun arkaluonteisen tiedon saisi kerätä ja tallettaa sotilastiedusteluviranomaisen henkilörekistereihin ja muuten käsitellä silloin, kun se on rekisterin käyttötarkoituksen kannalta tarpeellinen. Sen sijaan muiden henkilötietolain 11 §:ssä tarkoitettujen arkaluonteisten tietojen kerääminen, tallettaminen ja muu käsittely olisi sallittua ainoastaan silloin, kun se on yksittäisen tiedustelutehtävän suorittamiseksi välttämätöntä.

Kuitenkin henkilön terveydentilaa kuvaavia ja muita henkilötietolain 11 §:n 4 kohdassa tarkoitettuja tietoja saisi kerätä, tallettaa ja käsitellä myös silloin, kun se on rekisteröidyn oman turvallisuuden taikka viranomaisen työturvallisuuden varmistamiseksi välttämätöntä.

106 §. *Henkilön fyysisiin ominaisuuksiin perustuvien tunnistetietojen tietoturva.* Pykälässä säädettäisiin henkilön fyysisiin ominaisuuksiin perustuvien biometristen tunnisteiden käsittelyn tietoturvallisuudesta sotilastiedustelun henkilörekistereissä. Tällaisia biometrisiä tunnisteita ovat esimerkiksi ihmisen sormenjäljet, kasvot ja ääni. Vastaavan tyyppisiä säännöksiä ovat esimerkiksi henkilötietojen käsittelystä poliisitoimessa annetun lain 10 a § ja henkilötietojen käsittelystä Tullissa annetun lain (639/2005) 10 §.

Tunnistamiseen soveltuva biometrinen ominaisuus on pysyvä, muuttumaton ja peruuttamaton osa yksilöä. Tästä syystä biometriset tunnisteet asettavat erityisiä vaatimuksia tietoturvalle, jotta sen, jonka biometrisiä ominaisuuksia talletetaan tai käsitellään, yksityisyyden suojan toteutuminen voitaisiin varmistaa. Biometrisen tunnistamisen haasteet liittyvät tunnisteen pysyvyyteen. Biometristä tunnistetta ei voi vaihtaa, vaan se sitoo käyttäjänsä tunnistettuun identiteettiin mahdollisesti koko elinajaksi. Biometrisen ominaisuuden sähköinen (digitaalinen) tallenne on lisäksi helposti ja nopeasti kopioitavissa ja siten levitettävissä nykyisten tietojenkäsittelylaitteiden ja tietoverkkojen avulla. Tästä syystä pidetään tarkoituksenmukaisena säätää erikseen biometristen tunnistetietojen erityisistä tietoturvavaatimuksista etenkin kun yleisiä säännöksiä biometristen tunnisteiden käytöstä ei toistaiseksi ole. On tärkeää, että myös sotilastiedusteluviranomaisen henkilörekistereihin sisältyvät henkilön fyysisiin ominaisuuksiin perustuvat tunnistetiedot suojataan siten, että niiden oikeudeton luku ja käyttö voidaan estää.

Pykälän 1 momentin mukaan tallettaessaan tai muutoin käsitellessään sähköisessä muodossa olevia henkilön fyysisiin ominaisuuksiin perustuvia tunnistetietoja rekisterinpitäjän tulisi erityisesti huolehtia näiden tunnistetietojen tallettamisen ja muun käsittelyn tietoturvasta. Henkilön fyysisiin ominaisuuksiin perustuvien tunnistetietojen tietoturvasta huolehtiminen tarkoittaisi hallinnollisia ja teknisiä toimia, joilla varmistettaisiin se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla ja ettei tietoja voida muuttaa muiden kuin siihen oikeutettujen toimesta. Henkilön fyysisiin ominaisuuksiin perustuvien tunnistetietojen turvaaminen tapahtuu tiedon ominaisuuksien turvaamisen kautta. Tiedon käytettävyys tai saatavuus tarkoittaa sitä, että tiedot ja tietojärjestelmien palvelut ovat tiedonsaantiin oikeutettujen henkilöiden käytettävissä silloin, kun nämä työtehtävissään tietoja tarvitsevat. Käytettävyydellä tarkoitetaan lisäksi helppokäyttöisyyttä. Eheys tai aitous puolestaan sitä, että tiedot ovat oikeita ja ajan tasalla sekä yhtäpitäviä kaikkialla organisaatiossa eikä ehyttä tietoa ei ole oikeudettomasti tai tahattomasti muutettu ja mahdolliset muutokset ovat todennettavissa. Tiedon luottamuksellisuus tarkoittaa sitä, että tiedot ovat vain niiden henkilöiden saatavissa ja käytössä, jotka niitä työtehtävissään tarvitsevat ja jotka ovat oikeutettuja tietoja käsittelemään.

Pykälän 2 momentissa täsmennettäisiin 1 momentissa tarkoitettua tallettamisen ja muun käsittelyn tietoturvaa. Momentin mukaan henkilön fyysisiin ominaisuuksiin perustuvia tunnistetietoja talletettaessa ja muutoin käsitellessä olisi huolehdittava siitä, että tunnistamisessa ja tunnistetietojen käsittelyssä käytettävät tietojärjestelmät, laitteet ja ohjelmistot ovat turvallisia, sekä siitä, että tunnistetiedot on suojattu asiattomalta pääsyltä sekä tunnistetietojen luottamuksellisuuteen ja eheyteen kohdistuvilta loukkauksilta, muutoksilta ja väärentämiseltä sekä muulta vahingossa tai laittomasti tapahtuvalta käsittelyltä. Tunnistamisessa ja tunnistetietojen käsittelyssä olisi muutoinkin ehdotuksen mukaan toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet sen varmistamiseksi, että tunnistaminen ja tunnistetietojen käsittely voidaan toteuttaa tietoturvallisella ja yksityisyyden suojan turvaavalla tavalla.

Pykälän 3 momentin mukaan rekisterinpitäjä vastaisi edellä kuvatusta tietoturvasta myös sellaisen kolmannen osapuolen osalta, joka rekisterinpitäjän toimeksiannosta joko kokonaan tai osittain toteuttaa fyysisiin ominaisuuksiin perustuvien tunnistetietojen tallettamisen. Rekisterinpitäjä vastaisi erityisesti siitä, että toimeksisaajalla on sama velvollisuus suojata tiedot kuin rekisterinpitäjällä sekä siitä, ettei toimeksisaajalla ole muuta oikeutta käsitellä tietoa. Käsittelyllä tarkoitettaisiin tässä tapauksessa henkilötietolain 3 §:n 1 momentin 2 kohdan mukaista käsittelyä, eli muun muassa tiedon keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista ja tuhoamista.

107 §. *Yksittäiseen tehtävään liittymättömien henkilötietojen käsittely ja käyttäminen.* Pykälässä säädettäisiin yksittäiseen tehtävään liittymättömien tietojen käsittelystä tässä laissa tarkoitetun tiedustelutehtävän tai tehtäväkokonaisuuden suorittamiseksi.

Pykälän 1 momentin mukaan yksittäiseen tehtävään liittymättömillä tiedoilla tarkoitettaisiin yksittäisen tiedustelutehtävän tai tehtäväkokonaisuuden suorittamisen yhteydessä saatuja sotilastiedusteluviranomaiselle tarpeellisia tietoja, jotka eivät liittyisi kyseiseen tai muuhun jo suoritettavaan tehtävään tai tehtäväkokonaisuuteen. Tällaisia tietoja olisi tarpeen vaatiessa välttämätöntä käsitellä ja yhdistää, sillä sotilastiedustelun tiedonhankinta on usein pitkäkestoista työtä, jossa pienetkin yksityiskohdat voivat osoittautua myöhemmin merkittäviksi.

Tiedoilla ei tarkoitettaisi tiedustelumenetelmillä saatuja tietoja, joista säädettäisiin erikseen jäljempänä. Tietojen tallentaminen olisi mahdollista sotilastiedustelun tietojärjestelmään ja tilapäiseen henkilörekisteriin niillä edellytyksillä kuin kyseisiä rekistereitä koskevissa tämän lain pykälissä säädetään.

Pykälän 3 momentin mukaan tietojen käsittelyn perustetta ja tarpeellisuutta on arvioitava vähintään kolmen vuoden välein. Tietoja talletettaessa olisi niihin mahdollisuuksien mukaan liitettävä arvio tietojen antajan luotettavuudesta ja tietojen oikeellisuudesta. Arvio tehdään noudattaen kansainvälistä mallia ja kriteeristöä, jota nykyisin käytetään muun muassa kriisinhallintaoperaatioissa. Tämä tukisi mm. tiedon analysointia ja sotilastiedustelun uhka-arvioiden laatimista. Lisäksi sillä olisi merkitystä tehtävien hoitajien vaihtuessa. Tiedot poistettaisiin, kun tieto on todettu sen käyttötarkoituksen kannalta tarpeettomaksi.

108 §. *Oikeus saada tietoja rekistereistä ja tietojärjestelmistä.* Sotilastiedusteluviranomaisen tässä laissa säädettyä tiedustelutehtävää tai tehtäväkokonaisuutta hoitavilla virkamiehillä olisi oikeus salassapitosäännösten estämättä saada ja käsitellä tehtävien suorittamisen kannalta välttämättömiä tietoja.

Sotilastiedusteluviranomaisella olisi salassapitosäännösten estämättä oikeus saada viranomaiselta, julkista tehtävää hoitamaan asetetulta tai yksityiseltä yhteisöltä kaikki tarvitsemansa välttämättömät tiedot säännöksessä yksilöityjen tehtäviensä suorittamiseksi ja viranomaisen henkilörekisterien ylläpitämiseksi.

Sotilastiedustelulle ehdotetaan verrattain laajoja tiedonsaantioikeuksia eri viranomaisten ja muiden tahojen ylläpitämistä rekistereistä. Tietojen saannilla ja käytettävyydellä olisi erittäin tärkeä merkitys erityisesti henkilötiedustelun toimivaltuuksia käytettäessä, mutta niiden merkitys voisi korostua myös toimivaltuuksien käyttöä ja tiedonhankintaa suojattaessa. Riittävän kattavat tiedonsaantioikeudet takaisivat esimerkiksi avustajan turvallisen käyttämisen tehtäviin ja niillä tuettaisiin peitetoiminnan toteuttamista.

Rekistereitä, joista sotilastiedusteluviranomainen, voisi saada tietoja, ei nimenomaisesti yksilöitäisi säännöksessä. Sotilastiedusteluviranomaisella olisi tarve saada tietoja esimerkiksi väestötietojärjestelmästä, sakkorekisteristä ja oikeushallinnon valtakunnallisesta tietojärjestelmästä, ulkomaalaisrekisteristä, passirekisteristä, ulkoasiainministeriön tietojärjestelmistä, Tullin rekistereistä, ajoneuvoliikennerekisteristä, matkustajia koskevista henkilöluetteloista, asevelvollisuusrekisteristä ja muista puolustusministeriön hallinnonalan rekistereistä, kriisinhallintahenkilöstörekisteriin, verohallinnon, maahanmuuttoviraston ja rikosseuraamuslaitoksen rekistereistä. Tietoja voitaisiin saada myös poliisin tietojärjestelmistä.

Tietojen luovutusvelvollisuus rekisterinpitäjällä olisi siitä huolimatta, että hänellä olisi johonkin säännökseen perustuva niitä koskeva salassapitovelvollisuus. Tietoa pyytäessään sotilastiedusteluviranomainen suorittaisi pyydettäviä tietoja koskevan harkinnan siitä, että tieto on välttämätön kyseiseen käyttötarkoitukseen.

Säännös asettaisi rekisterinpitäjille velvollisuuden luovuttaa sotilastiedusteluviranomaiselle säännöksessä tarkoitetut pyydetyt tiedot, jotka sotilastiedusteluviranomaisella on kyseisestä rekisteristä oikeus saada. Tietojen luovuttamisen tavasta olisi edelleen sovittava asianomaisen rekisterinpitäjän kanssa. Tiedot voidaan luovuttaa myös teknisen käyttöyhteyden avulla tai muuten sähköisesti.. Julkisuuslain 29 §:n 3 momentin mukaan salassa pidettävien tietojen luovuttaminen viranomaiselta toiselle teknisen käyttöyhteyden avulla ei voi tapahtua pelkästään kyseisen lain yleisen säännöksen nojalla, vaan tietojen luovuttaminen edellyttää kohdehenkilön suostumusta tai lain säännöstä. Myös perustuslakivaliokunta on lausuntokäytännössään katsonut, että teknisen käyttöyhteyden avaaminen henkilörekisteriin edellyttää, että tällaisesta luovuttamisesta säädetään laissa (PeVL 12/2002 vp).

Käytännössä tietojen sähköinen luovuttaminen edellyttää, että osapuolet yhdessä määrittelevät käyttöyhteyden, sopivat sen toteuttamisesta ja avaamisesta sekä varmistuvat siitä, että tietoja koskevat suojaamis- ja huolellisuusvelvoitteet ja muut tietojen luovuttamista koskevat lainsäädännön vaatimukset täyttyvät asianmukaisesti. Jos henkilörekisteriä ei ole järjestetty automaattisen tietojen käsittelyn avulla, olisi rekisterinpitäjän annettava tarvittavat tiedot tilanteeseen soveltuvalla muulla osapuolten sopimalla tarkoituksenmukaisella tavalla.

Tiedot saisi luovuttaa teknisen käyttöyhteyden avulla ja maksutta.

109 §. *Tietojen saanti viranomaiselta.* Sotilastiedusteluviranomaisella olisi oikeus saada viranomaiselta ja julkista tehtävää hoitamaan asetetulta yhteisöltä ja henkilöltä virkatehtävän suorittamiseksi tarpeelliset tiedot ja asiakirjat maksutta ja salassapitovelvollisuuden estämättä, jollei sellaisen tiedon tai asiakirjan antamista tai tietojen käyttöä todisteena olisi laissa kielletty tai rajoitettu. Säännös olisi yhdenmukainen henkilötietojen käsittelystä rajavartiolaitoksessa annetun lain 17 §:n kanssa.

110 §. *Liikkeenharjoittajan velvollisuus lentomatkustajia koskevien tietojen antamiseen.* Lentoliikenteen harjoittajan eli ammattimaisesti henkilöiden kuljetusta ilmateitse harjoittavan luonnollisen henkilön tai oikeushenkilön olisi pyynnöstä toimitettava lentoliikenteen matkustajatiedot. Tiedot olisi luovutettava sähköisesti tai muulla asianmukaisella tavalla. Sotilastiedusteluviranomainen saisi käsitellä lentoliikenteen matkustajatietoja tässä laissa säädetyn tehtävän suorittamiseksi.

Luovutettavia tietoja olisivat matkustusasiakirjan numero ja tyyppi, kansalaisuus tai kansalaisuudettomuus, koko nimi, syntymäaika, rajanylityspaikka, jonka kautta henkilö saapuu jäsenvaltioiden alueelle tai lähtee jäsenvaltioiden alueelta, kuljetuksen koodi, kuljetuksen lähtö- ja saapumisaika, kuljetukseen kuuluvien henkilöiden kokonaismäärä ja alkuperäinen lähtöpaikka.

111 §. *Tietojen luovuttaminen sotilasviranomaiselle.* Rekisterin tietoja voitaisiin erityisissä tapauksissa käyttää muuhun kuin tietojen keräämis- ja tallentamistarkoitukseen. Rekisterinpitäjällä olisi oikeus salassapitosäännösten estämättä luovuttaa muulle sotilasviranomaiselle kuin sotilastiedusteluviranomaiselle sotilastiedustelun tietojärjestelmän ja tilapäisen henkilörekisterin tietoja, jos se olisi tarpeen Puolustusvoimille laissa säädettyjen tehtävien suorittamiseksi. Tietojen luovutukselle olisi kuitenkin asetettu verrattain korkea kynnys, sillä tietoja saisi luovuttaa vain silloin, kun se olisi tarpeen valtion turvallisuuden varmistamiseksi tai välittömän henkeä tai terveyttä uhkaavan vaaran taikka huomattavan omaisuusvahingon torjumiseksi. Tällaisia tilanteita voisivat olla esimerkiksi alueellisen koskemattomuuden valvontaan tai sen turvaamiseen liittyvät tehtävät taikka lain puolustusvoimien virka-avusta poliisille (781/1980) 4 §:ssä tarkoitettu sotilaallisten voimakeinojen käyttöä edellyttävä virka-apu.

Tiedot saisi luovuttaa myös teknisen käyttöyhteyden avulla tai muuten sähköisesti.

112 §. *Tietojen luovuttaminen suojelupoliisille.* Rekisterinpitäjä saisi luovuttaa salassapitosäännösten estämättä sotilastiedustelun tietojärjestelmästä ja muista henkilörekistereistä henkilötietoja muille kuin Puolustusvoimien viranomaisille. Oikeus luovuttaa henkilötietoja rajattaisiin koskemaan vain suojelupoliisia ja suojelupoliisin tiedustelutehtävää. Velvollisuudesta ja oikeudesta ilmoittaa tietoja rikostorjuntaviranomaisen toiminnan suuntaamiseksi säädettäisiin 6 luvussa.

Tiedot saisi luovuttaa myös teknisen käyttöyhteyden avulla tai muuten sähköisesti siten, kuin siitä rekisterinpitäjän kanssa sovitaan. Käytännössä sähköinen luovuttaminen olisi harvinaista.

113 §. *Tietojen luovuttaminen vaaran tai vahingon estämiseksi*. Pykälän 1 momentin mukaan rekisterinpitäjä saisi salassapitosäännösten estämättä luovuttaa rekisterissä olevia henkilötietoja hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi.

Tämä voisi koskea tilanteita, joissa sotilastiedusteluviranomaisen tietoon olisi tiedustelutehtävää suoritettaessa tullut esimerkiksi merkittävä kansallista tietoturvaa uhkaava tapahtuma, jolla voisi olla mittavia haitallisia vaikutuksia kansan- tai liiketaloudellisille eduille.

Pykälän 2 momentin mukaan toiselta viranomaiselta saatuja tietoja saisi luovuttaa vain tiedot luovuttaneen viranomaisen suostumuksella. Viranomaisen tulee tietoja luovuttaessaan kyetä arvioimaan ovatko siltä pyydetyt tiedot sellaisia, että ne voidaan luovuttaa pyytäjälle. Arviointiin voisi vaikuttaa esimerkiksi se, ovatko tiedot luovutettavissa edelleen.

114 §. *Tietojen luovuttamisesta päättäminen.* Tietojen luovutuksesta päättäisi pääsäännön mukaan rekisterinpitäjä. Tällä perusteella tietojen luovuttamisesta esimerkiksi sotilastiedustelun tietojärjestelmästä päättäisi pääesikunta kun taas tiedon tilapäisestä henkilörekisteristä voisi luovuttaa esimerkiksi rekisterin ylläpidosta vastaava alueellinen hallintoyksikkö. Tiedon luovuttamisesta teknisen käyttöyhteyden avulla tai tietojoukkona päättäisi aina pääesikunta, myös silloin, kun tilapäisen henkilörekisterin ylläpitäjänä olisi Puolustusvoimien muu hallintoyksikkö.

115 §. *Tietojen poistaminen sotilastiedustelun tietojärjestelmästä.* Tietojärjestelmästä poistettaisiin henkilöä koskevat tiedot 50 vuoden kuluttua viimeisen tiedon merkitsemisestä. Tietojen säilytysaika olisi poikkeuksellisen pitkä. Esimerkiksi turvallisuustietorekisteristä, joka on rikosten ennalta estämistä ja paljastamista koskevia tehtäviä hoitavien Puolustusvoimien virkamiesten käyttöön

tarkoitettu pysyvä henkilörekisteri, poistetaan henkilöä koskevat tiedot 25 vuoden kuluttua viimeisen tiedon merkitsemisestä.

Sotilastiedustelutoiminnassa tuotettavat analyysit ja ennakkovaroituskyvyn ylläpitäminen saattavat edellyttää henkilötietojen rekisteröintiä huomattavasti pidemmällä aikavälillä kuin mitä esimerkiksi rikostorjunnassa. Rikostorjunnan aikajänne voidaan poikkeuksetta sitoa yhteen muun muassa tekoja koskevien vanhentumissäännösten kanssa. Sotilastiedustelussa, jossa ei ole kyse rikoksesta, rikoksen estämisestä tai paljastamisesta, tämä ei ole mahdollista. Tuotettavat tiedot ja niistä tehtävä analyysi tulisikin käsittää syklinä, joka tietoa tuottaessaan synnyttää lähes aina mahdollisia uusia tietotarpeita.

Tietojen käsittelyn perustetta ja tarpeellisuutta tulisi kuitenkin arvioida säännöllisesti viiden vuoden välein. Tietojen uudelleen arvioinnista tehtäisiin rekisteriin merkintä. Tieto, joka ei enää olisi sotilastiedusteluviranomaisen tiedustelutehtävän kannalta tarpeellista, tulisi poistaa rekisteristä, ellei tietoa olisi tarpeen siirtää arkistoon. Pykälä vastaisi pääpiirteissään muiden viranomaisten vastaavantyyppistä voimassaolevaa sääntelyä.

116 §. *Tietojen poistaminen tilapäisestä henkilörekisteristä.* Tilapäisestä henkilörekisteristä poistettaisiin henkilöä koskevat tiedot kun tieto on todettu rekisterin käyttötarkoituksen kannalta tarpeettomaksi. Pykälä vastaisi pääpiirteissään muiden viranomaisten vastaavaa sääntelyä.

Tietojen perustetta ja käsittelyn tarpeellisuutta olisi arvioitava vähintään kolmen vuoden välein ja tietojen uudelleen tarkastamisesta tehtäisiin merkintä.

Sotilastiedusteluviranomaisen käyttöön perustettu tarpeettomaksi käynyt tilapäinen henkilörekisteri olisi hävitettävä, jollei sitä siirrettäisi arkistoitavaksi.

117 §. *Henkilötunnuksen käsittely.* Henkilötunnusta saisi käsitellä rekisteröidyn antamalla suostumuksella tai silloin kun se olisi välttämätöntä sotilastiedusteluviranomaisen tiedustelutehtävän kannalta.

Sotilastiedusteluviranomaisen on huolehdittava siitä, että henkilötunnusta ei merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

118 §. *Tarkastusoikeuden rajoitus.* Rekisteröidyn tarkastusoikeudesta säädetään henkilötietolain 26-28 §:ssä. Rekisteröidyllä ei olisi tarkastusoikeutta sotilastiedustelun tietojärjestelmään eikä tässä luvussa tarkoitettuun tilapäiseen henkilörekisteriin. Tietosuojavaltuutettu voisi kuitenkin rekisteröidyn pyynnöstä tarkastaa sotilastiedustelun tietojärjestelmään ja tilapäiseen henkilörekisteriin talletettujen rekisteröityä koskevien tietojen lainmukaisuuden. Säännökset vastaisivat muiden viranomaisten vastaavaa sääntelyä.

119 §. *Tietojen luovuttaminen kansainvälisessä yhteistyössä.* Pykälässä säädettäisiin henkilötietojen luovuttamisesta sotilastiedusteluviranomaisen kansainvälisessä yhteistyössä. Kansainvälistä yhteistyötä koskevan 18 §:n mukaan sotilastiedusteluviranomainen voisi Suomen kansallisen turvallisuuden varmistamiseksi tehtäviinsä liittyen vaihtaa tiedustelutietoja ulkomaisten tiedustelu- ja turvallisuuspalveluiden kanssa sekä osallistua tiedustelutietojen hankkimiseen ja arvioimiseen liittyvään kansainväliseen yhteistoimintaan.

Kansainvälisessä yhteistyössä voitaisiin luovuttaa salassa pidettäviä henkilötietoja. Henkilötietojen luovuttamisen kansainvälisessä yhteistyössä olisi aina oltava välttämätöntä Suomen kansallisen turvallisuuden varmistamiseksi ja liityttävä sotilas-tiedusteluviranomaisen tiedustelutehtävään. Tietoja ei saisi luovuttaa edes sotilastiedusteluviranomaisen lakisääteisten tehtävien suorittamiseksi, jos luovuttaminen ei olisi välttämätöntä Suomen kansallisen turvallisuuden varmistamiseksi. Tieto-

jen luovuttamisen välttämättömyyttä arvioitaisiin kansallisen turvallisuuden varmistamisen ja niiden seurausten välillä, jotka tiedon luovuttamisesta saattaisi aiheutua. Tiedon luovuttamisen olisi oltava puolustettavaa ottaen huomioon tiedon luonne sekä tiedon vastaanottajana oleva taho. Tällä intressivertailulla tarkoitettaisiin esimerkiksi sitä että Suomen kansalaisiin liittyvien henkilötietojen luovuttamiseen tulisi suhtautua erittäin pidättyvästi.

Pykälän 2 momentissa säädettäisiin luovutettavien tietojen laadun varmistamisesta. Laatu olisi varmennettava ja niihin on mahdollisuuksien mukaan lisättävä tietoja, joiden avulla vastaanottaja voi arvioida tietojen oikeellisuutta, täydellisyyttä, ajantasaisuutta ja luotettavuutta. Jos ilmenee, että on luovutettu virheellisiä tietoja tai että tietoja on luovutettu lainvastaisesti, asiasta olisi ilmoitettava viipymättä vastaanottajalle.

Tiedot saataisiin luovuttaa myös teknisen käyttöyhteyden avulla tai tietojoukkona. Säännös oikeuttaisi teknisen käyttöyhteyden avaamiseen, muttei velvoittaisi siihen. Luovuttavalle viranomaiselle jää siten harkintavalta siitä, katsooko se käyttöyhteyden antamisen pyydetyssä tilanteessa perustelluksi vai ei ja pystytäänkö yhteys toteuttamaan tietoturvallisesti. Jos käyttöoikeuden antamiseen päädytään, se tulee toteuttaa niin, ettei käyttöyhteyden saaja pysty katsomaan tietojärjestelmästä muita tietoja kuin vain sellaisia, joita varten hänelle käyttöoikeus on annettu ja jotka ovat tarpeellisia pyydettyyn tarkoitukseen. Käyttöyhteys pitää toteuttaa myös tietoturvallisesti siten, etteivät ulkopuoliset pääse rekisteritietoihin.

säännös oikeuttaa teknisen käyttöyhteyden avaamiseen, muttei velvoita siihen. Luovuttavalle viranomaiselle jää siten harkintavalta siitä, katsooko se käyttöyhteyden antamisen pyydetyssä tilanteessa perustelluksi vai ei ja pystytäänkö yhteys toteuttamaan tietoturvallisesti. Jos käyttöoikeuden antamiseen päädytään, se tulee toteuttaa niin, ettei käyttöyhteyden saaja pysty katsomaan asiakastietojärjestelmästä muita tietoja kuin vain sellaisia, joita varten hänelle käyttöoikeus on annettu ja jotka ovat tarpeellisia pyydettyyn tarkoitukseen. Käyttöyhteys pitää toteuttaa myös tietoturvallisesti siten, etteivät ulkopuoliset pääse asiakastietoihin.

Lisäksi teknisen käyttöyhteyden avaamisen edellytyksenä on julkisuuslain 29 §:n mukaisesti se, että tietojen hakemiseen teknisen käyttöyhteyden avulla on saatu asianomaisen asiakkaan tai hänen laillisen edustajan suostumus. Suostumus tarvitaan, koska mahdollisuudesta salassa pidettävien tietojen luovuttamiseen teknisen käyttöyhteyden avulla ei ole erikseen säädetty.

120 §. *Kansainvälisessä yhteistyössä saatujen tietojen käsittely*. Toisen valtion tiedustelu- tai turvallisuuspalvelulta saatujen tietojen käsittelyssä olisi noudatettava, mitä tietojen luovuttajan asettamissa ehdoissa määrätään salassapidosta, vaitiolovelvollisuudesta, tietojen käytön rajoituksista, tietojen edelleen luovutuksesta tai luovutetun aineiston palauttamisesta. Ehdoilla tarkoitettaisiin joko nimenomaisesti mainittuja ehtoja tai tiedonvaihdon osapuolten vakiintuneita käytäntöjä. Säännöksessä ei velvoitettaisi noudattamaan tietojen luovuttajan asettamia ehtoja aineiston hävittämisestä, vaan tältä osin sovellettaisiin voimassa olevia tietojen säilyttämisaikaa koskevia säännöksiä.

11 luku. Sotilastiedustelun valvonta puolustushallinnossa

121 §. *Sotilastiedustelun oikeudellinen ja parlamentaarinen valvonta.* Pykälän 1 momentissa viitattaisiin valvontaviranomaiseen tiedustelutoiminnan yleisenä laillisuusvalvojana. Tiedustelun valvontaviranomaisesta säädettäisiin erillisessä laissa.

Pykälän 2 momentissa todettaisiin informatiivisesti, että parlamentaarista valvontaa suorittaisi eduskunta. Parlamentaarisesta valvonnasta säädetäisiin samassa laissa, jossa säädettäisiin tiedustelun valvontaviranomaisesta.

122 §. *Sisäinen valvonta*. Pääesikunnan päällikkö valvoisi sotilastiedustelutoimintaa. Tämän lisäksi Puolustusvoimien asessori vastaa sisäisestä laillisuusvalvonnasta sotilastiedustelun toimialalla. Sisäinen tiedustelutoiminnan valvonta olisi ensisijaista valvontaa ja sitä täydentäisi ulkoinen laillisuusvalvonta.

Sotilastiedustelutoiminnan yleisen valvonnan vastuuttaminen pääesikunnan päällikölle ja sisäisen laillisuusvalvonnan vastuuttaminen Puolustusvoimien asessorille ei kuitenkaan poistaisi muuta esimiesvalvontaan. Tällä tarkoitettaisiin esimiesvalvontaa, joka olisi osa normaaleja työnjohdollisia tehtäviä. Tämä valvonnan muoto on erittäin tärkeä, koska se on jokapäiväistä ja se tapahtuu lähellä valvottavaa toimintaa. Pykälä täydentäisi Puolustusvoimien asessorin puolustusvoimista annetun valtioneuvoston asetuksen 5 §:n 1 momentin mukaista laillisuusvalvontaa. Myös henkilöstön oikeudellinen koulutus on keskeinen osa ennaltaehkäisevää sisäistä laillisuusvalvontaa.

123 §. *Puolustusministeriön suorittama valvonta.* Perustuslain 68 §:n 1 momentin mukaan kukin ministeriö vastaa toimialallaan hallinnon asianmukaisesta toiminnasta. Ministeriöiden toimialoista säädetään valtioneuvoston ohjesäännössä. Sen mukaan puolustusministeriön toimialaan kuuluvat puolustuspolitiikka, sotilaallinen maanpuolustus, kokonaismaanpuolustuksen yhteensovittaminen sekä sotilaallinen kriisinhallinta- ja rauhanturvaamistoiminta. Lisäksi puolustusministeriön suorittamasta valvonnasta on säädetty nimenomaisesti sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetussa laissa.

Puolustusministeriön Puolustusvoimien sotilastiedusteluun kohdistamasta valvonnasta säädettäisiin suoraan laissa. Nykyisin valvonta perustuu edellä kuvattuihin säännöksiin. Pykälän 1 momentin mukaan puolustusministeriöllä olisi oikeus tutustua tiedustelutoiminnassa syntyneisiin pöytäkirjoihin ja muihin tallenteisiin.

Pykälän 2 momentissa säädettäisiin puolustusministeriön oikeudesta saada tiedot yhteiskunnallisesti, taloudellisesti tai vakavuudeltaan merkittävistä sotilastiedusteluun liittyvistä asioista.

124 §. *Kertomus eduskunnan oikeusasiamiehelle.* Puolustusministeriö antaisi eduskunnan oikeusasiamiehelle vuosittain kertomuksen tiedustelumenetelmien käytöstä ja valvonnasta.

125 §. *Tarkemmat säännökset.* Pykälän mukaan valtioneuvoston asetuksella voitaisiin antaa tarkempia säännöksiä laissa tarkoitettujen tiedustelumenetelmien käytön järjestämisestä ja valvonnasta sekä toimenpiteiden kirjaamisesta ja valvontaa varten annettavista selvityksistä.

12 luku. Erinäiset säännökset

126 §. *Määräaikojen laskeminen.* Pykälän 1 momentin mukaan tässä laissa tarkoitettujen määräaikojen laskemiseen ei sovellettaisi säädettyjen määräaikain laskemisesta annettua lakia (150/1930). Pykälän 2 momentin mukaan aika, joka on määrätty kuukausina, päättyy sinä määräkuukauden päivänä, joka järjestysnumeroltaan vastaa sanottua päivää. Jos vastaavaa päivää ei ole siinä kuussa, jona määräaika päättyisi, pidetään sen kuukauden viimeistä päivää määräajan päättymispäivänä. Viimeinen virke tarkoittaisi esimerkiksi sitä, että jos kuukauden mittaisen luvan voimassaolo alkaisi 31.3., voimassaolo lakkaisi 30.4.

127 §. *Tiedustelukiellot*. Pykälän 1 momentin mukaan telekuuntelua, teknistä havainnointia tai tietoliikennetiedustelua ei saa kohdistaa sellaiseen viestintään tai viestiin, josta viestinnän osapuoli ei saisi todistaa oikeudenkäymiskaaren 17 luvun 13–14 §:n, 16 §:n tai 20 §:n nojalla.

Pykälän 1 momentin mukaan sotilastiedustelu ei saisi kohdistua rikoksesta epäillyn ja hänen oikeudenkäyntiavustajansa väliseen viestiin. Kyseeseen tulee tilanne, jossa tiedustelutehtävän suo-

rittamisen yhteydessä sotilastiedusteluviranomainen saisi käsiteltäväkseen viestin, jossa viestinnän osaspuolina ovat rikoksesta epäilty ja hänen oikeudenkäyntiavustajansa.

Toisaalta tiedustelutehtävän kannalta olennainen henkilö saattaa olla oikeudenkäyntiavustajan kanssa tekemisissä myös muussa yhteydessä kuin rikoksesta epäillyn asemassa. Kyseessä voi olla tilanne, jossa sotilastiedustelun tiedustelumenetelmien käytön yhteydessä tiedustelutehtävän kannalta olennainen henkilö käy läpi avioeroon tai testamenttiin liittyviä tietoja, jolloin tilannetta on EIT:n tulkintakäytännön mukaan arvioitu yksityiselämän suojaan puuttumisena.

Kummassakin edellä mainitussa tapauksessa edellytyksenä on se, että tietty lakimies on tiedustelutehtävän kannalta olennaisen henkilön oikeudenkäyntiavustaja ja tällainen suhde on syntynyt. Jotta suhteen syntyminen voitaisiin todentaa, on sotilastiedusteluviranomaisen seurattava jonkin aikaa osapuolten viestintää. Heti, kun tämä suhde olisi todennettu, olisi sotilastiedusteluviranomaisen poistettava kaikki tiedustelukiellon alainen tieto.

Samanlainen kielto koskisi sotilastiedustelun kohteena olevan henkilön lääkäriä tai muuta terveydenhuollon ammattihenkilöistä annetussa laissa (559/1994) tai sen nojalla annetussa asetuksessa tarkoitettua terveydenhuollon ammattihenkilöä, sotilastiedustelun kohteena olevan henkilön ja uskonnonvapauslaissa (453/2003) tarkoitetun rekisteröidyn uskonnollisen yhdyskunnan papin tai muussa vastaavassa asemassa olevan henkilön välistä kanssakäymistä sekä sotilastiedustelun kohteena olevan henkilön ja sananvapauden käyttämisestä joukkoviestinnässä annetussa laissa (460/2003) tarkoitetun yleisön saataville toimitetun viestin laatijan taikka julkaisijan tai ohjelmatoiminnan harjoittajan välistä kanssa käymistä.

Kaikissa 1 momentin tapauksissa olisi merkitystä annettava sotilastiedustelun kohteena olevan henkilön ja tiedustelukiellonalaisen henkilön väliselle suhteelle sekä sille, että tiedustelukiellonalainen henkilö täyttää tosiasiallisesti tiedustelukiellolle asetetut vaatimukset.

Pykälän 2 momentin mukaan jos telekuuntelun, jos teknisen kuuntelun tai teknisen katselun aikana tai muulloin ilmenisi, että kyseessä on viesti, jonka kuuntelu ja katselu on kielletty, toimenpide olisi keskeytettävä ja sillä saadut tallenteet ja sillä saatuja tietoja koskevat muistiinpanot olisi heti hävitettävä.

Ilmaisu ”muulloin” liittyisi esimerkiksi tilanteisiin, joissa henkilöiden nimet ja roolit eivät ole vielä kuuntelun aikana selvillä, ja vasta myöhemmin ilmenee, että kysymyksessä on ollut kuuntelu- tai katselukiellon alainen tilanne. Ilmaisu koskisi myös tilanteita, joissa kuuntelua ei seurata reaaliaikaisesti. Selvyyden vuoksi mainittaisiin myös se, että mahdollisten muistiinpanojen hävittämisvelvollisuus koskee nimenomaan kysymyksessä olevalla pakkokeinolla saatuja tietoja koskevia muistiinpanoja. Esimerkiksi toimenpidettä koskeva dokumentointi voitaisiin sitä vastoin säilyttää.

Pykälän 3 momentissa säädettäisiin, että tässä pykälässä tarkoitetut kuuntelu- ja katselukiellot eivät kuitenkaan koske tapauksia, joissa 1 momentissa tarkoitettu henkilö on tiedustelumenetelmän käytön kohteena samalla perusteella kuin 1 momentissa tarkoitettuun henkilöön yhteydessä oleva henkilö ja myös hänen osaltaan on tehty päätös telekuuntelusta, telekuuntelun sijasta toimitettavasta tietojen hankkimisesta, teknisestä havainnoinnista tai tietoliikennetiedustelusta.

Kohteena oleminen kattaisi tilanteet, joissa 1 momentissa tarkoitettu henkilö ja tiedustelutehtävän kannalta olennaisen henkilö tekisivät sotilastiedustelun kannalta merkittävää yhteistyötä. Pelkkä yhteistyö kahden henkilön välillä ei vielä riittäisi kiellon noudattamatta jättämiseen, vaan molempien henkilöiden osalta tulisi olla päätös saman tiedustelumenetelmän käyttämisestä. Molempien henkilöiden olisi siis oltava tiedustelutehtävän kohteena ja heidän toiminnastaan pitäisi voida hankkia tietoja samalla toimivaltuudella.

128 §. *Tallenteiden tarkastaminen.* Säännöksen mukaan tiedustelumenetelmän käyttöä johtavan ja tiedustelumenetelmää käyttävän virkamiehen on ilman aiheetonta viivytystä tarkastettava lain 4 tai 5 luvun tiedustelumenetelmien käytössä kertyneet tallenteet ja asiakirjat. Tiedustelumenetelmän käyttöä johtava ja tiedustelumenetelmää käyttävä virkamies ovat keskeisessä asemassa toimenpiteitä toteutettaessa ja ovat velvollisia valvomaan niiden lainmukaista suorittamista. Näin ollen hänen tulisi huolehtia myös tallenteiden ja asiakirjojen tarkastamisesta. Tallenteiden ja asiakirjojen tarkastamisella on olennainen merkitys, jotta toiminnasta vastaava virkamies voi tosiasiallisesti valvoa tiedustelumenetelmien lainmukaista käyttämistä reaaliaikaisesti.

Tallenteiden ja asiakirjojen tarkastamisessa voitaisiin hyödyntää teknistä laitetta, menetelmää tai ohjelmistoa siten, että sen avulla tarkastamisen piiriin tulisivat vain sellaiset tallenteiden kohdat, joilla on viestintää. Näin tyhjät kohdat voitaisiin pyyhkiä yli tai ohittaa.

Velvollisuus tallenteiden tarkastamiseen takaa tiedonhankintakeinojen ennakoitavuuden ja oikeasuhtaisuuden kannalta tärkeällä tavalla sitä, että sotilastiedusteluviranomainen ei käytä kielletyllä tavalla ylimääräistä tietoa, joka ei liity tiedustelun kohteeseen tai joka koskee sivullisia. Toisaalta tallenteiden tarkastaminen myös mahdollistaa tiedustelumenetelmän käytön jatkamisen edellytysten selvittämisen ja estää sotilastiedusteluviranomaista perustamasta luvattomia henkilörekistereitä

129 §. *Tallenteiden tutkiminen.* Pykälän 1 momentin mukaan tiedustelumenetelmän käytössä kertyneitä tallenteita saisi tutkia vain tuomioistuin ja tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies, sotilaslakimies tai muu tiedustelutehtävään määrätty sotilastiedusteluviranomaisen virkamies. Tallenteiden tutkimisella tarkoitetaan tiedustelutehtävään liittyvien asiakirjojen ja muiden tallenteiden käyttämistä, käsittelyä ja analysointia tiedustelutehtävän edellyttämän tiedon tuottamiseksi.

Tallenteiden tutkintaan oikeutettujen piiri olisi rajattu, jotta yksityiselämän suoja voidaan turvata riittävän tehokkaasti.

Pykälän 2 momentin mukaan tallenteita voisi tutkia lisäksi pääesikunnan tiedustelupäällikön määräyksestä sotilastiedusteluviranomaisen ulkopuolinen asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankinnassa. Näiden henkilöiden tietoon tulevan aineiston määrää rajoittaa se, että he saavat tarkastaa tallenteita ainoastaan pääesikunnan tiedustelupäällikön määräyksestä tietyssä tilanteessa. Määräyksen antaja vastaisi siitä, että kyseisellä henkilöllä on tarvittavat tiedot ja taito sekä kokemus tehtävän suorittamiseksi.

130 §. *Pöytäkirja*. Säännöksen mukaan tiedustelumenetelmää käyttävän sotilastiedusteluviranomaisen virkamiehen olisi laadittava tiedustelumenetelmän käytöstä pöytäkirja tai muu vastaava tallenne ilman aiheetonta viivytystä. Pöytäkirjan tai muun vastaava tallenteen sisällöstä säädettäisiin valtioneuvoston asetuksella tarkemmin.

Muulla vastaavalla tallenteella tarkoitettaisiin muussa kuin pöytäkirjamuodossa olevaa tallennetta, johon saattaisi sisältyä muutakin tietoa kuin kirjaamista. Ominaisuuksiltaan tallenteen tulisi kuitenkin vastata pöytäkirjaa ja siitä tulisi käydä ilmi kaikki vastaavat tiedot.

Pöytäkirja tai muu vastaava tallenne mahdollistaisi osaltaan lain 7 luvussa tarkoitetun valvonnan.

131 §. *Vaitiolovelvollisuus.* Pykälän 1 momentin mukaan sotilastiedusteluviranomaisen henkilöstöön kuuluvan virkamiehen vaitiolovelvollisuudesta olisi voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa ja muussa laissa sekä tässä luvussa jäljempänä säädetään.

Viranomaisten julkisuudesta annettu lain 23 §:n 1 momentin ensimmäisen virkkeen mukaan viranomaisen palveluksessa oleva ei saa paljastaan asiakirjan salassa pidettävää sisältöä tai tietoa,

joka asiakirjaan merkittynä olisi salassa pidettävä. Lain 24 §:ssä säädetään salassa pidettävistä viranomaisen asiakirjoista. Pykälän 1 momentin 10 kohdassa säädetään asiakirjoista, jotka koskevat muun muassa sotilastiedustelua, jollei ole ilmeistä, että tiedon antaminen ei vahingoita tai vaaranna maanpuolustuksen etua.

Momentin toisen virkkeen mukaan sama vaitiolovelvollisuus koskisi myös sitä, joka suorittaa tiedustelutehtävää sotilastiedusteluviranomaisen johdon ja valvonnan alaisena tai avustaa tiedustelutehtävän suorittamisessa. Näin momentin soveltamisala koskisi myös tiedustelutehtävää suorittavia asevelvollisuuslain mukaisessa palveluksessa olevia henkilöitä, kuten varusmiehiä ja reserviläisiä, sekä lain 24 §:ssä tarkoitettuja avustajia sekä 89 §:ssä tarkoitettuja muita henkilöitä, jotka ovat muuten avustaneet tiedustelutehtävän suorittamisessa.

Pykälän 2 momentin mukaan sotilastiedusteluviranomaisen henkilöstöön kuuluva kuuluvan virkamies ei saisi ilmaista luottamuksellisesti tietoja antaneen avustajan tai sotilastiedustelun peitehenkilönä toimineen henkilöllisyyttä koskevaa tietoa, jos tiedon ilmaiseminen vaarantaisi luottamuksellisesti tietoja antaneen tai peitehenkilönä toimineen tai hänen läheistensä turvallisuuden. Vaitiolovelvollisuus olisi voimassa myös, jos henkilöllisyyttä koskevan tiedon ilmaiseminen vaarantaisi jo käynnissä olevan tai tulevan tiedustelutehtävän. Momentti koskisi myös satunnaisesti luottamuksellisia tietoja antavat.

Momentin tarkoittamat tiedot ovat erittäin herkkiä ja voivat vaarantaa sotilastiedusteluviranomaisen virkamiehen lisäksi myös useita sivullisia. Tämän takia momentin tarkoittamia tietoja käsittelisivät ainoastaan tietyt sotilastiedusteluviranomaisen virkamiehet, joidenka piirin ulkopuolelle momentissa tarkoitetut tiedot eivät saisi joutua. Koska tämän lain mukaan tiedustelutehtävän suorittamiseen saattaisi muissa yhteyksissä osallistua myös muitakin henkilöitä kuin sotilastiedusteluviranomaisen virkamiehiä, vaitiolovelvollisuus olisi tarkoituksen mukaista säätää koskemaan myös näitä henkilöitä. Momentin toinen virke koskisikin vastaavaa henkilöpiiriä kuin 1 momentin toisessa virkkeessä olisi säädetty.

Pykälän 3 momentissa säädettäisiin vaitiolovelvollisuudesta tilanteissa, joissa henkilöllisyyttä koskevan tiedon ilmaiseminen vaarantaisi jo päättyneen, käynnissä olevan tai tulevan tiedonhankinnan. Koska tiedustelutoiminta on pitkäkestoista toimintaa, johon tietyt henkilöt saattavat liittyä hyvinkin pitkän aikaa toimimatta välillä aktiivisesti sotilastiedustelutoiminnassa, olisi vaitiolovelvollisuus pidempikestoinen. Myös sotilastiedustelutoimintaan liittyviin henkilöihin kohdistuva hengen tai terveyden vaara saattaa konkretisoitua vasta vuosien päästä toteutetusta tiedusteluoperaatiosta. Tämän takia olisi perusteltua, että tällaisia henkilöitä koskevien tietojen ilmaisemisen kielto olisi laaja.

Pykälän 4 momentti koskisi tilanteita, joissa muu kuin sotilastiedusteluviranomaisen palveluksessa oleva suorittaisin tiedusteluun liittyviä tehtäviä. Henkilöryhmänä laajimmillaan tämä saattaisi toteutua varusmiehiä ja reserviläisiä käytettäessä. Lisäksi momentin alaan tulisivat muut Puolustusvoimien virkamiehet, joita käytettäisiin tiedustelutehtävän suorittamisessa. 4 momentin tilanteissa tiedustelutehtävään osallistuvat tahot olisivat aina sotilastiedusteluviranomaisen johdon ja valvonnan alaisia.

Momentin viittauksella pykälä 1 momenttiin muut tahot kuin sotilastiedusteluviranomaisen palveluksessa olevat olisivat lähtökohtaisesti sidottu julkisuuslain mukaiseen tiedon ilmaisemisenkieltoon.

Tiedustelutoiminnassa tietoja antaneiden tahojen henkilöllisyyttä pyritään suojelemaan erittäin tarkasti. Tästä johtuen näitä tietoja käsittelisi sotilastiedusteluviranomaisessa vain pieni joukko virkamiehiä. Tietyissä tilanteissa tieto tietoja antaneesta saattaisi tulla muun kuin sotilastiedusteluviranomaisen virkamiehen tietoon, kuten valmiustilanteen tehostamisen edellyttämä tiettyjen reserviläis-

ten käyttö. Näissäkin tilanteissa olisi tarkoituksen mukaista säätää vaitiolovelvollisuudesta nimenomaisesti viittaamalla momentissa pykälän 2 momenttiin.

Pykälän 5 momentin mukaan vaitiolovelvollisuus olisi voimassa edelleen sen jälkeen, kun palvelussuhde sotilastiedusteluviranomaiseen olisi päättynyt. Palvelussuhteella tarkoitettaisiin kaikkia tilanteita, joissa henkilön ei enää katsottaisi olevan suhteessa sotilastiedusteluviranomaiseen.

132 §. *Vaitiolo-oikeus*. Pykälän 1 momentin mukaan sotilastiedustelun henkilöstöön kuuluva ei olisi velvollinen ilmaisemaan hänen palvelussuhteen aikana luottamuksellisesti tietoja antaneen henkilöllisyyttä koskevaa tietoa eikä salassa pidettäviä taktisia tai teknisiä menetelmiä. Vaitiolo-oikeus koskisi kaikkia tilanteita mukaan lukien tuomioistuimessa tapahtuvan kuulemisen ja muut kuulemistilanteet sekä tilanteen, joissa asioita tiedustelee esimerkiksi toinen viranomainen tai yksityinen taho.

Pykälän 2 momentissa säädettäisiin sotilastiedusteluun osallistuvien muiden kuin sotilastiedusteluviranomaisen palveluksessa olevien vaitiolo-oikeudesta. Momentin alaan kuuluisivat sotilastiedustelussa mahdollisesti käytettävät varusmiehet, reserviläiset sekä tahot, jotka ovat avustaneet sotilastiedustelu tiedustelutehtävässä, kuten asunto-osakeyhtiön talonmies.

133 §. *Virkamerkki.* Pykälän 1 momentin mukaan sotilastiedusteluviranomaisen virkamiehellä olisi puolustusministeriön asetuksella säädettävä virkamerkki. Ehdotuksessa on säännöksiä, jotka edellyttävät viranomaisaseman ilmaisemista. Tällaisia ovat esimerkiksi 57 §:ssä säädettävä lähetyksen pysäyttäminen jäljentämistä varten sekä 92 §:ssä säädetty ilmaisukielto. Viranomaisen on näissä tapauksissa pystyttävä ilmaisemaan viranomaisasemansa, jotta velvollisuuden kohteena oleva henkilö saa tiedon siitä, että kyseessä olisi tämän lain mukainen viranomainen ja että häntä koskee viranomaisen antama määräys.

Pykälän 2 momentin mukaan sotilastiedusteluviranomaisen virkamiehen olisi tarvittaessa pidettävä virkamerkki mukana virkatehtävää suorittaessaan. Kaikissa sotilastiedustelun tehtävissä ei ole tarkoituksen mukaista pitää virkamerkkiä mukana toiminnan luonteen vuoksi. Jos etukäteen on tiedossa, että toimenpiteen kohteena olevalle annettaisiin velvoitteita, olisi virkamerkki pidettävä mukana.

Momentin toinen virke koskee tilanteita, joissa virkamerkki olisi esitettävä. Virkamerkin esittämisvelvollisuus rajataan kuitenkin tilanteisiin joissa se on mahdollista toimenpiteen suorittamista vaarantamatta. edellä 1 momentin perusteluissa tarkoitetun vaitiolovelvollisuuden ilmaiseminen ei ole mahdollista ilman, että vaitiolovelvollisuuden kohteena oleva henkilö tietäisi kyseessä olevan virkamies.

Pykälän 3 momentin mukaan virkamiehen olisi oltava yksilöitävissä. Säännös on merkityksellinen toimenpiteen kohteena olevan henkilön oikeusturvan takia. Virkamiehen yksilöinti voidaan toteuttaa toimenpiteiden ja niiden suorittajan tarkalla kirjaamisella.

134 §. *Menettely tuomioistuimessa.* Pykälässä säädettäisiin tiedustelumenetelmän tuomioistuinkäsittelyä koskevista säännöksistä.

Pykälän 1 momentin mukaan tiedustelumenetelmää koskeva lupa-asia käsiteltäisiin Helsingin käräjäoikeudessa. Käräjäoikeus olisi päätösvaltainen, kun siinä on yksin puheenjohtaja. Istunto voitaisiin pitää myös muuna aikana ja muussa paikassa kuin yleisen alioikeuden istunnosta säädetään.

Tiedustelumenetelmiä koskevat lupa-asiat käsiteltäisiin vain ja ainoastaan Helsingin käräjäoikeudessa. Tämänkaltainen keskitetty päätöksentekojärjestely koskee voimassa olevassa lainsäädän-

nössä tällä hetkellä poliisilain 5 luvussa tarkoitetuista salaisista tiedonhankintakeinoista yksin peitetoimintaa. Yhteen käräjäoikeuteen keskitetyn päätöksenteon tueksi voidaan esittää useita perusteluita. Helsingin käräjäoikeudessa työskentelee useita pakkokeinoasioihin keskittyviä käräjätuomareita. Tämänkaltainen osaamiskertymä mahdollistaa erikoistumisen tiedustelumenetelmiä koskeviin lupa-asioihin sekä tiedustelumenetelmien käytöstä ilmoittamista koskeviin kysymyksiin. [Helsingin käräjäoikeuden muita alioikeuksia suurempi henkilöstömäärä antaa myös paremmat mahdollisuudet varmistua istuntojärjestelyin siitä, että päivystysvuorossa oleva tuomari on perehtynyt tiedustelumenetelmiä koskevien asioiden käsittelyyn. Keskittämistä puoltaa lisäksi tiedustelumenetelmien käytöstä tietoisten henkilöiden lukumäärän rajoittaminen sekä tarvittavien turvajärjestelyjen toteuttaminen.

Tuomioistuimen päätösvaltaista kokoonpanoa sekä istunnon aikaa ja paikkaa koskeva säännös olisi asiallisesti sama kuin vangitsemisesta päättävää viranomaista koskeva säännös pakkokeinolain 3 luvun 1 §:n 2 momentissa.

Pykälän 2 momentin mukaan vaatimus tiedustelumenetelmän käytöstä olisi tehtävä kirjallisesti. Tiedustelumenetelmän käyttöä koskevaa vaatimusta koskisi näin ollen sama kirjallista muotoa koskeva ehto kuin mistä pakkokeinolain 3 luvun 3 §:n 1 momentissa säädetään.

Momentissa säädettäisiin lisäksi, että tiedustelumenetelmän käyttöä koskeva vaatimus olisi otettava viipymättä tuomioistuimessa käsiteltäväksi vaatimuksen tehneen tai hänen määräämänsä asiaan perehtyneen virkamiehen läsnä ollessa. Käsittelyä koskeva viipymättömyyden vaatimus edellyttäisi jakamaan vireille saatetun tiedustelumenetelmäasian mahdollisimman nopeasti asian ratkaisevalle tuomarille sekä määräämään jutulle istuntoajankohdan. Määrätyltä virkamieheltä edellytettäisiin sellaista perehtyneisyyttä tiedustelumenetelmistä, että hän voisi vastata kysymyksiin ja perustella vaatimusta.

Pykälän 3 momentissa säädettäisiin, että asia on ratkaistava kiireellisesti. Tiedustelumenetelmien käyttö voisi ilman tuomioistuimelle asetettua velvoitetta kiireelliseen käsittelyyn menettää merkityksensä, ja pahimmassa tapauksessa johtaa sotilaallisen maanpuolustuksen ja kansallisen turvallisuuden vaarantumiseen.

Momentissa säädettäisiin edelleen, että käsittely voidaan pitää myös käyttäen videoneuvottelua tai muuta soveltuvaa teknistä tiedonvälitystapaa, jos käsittelyyn osallistuvilla on puhe- ja näköyhteys keskenään. Käsittelyn tiedonvälitystavat olisivat siten samat kuin mitkä tällä hetkellä ovat poliisilain 5 luvun 45 §:n 2 momentin nojalla salaisessa tiedonhankinnassa ja pakkokeinolain 10 luvun 43 §:n 2 momentin perusteella salaisissa pakkokeinoissa.

Pykälän 4 momentin mukaan tiedustelumenetelmää koskevan päätöksen sisällöstä säädettäisiin tiedustelumenetelmäkohtaisesti. Päätöksen sisältöä koskevalla säännöksellä kiinnitetään tuomioistuimen huomiota siihen, että sen on tiedustelumenetelmän käyttöä koskevassa päätöksessään mainittava ne seikat, joista tämän lain 24, 26, 28, 30, 34, 36, 38, 52, 67, 69, 71, 85 ja 87 §:ssä yksityiskohtaisesti säädetään.

Momentin mukaan päätös olisi annettava heti tai viimeistään samaan tiedustelua koskevaan kokonaisuuteen liittyvien tiedustelumenetelmiä koskevien asioiden käsittelyn päätyttyä. Säännös edellyttäisi tuomioistuinta toimimaan tiedustelumenetelmäasiassa annettavan päätöksen yhteydessä samoin kuin vangitsemispäätöstä pakkokeinolain 3 luvun 10 §:n 1 momentin nojalla julistettaessa.

Pykälän 5 momentissa säädettäisiin, että jos tuomioistuin on myöntänyt luvan telekuunteluun tai televalvontaan, se saisi tutkia ja ratkaista luvan myöntämistä uuteen henkilöön, teleosoitteeseen tai telepäätelaitteeseen koskevan asian vaatimuksen tehneen tai hänen määräämänsä virkamiehen läsnä olematta, jos on kulunut vähemmän kuin kuusi kuukautta aiemman lupa-asian suullisesta

käsittelystä. Asia voitaisiin käsitellä mainitun virkamiehen läsnä olematta myös, jos tiedustelumenetelmän käyttö on jo lopetettu.

Sotilastiedustelun ja tuomioistuimen voimavarojen tarkoituksenmukaiseksi ja tehokkaaksi käyttämiseksi esitetään, että teleosoitteiden ja telepäätelaitteiden vaihtamista koskevia asioita ei kaikissa tilanteissa tarvitsisi käsitellä istunnossa. Momentissa tarkoitetun kevennetyn menettelyn käyttäminen olisi tuomioistuimen harkinnassa ja sitä voitaisiin käyttää vain luvan voimassa ollessa. Lupa-asia tulisi siten käsitellä vähintään puolivuosittain vaatimuksen esittämisestä huolehtivan virkamiehen läsnä ollessa. Lisäksi kevennetyn menettelyn edellytyksenä olisi, että kysymys on samasta henkilöstä ja samasta tiedustelumenetelmän käytön perusteena olevasta kansallista turvallisuutta vakavasti vaarantavasta uhkasta kuin aikaisemmin myönnetyssä luvassa.

Momentin jälkimmäisen virkkeen mukaiseen tapaukseen liittyvät samanlaiset tarkoituksenmukaisuusnäkökohdat kuin ensimmäisenkin virkkeen tarkoittamissa tilanteissa. Jälkimmäinen virke koskisi siis tilanteita, jossa pääesikunnan tiedustelupäällikkö tai tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies on väliaikaisesti päättänyt tiedustelumenetelmän käytöstä 33 §:n 1 momentin, 35 §:n 1 momentin tai 46 §:n 2 momentin nojalla sekä tilanteita, joissa tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies on väliaikaisesti päättänyt tiedustelumenetelmän käytöstä 35 §:n 1 momentin, 25 §:n 1 momentin tai 27 §: 1 momentin nojalla.

Pykälän 6 momentin mukaan lupa-asiassa annettuun päätökseen ei saisi hakea muutosta valittamalla. Päätöksestä saisi ilman määräaikaa kannella Helsingin hovioikeuteen. Kantelu olisi käsiteltävä kiireellisenä.

Sääntely vastaisi tältä osin voimassa olevan poliisilain 5 luvun 45 §:n 5 momenttia sillä täsmennyksellä, että kantelutuomioistuimena mainittaisiin Helsingin hovioikeus.

Pykälän 7 momentissa säädettäisiin, että tiedustelumenetelmää koskevan asian käsittelyssä olisi kiinnitettävä erityistä huomiota salassapitovelvollisuuden toteutumiseen ja siihen, että asiakirjoihin ja tietojärjestelmiin sisältyvien tietojen suoja turvataan tarvittavin menettelytavoin ja tietoturvallisuusjärjestelyin.

Asian käsittely voitaisiin tarvittaessa pitää muualla kuin tuomioistuimessa, esimerkiksi suojelupoliisin tiloissa. Salassapitovelvollisuuden toteutumiseen ja tietoturvallisuuden varmistamiseen olisi kiinnitettävä erityistä huomiota. Keskeisimmät salassapitoa koskevat säännökset ovat oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetussa laissa (370/2007).

135 §. *Asianosaisjulkisuuden rajoittaminen eräissä tapauksissa.* Pykälän 1 momentin mukaan henkilöllä, jonka oikeutta tai velvollisuutta asia koskee, ei olisi viranomaisten toiminnan julkisuudesta annetun lain 11 §:ssä säädetystä huolimatta oikeutta saada tietoa tässä laissa tarkoitetun tiedonhankintakeinon käytöstä, ennen kuin 86 §:ssä tarkoitettu ilmoitus on tehty. Hänellä ei olisi myöskään henkilötietolaissa tarkoitettua rekisteröidyn tarkastusoikeutta.

Momentin tarkoituksena olisi lainsäädännöllisesti selkeyttää tilannetta suhteessa viranomaistentoiminnan julkisuudesta annettuun lakiin ja henkilötietolakiin.

Viranomaisten toiminnan julkisuudesta annetun lain 11 §:ssä on säädetty asianosaisen oikeudesta saada tieto viranomaisen asiakirjasta sekä tilanteista, jolloin asianosaisella ei ole oikeutta asiakirjaan. Mainitun pykälän 1 momentin 1 kohdan mukaan asianosaisella ei ole oikeutta saada tietoa asiakirjasta, josta tiedon antaminen olisi vastoin erittäin tärkeää yleistä etua. Erittäin tärkeä etu on esimerkiksi sotilastiedustelun taktisen tai teknisen menetelmän salassapitointressi.

Momentin mukaan henkilöllä olisi kuitenkin oikeus saada tietoja 1 momentissa tarkoitettuja tietoja, jos hänelle olisi tehty 86 §:ssä tarkoitettu ilmoitus.

Pykälän 2 momentissa olisi informatiivinen säännös, joka koskisi asianosaisjulkisuuden rajoittamista siviili-tiedustelussa. Tiedusteluviranomaiset tekevät tiivistä yhteistyötä keskenään, mistä johtuen tarvittaessa suojelupoliisin ja sotilastiedusteluviranomaisen välillä vaihdetaan tietoja aktiivisesti. Tietojen vaihdon jälkeen toimivaltaisen viranomaisen olisi itse huolehdittava itse asianosaisjulkisuuden rajoittamisesta viranomaisten velvoittavan lain mukaisesti. Tietojen vaihdon takia ja asianosaisjulkisuuden rajoittamisen selkeyttämiseksi informatiivista säännöstä voitaisiin pitää perusteltuna.

13 luku. Voimaantulo

136 §. *Voimaantulo.* Laki ehdotetaan tulemaan voimaan mahdollisimman pian.

2 Tarkemmat säännökset ja määräykset

Esitys sisältää neljä asetuksen antamiseen valtuuttavaa säännösehdotusta.

Valtioneuvoston asetuksella voitaisiin lakiehdotuksen 15 §:n 3 momentin mukaan antaa tarkempia säännöksiä sotilastiedusteluviranomaisen ja suojelupoliisin välisestä yhteistyöstä ja 126 §:n 1 momentin mukaan sotilastiedustelusta annetussa laissa tarkoitettujen tiedustelumenetelmien käytön järjestämisestä ja valvonnasta sekä toimenpiteiden kirjaamisesta ja valvontaa varten annettavista selvityksistä.

Pöytäkirjaa koskevan lakiehdotuksen 131 §:n 2 momentin mukaan valtioneuvoston asetuksella annettaisiin tarkemmat säännökset tiedustelutehtävän toimenpiteiden kirjaamisesta.

Sotilastiedusteluviranomaisen virkamiehellä olisi lakiehdotuksen 134 §:n mukaan puolustusministeriön asetuksella säädettävä virkamerkki. Virkamerkillä sotilastiedusteluviranomaisen virkamies osoittaisi tarvittaessa viranomaisasemansa. Asetuksessa säädettäisiin virkamerkin ulkoasusta ja siihen otettavista tiedoista sekä virkamerkkien haltijoista pidettävästä luettelosta.

3 Voimaantulo

Esitykseen sisältyvät säännösehdotukset, jotka koskevat teknistä kuuntelua (23 §), muuhun kuin valtiolliseen toimijaan kohdistuvaa telekuuntelua (32 §:n 3 momentti), tietojen hankkimista telekuuntelun sijasta (33 §), muuhun kuin valtiolliseen toimijaan kohdistuvaa televalvontaa (35 §:n 2 momentti), lähetyksen jäljentämistä (56 §) ja muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvaa tiedustelua (70 §), liittyvät oikeusministeriön ehdotukseen perustuslain 10 §:n sääntelyn tarkistamiseksi, joka on käsiteltävä perustuslain 73 §:ssä säädetyssä järjestyksessä.

Jos perustuslain muutosehdotus käsiteltäisiin pääsäännön mukaan perustuslain 73 §:n 1 momentin mukaisessa niin sanotussa normaalissa perustuslain säätämisjärjestyksessä, edellä mainitut säännökset voisivat tulla voimaan 1.1.2020.

Sen sijaa, jos perustuslain muutosehdotus käsiteltäisiin perustuslain 73 §:n 2 momentin mukaisessa nopeutetussa menettelyssä, edellä mainitut säännökset voisivat tulla voimaan vuonna 2018.

Laki ehdotetaan muilta kuin edellä mainituilta osin tulemaan voimaan mahdollisimman pian sen jälkeen kun se on hyväksytty ja vahvistettu.

4 Suhde perustuslakiin ja säätämisjärjestys

4.1 Johdanto

Lakiehdotukseen sisältyy sääntelyä, joka on merkityksellistä perustuslaissa säädettyjen perusoikeuksien kannalta. Laissa säänneltäisiin Puolustusvoimien tiedustelutoiminnasta, jonka tarkoituksena on turvata valtion itsemääräämisoikeutta ja perusoikeuksia, erityisesti oikeutta elämään ja henkilökohtaiseen turvallisuuteen, niihin kohdistuvilta uhkilta. Tältä osin lakiehdotuksen voidaan katsoa toteuttavan perustuslain 22 §:ssä julkiselle vallalle asetettua perusoikeuksien turvaamisvelvoitetta.

Esitykseen sisältyvän lakiehdotuksen 4 luvussa ehdotetaan säädettäväksi tiedonhankintatoimivaltuuksista ja 5 luvussa erityisesti tiedonhankinnasta tietoliikenteestä.

Tiedustelumenetelmillä puututtaisiin monin paikoin yksilön perusoikeuksiin. Perustuslain kannalta merkityksellisimpiä ovat säännösehdotukset, joilla annetaan viranomaisille uusia yksilöön kohdistuvia toimivaltuuksia tai joilla muuten rajoitettaisiin yksilön oikeuksia tai toimintavapautta.

Esitystä on tältä osin arvioitava perusoikeussäännöksiin sisältyvien lakivarausten kannalta ottaen samalla huomioon perusoikeuksien yleiset rajoitusedellytykset. Näitä ovat vaatimukset

- lailla säätämisestä
- lain täsmällisyydestä ja tarkkarajaisuudesta
- rajoituksen hyväksyttävyydestä
- rajoituksen suhteellisuudesta
- perusoikeuden ydinalueen koskemattomuudesta
- oikeusturvajärjestelyjen riittävyydestä ja
- ihmisoikeusvelvoitteiden noudattamisesta (PeVM 25/1994 vp)

Toisaalta lakiehdotus sisältää sääntelyä, joka rajoittaa joitakin perusoikeuksia. Lailla olisi tällaisia vaikutuksia perustuslain 10 §:n 1 momentissa säädettyyn yksityiselämän suojaan ja 9 §:n 1 momentissa turvattuun liikkumisvapauteen. Lisäksi lakiehdotuksen säännöksiä tulee tarkastella perustuslain 12 §:ssä säädetyn sananvapauden ja perustuslain 15 §:ssä säädetyn omaisuuden suojan kannalta.

Sotilastiedusteluviranomainen saisi virkatehtävien sitä edellyttäessä puuttua kansalaisten perusoikeuksiin. Ehdotetussa laissa säännökset määrittäisivät viranomaisen toimivaltuudet mahdollisimman tarkasti ja siten, että valtuuksien käyttö olisi sallittu vain tehtävien edellyttämässä laajuudessa.

Ehdotetun lain mukaiset valtuudet puuttua kansalaisten perusoikeuksiin kuuluisivat lähtökohtaisesti vain virkavastuulla toimiville virkamiehille, jotka olisivat vastuussa myös heitä pyynnöstä avustavien reserviläisten toimista.

Koska esityksellä luodaan viranomaisille uusia tehtäviä ja niihin liittyviä toimivaltuuksia, on sekä tehtävistä että toimivaltuuksista säädettävä lailla. Lakiehdotukseen on sisällytetty nimenomaiset täsmälliset ja tarkkarajaiset säännökset lain soveltamisalasta, sotilastiedustelun tarkoituksesta ja tiedonhankinnan kohteista, toiminnassa noudatettavista periaatteista ja tiedustelumenetelmien käytön yleisistä ja erityisistä edellytyksistä, ohjauksesta ja siitä, kenen toimeksiannosta tiedustelutoimintaan voidaan ryhtyä. Toimivaltuuksia koskevia säännösehdotuksia on tarkasteltava kokonaisuutena muun ehdotetun sääntelyn kanssa.

Esityksessä on myös pidetty huolta siitä, että viranomaistoimivaltuuksien kohteena olevien henkilöiden oikeusturva on asianmukaisesti järjestetty.

Perusoikeuksien yleisiin rajoitusedellytyksiin kuuluu vaatimus, jonka mukaan perusoikeusrajoitusten on oltava sopusoinnussa Suomen kansainvälisten ihmisoikeusvelvoitteiden kanssa. Merkitystä on Euroopan ihmisoikeussopimuksella ja Euroopan ihmisoikeustuomioistuimen oikeuskäytännöllä.

Tiedustelutoiminnan lainmukaisuuden valvonnasta säädetään lakiehdotuksen 11 luvussa. EIT:n ratkaisukäytännön mukaan oikeudellisen valvontaelimen tulee olla riippumaton suh-teessa valvonnan kohteeseen, minkä lisäksi sillä tulee olla pääsy kaikkeen tiedustelussa kertyneeseen aineistoon. EIT on pitänyt lisäksi tärkeänä, että tiedustelun valvontaan osallistuvat myös kansanedustuslaitoksen jäsenet. Tiedustelun oikeudellisen valvonnan järjestämistä koskeva lainvalmistelu on tehty oikeusministeriössä. Parlamentaarista valvontaa koskevaa sääntely on valmisteltu eduskunnan pääsihteerin asettamassa työryhmässä.

Luottamuksellisen viestin salaisuuden suoja

Perustuslain 10 §:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu ja kirjeen, puhelun sekä muun luottamuksellisen viestin salaisuus on loukkaamaton. Säännöksen lähtökohtana on, että yksilöllä on oikeus elää elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä. Pykälä turvaa jokaiselle oikeuden luottamukselliseen viestintään ilman, että ulkopuoliset saavat oikeudettomasti tiedon hänen lähettämiensä tai hänelle osoitettujen luottamuksellisten viestien sisällöstä.

Tämä merkitsee esimerkiksi suojaa kirjeiden tai muiden suljettujen viestien avaamista tai hävittämistä sekä puhelujen kuuntelemista tai nauhoittamista vastaan. Sääntely ei suojaa ainoastaan viestin lähettäjää, vaan kysymyksessä on viestinnän molempien osapuolten perusoikeus.

Perustuslain 10 §.n 3 momentissa säädetään, että lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana.

Nämä mahdollisuudet rajoittaa luottamuksellisen viestin suojaa on perusoikeusuudistuksen yhteydessä tarkoitettu tyhjentäväksi luetteloksi (HE 309/1993 vp, s. 54). Esimerkiksi Euroopan ihmisoikeussopimuksen 8 artiklasta poiketen perustuslain 10 §:n 3 momentti ei mainitse kansallista turvallisuutta sellaisena etuna, joka oikeuttaisi säätämään lailla luottamuksellisen viestin salaisuuden rajoittamisesta.

Luottamuksellisen viestin salaisuutta koskevan perustuslakisääntelyn ensisijaisena tarkoituksena on suojata luottamukselliseksi tarkoitetun viestin sisältö ulkopuolisilta. Perustuslaki turvaa jokaiselle oikeuden luottamukselliseen viestintään ilman, että ulkopuoliset saavat oikeudettomasti tiedon hänen lähettämiensä tai hänelle osoitettujen luottamuksellisten viestien sisällöstä. Tämä merkitsee esimerkiksi suojaa kirjeiden tai muiden suljettujen viestien avaamista tai hävittämistä sekä puhelujen kuuntelemista tai nauhoittamista vastaan. Sääntely ei suojaa ainoastaan viestin lähettäjää, vaan kysymyksessä on viestinnän molempien osapuolten perusoikeus.

Perusoikeussäännökset suojaavat luonnollisia henkilöitä ja oikeushenkilöitä välillisesti. Valtio ja muut julkisyhteisöt jäävät perusoikeussuojan ulkopuolelle. Vieraan valtion viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa. Tällaisen viestinnän havaitsemiseksi voi kuitenkin olla välttämätöntä puuttua luottamuksellisen viestinnän salaisuuteen. Viestintä ammattitoiminnassa voi toiminnan luonteen ja viestinnän osapuolten viestien taltiointia koskevan tietoisuuden vuoksi jäädä luottamuksellisen viestin salaisuuden suojan ulkopuolelle, vaikka tällaisessa viestinnässä voitaisiinkin sinänsä välittää myös luottamuksellisia viestejä henkilöiden välillä (liikenteen ohjauksessa syntyvä puhe- ja viestiliikenne; PeVL 62/2010 vp).

Luottamuksellisen viestin tunnistamistiedot

Viestin sisällön lisäksi perustuslain säännökset suojaavat myös viestin lähettäjän ja vastaanottajan tunnistamistietoja sekä muita tietoja, joilla voi olla merkitystä viestin luottamuksellisuuden säilymiselle. Viestin tunnistamistietojen on perustuslakivaliokunnan vakiintuneessa käytännössä katsottu jäävän luottamuksellisen viestin salaisuutta suojaavan perusoikeuden ydinalueen ulkopuolelle.

Tunnistamistietojen salaisuuden suojaan puuttuvan sääntelyn on täytettävä perusoikeuksien rajoittamisen yleiset edellytykset (PeVL 62/2010 vp, s. 4-5, PeVL 23/2006 vp, s. 3, PeVL 7/1997 vp). Perustuslakivaliokunnan käytännössä on tältä pohjalta pidetty mahdollisena, että tunnistamistietojen saaminen rikosten tutkinnassa jätetään sitomatta tiettyihin rikostyyppeihin, jos sääntely muutoin täyttää perusoikeuksien yleiset rajoitusedellytykset (PeVL 29/2008 vp, s. 2, PeVL 11/2005 vp, s. 4, PeVL 9/2004 vp, s. 4, PeVL 26/2001 vp, s. 3, PeVL 37/2002 vp, vp, s. 3, PeVL 7/1997 vp.). Sääntely tulee tällöin kuitenkin rajata yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tyyppisiin tai niihin törkeysasteeltaan verrattaviin rikoksiin (PeVL 66/2010 vp, s. 7, PeVL 67/2010 vp, s. 4.).

Perustuslakivaliokunta on kuitenkin unionin tuomioistuimen Digital Rights Ireland -asiassa antaman tuomion jälkeen arvioinut, että käytännössä sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen (PeVL 18/2014 vp, s. 6). Valiokunnan uusimmasta lausuntokäytännöstä ei ole vielä selvästi pääteltävissä, miten tällainen uudelleenarviointi muuttaa aiempaa perusoikeuksien yleisiin rajoittamisedellytyksiin nojaavaa tulkintalinjaa. Unionin tuomioistuin on toistanut Digital Rights Ireland -asiassa tietojen kokoamista ja yhdistämistä koskevat huomionsa asiassa Tele2 Sverige AB antamassaan ratkaisussa.

Luottamuksellisen viestin salaisuuden uusi rajoitusperuste

Oikeusministeriön perustuslakisääntelyn tarkistamista arvioinut työryhmä on arvioinut, että perustuslain sanamuodon ja sen nykyisen tulkintakäytännön valossa ei ole mahdollista säätää sellaisista rajoituksista luottamuksellisen viestin salaisuuteen, jonka tarkoituksena olisi laajemmalti kansallisen turvallisuuden kannalta välttämätön tiedon hankkiminen vakavista uhkista. Perustuslain nykyinen sanamuoto ei mahdollista luottamuksellisen viestin salaisuuden suojaan puuttumista tiedon hankkimiseksi esimerkiksi sellaisesta kansallista turvallisuutta uhkaavasta toiminnasta, joka ei ole edennyt niin pitkälle, että siihen voitaisiin kohdistaa konkreettinen ja yksilöity rikosepäily, tai jota ei ole säädetty rangaistavaksi.

Työryhmä on ehdottanut, että perustuslain 10 §:ää muutettavaksi niin, että siihen lisättäisiin uusi 4 momentti, johon koottaisiin säännökset luottamuksellisen viestin salaisuuden rajoittamisen edellytyksistä. Lailla voitaisiin ehdotuksen mukaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten torjunnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

4.2 Toimivaltuuksia koskevat säännösehdotukset

Esityksessä ehdotetut tiedonhankintamenetelmät ovat suurelta osin sellaisia, joista on muissa yhteyksissä säädetty perustuslakivaliokunnan myötävaikutuksella. Näin ollen perusoikeussääntelyn kehittyminen on voitu esityksessä ottaa huomioon.

Tietoliikennetiedustelua, radiosignaalitiedustelua ja tietoliikennetiedustelua sekä tiedustelumenetelmien yleistä käyttötarkoitusta lukuun ottamatta sotilastiedusteluviranomaisille lakiehdotuksessa ehdotettavat tiedustelumenetelmät olisivat paikkatiedustelua ja jäljentämistä lukuun ottamatta vastaavat kuin poliisin poliisilain 5 luvussa säädetyt salaiset tiedon-hankintakeinot, joita poliisilla on oikeus käyttää rikoksen estämiseksi tai paljastamiseksi taikka vaaran torjumiseksi. Toisin kuin poliisin salaisissa tiedonhankintakeinoissa, sotilastiedusteluviranomaisten tiedustelutoimivaltuudet eivät edellyttäisi konkreettista, yksilöityä rikosepäilyä.

Yleisen järjestyksen ja turvallisuuden ylläpitäminen on lainsäädännössä osoitettu poliisin tehtäväksi. Lähtökohtaisesti poliisille kuuluvien tehtävien ja toimivaltuuksien osoittaminen muulle viranomaiselle on poikkeuksellista ja edellyttää erityisiä perusteita. Perustuslakivaliokunta on aikaisemmissa lausunnoissaan katsonut, että poliisin käytössä olevien toimivaltuuksien kanssa samojen valtuuksien säätäminen muulle viranomaiselle ei välttämättä ole sopusoinnussa perusoikeuksien rajoitusedellytyksiin kuuluvan välttämättömyysvaatimuksen näkökulmasta (ks. PeVL 10/2016 vp, s. 3, PeVL 49/2014 vp, s. 2/I, PeVL 37/2002 vp, s. 1-2 ja PeVL 2/1996 vp, s. 3/I).

Sotilastiedustelun tarkoituksena olisi hankkia tietoa ulkoisista uhkista Puolustusvoimien laissa säädettyjen tehtävien suorittamiseksi sekä ylimmän valtiojohdon päätöksenteon tueksi. Lakiehdotuksen 4 §:ssä määriteltäisiin tarkemmin sotilastiedustelun kohteet.

Sotilastiedusteluviranomaisille ehdotettavien tiedustelumenetelmien käytön yleisenä edellytyksenä olisi, että menetelmillä voitaisiin olettaa saatavan tietoa tiedustelutehtävän kannalta. Menetelmiä voitaisiin käyttää salassa niiden kohteilta. Käyttö olisi lopetettava heti, kun käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole.

Hallituksen esityksen yleisperusteluissa ja yksityiskohtaisissa perusteluissa kuvataan yhteiskunnallisia tarpeita ehdotetuille tiedustelutoimivaltuuksille. Ehdotettuja toimivaltuuksia on mahdollista pitää Puolustusvoimien tehtävien kannalta välttämättöminä ja oikeasuhtaisina.

Suunnitelmallinen tarkkailu, tekninen kuuntelu, tekninen katselu ja tekninen seuranta

Sotilastiedusteluviranomaisella olisi suunnitelmallista tarkkailua koskevan 19 §:n mukaan oikeus havainnoida henkilöä tai henkilöryhmää, esinettä, ainetta, omaisuutta, tilaa tai aluetta. Suunnitelmallinen tarkkailu salaisena tiedonhankintamenetelmänä olisi merkityksellinen seurattavan henkilön yksityisyyden suojan kannalta, koska sen avulla hänen elämäänsä seurattaisiin jonkin aikaa. Suunnitelmallisen tarkkailun kohteena voisi olla esimerkiksi se, mitä hän tekee vapaa-aikanaan ja keitä henkilöitä hän tuolloin tapaa.

Lisäksi sotilastiedusteluviranomaisella olisi oikeus kohdistaa henkilöön tai henkilöryhmään teknistä kuuntelua ja teknistä katselua.

Teknisestä kuuntelusta säädettäisiin 23 §:ssä. Pykälän 2 momentin mukaan sotilastiedusteluviranomainen saisi vakituiseen asumiseen käytettävän tilan ulkopuolella kohdistaa henkilöön tai henkilöryhmään teknistä kuuntelua, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

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

Teknisen kuuntelun tarkoituksena on keskustelun tai viestin sisällön selvittäminen. Teknisessä kuuntelussa olisi mahdollista, että muutkin kuin tiedustelutehtävän kannalta merkitykselliset henkilöt voisivat joutua kuuntelun kohteeksi. Tekninen kuuntelu merkitsee puuttumista perustuslain 10 §:n 2 momentissa turvattuun luottamuksellisen viestin salaisuuteen. Perustuslain 10 §:n 3 momentin sanamuoto ei mahdollista teknistä kuuntelua tietojen saamiseksi ulkoisista uhkista Puolustusvoimien lakisääteisten tehtävien suorittamiseksi tai valtion ylimmän johdon päätöksenteon tueksi. Teknisestä kuuntelusta olisi kuitenkin mahdollista säätää tavallisen lain säätämisjärjestyksessä perustuslain 10 §:n 4 momenttiin ehdotetun tiedon hankkimista koskevan uuden rajoitusperusteen nojalla.

Teknisen katselua koskeva sääntely ehdotetaan otettavaksi lakiehdotuksen 25 ja 26 §:ään. Kyseistä tiedustelumenetelmää saisi käyttää vain, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Teknisestä katselusta päättäisi tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies.

Lakiehdotuksen 27 §:ssä säädettäisiin teknisestä seurannasta. Jos teknisen seurannan tarkoituksena on seurata henkilön liikkumista sijoittamalla seurantalaite hänen yllään olevaan vaatteeseen tai mukanaan olevaan esineeseen, saadaan toimenpide suorittaa vain, jos toimenpiteellä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Käytännössä esineiden seuranta usein tarkoittaa niitä kuljettavan henkilön seuraamista.

Tuomioistuin päättäisi henkilön teknisestä seurannasta. Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies saisi päättää toimivaltuuden käyttämisestä väliaikaisesti kiireellisissä tilanteissa.

Henkilön teknistä seurantaa saisi käyttää vain jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

Teknisellä seurannalla on merkitystä perustuslain 9 §:n liikkumisvapauden ja 10 §:n yksityiselämän suojan kannalta. Teknistä katselua ja teknistä seurantaa koskevia toimivaltuuspykäliä voidaan pitää perusoikeusnäkökulmasta ongelmattomina ottaen huomioon kyseisten menetelmien melko vähäisenä pidettävä puuttuminen yksityiselämän suojaan ja liikkumisvapauteen suhteessa siihen tiedustelutehtävän tärkeyteen.

Ehdotetuissa säännöksissä tarkkailu-, kuuntelu- ja katseluoikeudet rajattaisiin siten, että suunnitelmallista tarkkailua, teknistä kuuntelua tai teknistä katselua ei saisi kohdistaa koti-rauhan suojan ydinalueeseen kohdistuvaan vakituiseen asumiseen käytettävään tilaan. Suunnitelmallinen tarkkailu, tekninen kuuntelu ja tekninen katselu eivät näin ollen olisi ongelmallisia perustuslain 10 §:n kotirauhan suojan kannalta.

Peitelty tiedonhankinta

Peitellystä tiedonhankinnasta säädettäisiin lakiehdotuksen 21 §:ssä. Sillä tarkoitettaisiin tiettyyn henkilöön kohdistuvaa lyhytkestoisessa vuorovaikutuksessa tapahtuvaa tiedonhankintaa, jossa sotilastiedusteluviranomaisen virkamiehen tehtävän salaamiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja. Kyseistä tiedonhankintamenetelmää saataisiin käyttää tiedustelutehtävän suorittamiseksi.

Toimivaltuus asettuisi suunnitelmallisen tarkkailun ja peitetoiminnan välimaastoon, koska sitä käyttämällä pyrittäisiin henkilökohtaiseen kontaktiin tiedonhankinnan kohteen kanssa, ei kuitenkaan pitkäaikaiseen kanssakäymiseen ja erityisen luottamussuhteen muodostamiseen kuten peitetoiminnassa. Peitellyssä tiedonhankinnassa ei puututtaisi yksityiselämän suojaan niin syvällisesti kuin peitetoiminnassa. Edellytysten osalta se rinnastuisi suunnitelmalliseen tarkkailuun.

Tekninen laitetarkkailu

Lakiehdotuksen 29 §:ssä ehdotetaan säädettäväksi teknisestä laitetarkkailusta. Teknisellä laitetarkkailulla ei saisi hankkia tietoa viestin sisällöstä tai tunnistamistiedoista. Teknisestä laitetarkkailusta päättäisi tuomioistuin, joskin tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies saisi kiireellisessä tilanteessa päättää tilapäisestä toimenpiteestä. Kysymys olisi tältäkin osin viranomaistoimivaltuuksien kattavasta ja täsmällisestä sääntelystä. Huomioon on myös otettava sotilastiedustelun tarkoitus.

Telekuuntelu, tietojen hankkiminen telekuuntelun sijasta sekä televalvonta

Lakiehdotuksen 32 §:ssä säädettäisiin telekuuntelusta ja 33 §:ssä tietojen hankkimisesta telekuuntelun sijasta. Sotilastiedusteluviranomaiselle voidaan antaa lupa tiedustelutehtävään perustellusti liittyvän viestintään kohdistuvaan telekuunteluun.

Jos on todennäköistä, että tietoa viestin sisällöstä ja siihen liittyviä tunnistamistietoja ei ole enää saatavissa telekuuntelulla, Puolustusvoimien tiedustelulaitokselle voitaisiin antaa lupa hankkia ne teleyritykseltä tai yhteisötilaajalta samoilla edellytyksillä kuin telekuuntelua voidaan suorittaa. Lisäksi 33 §:n 2 momentissa säädettäisiin, että jos tietojen hankkiminen kohdistetaan viestin sisällön selvittämiseksi telepäätelaitteeseen välittömästi yhteydessä olevaan viestin lähettämiseen ja vastaanottamiseen soveltuvaan henkilökohtaiseen tekniseen laitteeseen tai tällaisen laitteen ja telepäätelaitteen väliseen yhteyteen, tiedustelulaitokselle voidaan antaa lupa tekniseen tarkkailuun vain, jos telekuuntelua koskevassa 32 §:ssä säädetyt edellytykset täyttyvät.

Tietojen hankkiminen telekuuntelulla voisi kohdistua sekä valtiollisen toimijan että muun kuin valtiollisen toimijan viestintään. Muun kuin valtiollisen toimijan telekuuntelulla tulisi olla erittäin tärkeä merkitys tiedustelutehtävän suorittamiseksi.

Suhteellisuusperiaate ohjaa tiedustelumenetelmien käyttämistä niin, että niitä ei käytetä vähäisimmissä tapauksissa. Telekuuntelusta päättäisi aina tuomioistuin. Lupa voitaisiin antaa kolmeksi kuukaudeksi kerrallaan muun kuin valtiollisen toimijan telekuunteluun ja kuudeksi kuukaudeksi kerrallaan valtiolliseen toimijaan kohdistuvaan telekuunteluun.

Televalvonta olisi telekuuntelua vähäisempi kajoaminen luottamuksellisen viestinnän suojaan. Perustuslakivaliokunta on todennut, että televalvonnalla hankitaan viestin tunnistamistietoja, jotka valiokunnan vakiintuneen lausuntokäytännön mukaan jäävät viestin salaisuutta koskevan perusoikeuden ydinalueen ulkopuolelle (PeVL 37/2002 vp ja PeVL 11/2005 vp). Perustuslakivaliokunta on kuitenkin unionin tuomioistuimen Digital Rights Ireland -asiassa antaman tuomion jälkeen arvioinut, että käytännössä sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen (PeVL 18/2014 vp). Valiokunnan uusimmista lausunnoista ei ole vielä selvästi pääteltävissä, miten tällainen uudelleenarviointi muuttaa aiempaa perusoikeuksien yleisiin rajoittamisedellytyksiin nojaavaa tulkintaa.

Televalvonnasta säädettäisiin lakiehdotuksen 35 ja 36 §:ssä. Televalvonnasta päättäisi lähtökohtaisesti tuomioistuin, joskin kiireellisessä tilanteessa sallittaisiin sotilastiedusteluviran-omaisen tiedustelumenetelmien käyttöön erityisesti koulutetun virkamiehen tekemä väliaikainen päätös kyseisen menetelmän käyttämisestä. Lisäksi sallittaisiin suostumusperusteinen televalvonta (36 §:n 2 momentti), missä tilanteessa riittäisi pääesikunnan tiedustelupäällikön tai sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen tekemä päätös (3 momentti). Edellä telekuuntelun ja muun vastaavan tietojen hankkimisen yhteydessä lupa-ajasta,

tiedustelumenetelmän käytön perusteesta ja tietojen hankkimista johtavasta ja valvovasta tahosta mainittu, koskisi myös ehdotettua televalvontatoimivaltuutta.

Telekuuntelu, tietojen hankkiminen telekuuntelun sijasta ja televalvonta kohdistuisivat sekä viestin sisältöön että viestin tunnistamistietoihin. Toisaalta vieraan valtion viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa.

Perustuslain 10 §:n 3 momentissa mainitut niin sanotut kvalifioidut lakivaraukset eivät mahdollista säätämistä sellaisista rajoituksista viestin salaisuuteen, joiden tarkoituksena ei olisi yksilöidyn rikoksen torjuminen tai selvittäminen vaan laajemmin Puolustusvoimien lakisääteisten tehtävien suorittamiseksi välttämättömän tiedon hankkiminen vakavista uhkista niihin varautumiseksi sekä valtion ylimmän johdon päätöksenteon tueksi. Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta ja televalvonnasta, joka kohdistuu muun kuin valtiollisen toimijan viestintään, olisi mahdollista säätää tavallisen lain säätämisjärjestyksessä perustuslain 10 §:n 4 momenttiin ehdotetun tiedon hankkimista koskevan uuden rajoitusperusteen nojalla.

Tukiasematiedot

Lakiehdotuksen 37 ja 38 §:ssä säädettäisiin tukiasematietojen hankkimisesta tavalla, joka vastaisi pääosin voimassa olevan poliisilain 5 luvun 11 ja 12 §:n säännöksiä. Kysymys on perustuslain 9 §:ssä turvattuun liikkumisvapauteen ja 10 §:ssä turvattuun yksityiselämän suojaan liittyvästä sääntelystä (PeVL 36/2002 vp).

Sotilastiedusteluviranomainen hankkisi luvan voimassaoloaikana tietyn tukiaseman kautta tietoja tukiasemaan kirjautuneista tai kirjautuvista telepäätelaitteista ja teleosoitteista. Tukiasematietojen hankkiminen kohdistuisi ennalta määräämättömään joukkoon teleosoitteita ja telepäätelaitteita, kuten matkaviestimiä. Toimivaltuus oikeuttaa tiedon saamiseen vain matkaviestimen sijainnista tiettynä hetkenä, mutta sitä vastoin ei siitä, onko matkaviestimellä otettu yhteyttä toiseen matkaviestimeen.

Edellytyksenä tukiasematietojen hankkimiselle olisi, että tukiasematiedot olisivat tarpeellisia tiedustelutehtävän kannalta.

Teleosoitteen ja telepäätelaitteen kirjautumistiedoista ei suoraan saataisi tietoa yksittäisten henkilöiden liikkumisesta tietyllä alueella, vaan teleosoitteiden ja telepäätelaitteiden tiedot olisi erikseen muilla keinoin liitettävä yksittäiseen henkilöön. Tukiasematietojen hankkimisessa ei puututtaisi kohteen perus- ja ihmisoikeuksiin kovinkaan tuntuvasti, jolloin sääntely voidaan jättää toimivaltuutta koskevien edellytysten varaan.

Peitetoiminta ja valeosto

Peitetoiminnasta ja valeostosta ehdotetaan säädettäväksi lakiehdotuksen 40 ja 47 §:ssä. Perustuslakivaliokunta on tarkastellut näitä menetelmiä siinä yhteydessä, kun niitä koskevat säännökset ehdotettiin otettavaksi poliisilakiin (PeVL 5/1999 vp).

Peitetoiminnan edellytyksenä on 40 §:n 2 momentin mukaan se, että peitetoiminta on välttämätöntä tietojen saamiseksi tiedustelutehtävän kannalta ja tiedonhankintaa on tiedustelutehtävän kohteena olevan toiminnan suunnitelmallisuuden, järjestäytyneisyyden tai ammattimaisuuden taikka ennakoitavissa olevan jatkuvuuden tai toistuvuuden vuoksi pidettävä tarpeellisena. Tämä vaatimus ei kuitenkaan koskisi tietoverkossa suoritettavaa peitetoimintaa, koska siihen ei liity fyysisiä turvallisuusriskejä ja se on muuhun peitetoimintaan verrattuna helpommin dokumentoitavissa.

Eduskunnan perustuslakivaliokunta on todennut hallituksen esityksestä laiksi poliisilain muuttamisesta (HE 34/1999 vp) antamassaan lausunnossa (PeVL 5/1999 vp) peitetoiminnan olevan perusoikeusnäkökulmasta valeostoa merkittävämpi. Valiokunta totesi olevan aihetta arvioida peitetoimintaa ennen muuta yksityiselämän suojan kannalta. Lisäksi todettiin tarve arvioida näitä tiedonhankintakeinoja oikeudenmukaista oikeudenkäyntiä koskevan perusoikeuden kannalta. Valiokunta piti asianmukaisena sitä, että peitetoiminnan ala ehdotettiin rajattavaksi pelkästään törkeisiin rikoksiin, jotka lisäksi ovat sellaisia, että niihin liittyvä rikollisuus kokemuksen mukaan kehittyy herkästi luonteeltaan järjestäytyneeksi. Valiokunnan mukaan peitetoiminnan taustalla on erityisen painava yhteiskunnallinen intressi ja tämä intressi liittyy myös tavoitteeseen turvata toisten ihmisten perusoikeuksia.

Peitetoimintaa voitaisiin käyttää vain tiedon hankkimisessa lakiehdotuksen 4 §:ssä säädetyistä kohteista, jotka liittyvät sotilaalliseen toimintaan ja muuhun kaikkein vakavimmin Suomen koskemattomuutta vaarantavaan toimintaan. Välttämättömyyden lisäksi peitetoiminta edellyttäisi siten myös erityisen painavan yhteiskunnallisen intressin olemassaoloa.

Valeostosta säädettäisiin lakiehdotuksen 47 - 50 §:ssä. Säännökset vastaisivat poliisilain 5 luvun säännöksiä. Perustuslakivaliokunta on edellä mainitussa lausunnossaan todennut tarpeen arvioida peitetoimintaa ja valeostoa oikeudenmukaista oikeudenkäyntiä koskevan perusoikeuden kannalta.

Tiedonhankinnasta ilmoittamista koskevassa sääntelyssä otettaisiin huomioon vaatimukset, joita perustuslain 21 § ja EIT:n ratkaisukäytäntö asettavat oikeudenmukaisen oikeudenkäynnin toteuttamiselle rikosprosessissa. Peitetoiminnasta ja valeostosta olisi velvollisuus ilmoittaa tiedonhankinnan kohteelle, jos asiassa aloitetaan esitutkinta (lakiehdotuksen 87 §:n 6 momentti).

Tietolähdetoiminta ja tietolähteen turvaaminen

Tietolähteen ohjatusta käytöstä säädettäisiin lakiehdotuksen 43 §:ssä. Tietolähteen ohjatussa käytössä tietoja ei saisi pyytää hankittavaksi sellaisella tavalla, joka edellyttäisi viranomaiselle kuuluvien toimivaltuuksien käyttöä tai joka vaarantaisi tietolähteen tai muun henkilön hengen tai terveyden. Tietolähteen ohjatusta käytöstä päättäisi pääesikunnan tiedustelupäällikkö. Tietolähteen ohjatusta käytöstä olisi velvollisuus ilmoittaa tiedonhankinnan kohteelle, jos asiassa aloitetaan esitutkinta (87 §:n 6 momentti). Tällöin noudatettaisiin pakkokeinolain 10 luvun 60 §:n säännöksiä salaisen pakkokeinon käytöstä ilmoittamisesta. Vastaavantyyppinen sääntely on poliisilain 5 luvussa.

Säännösehdotuksen voidaan katsoa täyttävän perustuslain vaatimukset tarkkarajaisesta ja täsmällisestä sääntelystä.

Tietolähteen turvaamisesta ehdotetaan otettavaksi säännökset lakiehdotuksen 46 §:ään. Sotilastiedusteluviranomaisille asetettaisiin velvollisuus huolehtia tietolähteidensä turvallisuudesta tarpeen mukaan tiedustelumenetelmän käytön aikana ja myös sen jälkeen valvomalla tietolähteen suostumuksella tämän asuntoa tai muuta tietolähteen asumiseen käyttämää tilaa ja sen välitöntä lähiympäristöä kameran tai muun paikkaan sijoitetun teknisen laitteen, menetelmän tai ohjelmiston avulla, jos se olisi tarpeen tietolähteen henkeä tai terveyttä uhkaavan vaaran torjumiseksi. Säännöksellä suojattaisiin tietolähteen perustuslain 7 §:n 1 momentissa säädettyä oikeutta turvallisuuteen. Turvaamisesta kuten toiminnassa kertyneiden tallenteiden säilyttämisestä ja käyttämisestä säädettäisiin täsmällisemmin kuin tietolähteen turvaamisesta voimassa olevan poliisilain 5 luvun 40 §:n 3 momentissa.

Paikkatiedustelu ja jäljentäminen

Paikkatiedustelusta säädettäisiin 51 ja 52 §:ssä. Paikkatiedustelulla tarkoitettaisiin paikassa toimitettavaa tiedustelua esineen, omaisuuden, asiakirjan, tiedon tai seikan löytämiseksi. Paikkatiedus-

telun kohteena voisi olla esimerkiksi suljettu kulkuneuvo, jota ei käytetä asumiseen, myymälä, virasto tai kahvila. Paikkatiedustelua ei saisi kohdistaa rikoslain 24 luvun 11 §:ssä tarkoitettuun kotirauhan suojaamaan paikkaan, kuten asuntoon tai muuhun asumiseen tarkoitettuun tilaan, jollei voitaisi osoittaa paikkaa tosiasiallisesti käytettävän muuhun kuin pysyväluonteiseen asumiseen (PeVL 36/1998 vp, KKO 2009:54).

Paikkatiedustelua ei voida pitää ongelmallisena perustuslain 10 §:n 1 momentissa suojatun kotirauhan turvan kannalta. Koska paikkatiedustelu tapahtuisi salaa eikä paikkatiedustelussa noudatettaisi kotietsintämenettelyä, olisi huolehdittava riittävistä oikeusturvajärjestelyistä. Ehdotuksen mukaan tuomioistuin päättäisi paikkatiedustelusta, kun se kohdistuu paikkaan, johon ei ole pääsyä tai pääsy siihen on rajoitettu tai estetty (52 §:n 1 momentti), minkä lisäksi paikkatiedustelua koskevalta päätökseltä edellytettäisiin riittävän tarkkaa yksilöintiä (52 §:n 5 momentti). Ehdotukseen sisältyisi myös tiedustelun lopettamista sekä muistiinpanojen ja jäljennösten hävittämistä koskeva velvollisuus eräissä tilanteissa (52 §:n 7 momentti) ja velvollisuus ilmoittaa paikkatiedustelusta sen kohteelle, jos asiassa on aloitettu esitutkinta (87 §:n 6 momentti).

Jäljentämisestä säädettäisiin lakiehdotuksen 53 - 55 §:ssä. Sotilastiedusteluviranomaisella olisi oikeus jäljentää asiakirja tai muu esine käyttämällä teknistä laitetta tietojen hankkimiseksi tiedustelutehtävää varten. Jäljentämistoimivaltuus olisi tarpeen, jottei tiedonhankinta paljastuisi asiakirjan tai muun esineen haltuun ottamisen vuoksi tai siksi, että tiedonhankinta pitkittyisi asiakirjan sisällön ylöskirjaamisen vuoksi. Lisäksi säädettäisiin jäljentämiskielloista vastaavasti kuin pakkokeinolain 7 luvun 3 §:n 1 - 3 momentissa. Edellät tarkoitettua jäljentämistä voidaan pitää perusoikeusnäkökulmasta ongelmattomana.

Lähetyksen jäljentämisestä ehdotetaan säädettäväksi lakiehdotuksen 56 §:ssä. Pykälän mukaan kirje tai muu vastaava lähetys saadaan ennen sen saapumista vastaanottajalle jäljentää, jos lähetyksen jäljentämisellä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

Lähetyksen jäljentämisestä olisi mahdollista säätää tavallisella lailla perustuslain 10 §:n 4 momenttiin ehdotetun tiedon hankkimista koskevan uuden rajoitusperusteen nojalla.

Radiosignaalitiedustelu ja ulkomaan tietojärjestelmätiedustelu

Puolustusvoimien tiedustelulaitos ja puolustushaarat voisivat lakiehdotuksen 60 §:n mukaan tehdä Suomen alueen ulkopuolella olevasta laitteesta lähteviin tai tällaiseen laitteeseen saapuviin radioaaltoihin kohdistuvaa tiedonhankintaa. Radioaaltoja käytetään esimerkiksi asevoimien viestinnässä. Valtioiden hallitsemista taajuusalueista on usein varattu tietyt taajuudet pelkästään asevoimien käyttöön, eikä näillä taajuusalueilla tapahtuvan viestinnän voida katsoa nauttivan yksityisen viestin suojasta. Tiedustelun kohteeksi voi kuitenkin joutua myös radiosignaaleja, jotka sisältävät luottamuksellisen viestin suojan alaan kuuluvaan viestintää. Jos näin kävisi, tällaiset tiedot olisi hävitettävä välittömästi.

Lakiehdotuksen 62 §.n mukaan Puolustusvoimien tiedustelulaitos saisi suorittaa ulkomaan tietojärjestelmätiedustelua eli hankkia tietoteknisin menetelmin tietoa Suomen ulkopuolella olevasta ulkomaisesta tietojärjestelmästä. Kohteena voisivat olla esimerkiksi tietojärjestelmään tallennettujen asiakirjojen sisältämät tiedot ja lähetetyt viestit.

Pykälän 3 momentissa olisi erillinen kielto hankkia tietojärjestelmätiedustelulla tietoja henkilöiden välisestä luottamuksellisesta viestistä. Tämä tarkoittaisi esimerkiksi sitä, että ulkomaan tietojärjestelmätiedustelu on kohdennuttava järjestelmässä oleviin tietoihin pois lukien viestit, jotka nauttivat luottamuksellisen viestin suojaa. Toisaalta tietojärjestelmästä voisi hakea tietoa valtiollisen toimijan toiminnassaan käyttämistä viesteistä.

Koska radiosignaalitiedustelu ja ulkomaan tietojärjestelmätiedustelu eivät saisi 60 §:n 3 momentin ja 62 §:n 3 momentin mukaan kohdistua henkilöiden väliseen luottamukselliseen viestintään, ehdotettu tiedustelumenetelmä ei olisi ongelmallinen perustuslain 10 §:ssä säädetyn luottamuksellisen viestin salaisuuden suojan kannalta.

Tietoliikennetiedustelu ja teknisten tietojen käsittely

Tietoliikennetiedustelusta ehdotetaan säädettäväksi lakiehdotuksen 5 luvussa. Tietoliikennetiedustelulla tarkoitettaisiin Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen kohdistuvaa, tietoliikenteen automatisoituun erotteluun perustuvaa teknistä tiedonhankintaa sekä hankitun tiedon käsittelyä (65 §).

Tietoliikennetiedustelua saataisiin tehdä, jos kohteena olisi tiedustelutehtävän kannalta olennainen toimija ja tiedustelulla voitaisiin saada tiedustelutehtävän kannalta välttämätöntä tietoa (70 §:n 1 momentti).

Sen sijaan sellaiselle tietoliikennetiedustelulle, joka voidaan kohdistaa pelkästään vieraan valtion viranomaisen tai sellaiseen rinnastuvan tahon tietoliikenteeseen, ei asetettaisi muita edellytyksiä, kuin että kohteen olisi oltava tiedustelutehtävän kannalta olennainen (68 §:n 1 momentti).

Tätä tiukempien edellytysten asettamista ei ole pidettävä perusteltuna, sillä valtio ja muut julkisyhteisöt jäävät perusoikeussuojan ulkopuolelle (HE 309/1993 vp ja PeVL 9/2015 vp). Näin ollen esimerkiksi vieraan valtion viranomaisorganisaation tietoliikenne tai muu viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa, eikä pelkästään tällaisten organisaatioiden viesteihin kohdistuvasta tietoliikennetiedustelusta säätäminen muodostuisi perustuslain 10 §:n 3 momentin kannalta ongelmalliseksi.

Tietoliikennetiedustelua ei kuitenkaan arvioida olevan mahdollista kohdistaa kaikissa tapauksissa niin täsmällisesti, ettei olisi vaaraa viranomaisten tilapäisestä pääsystä yksittäisten, tiedustelutehtävään liittymättömien henkilöiden viestintään. Arvioitaessa, onko ehdotetuissa tietoliikennetiedustelua koskevissa toimivaltuuksissa kyse luottamuksellisen viestin salaisuuden rajoittamisesta, on otettava huomioon EIT:n ja EU-tuomioistuimen ratkaisukäytäntö, jonka mukaan tietojen kerääminen tai jo pääsy niihin muodostaa puuttumisen yksityiselämän suojaan. Tämän vuoksi kummatkin tuomioistuimet ovat nostaneet ratkaisevaksi kriteeriksi tietoliikennetiedustelun hyväksyttävyyden kannalta sen, onko kansallisen sääntelyn katsottu olevan suhteellisuusperiaatteen mukainen perusoikeutta rajoitettaessa.

Euroopan ihmisoikeustuomioistuimen oikeuskäytännön mukaan luottamuksellisen viestinnän salaisuuden rajoitukselle on aina oltava painava yhteiskunnallinen tarve, puuttumisen ja tavoiteltavan hyväksytyn päämäärän tulee olla oikeassa suhteessa keskenään ja puuttumiselle pitää olla riittävän painavat ja hyväksyttävät perustelut. Lisäksi rajoitusten on oltava lain sallimia. Ihmisoikeustuomioistuimen oikeuskäytännössä on painotettu lain laatua, kuten täsmällisyyttä sekä viranomaistoiminnan ennustettavuutta turvaavaa sääntelyä.

Ihmisoikeustuomioistuin on pitänyt luottamuksellisen viestin salaisuuden rajoittamisen välttämättömyyden ja lainmukaisuuden kannalta ongelmallisena muun muassa tiedusteluviranomaisille laissa säädettyä rajoittamatonta toimivaltaa määritellä luottamuksellisiin viesteihin puuttumisen edellytykset (Roman Zakharov v. Venäjä). Myös Euroopan unionin oikeus edellyttää tiedonhankinnan perustumista unionin perusoikeusjärjestelmän kannalta hyväksyttäviin päämääriin sekä sitä, ettei tiedonhankinnalla puututa yksityiselämän suojaan suhteettomasti tai tämän oikeuden keskeistä sisältöä loukaten. Euroopan unionin tuomioistuimen oikeuskäytännössä on erityisesti painotettu sitä, että tiedonhankinnan on oltava riittävän kohdennettua ja yksilöityä (ratkaisut Digital Rights Ireland ja Schrems).

EIT:n kantaa suhteellisuusperiaatteen mukaisuudesta ilmentää sen jo vuonna 1990 ratkaisuissa Huvig v. Ranska ja Kruslin v. Ranska luoma testi, jota se myöhemmissä ratkaisuissaan on toistuvasti soveltanut ja jossain määrin myös edelleen kehittänyt. EU-tuomioistuin on Digital Rights Ireland -asiassa ja Schrems -asiassa (C-362/14) antamissaan tuomioissa käytännössä samaa argumentaatiomallia kuin EIT edellä mainituissa ratkaisuissaan. Kyseisen testin mukaan viestintäsalaisuuteen puuttumisen oikeuttavan kansallisen sääntelyn on sisällettävä: 1) niiden henkilöiden määrittelyn, joiden viestintäsalaisuuteen puututaan, 2) niiden rikosten tai uhkien määrittelyn, joilla puuttumista viestintäsalaisuuteen perustellaan, 3) säännökset siitä, kuinka puuttumisesta päätetään ja 4) kuinka tietoja käsitellään, käytetään ja säilytetään, 5) säännökset viestintäsalaisuuteen puuttumisen kestosta ja toimenpiteiden avulla kerättyjen tietojen säilytysajoista sekä 6) varotoimenpiteistä, kun tietoa annetaan muiden käyttöön ja 7) menettelystä tietojen poistamista ja hävittämistä varten.

Lakiehdotus sisältää edellä mainitun testin järjestystä noudattaen säännökset tietoliikennetiedustelun kohdistamisesta ja tiedon käsittelystä ja viestintäsalaisuuteen puuttumisen kestosta (65, 68 ja 70 §), uhkista, joista tietoa voidaan hakea (4 §), päätöksenteosta ja tuomioistuimen luvasta sekä kiiretilanteen päätösmenettelystä (69 ja 71 §), tietoliikennetiedustelun käytöstä ilmoittamisesta (87 §), menettelystä tuomioistuimessa (136 §), tiedon luovuttamisesta rikostorjuntaan (78 §), tiedustelukiellosta (128 §) ja tietojen hävittämisestä (74 §). Tietoliikennetiedustelulla kerättyjen tietojen säilytysajat määräytyvät arkistolain säännösten mukaan. Henkilötietojen poistamisesta sotilastiedustelun tietojärjestelmästä ja muista henkilörekistereistä säädetään 116 ja 117 §:ssä.

Tietoliikennetiedustelua koskevaa säännösehdotuksia on pidettävä perustuslakivaliokunnan mietinnössä PeVM 25/1994 vp muotoilemien perusoikeuksien rajoittamista koskevien yleisten oppien mukaisena paitsi muilta osin, myös Suomen kansainvälisten ihmisoikeusvelvoitteiden kannalta. Tietoliikennetiedustelusta, joka kohdistuu muuhun kuin vieraaseen valtioon tai siihen rinnastettavaan tahoon eli valtiolliseen toimijaan, olisi mahdollista säätää tavallisen lain säätämisjärjestyksessä perustuslain 10 §:n 4 momenttiin ehdotetun tiedon hankkimista koskevan uuden rajoitusperusteen nojalla.

Tietoliikennetiedustelu olisi hakuehtoihin perustuvaa, mahdollisimman kohdennettua sekä rajattua ja edellyttäisi aina tuomioistuimen lupaa. Ehdotettu sääntely ei mahdollistaisi yleistä, kaikenkattavaa tietoliikenteen seurantaa.

Lakiehdotuksen 66 §:n mukaan tietoliikennetiedustelun kohdentamiseksi Puolustusvoimien tiedustelulaitoksella olisi oikeus kerätä ja tallentaa tietoliikenteen teknisiä tietoja eli muun muassa viestien tunnistamistietoja ja käsitellä niitä tilastollista analyysiä varten. Teknisten tietojen kerääminen ja tallentaminen tapahtuisi hetkellisesti. Teknisiä tietoja analysoimalla voitaisiin hankkia tarkempia tietoja tietoliikennetiedustelua koskevaa lupahakemusta varten.

Tiedustelu ei kohdistuisi viestin sisältöön vaan viestinnän teknisiin tietoihin, joiden avulla tietoliikennetiedustelua voitaisiin kohdistaan paremmin vain niihin viestintäverkon osiin, joissa liikkuisi tiedustelutehtävän kannalta olennaista viestintää.

Koska mainitussa pykälässä tarkoitettu 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.

4.3 Sotilastiedustelun tietojärjestelmä ja muut henkilörekisterit

Henkilötietojen suojasta on perustuslain 10 §:n 1 momentin mukaan säädettävä lailla. Yleinen henkilötietojen suojaa koskeva laki on henkilötietolaki. Jos on tarkoitus poiketa henkilötietolaissa säädetyistä velvoitteista, säännökset on otettava lakiin. Lain tasoista sääntelyä tarvitaan, jos kysymys on erityissäännöksistä, jotka koskevat rekisteröinnin tavoitetta, rekisteröitävien henkilötietojen sisältöä, henkilötietojen sallittuja käyttötarkoituksia, mukaan luettuina tietojen luovutettavuus, henkilörekisterien yhdistämistä sekä tietojen antamista teknisen käyttöyhteyden avulla ja tietojen säilytysaikaa (PeVL 25/1998 vp, PeVL 14/2002 vp, PeVL 30/2006 vp, PeVL 12/2002 vp).

Perustuslakivaliokunta on arvioidessaan viranomaisten oikeutta saada salassa pidettäviä tietoja muilta viranomaisilta tarkastellut sitä, millä ehdoilla tietoja pyytävän viranomaisen tiedonsaantiintressi voi syrjäyttää salassapitointressit. Valiokunta on arviossaan kiinnittänyt huomiota muun muassa siihen, mihin ja ketä koskeviin tietoihin tiedonsaantioikeus ulottuu ja miten tiedonsaantioikeus sidotaan tietojen välttämättömyyteen (PeVL 7/2000 vp, s. 4; PeVL 7a/2000 vp, s. 2—3; PeVL 23/2006 vp, s. 3).

Väljässä ja ulottuvuudeltaan laajassa sääntely-yhteydessä perustuslakivaliokunta on pitänyt erityisen tärkeänä, että tietojensaantioikeus rajoitetaan koskemaan ainoastaan välttämättömiä tietoja. Jos luovutettavien tietojen sisältö on rajattu täsmällisesti, on tietojen luovuttaminen voinut koskea jonkin tarkoituksen vuoksi tarpeellisia tietoja (PeVL 14/2002 vp, s. 2).

Lakiehdotuksen 10 luvussa säädettäisiin yksityiskohtaisesti sotilastiedustelun tietojärjestelmän ja tilapäisen henkilörekisterin käyttötarkoituksesta ja tietosisällöstä (102, 103 ja 105 §), oikeudesta saada tietoa muista rekistereistä ja tietojärjestelmistä, viranomaisilta ja liiken-teenharjoittajalta(109 - 111 §) sekä tietojen luovuttamisesta sotilastiedustelun henkilörekistereistä (112 - 116 §).

Niiltä osin kuin ehdotetussa laissa ei toisin säädettäisi, rekisteröidyn oikeudet määräytyisivät henkilötietolain mukaan. Rekisterien tietosisällöt sekä niiden tietolähteet ja tietojen luovutus niistä perustuvat Puolustusvoimien sotilastiedusteluviranomaisille lakiehdotuksessa säädettyihin tehtäviin ja viranomaisten lain nojalla tekemiin päätöksiin.

Rekistereihin talletettavien henkilötietojen säilytysajasta säädettäisiin mahdollisimman tarkasti, mitä on pidettävä olennaisena henkilötietojen suojan kannalta.

4.4 Eräät muut säännökset

Lakiehdotuksen 93 §:ssä ehdotetaan säädettäväksi tiedustelumenetelmää koskevasta ilmaisukiellosta. Tiedustelutehtävän suorittamisessa avustanut sivullinen tai asevelvollisuuslain mukaisessa palveluksessa oleva ei saa ilmaista tietoonsa tullutta tietoa tai seikkaa tiedustelutehtävästä.

Ilmaisukiellon ei voida katsoa rajoittavan perustuslain 12 §:n 1 momentissa turvattua sananvapautta ottaen huomioon perusoikeuden yleiset rajoitusedellytykset, erityisesti täsmällisyys- ja tarkkarajaisuusvaatimus sekä hyväksyttävyysvaatimus. Ilmaisukiellosta säädettäisiin lain tasolla. Ilmaisukieltoa on pidettävä välttämättömänä, koska tiedustelumenetelmän käytön tuleminen sivullisen välityksellä kohdehenkilön tietoon voisi estää menetelmän käytön tai vaarantaa sen tarkoituksen toteutumisen. Koska ilmaisukiellon rikkominen olisi rangaistavaa salassapitorikoksena tai -rikkomuksena rikoslain 38 luvun 1 tai 2 §:n nojalla, ehdotettava säännös kytkeytyisi lisäksi sananvapauden rikosoikeudelliseen rajoitukseen eli niin sanottuun ilmaisuvapausrikokseen.

Lakiehdotuksen 94 §:ään ehdotetaan otettavaksi säännökset teleyrityksen ja 95 §:ään tiedonsiirtäjän avustamisvelvollisuudesta. Avustamisvelvollisuus koskisi muun muassa tele-kuuntelun ja tele-

valvonnan edellyttämien kytkentöjen tekemistä televerkkoon sekä tietojen, välineiden ja henkilöstön käyttöön antamista telekuuntelun toimeenpanoa varten. Lakiehdotuksen 95 §:n mukaan Puolustusvoimien tiedustelulaitoksella on oikeus sijoittaa tietoliikennetiedustelun edellyttämä laite tiedonsiirtäjän hallinnoiman viestintäverkon osaan. Tiedonsiirtäjällä olisi velvollisuus a antaa tiedustelulaitoksen käyttöön tietoliikennetiedustelun edellyttämät tarpeelliset tilat, tiedot, välineet ja henkilöstö.

Teleyrityksille ja tiedonsiirtäjille asetettavia velvoitteita on pidettävä perustuslain 15 §:n 1 momentissa turvatun omaisuudensuojan kannalta ongelmattomina, sillä velvoitteet perustuisivat täsmällisiin säännöksiin ja olisivat nyt kyseessä olevien yritysten kannalta kohtuullisia (PeVL 8/2002 vp ja 61/2002 vp). Kohtuullisuusarvioinnin kannalta on huomioitava, ettei tiedonsiirtäjä olisi velvoitettu antamaan sotilastiedusteluviranomaiselle mitään kohdentamisen kannalta merkityksetöntä tietoa ja että tiedonsiirtäjän velvollisuus antaa tietoja koskisi ainoastaan sellaisia tietoja, jotka sillä hallussaan jo on. Sekä teleyritykselle sen avustamisvelvollisuuden että tiedonsiirtäjälle sen tietojenantovelvollisuuden täyttämisestä aiheutuvat kustannukset ehdotetaan korvattavaksi.

Säännöksillä tiedustelumenetelmän käytön lopettamisesta eräissä tilanteissa (10 ja 86 §), tiedon ilmoittamisesta rikostorjuntaan (78 §), tietojen hävittämisestä (59, 74, 84 ja 86 §) ja tiedustelukielloista (128 §) rajoitettaisiin tiedustelumenetelmillä saatujen tietojen hyödyntämistä. Säännöksillä toteutettaisiin lakiehdotuksen 1 luvussa säädettyjä yleisiä periaatteita, kuten suhteellisuusperiaatetta, vähimmän haitan periaatetta ja tarkoitussidonnaisuuden periaatetta sekä perustuslain 21 §:ssä suojattua oikeusturvaa.

Lakiehdotuksen 72 §:ssä säädettäisiin tietoliikennetiedustelun edellyttämän kytkennän toteuttamisesta. Tietoliikennetiedustelun kytkennän suorittaja panisi täytäntöön tietoliikennetiedustelua koskevassa luvussa tarkoitetut luvat yhteistyössä tiedonsiirtäjän kanssa. Kytkennän suorittaja luovuttaisi luvassa tarkoitetun liitynnän mukaisessa viestintäverkon osassa liikkuvan tietoliikenteen Puolustusvoimien tiedustelulaitokselle. Kytkennän suorittajana toimisi Suomen Erillisverkot Oy, joka on valtion täysin omistama yritys.

Lakiehdotuksen 89 §:n mukaan kertausharjoituksessa oleva riittävän koulutuksen saanut reserviläinen voisi avustaa sotilastiedusteluviranomaista radiosignaalitiedustelussa, ulkomaan tietojärjestelmätiedustelussa, teknisten tietojen käsittelyssä ja tietoliikennetiedustelun kohdentamisessa. Sotilaallisen valmiuden joustavaan kohottamiseen tarkoitetussa kertausharjoituksessa tai asevelvollisuuslaissa tarkoitetussa ylimääräisessä palveluksessa oleva taikka liikekannallepanon aikaiseen palvelukseen määrätty riittävän koulutuksen saanut reserviläinen voisi käyttää lisäksi suunnitelmallista tarkkailua, teknistä kuuntelua, teknistä katselua ja teknistä laitetarkkailua sekä ulkomaan tietojärjestelmätiedustelua tiedustelutehtävän suorittamiseksi. Myös sotilastiedusteluviranomaisen palveluksesta eroamisiän saavuttamisen vuoksi eronnut kertausharjoituksessa oleva reserviläinen saisi käyttää 4 luvun toimivaltuuksia.

Reserviläinen olisi valtuuksia käyttäessään rikoslain virkavastuuta koskevien säännösten alainen (91 §) ja häneen sovellettaisiin vahingonkorvauslain 4 luvun säännöksiä asevelvollisen korvausvastuusta (92 §).

Säännösehdotuksia, jotka koskevat Suomen Erillisverkot Oy:n toimimista tietoliikennetiedustelun edellyttämän kytkennän suorittajana sekä asevelvollisuuslain mukaisessa palveluksessa olevan reserviläisen osallistumista sotilastiedusteluun, on arvioitava hallintotehtävän antamista muulle kuin viranomaiselle koskevan perustuslain sääntelyn kannalta.

Perustuslain 124 §:n mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaa-

ranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle.

Perustuslain esitöiden ja perustuslakivaliokunnan käytännön perusteella merkittävän julkisen vallan käyttämisenä on pidettävä esimerkiksi itsenäiseen harkintaan perustuvaa oikeutta käyttää voimakeinoja tai puuttua muuten merkittävällä tavalla yksilön perusoikeuksiin.

Suomen Erillisverkot Oy:n tehtävä ohjata luvan mukainen tietoliikenne sotilastiedusteluviranomaiselle ei olisi luonteeltaan itsenäistä harkintavaltaa edellyttävää julkisen vallan käyttöä vaan tuomioistuimen myöntämän luvan toimeenpanoa. Tietoliikennetiedustelun uskot-tavuutta ja luotettavuutta lisää se, että sotilastiedusteluviranomaisella ei ole pääsyä muuhun tietoliikenteeseen kuin siihen, jota luvat koskevat.

Koska reserviläisillä olisi 89 §:n 3momentin nojalla oikeus käyttää toimivaltuuksia ainoastaan tiedustelumenetelmän käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa, kyse ei siten olisi itsenäisen harkintavallan eikä merkittävästä julkisen vallan käytöstä.

Perustuslain 12 §:n 2 momentin mukaan viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Jokaisella on oikeus saada tieto julkisesta asiakirjasta.

Pääsääntöisesti asiakirjojen salassapidosta säädetään viranomaisten toiminnan julkisuudesta annetussa laissa. Julkisuuslain 24 §:n 1 momentissa säädetään, että sotilastiedustelua koskevat asiakirjat ovat salassa pidettäviä (10 kohta).

Perustuslakivaliokunnan käytännön mukaan toisen perusoikeuden edistäminen on sellainen välttämätön syy, jonka vuoksi viranomaisen hallussa olevien asiakirjojen julkisuutta on mahdollista perustuslain 12 §:n 2 momentin nojalla lailla erikseen rajoittaa (PeVL 39/2009 vp, s. 3; PeVL 2/2008 vp, s. 2). Sotilastiedustelun tarkoituksena on myös turvata perusoikeuksia, kuten oikeutta elämään ja henkilökohtaiseen turvallisuuteen, omaisuuden suojaa ja ympäristöä niihin kohdistuvilta uhkilta. Suomeen kohdistuvien ulkoisten uhkien kartoittaminen on osa perusoikeuksien suojaamista.

Tietojen salassapito ei olisi täysin ehdotonta. Lakiehdotukseen ehdotetaan säännöksiä salassa pidettävien sotilastiedustelu- ja rekisteritietojen luovuttamisesta (18, 76 ja 112 - 115 §). Ehdotuksen katsotaan täyttävän perustuslain 12 §:n 2 momentista johtuvat vaatimukset.

Lakiehdotuksen 134 §:ään ehdotetaan säännöstä, jonka mukaan sotilasviranomaisen virka-miehen on tarvittaessa ilmaistava tiedustelutehtävään liittyvän toimenpiteen kohteena olevalle henkilölle olevansa sotilastiedusteluviranomaisen virkamies ja pyynnöstä esitettävä virkamerkkinsä. Sotilastiedusteluviranomaisen on huolehdittava siitä, että virkatoimen suorittanut virkamies on tarvittaessa yksilöitävissä. Vaatimus virkamiehen yksilöitävyydestä pohjautuu viime kädessä perustuslain 118 §:ään, jonka mukaan virkamies vastaa virkatoimensa lainmukaisuudesta.

Perustuslain 118 §:n 3 momentin mukaan jokaisella, joka on kärsinyt oikeudenloukkauksen tai vahinkoa virkamiehen tai julkista tehtävää hoitavan henkilön lainvastaisen toimenpiteen tai laiminlyönnin vuoksi, on oikeus vaatia tämän tuomitsemista rangaistukseen sekä vahingonkorvausta. Jotta perustuslain 118 §:n 3 momentissa säädetty oikeus voisi käytännössä toteutua, tulee virkatoimen suorittanut virkamies tarvittaessa pystyä yksilöimään. Tarkemmat säännökset virkamerkistä annettaisiin puolustusministeriön asetuksella.

4.5 Säätämisjärjestyksen arviointi

Esitykseen sisältyvä lakiehdotus voidaan hallituksen käsityksen mukaan käsitellä tavallisen lain säätämisjärjestyksessä lukuun ottamatta säännösehdotuksia, jotka koskevat teknistä kuuntelua (23 §), muuhun kuin valtiolliseen toimijaan kohdistuvaa telekuuntelua (32 §:n 3 momentti), muun kuin valtiollisen toimijan tietojen hankkimista telekuuntelun sijasta (33 §), muuhun kuin valtiolliseen toimijaan kohdistuvaa televalvontaa (35 §:n 2 momentti), lähetyksen jäljentämistä (56 §) ja muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvaa tiedustelua (70 §). Niistä olisi kuitenkin mahdollista säätää tavallisen lain säätämisjärjestyksessä perustuslain 10 §:n 4 momenttiin ehdotetun tiedon hankkimista koskevan uuden rajoitusperusteen nojalla.

Koska esitys sisältää perustuslain kannalta merkityksellisiä asioita ja osa säätämisjärjestystä koskevista kysymyksistä ovat tulkinnanvaraisia, hallitus pitää tarkoituksenmukaisena, että eduskunta pyytää esityksestä perustuslakivaliokunnan lausunnon.

Edellä esitetyn perusteella annetaan eduskunnan hyväksyttäviksi seuraava lakiehdotus:

Lakiehdotus

Laki
sotilastiedustelusta

1 luku

Yleiset säännökset

1 §

Lain soveltamisala

Tässä laissa säädetään Puolustusvoimien tiedustelutoiminnan (sotilastiedustelu) tarkoituksesta, viranomaisen tehtävistä ja toimivaltuuksista, päätöksenteosta sekä tiedustelun ohjauksesta ja valvonnasta.

2 §

Suhde muuhun lainsäädäntöön

Siviilitiedustelusta säädetään poliisilain 5 a luvussa (/) ja tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa (/). Tiedustelutoiminnan valvonnasta säädetään laissa (/).

Puolustusvoimien rikostorjunnasta säädetään sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetussa laissa (255/2014).

Henkilötietojen käsittelystä säädetään henkilötietolaissa (523/1999) ja viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999), jollei tässä laissa toisin säädetä.

3 §

Sotilastiedustelun tarkoitus

Sotilastiedustelun tarkoituksena on hankkia ja käsitellä tietoa ulkoisista uhkista ylimmän valtiojohdon päätöksenteon tueksi ja Puolustusvoimista annetun lain (551/2007) 2 §:ssä tarkoitettujen Puolustusvoimien tehtävien suorittamiseksi.

4 §

Sotilastiedustelun kohteet

Sotilastiedustelulla voidaan hankkia kotimaassa ja ulkomailla tietoja:
1) sotilaallisesta toiminnasta;
2) ulkomaisesta tiedustelutoiminnasta;
3) valtio- ja yhteiskuntajärjestystä uhkaavasta toiminnasta;
4) joukkotuhoaseista;
5) sotatarvikkeiden kehittämisestä ja levittämisestä;

6) valtioon tai yhteiskunnan elintärkeisiin toimintoihin kohdistuvista vakavista uhkista;
7) vieraan valtion suunnitelmista tai toiminnasta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille taikka muille tärkeille eduille;
8) kansainvälistä rauhaa ja turvallisuutta uhkaavista kriiseistä;
9) kansainvälisten kriisinhallintaoperaatioiden turvallisuuteen kohdistuvista uhkista;
10) Puolustusvoimien kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuuteen kohdistuvista uhkista.

5 §

Suhteellisuusperiaate

Sotilastiedustelun toimenpiteiden on oltava puolustettavia suhteessa tiedon hankinnalla saatavien tietojen tärkeyteen sekä välttämättömyyteen ja tietojen saamisen kiireellisyyteen, tavoiteltavaan sotilastiedustelun päämäärään, sotilastiedustelun kohteeseen, muille tiedustelutoimenpiteen käytöstä aiheutuvaan oikeuksien loukkaamiseen sekä muihin asiaan vaikuttaviin seikkoihin.

6 §

Vähimmän haitan periaate

Sotilastiedustelun toimivaltuuden käytöllä ei kenenkään oikeuksiin saa puuttua enempää eikä kenellekään saa aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi.

7 §

Tarkoitussidonnaisuuden periaate

Sotilastiedustelun toimivaltuutta saadaan käyttää vain tässä laissa säädettyyn tarkoitukseen.

8 §

Syrjinnän kielto

Sotilastiedustelun toimenpiteiden kohdentaminen on toteutettava syrjimättömästi. Sotilastiedustelun toimenpiteen kohdentaminen ei saa perustua ainoastaan henkilön alkuperää, kansalaisuutta, kieltä, uskontoa, vakaumusta, mielipidettä, poliittista toimintaa, ammattiyhdistystoimintaa, perhesuhteita, seksuaalista suuntautumista koskeviin tietoihin, jollei tiedonhankinnan välttämättömyydestä muuta johdu.

9 §

Määritelmät

Tässä laissa tarkoitetaan:
1) *kytkennän suorittajalla* julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain (10/2015) 6 §:ssä tarkoitettua verkko- ja infrastruktuuripalvelujen tuottajaa tai sen täysin omistamaa yritystä;
2) *sijaintitiedolla* viestintäverkosta tai päätelaitteesta saatavaa tietoa, joka ilmaisee liittymän tai päätelaitteen maantieteellisen sijainnin ja jota käytetään muuhun kuin viestin välittämiseen;
3) *teleyrityksellä* sitä, joka tarjoaa verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille eli harjoittaa yleistä teletoimintaa;
4) *tiedonsiirtäjällä* tahoa, joka omistaa tai hallitsee Suomen rajan ylittävää viestintäverkon osaa;

5) *tiedustelumenetelmällä* 4 ja 5 luvussa säädettyjä sotilastiedusteluviranomaisen toimivaltuuksia;
6) *tietoliikenteen teknisillä tiedoilla* muita kuin viestin sisältöön kuuluvia tietoliikenteen tietoja;
7) *tunnistamistiedolla* tietoyhteiskuntakaaren (917/2014) 3 §:n 7 kohdassa tarkoitettuun tilaajaan tai mainitun pykälän 30 kohdassa tarkoitettuun käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa;
8) *valtiollisella toimijalla* vieraan valtion viranomaista tai sellaiseen rinnastuvaa toimijaa;
9) *viestintäverkolla* toisiinsa liitetyistä johtimista sekä laitteista muodostuvaa järjestelmää, joka on tarkoitettu viestien siirtoon tai jakeluun johtimella, radioaalloilla, optisesti tai muulla sähkömagneettisella tavalla;
10) *yhteisötilaajalla* tietoyhteiskuntakaaren 3 §:n 41 kohdassa tarkoitettua yhteisötilaajaa.

10 §

Tiedustelumenetelmien käytön edellytykset

Tiedustelumenetelmän käytön edellytyksenä on, että sillä voidaan olettaa saatavan tietoa tiedustelutehtävän kannalta.

Tässä laissa säädettyjä tiedustelumenetelmiä voidaan käyttää salassa niiden kohteilta.

Tiedustelumenetelmän käyttö on lopetettava ennen päätöksessä tai luvassa mainitun määräajan päättymistä heti, kun käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole.

2 luku

Sotilastiedustelun viranomaiset sekä ohjaus ja seuranta

11 §

Sotilastiedustelun ohjaus ja johtaminen

Ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteinen kokous käsittelee valmistelevasti sotilastiedustelun kohteita koskevat painopisteet.

Puolustusministeriö ohjaa sotilastiedustelua hallinnollisesti ja antaa 1 momentissa tarkoitetut valmistelevasti käsitellyt painopisteet Puolustusvoimille.

Pääesikunta johtaa sotilastiedustelutoimintaa noudattaen sotilastiedustelun painopisteitä.

12 §

Sotilastiedusteluviranomaiset

Sotilastiedusteluviranomaisia ovat pääesikunta ja Puolustusvoimien tiedustelulaitos, jotka voivat hankkia tietoa tiedustelutehtävän suorittamiseksi siten kuin jäljempänä säädetään.

Sotilastiedustelutoiminnasta puolustushaaroissa säädetään 60 §:ssä. Puolustushaarat ovat sotilastiedustelutoiminnassa sotilastiedusteluviranomaisen alaisia.

13 §

Tiedustelutehtävä

Tiedustelutehtävällä tarkoitetaan pääesikunnan tiedustelupäällikön sotilastiedusteluviranomaiselle antamaa toimeksiantoa tiedustelutiedon hankkimiseksi 4 §:ssä tarkoitetusta sotilastiedustelun kohteesta. Tiedustelutehtävän on perustuttava 3 §:ssä säädettyyn sotilastiedustelun tarkoitukseen tai 16 §:ssä tarkoitettuun tietopyyntöön.

14 §

Sotilastiedustelun seuranta

Puolustusministeriö antaa ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteiselle kokoukselle selvityksen ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin valmistelevasti käsittelemistä painopisteistä kerran vuodessa tai ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteisen kokouksen pyynnöstä taikka puolustusministeriön aloitteesta.

Pääesikunta antaa vuosittain selvityksen puolustusministeriölle sotilastiedustelun laadusta ja laajuudesta sekä sen kohdentumisesta. Selvitys on lisäksi annettava viivytyksettä puolustusministeriön sitä pyytäessä.

3 luku

Yhteistoiminta muiden viranomaisten kanssa ja kansainvälinen yhteistyö

15 §

Yhteistyö suojelupoliisin ja muiden viranomaisten kanssa

Sotilastiedusteluviranomaisten on toimittava yhteistyössä suojelupoliisin kanssa tiedustelun tarkoituksenmukaiseksi hoitamiseksi sekä annettava suojelupoliisille tässä tarkoituksessa tarpeellisia tietoja sen estämättä, mitä salassapitovelvollisuudesta säädetään.

Muut viranomaiset voivat avustaa tarvittaessa sotilastiedusteluviranomaista tiedustelutehtävän suorittamisessa.

Valtioneuvoston asetuksella voidaan antaa tarkempia säännöksiä sotilastiedusteluviranomaisen ja suojelupoliisin välisestä yhteistyöstä.

16 §

Tietopyyntö

Ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteisen kokouksen valmistelevasti käsittelemien painopisteiden mukaisia tietopyyntöjä sotilastiedustelun kohteista voivat tehdä pääesikunnalle tasavallan presidentti, valtioneuvoston kanslia, ulkoasiainministeriö ja puolustusministeriö.

17 §

Tiedustelutoiminnan yhteensovittaminen

Sotilas- ja siviilitiedustelutoimintaa sovitetaan yhteen tasavallan presidentin, valtioneuvoston kanslian, ulkoasiainministeriön, puolustusministeriön ja sisäministeriön kesken sekä tarvittaessa muiden ministeriöiden ja viranomaisten kesken.

Jos sotilastiedustelutoiminnan arvioidaan olevan ulko- ja turvallisuuspoliittisesti merkittävää, asia on valmistelevasti käsiteltävä 1 momentissa tarkoitettujen viranomaisten kesken.

18 §

Kansainvälinen yhteistyö

Sotilastiedusteluviranomainen voi Suomen kansallisen turvallisuuden varmistamiseksi tehtäviinsä liittyen:

1) vaihtaa tiedustelutietoja ulkomaisten tiedustelu- ja turvallisuuspalveluiden kanssa salassapitosäännösten estämättä;

2) osallistua tiedustelutietojen hankkimiseen ja arvioimiseen liittyvään kansainväliseen yhteistoimintaan.

Pääesikunnan tiedustelupäällikkö päättää kansainvälisestä yhteistyöstä Suomessa tai ulkomailla sekä siihen liittyvien toimivaltuuksien käytöstä.

Tietojen luovuttamisessa ja vastaanottamisessa noudatetaan lisäksi, mitä siitä erikseen Suomea velvoittavissa kansainvälisissä sopimuksissa määrätään tai kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) säädetään.

4 luku

Tiedonhankintatoimivaltuudet

19 §

Tarkkailu ja suunnitelmallinen tarkkailu

Tarkkailulla tarkoitetaan tiettyyn henkilöön tai henkilöryhmään taikka esineeseen, aineeseen, omaisuuteen, tilaan tai alueeseen salaa kohdistettavaa havaintojen tekemistä tiedustelutarkoituksessa.

Suunnitelmallisella tarkkailulla tarkoitetaan muun kuin lyhytaikaisen tarkkailun kohdistamista henkilöön tai henkilöryhmään, jonka voidaan perustellusti olettaa liittyvän tiedustelutehtävään.

Sotilastiedusteluviranomainen saa tiedustelutehtävän suorittamiseksi kohdistaa 2 momentissa tarkoitettuun kohteeseen suunnitelmallista tarkkailua, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

Tässä pykälässä tarkoitettua tarkkailua ei saa kohdistaa vakituiseen asumiseen käytettävään tilaan.

20 §

Suunnitelmallisesta tarkkailusta päättäminen

Tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää suunnitelmallisesta tarkkailusta.

Päätös suunnitelmallisesti tarkkailusta voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Päätös suunnitelmallisesta tarkkailusta on tehtävä kirjallisesti. Päätöksessä on mainittava:

1) toimenpiteen perusteena oleva tiedustelutehtävä;
2) toimenpiteen kohteena oleva henkilö tai henkilöryhmä;
3) tosiseikat, joihin suunnitelmallisen tarkkailun edellytykset ja kohdistaminen perustuvat;
4) päätöksen voimassaoloaika;
5) suunnitelmallisen tarkkailun suorittamista johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;
6) mahdolliset suunnitelmallisen tarkkailun rajoituksen ja ehdot.

21 §

Peitelty tiedonhankinta

Peitellyllä tiedonhankinnalla tarkoitetaan tiettyyn henkilöön kohdistuvaa lyhytkestoisessa vuorovaikutuksessa tapahtuvaa tiedonhankintaa, jossa sotilastiedusteluviranomaisen virkamiehen tehtävän salaamiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja.

Sotilastiedusteluviranomainen saa käyttää peiteltyä tiedonhankintaa tiedustelutehtävän suorittamiseksi.

Peitelty tiedonhankinta ei ole sallittua asunnossa edes asunnonhaltijan myötävaikutuksella.

22 §

Peitellystä tiedonhankinnasta päättäminen

Tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää peitellystä tiedonhankinnasta.

Päätös peitellystä tiedonhankinnasta on tehtävä kirjallisesti. Päätöksessä on mainittava:
1) toimenpiteen perusteena oleva tiedustelutehtävä;
2) toimenpiteen kohteena oleva henkilö tai henkilöryhmä;
3) tosiseikat, joihin peitellyn tiedonhankinnan edellytykset ja kohdistaminen perustuvat;
4) peitellyn tiedonhankinnan suorittamista johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;
5) toimenpiteen suunniteltu toteuttamisajankohta;
6) mahdolliset peitellyn tiedonhankinnan rajoitukset ja ehdot.

Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava.

Jos toimenpide ei siedä viivytystä, 1 momentissa tarkoitettua päätöstä ei tarvitse laatia kirjallisesti ennen peiteltyä tiedonhankintaa. Päätös on kuitenkin laadittava kirjallisesti viipymättä toimenpiteen jälkeen.

23 §

Tekninen kuuntelu

Teknisellä kuuntelulla tarkoitetaan rikoslain 24 luvun 5 §:n estämättä tapahtuvaa tietyn henkilön tai henkilöryhmän sellaisen keskustelun tai viestin, joka ei ole ulkopuolisten tietoon tarkoitettu ja johon keskustelun kuuntelija ei osallistu, kuuntelua, tallentamista ja muuta käsittelyä teknisellä laitteella, menetelmällä tai ohjelmistolla keskustelun tai viestin sisällön tai sen osapuolten toiminnan selvittämiseksi.

Sotilastiedusteluviranomainen saa vakituiseen asumiseen käytettävän tilan ulkopuolella kohdistaa henkilöön tai henkilöryhmään teknistä kuuntelua, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Kuuntelu voidaan toteuttaa kohdistamalla se tilaan tai muuhun paikkaan, jossa tiedustelutehtävään liittyvän henkilön tai henkilöryhmän voidaan olettaa todennäköisesti oleskelevan tai käyvän.

24 §

Teknisestä kuuntelusta päättäminen

Tuomioistuin päättää vapautensa menettäneen henkilön teknisestä kuuntelusta tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta. Jos asia ei siedä viivytystä tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää teknisestä kuuntelusta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta.

Tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää muusta kuin 1 momentissa tarkoitetusta teknisestä kuuntelusta.

Lupa voidaan antaa ja päätös tehdä enintään kuudeksi kuukaudeksi kerrallaan.

Teknistä kuuntelua koskevassa päätöksessä on mainittava:

1) toimenpiteen perusteena oleva tiedustelutehtävä;
2) toimenpiteen kohteena oleva henkilö tai henkilöryhmä taikka tila tai muu paikka;
3) tosiseikat, joihin teknisen kuuntelun edellytykset ja kohdistaminen perustuvat;
4) luvan voimassaolo kellonajan tarkkuudella;
5) teknisen kuuntelun suorittamista johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;
6) mahdolliset teknisen kuuntelun rajoitukset ja ehdot.

25 §

Tekninen katselu

Teknisellä katselulla tarkoitetaan rikoslain 24 luvun 6 §:n estämättä tapahtuvaa tietyn henkilön tai henkilöryhmän taikka tilan tai muun paikan tarkkailua tai tallentamista kameralla tai muulla sellaisella paikaan sijoitetulla teknisellä laitteella, menetelmällä tai ohjelmistolla.

Sotilastiedusteluviranomainen saa vakituiseen asumiseen käytettävän tilan ulkopuolella kohdistaa henkilöön tai henkilöryhmään teknistä katselua, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Katselu voidaan toteuttaa kohdistamalla se tilaan tai muuhun paikkaan, jossa kohteena olevan henkilön tai henkilöryhmän voidaan olettaa todennäköisesti oleskelevan tai käyvän.

26 §

Teknisestä katselusta päättäminen

Tuomioistuin päättää vapautensa menettäneen henkilön teknisestä katselusta tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen tai sotilaslakimiehen vaatimuksesta. Jos asia ei siedä viivytystä tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää teknisestä katselusta siihen asti, kunne tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta.

Tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää muusta kuin 1 momentissa tarkoitetusta teknisestä katselusta.

Lupa voidaan antaa ja päätös tehdä enintään kuudeksi kuukaudeksi kerrallaan.

Teknistä katselua koskevassa päätöksessä on mainittava:

1) toimenpiteen perusteena oleva tiedustelutehtävä;
2) toimenpiteen kohteena oleva henkilö tai henkilöryhmä taikka tila tai muu paikka;
3) tosiseikat, joihin teknisen katselun edellytykset ja kohdistaminen perustuvat;
4) luvan voimassaolo kellonajan tarkkuudella;

5) teknisen katselun suorittamista johtava ja valvova Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;
6) mahdolliset teknisen katselun rajoitukset ja ehdot.

27 §

Tekninen seuranta

Teknisellä seurannalla tarkoitetaan henkilön, esineen, aineen tai omaisuuden liikkumisen seurantaa siihen erikseen sijoitettavalla tai siinä jo olevalla radiolähettimellä tai muulla sellaisella teknisellä laitteella taikka menetelmällä tai ohjelmistolla.

Sotilastiedusteluviranomainen saa kohdistaa teknistä seurantaa esineeseen, aineeseen tai omaisuuteen taikka oletettavasti henkilön hallussa olevaan tai käyttämään esineeseen, aineeseen tai omaisuuteen.

Jos teknisen seurannan tarkoituksena on seurata henkilön liikkumista sijoittamalla seurantalaite hänen yllään oleviin vaatteisiin tai mukanaan olevaan esineeseen (*henkilön tekninen seuranta*), saadaan toimenpide suorittaa vain, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

28 §

Teknisestä seurannasta päättäminen

Tuomioistuin päättää henkilön teknisestä seurannasta tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta. Jos asia ei siedä viivytystä, sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää henkilön teknisestä seurannasta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua tiedustelumenetelmän käytön aloittamisesta.

Sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää muusta kuin 1 momentissa tarkoitetusta teknisestä seurannasta.

Lupa voidaan antaa tai päätös tehdä enintään kuudeksi kuukaudeksi kerrallaan.

Teknistä seurantaa koskevassa vaatimuksessa ja päätöksessä on mainittava:
1) toimenpiteen perusteena oleva tiedustelutehtävä;
2) toimenpiteen kohteena olevan henkilö taikka esine, aine tai omaisuus;
3) tosiseikat, joihin teknisen seurannan edellytykset ja kohdistaminen perustuvat;
4) luvan voimassaoloaika kellonajan tarkkuudella;
5) teknisen seurannan suorittamista johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;
6) mahdolliset teknisen seurannan rajoitukset ja ehdot.

29 §

Tekninen laitetarkkailu

Teknisellä laitetarkkailulla tarkoitetaan tietokoneen tai muun vastaavan teknisen laitteen taikka sen ohjelmiston toiminnan, sisältämien tietojen tai yksilöintitietojen muuta kuin yksinomaan aistinvaraista tarkkailua, tallentamista tai muuta käsittelyä tiedustelutehtävän kannalta tarpeellisen seikan selvittämiseksi.

Teknisellä laitetarkkailulla ei saa hankkia tietoa viestin sisällöstä eikä tunnistamistiedoista.

Sotilastiedusteluviranomaiselle voidaan antaa lupa tekniseen laitetarkkailuun, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Sotilastie-

dusteluviranomainen voi kohdistaa teknistä laitetarkkailua mainitun henkilön todennäköisesti käyttämään tietokoneeseen tai muuhun vastaavaan tekniseen laitteeseen taikka sen ohjelmiston toimintaan.

30 §

Teknisestä laitetarkkailusta päättäminen

Tuomioistuin päättää teknisestä laitetarkkailusta tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta. Jos asia ei siedä viivytystä, tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää teknisestä laitetarkkailusta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavakasi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua tiedustelumenetelmän käytön aloittamisesta.

Lupa voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) toimenpiteen perusteena oleva tiedustelutehtävä;
2) toimenpiteen kohteena oleva tekninen laite tai ohjelmisto;
3) tosiseikat, joihin teknisen laitetarkkailun edellytykset ja kohdistaminen perustuvat;
4) luvan voimassaoloaika kellonajan tarkkuudella;
5) teknisen laitetarkkailun suorittamista johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;
6) teknisen laitetarkkailun rajoitukset ja ehdot.

31 §

Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen

Sotilastiedusteluviranomaisen palveluksessa olevalla virkamiehellä on oikeus sijoittaa telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tekniseen kuunteluun, tekniseen katseluun, tekniseen seurantaan tai tekniseen laite tarkkailuun käytettävä laite, menetelmä tai ohjelmisto toimenpiteen kohteena olevaan esineeseen, aineeseen, omaisuuteen, tilaan tai muuhun paikkaan taikka tietojärjestelmään, jos tekniseen kuunteluun, teknisen katselun, teknisen laitetarkkailun tai teknisen seurannan toteuttaminen sitä edellyttää. Sotilastiedusteluviranomaisen virkamiehellä on tällöin oikeus laitteen, menetelmän tai ohjelmiston asentamiseksi, käyttöön ottamiseksi ja poistamiseksi salaa mennä edellä mainittuihin kohteisiin tai tietojärjestelmään sekä kiertää, purkaa tai muulla vastaavalla tavalla tilapäisesti ohittaa kohteen tai tietojärjestelmän suojaus tai haitata sitä.

32 §

Telekuuntelu

Telekuuntelulla tarkoitetaan tietoyhteiskuntakaaren 3 §:n 43 kohdassa tarkoitetun yleisen viestintäverkon tai siihen liitetyn viestintäverkon kautta teleosoitteeseen tai telepäätelaitteeseen vastaanotettavan taikka siitä lähetetyn viestin kuuntelua, tallentamista ja muuta käsittelyä viestin sisällön ja siihen liittyvien tunnistamistietojen selvittämiseksi. Telekuuntelua saadaan kohdistaa vain siltä henkilöltä lähtöisin olevaan tai sellaiselle henkilölle tarkoitettuun viestiin, jonka voidaan perustellusti olettaa liittyvän tiedustelutehtävään.

Sotilastiedusteluviranomaiselle voidaan antaa lupa valtiollisen toimijan telekuunteluun.

Sotilastiedusteluviranomaiselle voidaan antaa lupa muun kuin valtiollisen toimijan telekuunteluun, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

33 §

Tietojen hankkiminen telekuuntelun sijasta

Jos on todennäköistä, että 32 §:ssä tarkoitettua viestiä ja siihen liittyviä tunnistamistietoja ei ole enää saatavissa telekuuntelulla, sotilastiedusteluviranomaiselle voidaan antaa lupa tietojen hankkimiseen teleyrityksen tai yhteisötilaajan hallusta 32 §:ssä säädetyillä edellytyksillä.

Jos tietojen hankkiminen kohdistetaan viestin sisällön selvittämiseksi, telepäätelaitteeseen välittömästi yhteydessä olevaan viestin lähettämiseen ja vastaanottamiseen soveltuvaan henkilökohtaiseen tekniseen laitteeseen tai tällaisen laitteen ja telepäätelaitteen väliseen yhteyteen, sotilastiedusteluviranomaiselle voidaan antaa lupa tietojen hankkimiseen telekuuntelun sijasta, jos 32 §:ssä säädetyt edellytykset täyttyvät.

34 §

Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättäminen

Tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta.

Lupa telekuunteluun tai telekuuntelun sijasta toimitettavaan tietojen hankkimiseen voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Telekuuntelua ja telekuuntelun sijasta toimitettavaa tietojen hankkimista koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) toimenpiteen perusteena oleva tiedustelutehtävä;
2) toimenpiteen kohteena oleva henkilö, teleosoite tai telepäätelaite;
3) tosiseikat, joihin telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen edellytykset ja kohdistaminen perustuvat;
4) telekuuntelua tai telekuuntelun sijasta toimitettavaa tietojen hankkimista koskevan luvan voimassaoloaika kellonajan tarkkuudella;
5) telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen suorittamista johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;
6) mahdolliset telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen rajoitukset ja ehdot.

35 §

Televalvonta

Televalvonnalla tarkoitetaan välitystietojen hankkimista viestistä, joka on lähetetty viestintäverkkoon kytketystä teleosoitteesta tai telepäätelaitteesta taikka vastaanotettu tällaiseen osoitteeseen tai laitteeseen, sekä teleosoitteen tai telepäätelaitteen sijaintitiedon hankkimista. Välitystiedolla tarkoitetaan tilaajaan tai käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

Sotilastiedusteluviranomaiselle voidaan antaa lupa valtiollisen toimijan teleosoitteen tai telepäätelaitteen televalvontaan.

Sotilastiedusteluviranomaiselle voidaan antaa lupa muun kuin valtiollisen toimijan hallussa olevaan tai hänen muuten käyttämän teleosoitteen tai telepäätelaitteen televalvontaan, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

36 §

Televalvonnasta päättäminen

Tuomioistuin päättää televalvonnasta tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta. Jos televalvontaa koskeva asia ei siedä viivytystä, tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää televalvonnasta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta.

Sotilastiedusteluviranomainen saa kohdistaa televalvontaa tietojen hankkimiseksi tiedustelutehtävän kannalta henkilön suostumuksella tämän hallinnassa olevaan teleosoitteeseen tai telepäätelaitteeseen.

Pääesikunnan tiedustelupäällikkö taikka tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää 2 momentissa tarkoitetusta televalvonnasta.

Lupa voidaan antaa ja päätös tehdä enintään kuudeksi kuukaudeksi kerrallaan ja lupa tai päätös voi koskea myös luvan antamista tai päätöksen tekemistä edeltänyttä määrättyä aikaa, joka voi olla kuutta kuukautta pidempi.

Televalvontaa koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) toimenpiteen perusteena oleva tiedustelutehtävä ja toimenpiteen tavoite;
2) toimenpiteen kohteena oleva henkilö, teleosoite tai telepäätelaite;
3) tosiseikat, joihin televalvonnan edellytykset ja kohdistaminen perustuvat;
4) luvan voimassaoloaika kellonajan tarkkuudella;
5) televalvonnan suorittamista johtava ja valvova Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;
6) mahdolliset televalvonnan rajoitukset ja ehdot.

37 §

Tukiasematietojen hankkiminen

Tukiasematietojen hankkimisella tarkoitetaan tiedon hankkimista tietyn tukiaseman kautta telejärjestelmään kirjautuneista tai kirjautuvista telepäätelaitteista ja teleosoitteista.

Sotilastiedusteluviranomaiselle voidaan antaa lupa tiedustelutehtävän kannalta tarpeellisten tukiasematietojen hankkimiseen.

38 §

Tukiasematietojen hankkimisesta päättäminen

Tuomioistuin päättää tukiasematietojen hankkimisesta tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta. Jos asia ei siedä viivytystä, tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää tukiasematietojen hankkimisesta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin 24 tunnin kuluttua tiedustelumenetelmän käytön aloittamisesta.

Lupa annetaan tietyksi ajanjaksoksi.

Tukiasematietojen hankkimista koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) toimenpiteen perusteena oleva tiedustelutehtävä ja toimenpiteen tavoite;
2) tukiasema, jota lupa koskee;
3) tosiseikat, joihin tukiasematietojen hankkimisen edellytykset ja kohdistaminen perustuvat;
4) ajanjakso, jota lupa koskee;

5) tukiasematietojen hankkimisen suorittamista johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;
6) mahdolliset tukiasematietojen hankkimisen rajoitukset ja ehdot.

39 §

Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen

Sotilastiedusteluviranomainen saa tiedustelutehtävän suorittamiseksi hankkia teknisellä laitteella teleosoitteen tai telepäätelaitteen yksilöintitiedot.

Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisesta päättää tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

40 §

Peitetoiminta

Peitetoiminnalla tarkoitetaan tiettyyn henkilöön, hänen toimintaansa tai henkilöryhmään kohdistuvaa suunnitelmallista tiedonhankintaa käyttämällä soluttautumista, jossa tiedonhankinnan edellyttämän luottamuksen hankkimiseksi tai tiedonhankinnan paljastumisen estämiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka valmistetaan tai käytetään vääriä asiakirjoja.

Sotilastiedusteluviranomainen saa kohdistaa henkilöön tai henkilöryhmään peitetoimintaa, jos sen käyttö on välttämätöntä tietojen saamiseksi tiedustelutehtävän kannalta ja tiedonhankintaa on tiedustelutehtävän kohteena olevan toiminnan suunnitelmallisuuden, järjestäytyneisyyden tai ammattimaisuuden taikka ennakoitavissa olevan jatkuvuuden tai toistuvuuden vuoksi pidettävä tarpeellisena.

Peitetoiminta asunnossa on sallittua vain, jos sisäänkäynti tai oleskelu tapahtuu asuntoa käyttävän aktiivisella myötävaikutuksella.

Sotilastiedustelun viranomaisilla on oikeus kohdistaa henkilöön tai henkilöryhmään peitetoimintaa tietoverkossa, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

41 §

Peitetoimintaa koskeva esitys ja suunnitelma

Peitetoimintaa koskevassa esityksessä on mainittava:
1) toimenpiteen esittäjä;
2) tiedonhankinnan kohteena oleva henkilö tai henkilöryhmä riittävästi yksilöitynä;
3) toimenpiteen perusteena oleva tiedustelutehtävä;
4) peitetoiminnan tavoite;
5) peitetoiminnan tarpeellisuus;
6) muut peitetoiminnan edellytysten arviointia varten tarvittavat tiedot.

Peitetoiminnan toteuttamisesta on laadittava kirjallinen suunnitelma, jonka tulee sisältää peitetoimintaa koskevan päätöksenteon ja peitetoiminnan toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava.

42 §

Peitetoiminnasta päättäminen

Pääesikunnan tiedustelupäällikkö päättää 40 §:ssä tarkoitetusta peitetoiminnasta. Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättää tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

Peitetoimintaa koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Päätös peitetoiminnasta on tehtävä kirjallisesti. Päätöksessä on mainittava:

1) toimenpiteen esittäjä;
2) peitetoiminnan toteuttamisesta vastaava tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;
3) tunnistetiedot peitetoiminnan suorittavista virkamiehistä;
4) toimenpiteen perusteena oleva tiedustelutehtävä;
5) tiedonhankinnan kohteena oleva henkilö tai henkilöryhmä riittävästi yksilöitynä;
6) tosiseikat, joihin peitetoiminnan edellytykset ja kohdistaminen perustuvat;
7) peitetoiminnan tavoite ja toteuttamissuunnitelma;
8) päätöksen voimassaoloaika;
9) peitetoiminnan mahdolliset rajoitukset ja ehdot.

Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava. Peitetoiminnan lopettamisesta on tehtävä kirjallinen päätös.

43 §

Tietolähdetoiminta

Tietolähdetoiminnalla tarkoitetaan muuta kuin satunnaista luottamuksellista, tiedustelutehtävien hoitamiseksi merkityksellisten tietojen vastaanottamista suomalaisen viranomaisen ulkopuoliselta henkilöltä (*tietolähde*).

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

Tietolähteen ohjatussa käytössä tietoja ei saa pyytää hankittavaksi sellaisella tavalla, joka edellyttäisi viranomaiselle kuuluvien toimivaltuuksien käyttöä tai joka vaarantaisi tietolähteen tai muun henkilön hengen tai terveyden. Ennen tietolähteen ohjattua käyttöä tietolähteelle on tehtävä selkoa hänen oikeuksistaan ja velvollisuuksistaan sekä erityisesti hänelle lain mukaan sallitusta ja kielletystä toiminnasta. Tietolähteen turvallisuudesta on tarpeen mukaan huolehdittava tiedonhankinnan aikana ja sen jälkeen.

44 §

Tietolähdettä koskevien tietojen käsittely ja palkkion maksu

Tietolähdettä koskevat tiedot voidaan tallettaa henkilörekisteriin.

Rekisteröidylle tietolähteelle voidaan maksaa palkkio. Perustellusta syystä palkkio voidaan maksaa myös rekisteröimättömälle tietolähteelle. Palkkion veronalaisuudesta säädetään erikseen.

45 §

Tietolähteen ohjatusta käytöstä päättäminen

Pääesikunnan tiedustelupäällikkö päättää tietolähteen ohjatusta käytöstä.

Tietolähteen ohjattua käyttöä koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Päätös tietolähteen ohjatusta käytöstä on tehtävä kirjallisesti. Päätöksessä on mainittava:

1) toimenpiteen esittäjä;
2) tiedustelutehtävän toteuttamisesta vastaava Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;
3) tunnistetiedot tietolähteestä;
4) toimenpiteen perusteena oleva tiedustelutehtävä;
5) tiedonhankinnan tavoite ja toteuttamissuunnitelma;
6) päätöksen voimassaoloaika;
7) mahdolliset tietolähteen ohjatun käytön ja suojaamisen rajoitukset ja ehdot.

Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava. Tietolähteen ohjatun käytön lopettamisesta on tehtävä kirjallinen päätös.

46 §

Tietolähteen turvaaminen

Sotilastiedusteluviranomainen voi tietolähteen suostumuksella valvoa tämän asuntoa tai muuta tietolähteen asumiseen käyttämää tilaa ja sen välitöntä lähiympäristöä kameran tai muun paikkaan sijoitetun teknisen laitteen, menetelmän tai ohjelmiston avulla, jos se on tarpeen tietolähteen henkeä tai terveyttä uhkaavan vaaran torjumiseksi. Tietolähteen turvaamisesta ei tarvitse ilmoittaa sivullisille.

Tietolähteen turvaamisen edellytyksenä on lisäksi, että tietolähde on henkilökohtaisilta ominaisuuksiltaan arvioitu tähän soveltuvaksi.

Valvonta on lopetettava viipymättä, jos se ei ole enää tarpeen tietolähteen henkeä tai terveyttä uhkaavan vaaran torjumiseksi.

Edellä 1 momentissa kertyneet tallenteet on hävitettävä heti sen jälkeen, kun niitä ei tarvita tietolähteen turvaamiseen. Jos niitä on kuitenkin tarpeen säilyttää asiaan osallisen oikeusturvaan liittyvistä syistä, tallenteet saadaan säilyttää ja niitä saadaan käyttää tässä tarkoituksessa. Tällöin tallenteet on hävitettävä, kun asia on lainvoimaisesti ratkaistu tai jätetty sillensä.

47 §

Valeosto

Valeostolla tarkoitetaan sotilastiedusteluviranomaisen tekemää esineen, aineen, omaisuuden tai palvelun ostotarjousta tai ostoa, jonka tavoitteena on saada sotilastiedusteluviranomaisen haltuun tai löytää tiedustelutehtävään liittyvä esine, aine tai omaisuus.

Sotilastiedustelun viranomainen saa tehdä valeoston, jos se on välttämätöntä tiedon saamiseksi tiedustelutehtävän kannalta.

Valeoston toteuttaja saa tehdä vain sellaista tiedonhankintaa, joka on välttämätöntä valeoston toteuttamiseksi. Valeosto on toteutettava siten, ettei se saa kohteena olevaa tai muuta henkilöä tekemään rikosta, jota hän ei muuten tekisi.

Valeosto asunnossa on sallittua vain, jos sisäänkäynti tai oleskelu tapahtuu asuntoa käyttävän aktiivisella myötävaikutuksella.

48 §

Valeostosta päättäminen

Pääesikunnan tiedustelupäällikkö päättää valeostosta. Yksinomaan yleisön saataville toimitetusta myyntitarjouksesta tehtävästä valeostosta saa päättää myös tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies.

Valeostoa koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Päätös valeostosta on tehtävä kirjallisesti. Päätöksessä on mainittava:

1) toimenpiteen perusteena oleva tiedustelutehtävä;
2) valeoston kohteena oleva henkilö;
3) tosiseikat, joihin valeoston edellytykset ja kohdistaminen perustuvat;
4) valeoston kohteena oleva esine, aine, omaisuus tai palvelu;
5) valeoston tarkoitus;
6) päätöksen voimassaoloaika;
7) valeoston suorittamista johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;
8) mahdolliset valeoston rajoitukset ja ehdot.

49 §

Valeoston toteuttamista koskeva suunnitelma

Valeoston toteuttamisesta on laadittava kirjallinen suunnitelma, jos se on tarpeen toiminnan laajuuden tai muun vastaava syyn vuoksi.

Valeoston toteuttamista koskevaa suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava.

50 §

Valeoston toteuttamista koskeva päätös

Päätös valeoston toteuttamisesta on tehtävä kirjallisesti. Päätöksen tekee valeoston toteuttamisesta vastaava tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies.

Päätöksessä on mainittava:

1) valeostosta päättänyt sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies sekä päätöksen antopäivä ja sisältö;
2) tunnistetiedot valeoston suorittavista sotilastiedusteluviranomaisen virkamiehistä;
3) selvitys siitä, miten on varmistuttu, että valeosto ei saa sen kohteena olevaa tai muuta henkilöä tekemään rikosta, jota hän ei muuten tekisi;
4) mahdolliset valeoston rajoitukset ja ehdot.

Jos toimenpide ei siedä viivytystä, 2 momentissa tarkoitettua päätöstä ei tarvitse laatia kirjallisesti ennen valeostoa. Päätös on kuitenkin laadittava kirjallisesti viipymättä valeoston jälkeen.

Valeoston toteuttamista koskevaa päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava.

51 §

Paikkatiedustelu

Paikkatiedustelulla tarkoitetaan paikassa toimitettavaa tiedustelua esineen, omaisuuden, asiakirjan, tiedon tai seikan löytämiseksi.

Paikkatiedustelua ei saa toimittaa paikassa, jossa tiedustelun kohteeksi on syytä olettaa joutuvan tietoa, josta oikeudenkäymiskaaren 17 luvun 23 §:n 1 momentissa tarkoitettu henkilö ei saa todistaa oikeudenkäynnissä tai josta mainitun luvun 24 §:n 2 tai 3 momentissa tarkoitettu henkilö saa kieltäytyä kertomasta. Paikkatiedustelu saadaan kuitenkin suorittaa, jos tiedonhankinnan kohteeksi on syytä olettaa joutuvan tietoa, josta henkilö voidaan velvoittaa todistamaan oikeudenkäymiskaaren 17 luvun 23 §:n 3 momentin nojalla tai vastaamaan kysymykseen oikeudenkäymiskaaren 17 luvun 24 §:n 4 momentin nojalla.

Sotilastiedusteluviranomaiselle voidaan vakituiseen asumiseen käytettävän tilan ulkopuolella antaa lupa paikkatiedusteluun, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

52 §

Paikkatiedustelusta päättäminen

Tuomioistuin päättää paikkatiedustelusta, jos se kohdistuu paikkaan, johon ei ole yleistä pääsyä tai johon yleinen pääsy siihen on rajoitettu tai estetty paikkatiedustelun toimittamisajankohtana, tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta.

Jos 1 momentissa tarkoitettu asia ei siedä viivytystä, pääesikunnan tiedustelupäällikkö tai tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää paikkatiedustelusta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta.

Pääesikunnan tiedustelupäällikkö tai tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää muusta kuin 1 momentissa tarkoitetusta paikkatiedustelusta.

Lupa voidaan antaa ja päätös tehdä enintään kuukaudeksi kerrallaan.

Paikkatiedustelu koskevassa vaatimuksessa tai päätöksessä on riittävällä tarkkuudella yksilöitävä:

1) toimenpiteen perusteena oleva tiedustelutehtävä,
2) paikkatiedustelun kohteena oleva paikka,
3) ne seikat, joiden perusteella paikkatiedustelun edellytysten katsotaan olevan olemassa,
4) mahdollisuuksien mukaan se, mitä paikkatiedustelulla pyritään löytämään,
5) mahdolliset paikkatiedustelun rajoitukset.

Asian kiireellisyyden sitä edellyttäessä paikkatiedustelua koskeva päätös saadaan kirjata paikkatiedustelun toimittamisen jälkeen.

Paikkatiedustelussa ei saa hankkia pakkokeinolain 8 luvun 1 §:n 3 momentissa tarkoitettua tietoa. Jos paikkatiedustelussa ilmenee, että tiedustelu on kohdistunut sellaiseen tietoon, on tiedustelu siltä osin heti lopetettava ja tietoa koskevat muistiinpanot ja jäljennökset heti hävitettävä.

53 §

Jäljentäminen

Sotilastiedusteluviranomaisella on tietojen hankkimiseksi tiedustelutehtävän kannalta oikeus jäljentää asiakirja tai muu esine käyttämällä teknistä laitetta.

54 §

Jäljentämiskiellot

Asiakirjaa tai muuta 53 §:ssä tarkoitettua kohdetta ei saa jäljentää, jos se sisältää tietoa, josta oikeudenkäymiskaaren 17 luvun 10–14, 16, 20 tai 21 §:n nojalla on velvollisuus tai oikeus kieltäytyä todistamasta.

Jos salassapitovelvollisuus tai -oikeus perustuu oikeudenkäymiskaaren 17 luvun 11 §:n 2 tai 3 momenttiin tai 13, 14, 16 tai 20 §:ään, edellytyksenä kiellolle 1 momentissa säädetyn lisäksi on, että kohde on mainitussa lainkohdassa tarkoitetun henkilön tai häneen mainitun luvun 22 §:n 2 momentissa tarkoitetussa suhteessa olevan henkilön hallussa taikka sen hallussa, jonka hyväksi salassapitovelvollisuus tai -oikeus on säädetty.

Jäljentämiskieltoa ei kuitenkaan ole, jos:

1) oikeudenkäymiskaaren 17 luvun 11 §:n 2 tai 3 momentissa, 12 §:n 1 tai 2 momentissa, 13 §:n 1 tai 3 momentissa, 14 §:n 1 momentissa taikka 16 §:n 1 momentissa tarkoitettu henkilö, jonka hyväksi salassapitovelvollisuus on säädetty, suostuu jäljentämiseen;

2) oikeudenkäymiskaaren 17 luvun 20 §:n 1 momentissa tarkoitettu henkilö suostuu jäljentämiseen.

55 §

Telekuunteluun, televalvontaan ja tukiasematietoihin liittyvät jäljentämiskiellot

Teleyrityksen tai yhteisötilaajan hallusta ei saa jäljentää asiakirjaa tai dataa, joka sisältää tämän lain 4 luvun 32 §:n 1 momentissa tarkoitettuun viestiin liittyviä tietoja taikka mainitun luvun 35 §:n 1 momentissa tarkoitettuja tunnistamistietoja tai 37 §:n 1 momentissa tarkoitettuja tukiasematietoja.

56 §

Lähetyksen jäljentäminen

Kirje tai muu vastaava lähetys saadaan ennen sen saapumista vastaanottajalle jäljentää, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

57 §

Lähetyksen pysäyttäminen jäljentämistä varten

Jos on syytä olettaa, että kirje tai muu vastaava lähetys, joka voidaan jäljentää, on tulossa postitoimistoon, rautateiden liikennepaikkaan tai lähetysten kuljetusta ammatikseen liikennöinnin yhteydessä tai muuten harjoittavan toimipaikkaan taikka on jo siellä, tehtävään määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa määrätä lähetyksen pidettäväksi postitoimistossa, liikennepaikassa tai toimipaikassa, kunnes jäljentäminen on ehditty suorittaa.

Edellä 1 momentissa tarkoitettu määräys annetaan enintään kuukauden määräajaksi, joka alkaa siitä, kun postitoimiston, liikennepaikan tai toimipaikan esimies on saanut tiedon määräyksestä. Lähetystä ei saa ilman 1 momentissa tarkoitetun virkamiehen lupaa luovuttaa muulle kuin hänelle tai hänen määräämälleen henkilölle.

Postitoimiston, liikennepaikan tai toimipaikan esimiehen on heti ilmoitettava määräyksen antajalle lähetyksen saapumisesta. Tämän on ilman aiheetonta viivytystä päätettävä jäljentämisestä.

58 §

Jäljentämisestä päättäminen

Tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää jäljentämisestä.

Jos asia ei siedä viivytystä, myös muu kuin tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa yksittäistapauksessa päättää jäljentämisestä, kunnes 1 momentissa tarkoitettu virkamies on ratkaissut asian. Asia on saatettava 1 momentissa tarkoitetun sotilaslakimiehen tai muun virkamiehen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua tiedonhankintakeinon käytön aloittamisesta.

59 §

Jäljentämisen kirjaaminen ja jäljennöksen hävittäminen

Asiakirjan tai muun kohteen jäljentämisestä on ilman aiheetonta viivytystä laadittava pöytäkirja. Siinä on riittävästi mainittava jäljentämisen tarkoitus, selostettava jäljentämiseen johtanut menettely sekä yksilöitävä jäljentämisen kohde.

Tarpeettomaksi osoittautunut jäljennös on heti hävitettävä.

60 §

Radiosignaalitiedustelu

Radiosignaalitiedustelulla tarkoitetaan radiotaajuisiin sähkömagneettisiin aaltoihin (radioaalto) kohdistuvaa tiedonhankintaa.

Puolustusvoimien tiedustelulaitos tai puolustushaarat voi kohdistaa radiosignaalitiedustelua Suomen alueen ulkopuolella olevasta laitteesta lähteviin tai tällaiseen laitteeseen saapuviin radioaaltoihin.

Radiosignaalitiedustelu ei saa kohdistua henkilöiden väliseen luottamukselliseen viestintään.

61 §

Radiosignaalitiedustelusta päättäminen

Pääesikunnan tiedustelupäällikkö päättää radiosignaalitiedustelusta.

62 §

Ulkomaan tietojärjestelmätiedustelu

Ulkomaan tietojärjestelmätiedustelulla tarkoitetaan tietoteknisin menetelmin suoritettavaa tietojen hankkimista Suomen ulkopuolella olevasta tietojärjestelmästä.

Puolustusvoimien tiedustelulaitos saa kohdistaa tietojärjestelmään ulkomaan tietojärjestelmätiedustelua, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta.

Ulkomaan tietojärjestelmätiedustelu ei saa kohdistua henkilöiden väliseen luottamukselliseen viestintään.

63 §

Ulkomaan tietojärjestelmätiedustelussa päättäminen

Pääesikunnan tiedustelupäällikkö päättää ulkomaan tietojärjestelmätiedustelusta.

Sotilastiedusteluviranomaisen on pidettävä puolustusministeriö tietoisena käynnissä olevasta ulkomaan tietojärjestelmätiedustelusta.

64 §

Ulkomailla tapahtuva sotilastiedustelusta päättäminen

Muualla kuin Suomessa toteutettavasta sotilastiedustelusta ja tiedustelumenetelmien käytöstä päättää pääesikunnan tiedustelupäällikkö.

Päätös on tehtävä kirjallisesti. Tiedustelumenetelmän käyttöä koskevan päätöksen, esityksen ja suunnitelman sisällön osalta noudatetaan mitä esityksestä, suunnitelmasta, vaatimuksesta tai päätöksestä tässä laissa säädetään.

Sen lisäksi, mitä vakituiseen asumiseen käytettävään tilaan kohdistuvista kielloista säädetään, tämän lain 55, 76, 77, 85, 86, 126 ja 127 §:n säännöksiä ei sovelleta 1 momentissa tarkoitettuun sotilastiedusteluun ja tiedustelumenetelmän käyttöön.

5 luku

Tiedonhankinta tietoliikenteestä

65 §

Soveltamisala

Tässä luvussa säädetään Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen kohdistuvasta, tietoliikenteen automatisoituun erotteluun perustuvasta teknisestä tiedonhankinnasta sekä hankitun tiedon käsittelystä (*tietoliikennetiedustelu*).

66 §

Teknisten tietojen käsittely

Tietoliikennetiedustelun kohdentamiseksi Puolustusvoimien tiedustelulaitos voi viestintäverkon tietoliikenteestä hetkellisesti kerätä ja tallentaa tietoliikenteen teknisiä tietoja ja automaattisen tietojenkäsittelyn avulla käsitellä niitä tilastollista analyysiä varten.

Tilastollisen analyysin tulokseen ei saa sisältyä tietoa, josta voidaan tunnistaa yksittäinen luonnollinen henkilö.

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

67 §

Teknisten tietojen käsittelystä päättäminen

Tuomioistuin päättää teknisten tietojen käsittelystä tiedustelumenetelmien käyttöön erityisesti perehtyneen Puolustusvoimien tiedustelulaitoksen sotilaslakimiehen tai virkamiehen vaatimuksesta.

Lupa voidaan antaa enintään kolmeksi kuukaudeksi kerrallaan.

Teknisten tietojen käsittelyä koskevassa vaatimuksessa ja päätöksessä on käytävä ilmi:

1) maantieteellinen alue, jolta tulevaan tai jolle menevään tietoliikenteeseen teknisten tietojen käsittely kohdistetaan;
2) viestintäverkon osat, joista tietoa haetaan;
3) teknisten tietojen käsittelyn suorittamista johtava ja valvova Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies;
4) suunnitelma teknisten tietojen käsittelyn toteuttamisesta.

68 §

Valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu

Puolustusvoimien tiedustelulaitos voi Suomen rajan ylittävästä viestintäverkon tietoliikenteestä automaattisen tietojenkäsittelyn avulla hankkia tietoa tiedustelutehtävän kannalta olennaisen valtiollisen toimijan tietoliikenteestä sekä käsitellä valtiollisen toimijan viestintää. Tietojen hankkiminen tietoliikenteestä perustuu hakuehtojen käyttöön.

Puolustusvoimien tiedustelulaitos voi käsitellä tietoliikenteestä hankittua tietoa automaattisesti ja manuaalisesti.

Hakuehtona ei saa käyttää Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.

69 §

Valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta päättäminen

Tuomioistuin päättää valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta pääesikunnan tiedustelupäällikön vaatimuksesta. Jos asia ei siedä viivytystä, pääesikunnan tiedustelupäällikkö saa päättää valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Päätös on tehtävä kirjallisesti. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua tietoliikennetiedustelun aloittamisesta.

Lupa voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Valtiollisen toimijan tietoliikenteeseen kohdistuvaa tiedustelua koskevassa vaatimuksessa ja päätöksessä on käytävä ilmi:

1) tiedustelutehtävä, jota varten tietoliikennettä hankitaan;
2) toiminnassa käytettävät hakuehdot tai hakuehtojen luokat sekä perustelut niille;
3) viestintäverkon osa, johon tiedustelu kohdistetaan sekä perustelut kohdistamiselle;
4) luvan voimassaoloaika kellonajan tarkkuudella;
5) valtiollisen toimijan tietoliikenteeseen kohdistuvan tiedustelun suorittamista johtava ja valvova Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtynyt Puolustusvoimien tiedustelulaitoksen virkamies;
6) mahdolliset valtiollisen toimijan tietoliikenteen tiedustelun rajoitukset ja ehdot.

70 §

Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu

Puolustusvoimien tiedustelulaitos voi Suomen rajan ylittävästä viestintäverkon tietoliikenteestä automaattisen tietojenkäsittelyn avulla hankkia tietoa tiedustelutehtävän kannalta olennaisen muun kuin valtiollisen toimijan tietoliikenteestä, jos muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvan tiedustelun voidaan olettaa olevan välttämätöntä tiedon saamiseksi tiedustelutehtävän kannalta. Tietojen hankkiminen tietoliikenteestä perustuu hakuehtojen käyttöön.

Hakuehtona ei saa käyttää Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.

Muun kuin valtiollisen toimijan tietoliikenteen tiedustelun kohdentaminen ei saa tapahtua viestin sisällön perusteella, jollei kohdentamisessa käytetä haittaohjelman sisältöä kuvaavaa tietoa.

Puolustusvoimien tiedustelulaitos voi käsitellä tietoliikenteestä hankittua tietoa automaattisesti ja manuaalisesti.

71 §

Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelusta päättäminen

Tuomioistuin päättää muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta pääesikunnan tiedustelupäällikön vaatimuksesta. Jos asia ei siedä viivytystä, pääesikunnan tiedustelupäällikkö saa päättää muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Päätös on tehtävä kirjallisesti. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua tietoliikennetiedustelun aloittamisesta.

Lupa voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvaa tiedustelua koskevassa vaatimuksessa ja päätöksessä on käytävä ilmi:

1) tiedustelutehtävä, jota varten tietoliikennettä hankitaan;
2) tiedustelun kohdetta koskevat tosiseikat;
3) tosiseikat, joihin tietoliikennetiedustelun käytön edellytykset perustuvat;
4) tiedonhankinnassa käytettävät hakuehdot tai hakuehtojen luokat sekä perustelut niille
5) viestintäverkon osa, johon tiedustelu kohdistetaan sekä perustelut kohdistamiselle;
6) luvan voimassaoloaika kellonajan tarkkuudella;
7) muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvan tiedustelun suorittamista johtava ja valvova Puolustusvoimien tiedustelulaitoksen tiedustelumenetelmien käyttöön erityisesti perehtynyt Puolustusvoimien tiedustelulaitoksen virkamies;
8) mahdolliset tietoliikennetiedustelun rajoitukset ja ehdot.

72 §

Tietoliikennetiedustelun edellyttämän kytkennän toteuttaminen

Tietoliikennetiedustelun kytkennän suorittaja panee täytäntöön tässä luvussa tarkoitetut luvat ja ohjaa luvassa tarkoitetun viestintäverkon osan tietoliikenteen Puolustusvoimien tiedustelulaitokselle.

Kytkennän suorittaja luovuttaa luvassa tarkoitetun liitynnän mukaisessa viestintäverkon osassa liikkuvan tietoliikenteen edelleen Puolustusvoimien tiedustelulaitokselle.

73 §

Tietoliikennetiedustelun tekninen toteuttaminen suojelupoliisin puolesta

Tietoliikennetiedustelun teknisellä toteuttamisella suojelupoliisin puolesta tarkoitetaan:

1) suojelupoliisin Puolustusvoimien tiedustelulaitokselle antamaan toimeksiantoon perustuvaa teknisten tietojen tilastollista analyysiä ja analyysin toimittamista suojelupoliisille; sekä
2) tuomioistuimen suojelupoliisille myöntämän luvan mukaista Suomen rajan ylittävässä viestintäverkon osassa liikkuvan tietoliikenteen hankkimista automatisoidun tietojen käsittelyn avulla ja hankittujen tietojen luovuttamista edelleen suojelupoliisille.

Tietoliikennetiedustelun teknisestä toteuttamisesta suojelupoliisille säädetään tietoliikennetiedustelusta siviilitiedustelussa annetun lain 10 §:ssä.

Puolustusvoimien tiedustelulaitos ei voi tietoliikennetiedustelun teknisessä toteuttamisessa suojelupoliisin puolesta selvittää viestin sisältöä.

74 §

Tietojen hävittäminen

Tietoliikennetiedustelun avulla hankitut tiedot on hävitettävä viipymättä, jos
1) käy ilmi, että luottamuksellisen viestinnän molemmat osapuolet olivat Suomessa silloin, kun viestintä tapahtui;
2) lähettäjällä tai vastaanottajalla on velvollisuus tai oikeus kieltäytyä todistamasta kyseisestä tiedosta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n nojalla.

75 §

Haitallista tietokoneohjelmaa koskevien tietojen luovuttaminen yrityksille ja yhteisöille

Sotilastiedusteluviranomainen saa salassapitosäännösten estämättä luovuttaa tietoliikennetiedustelun avulla hankittuja tietoja haitallisesta tietokoneohjelmasta ja sen toiminnasta yritykselle, yhteisölle tai viranomaiselle, jos tietojen luovuttaminen on tarpeen maanpuolustuksen turvaamiseksi, kansallisen turvallisuuden suojaamiseksi tai yrityksen tai yhteisön etujen turvaamiseksi.

6 luku

Tiedustelutietojen ilmoittaminen eräissä tilanteissa

76 §

Ilmoitus rikosepäilystä

Sotilastiedusteluviranomaisen on ilman aiheetonta viivytystä ilmoitettava toimivaltaiselle esitutkintaviranomaiselle esitutkinnan käynnistämiseksi tarpeelliset tiedot, jos tiedustelumenetelmän käytön aikana ilmenee, että on syytä epäillä rikoslain 15 luvun 10 §:ssä tarkoitettua rikosta.

Sotilastiedusteluviranomainen saa ilmoittaa epäillystä rikoksesta esitutkintaviranomaiselle, jos rikoksesta säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta ja ilmoituksella voidaan olettaa olevan erittäin tärkeä merkitys rikoksen selvittämiselle.

Tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää tässä pykälässä tarkoitetun ilmoituksen tekemisestä.

77 §

Ilmoittaminen eräissä tapauksissa

Sotilastiedusteluviranomaisen on ilman aiheetonta viivytystä ilmoitettava rikostorjuntaviranomaiselle, jos tiedustelumenetelmän käytön aikana ilmenee rikoslain 15 luvun 10 §:ssä tarkoitettu vielä estettävissä oleva rikos.

Sotilastiedusteluviranomainen saa ilmaista rikostorjuntaviranomaiselle tiedustelumenetelmän käytöllä saadun tiedon sellaisen rikoksen estämiseksi, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta.

Tiedustelumenetelmän käytöllä saatua tietoa saa aina ilmaista syyttömyyttä tukevaksi selvitykseksi sekä hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi.

Pääesikunnan tiedustelupäällikkö päättää tässä pykälässä tarkoitetun ilmoituksen tekemisestä.

78 §

Ilmoitus esitutkinnan tai rikostorjunnan aloittamisesta

Jos tässä luvussa tarkoitetun ilmoituksen perusteella esitutkintaviranomainen käynnistää esitutkinnan tai ryhtyy esitutkintatoimenpiteen käyttämiseen taikka rikostorjuntaviranomainen käynnistää rikoksen estämiseen tähtäävän toimenpiteen, on esitutkintaviranomaisen tai rikostorjuntaviranomaisen riittävän ajoissa ennen esitutkinnan käynnistämistä, esitutkintatoimenpiteen käyttämiseen ryhtymistä tai rikostorjuntatoimenpiteen käyttämiseen ryhtymistä ilmoitettava käynnistämisestä tai ryhtymisestä sotilastiedusteluviranomaiselle.

79 §

Ilmoittaminen tuomioistuimen luvasta

Sotilastiedusteluviranomaisen on annettava tieto tiedustelun valvontaviranomaiselle tämän lain 4 ja 5 luvun nojalla myönnetyistä tuomioistuimen luvista mahdollisimman pian tuomioistuimen päätöksen jälkeen.

7 luku

Sotilastiedustelun suojaaminen ja turvaaminen, tietojen hävittäminen sekä tiedustelusta ilmoittaminen

80 §

Sotilastiedustelun suojaaminen

Sotilastiedusteluviranomainen saa käyttää vääriä, harhauttavia tai peiteltyjä tietoja, tehdä ja käyttää vääriä, harhauttavia tai peiteltyjä rekisterimerkintöjä sekä valmistaa ja käyttää vääriä asiakirjoja, kun se on tarpeen sotilastiedustelun paljastumisen estämiseksi.

Edellä 1 momentissa tarkoitettu rekisterimerkintä on oikaistava sen jälkeen, kun momentissa tarkoitettuja edellytyksiä ei enää ole.

81 §

Sotilastiedustelun suojaamisesta päättäminen

Pääesikunnan tiedustelupäällikkö päättää 80 §:ssä tarkoitetun rekisterimerkinnän tekemisestä sekä asiakirjan valmistamisesta.

Tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies päättää muusta kuin 1 momentissa tarkoitetusta suojaamisesta.

Rekisterimerkintöjen tekemisestä sekä asiakirjojen valmistamisesta päättäneen viranomaisen on pidettävä luetteloa merkinnöistä ja asiakirjoista, valvottava niiden käyttöä sekä huolehdittava merkintöjen oikaisemisesta.

82 §

Tiedustelumenetelmää käyttävän virkamiehen turvaaminen

Tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies saa päättää, että peiteltyä tiedonhankintaa, peitetoimintaa tai valeostoa toteuttava virkamies varustetaan kuuntelun ja katselun mahdollistavalla teknisellä laitteella, jos varustaminen on perusteltua hänen turvallisuutensa varmistamiseksi.

Kuuntelu ja katselu saadaan tallentaa. Tallenteet on hävitettävä heti sen jälkeen, kun niitä ei tarvita virkamiehen turvaamiseen. Jos niitä on kuitenkin tarpeen säilyttää asiaan osallisen oikeusturvaan liittyvistä syistä, tallenteet saadaan säilyttää ja niitä saadaan käyttää tässä tarkoituksessa. Tällöin tallenteet on hävitettävä, kun asia on lainvoimaisesti ratkaistu tai jätetty sillensä.

83 §

Tiedustelutietojen hävittäminen

Tämän lain perusteella saatu tieto on hävitettävä viipymättä sen jälkeen, kun on käynyt ilmi, ettei tietoa tarvita tai tietoa ei saa käyttää sotilastiedustelun tehtävien hoitamiseksi.

84 §

Tiedustelutehtävään liittymättömän tiedon käyttäminen

Tiedustelutehtävään liittymätöntä tietoa saa käyttää käynnissä olevan tai tulevan tiedustelutehtävän suorittamisessa, jos tieto olisi saatu hankkia samalla tiedustelumenetelmällä kuin tiedustelutehtävään liittymätön tietokin hankittiin. Tiedustelutehtävään liittymättömän tiedon käyttämisestä päättää tuomioistuin, jos sillä on toimivalta päättää siitä tiedonhankintakeinosta, jolla tieto on saatu.

Sotilastiedustelutiedon ilmoittamisesta eräissä tilanteissa säädetään 6 luvussa.

85 §

Tiedustelumenetelmän käytön lopettaminen kiiretilanteessa ja sillä saadun tiedon hävittäminen

Jos pääesikunnan tiedustelupäällikkö taikka tiedustelumenetelmien käyttöön erityisesti perehtynyt sotilaslakimies tai muu virkamies on 24, 26, 28, 30, 36, 38, 52, 58, 69 tai 71 §:ssä tarkoitetussa kiireellisessä tilanteessa päättänyt tukiasematietojen hankkimisen, henkilön teknisen seurannan, teknisen kuuntelun, teknisen katselun tai teknisen laitetarkkailun, valtiollisen toimijan tietoliikenteen tiedustelun tai muun kuin valtiollisen toimijan tietoliikenteen tiedustelun aloittamisesta, mutta tuomioistuin katsoo, että edellytyksiä toimenpiteelle ei ole ollut, tiedustelumenetelmän käyttö on lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot on heti hävitettävä.

86 §

Tiedonhankinnasta ilmoittaminen

Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta, suunnitelmallisesta tarkkailusta, peitellystä tiedonhankinnasta ja teknisestä tarkkailusta on viipymättä ilmoitettava tiedonhankinnan kohteelle kirjallisesti sen jälkeen, kun tiedonhankinnan tarkoitus on saavutettu ja toimenpiteen kohteena on henkilö.

Muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta on ilmoitettava tiedonhankinnan kohteena olleelle henkilölle kirjallisesti sen jälkeen, kun tiedonhankinnan tarkoitus on saavutettu, ja jos käsittelyssä on selvitetty tietyn Suomessa olevan henkilön luottamuksellisen

viestin sisältö. Velvollisuutta ilmoittaa ei kuitenkaan ole, jos tietoliikennetiedustelulla saatu tieto on hävitetty 74 §:n perusteella.

Kohteelle ilmoittamisesta on samalla annettava kirjallisesti tieto luvan myöntäneelle tuomioistuimelle.

Tuomioistuin voi pääesikunnan tiedustelupäällikön tai tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai virkamiehen vaatimuksesta päättää, että 1 tai 2 momentissa tarkoitettua ilmoitusta kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedonhankinnan turvaamiseksi, maanpuolustuksen tai kansallisen turvallisuuden suojaamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saadaan tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä sotilaallisen maanpuolustuksen tai kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi.

Jos tiedonhankinnan kohteen henkilöllisyys ei ole tiedossa 1, 2 tai 4 momentissa tarkoitetun määräajan tai lykkäyksen päättyessä, tiedustelumenetelmän käytöstä on ilmoitettava kirjallisesti hänelle ilman aiheetonta viivytystä henkilöllisyyden selvittyä.

Peitetoiminnasta, valeostosta, tietolähteen ohjatusta käytöstä tai paikkatiedustelusta ei ole velvollisuutta ilmoittaa tiedustelumenetelmän käytön kohteelle, jos asiassa ei ole aloitettu esitutkintaa. Jos esitutkinta aloitetaan, noudatetaan, mitä pakkokeinolain 10 luvun 60 §:ssä säädetään.

Ilmoitusta koskevan asian käsittelyssä tuomioistuimessa noudatetaan, mitä 134 §:ssä säädetään.

8 luku

Puolustusvoimien muun virkamiehen ja asevelvollisten osallistuminen sotilastiedusteluun sekä kansainvälinen toiminta

87 §

Puolustusvoimien muun virkamiehen osallistuminen sotilastiedusteluun

Tiedustelumenetelmien käyttöön riittävän koulutuksen saanut Puolustusvoimien virkamies voi käyttää sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa 4 luvussa tarkoitettuja tiedustelumenetelmiä tiedonhankkimiseksi tiedustelutehtävään. Nämä virkamiehet ovat tiedustelutehtävää suorittavan sotilastiedusteluviranomaisen alaisia.

88 §

Asevelvollisuuslain mukaisessa palveluksessa olevan reserviläisen toimivaltuudet

Asevelvollisuuslain mukaisessa kertausharjoituksessa oleva riittävän koulutuksen saanut reserviläinen saa avustaa sotilastiedusteluviranomaista radiosignaalitiedustelussa, ulkomaan tietojärjestelmätiedustelussa, teknisten tietojen käsittelyssä ja tietoliikennetiedustelun kohdentamisessa.

Asevelvollisuuslain 32 §:n 3 momentissa tarkoitetussa kertausharjoituksessa, sanotun lain 82 §:ssä tarkoitetussa ylimääräisessä palveluksessa oleva tai 86 §:n liikekannallepanon aikaiseen palvelukseen määrätty riittävän koulutuksen saanut reserviläinen voi käyttää 1 momentissa säädetyn lisäksi suunnitelmallista tarkkailua, teknistä kuuntelua, teknistä katselua, teknistä seurantaa ja teknistä laitetarkkailua sekä ulkomaan tietojärjestelmätiedustelua tiedustelutehtävän suorittamiseksi.

Puolustusvoimista annetun lain 47 §:n perusteella sotilastiedusteluviranomaisen palveluksesta eronnut asevelvollisuuslain mukaisessa kertausharjoituksessa oleva reserviläinen saa käyttää 4 luvun toimivaltuuksia.

Reserviläinen saa käyttää tässä pykälässä tarkoitettuja toimivaltuuksia ainoastaan tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen ohjauksessa ja valvonnassa.

89 §

Reserviläisen osallistuminen kansainväliseen toimintaan

Tiedustelumenetelmien käyttöön erityisesti perehtynyt puolustusvoimista annetun lain 47 §:n perusteella sotilastiedusteluviranomaisen palveluksesta eronnut kansainvälisen avun antamiseen ja muuhun kansainväliseen toimintaan osallistuva Puolustusvoimien palvelusuhteeseen otettu tai sotilaallisesta kriisinhallinnasta annetun lain mukaisessa palvelussuhteessa oleva päättää 4 luvussa säädettyjen tiedustelumenetelmien käytöstä Puolustusvoimien kansainvälisen avun antamisessa ja muussa kansainvälisessä toiminnassa sekä sotilaallisessa kriisinhallintaoperaatiossa.

Tiedustelumenetelmien käyttöön riittävän koulutuksen saanut Puolustusvoimien palvelussuhteeseen otettu reserviläinen voi käyttää 4 luvussa säädettyjä tiedustelumenetelmiä tiedustelumenetelmien käyttöön erityisesti perehtyneen virkamiehen tai 1 momentissa tarkoitetun reserviläisen ohjauksessa ja valvonnassa.

Pääesikunnan tiedustelupäällikkö tekee päätöksen tässä pykälässä tarkoitetun henkilön osallistumisesta kansainväliseen avun antamiseen tai sotilaalliseen kriisinhallintaan sekä kansainvälisessä toiminnassa käytettävistä tiedustelumenetelmistä.

90 §

Asevelvollisuuslain mukaisessa palveluksessa olevan virkavastuu

Asevelvollisuuslain mukaisessa palveluksessa olevaan, joka käyttää 89 §:ssä tarkoitettua toimivaltaa, sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä.

91 §

Asevelvollisuuslain mukaisessa palveluksessa olevan vahingonkorvausvastuu

Asevelvollisuuslain mukaisessa palveluksessa olevan reserviläisen aiheuttamasta vahingosta vastaa valtio sen mukaan kuin vahingonkorvauslaissa (412/1974) säädetään.

Asevelvollisuuslain mukaisessa palveluksessa olevan reserviläisen korvausvastuuseen sovelletaan vahingonkorvauslain 4 luvun säännöksiä asevelvollisen korvausvastuusta.

9 luku

Ilmaisukielto, teleyrityksiä ja tiedonsiirtäjää koskevat velvollisuudet ja oikeudet sekä tietojen saanti eräiltä tahoilta

92 §

Ilmaisukielto

Tiedustelutehtävän suorittamisessa avustanut sivullinen tai asevelvollisuuslain mukaisessa palveluksessa oleva ei saa ilmaista tietoonsa tullutta tietoa tai seikkaa tiedustelutehtävästä.

Rangaistus ilmaisukiellon rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teosta muualla laissa säädetä ankarampaa rangaistusta.

93 §

Teleyrityksen avustamisvelvollisuus

Teleyrityksen on ilman aiheetonta viivytystä tehtävä televerkkoon telekuuntelun ja televalvonnan edellyttämät kytkennät sekä annettava sotilastiedusteluviranomaisen käyttöön telekuuntelun toimeenpanoa varten tarpeelliset tiedot, välineet ja henkilöstö. Sama koskee myös niitä tilanteita, joissa telekuuntelu tai televalvonta toteutetaan sotilastiedusteluviranomaisen toimesta teknisellä laitteella.

94 §

Tiedonsiirtäjän avustamisvelvollisuus

Tiedonsiirtäjä on velvollinen myötävaikuttamaan tietoliikennetiedustelun edellyttämän liityntäpisteen toteuttamiseen antamalla Puolustusvoimien tiedustelulaitokselle tätä tarkoitusta varten välttämättömät tiedot ja pääsyn tiloihin, jossa liityntäpiste on määrä toteuttaa. Puolustusvoimien tiedustelulaitoksen on toteutettava liityntäpiste siten, että toteuttamisesta aiheutuu mahdollisimman vähän haittaa tiedonsiirtäjälle. Tiedonsiirtäjällä on oikeus osallistua toimenpiteisiin liityntäpisteen toteuttamiseksi.

Jos 1 momentissa tarkoitettua liityntäpistettä ei voida toteuttaa tiedonsiirtäjän myötävaikutuksella, Puolustusvoimien tiedustelulaitoksella on oikeus toteuttaa liityntäpiste tiedonsiirtäjän hallinnoimaan viestintäverkon osaan. Tiedonsiirtäjän tulee mahdollisuuksien mukaan olla paikalla tietoliikennetiedustelun edellyttämän liityntäpistettä toteutettaessa.

Tiedonsiirtäjän on ilman aiheetonta viivytystä annettava Puolustusvoimien tiedustelulaitokselle sen yksilöidystä pyynnöstä hallussaan olevat tiedot, jotka ovat tarpeen viestintäverkon osan yksilöimiseksi 5 luvussa tarkoitettua tuomioistuimelle esitettävää lupavaatimusta ja -päätöstä varten.

95 §

Korvaus teleyritykselle

Teleyrityksellä on oikeus saada valtion varoista korvaus tässä laissa tarkoitetusta sotilastiedusteluviranomaisen avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista siten kuin tietoyhteiskuntakaaren 299 §:ssä säädetään. Korvauksen maksamisesta päättää toimenpiteen suorittanut sotilastiedusteluviranomainen.

96 §

Korvaus tiedonsiirtäjälle

Tiedonsiirtäjällä on oikeus saada valtion varoista korvaus tässä laissa tarkoitetusta sotilastiedusteluviranomaisen avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista. Korvauksen maksamisesta päättää Puolustusvoimien tiedustelulaitos.

97 §

Muutoksenhaku korvauspäätökseen

Teleyritykselle tai tiedonsiirtäjälle annettuun korvauspäätökseen saa vaatia oikaisua siten kuin hallintolaissa (434/2003) säädetään.

Oikaisuvaatimukseen annettuun päätökseen saa hakea muutosta valittamalla hallinto-oikeuteen siten kuin hallintolainkäyttölaissa (586/1996) säädetään.

Hallinto-oikeuden päätökseen saa hakea muutosta valittamalla vain, jos korkein hallinto-oikeus myöntää valitusluvan.

Hallinto-oikeuden on varattava Viestintävirastolle tilaisuus tulla kuulluksi.

98 §

Kytkennän suorittamisen maksullisuus

Kytkennän suorittaja voi periä Puolustusvoimien tiedustelulaitokselta 5 luvun perusteella tuottamistaan palveluista maksuja. Maksujen suuruus ei saa ylittää kytkennän suorittamisesta kytkennän suorittajalle aiheutuvien kokonaiskustannusten määrää.

99 §

Teleyrityksen säilyttämien tietojen käyttäminen

Tietoyhteiskuntakaaren 157 §:n 1 momentissa tarkoitettuja tietoja saadaan käyttää sotilastiedustelutehtävän suorittamista varten.

100 §

Tietojen saanti yksityiseltä yhteisöltä tai henkilöltä

Sotilastiedusteluviranomaisella on tiedustelumenetelmien käyttöön perehtyneen sotilaslakimiehen tai muun virkamiehen pyynnöstä oikeus saada yhteisön jäsentä, tilintarkastajaa, toimitusjohtajaa, hallituksen jäsentä tai työntekijää velvoittavan yritys-, pankki- tai vakuutussalaisuuden estämättä sellaisia tietoja, joilla yksittäistapauksessa voidaan olettaa olevan tarpeen 4 §:ssä tarkoitetun toiminnan selvittämisessä ja joilla voidaan olettaa olevan merkitystä:

1) sotilastiedustelun kohteena olevan henkilön tai oikeushenkilön tunnistamiseksi, tavoittamiseksi tai yhteystietojen selvittämiseksi taikka henkilön liikkumisen selvittämiseksi;
2) tiedustelumenetelmän käytön kohdentamiseksi tiettyyn henkilöön; tai
3) henkilön tai oikeushenkilön taloudellisen toiminnan selvittämiseksi.

Sotilastiedusteluviranomaisilla on yksittäistapauksessa oikeus pyynnöstä saada teleyritykseltä ja yhteisötilaajalta yhteystiedot sellaisesta teleosoitteesta, jota ei mainita julkisessa luettelossa, taikka teleosoitteen tai telepäätelaitteen yksilöivät tiedot, jos tiedot ovat tarpeen tiedustelutehtävän suorittamiseksi. Sotilastiedustelun viranomaisilla on vastaava oikeus saada postitoimintaa harjoittavalta yhteisöltä jakeluosoitetietoja.

10 luku

Sotilastiedustelun tietojärjestelmä ja muut henkilörekisterit

101 §

Sotilastiedustelun tietojärjestelmä

Sotilastiedustelun tietojärjestelmä on sotilastiedusteluviranomaisen käyttöön tarkoitettu pysyvä, automaattisen tietojenkäsittelyn avulla ylläpidettävä henkilörekisteri. Sotilastiedustelun tietojärjestelmän rekisterinpitäjä on pääesikunta. Tietojärjestelmään voi lisäksi kuulua manuaalisesti ylläpidettäviä osia.

Tietojärjestelmästä on käytävä ilmi tiedon tallettaja.

102 §

Sotilastiedustelun tietojärjestelmän tietosisältö

Sotilastiedustelun tietojärjestelmä voi sisältää tietoja, joita on tarpeellista käsitellä ja yhdistää sotilastiedusteluviranomaiselle tässä laissa säädettyjen tehtävien suorittamiseksi.

Sotilastiedustelun tietojärjestelmään saadaan tallettaa henkilöstä seuraavat tarpeelliset tiedot:

1) henkilötunnus;
2) henkilön fyysisiin ominaisuuksiin perustuvat ja muut tunnistetiedot sekä ääni- ja kuvatallenteet;
3) kansalaisuutta ja perhesuhteita koskevat tiedot;
4) asuinpaikkatiedot;
5) koulutusta ja ammattia koskevat tiedot sekä työ- ja palvelushistoria;
6) yhteystiedot;
7) matkustamiseen liittyvät tiedot;
8) muut henkilön tai oikeushenkilön yksilöimiseksi tai hänen turvallisuutensa taikka Puolustusvoimien työturvallisuuden kannalta tarpeelliset tiedot;
9) tunnistamistiedot;
10) muut henkilön toimintaa ja käyttäytymistä koskevat tiedot.

Rekisteriin saadaan lisäksi tallettaa tarpeelliset tiedot henkilön tai yrityksen luotettavuuden selvittämisestä.

103 §

Sotilastiedustelun tietojärjestelmän käyttöoikeus

Sotilastiedustelun tietojärjestelmää saavat käyttää tässä laissa tarkoitettuihin tehtäviin määrätyt virkamiehet. Tietojärjestelmän käyttöoikeus voidaan myöntää myös asevelvollisuuslain mukaisessa kertausharjoituksessa oleville reserviläisille 89 §:ssä säädettyjen tehtävien suorittamiseksi. Tietojärjestelmän käytön on silloin tapahduttava sotilastiedustelutehtävään määrätyn virkamiehen johdon ja valvonnan alaisena.

104 §

Tilapäiset henkilörekisterit

Sotilastiedusteluviranomaisen valtakunnallisessa taikka sotilastiedusteluviranomaisen yhden tai useamman hallintoyksikön käytössä voi olla tilapäisiä henkilörekistereitä.

Tilapäiseen henkilörekisteriin saa tallettaa ja siellä saa käsitellä vain tässä laissa tarkoitetun tehtävän tai -tehtäväkokonaisuuden suorittamiseksi välttämättömiä henkilötietoja. Tilapäisen henkilörekisterin käyttöoikeus on niillä virkamiehillä, joiden käyttöön rekisteri on perustettu. Rekisteristä on käytävä ilmi tiedon tallettaja.

Valtakunnallisen tilapäisen henkilörekisterin rekisterinpitäjä on pääesikunta. Muun kuin valtakunnallisen tilapäisen henkilörekisterin rekisterinpitäjänä on toiminnasta vastaava hallintoyksikkö.

Valtakunnallisen tilapäisen henkilörekisterin perustamisesta päättää pääesikunta. Muun kuin valtakunnallisen tilapäisen henkilörekisterin perustamisesta päättää toiminnasta vastaava hallintoyksikkö. Rekisterin perustamisesta tehdään kirjallinen päätös. Valtakunnallisessa käytössä olevan tilapäisen henkilörekisterin perustamista koskevasta päätöksestä ja sen olennaisesta muuttamisesta on ilmoitettava viimeistään kuukautta ennen rekisterin perustamista tai muuttamista tietosuojavaltuutetulle. Perustamispäätöksessä on mainittava henkilörekisterin käyttötarkoitus.

105 §

Arkaluonteisten tietojen käsittely

Henkilötietolain 11 §:n 3 kohdassa tarkoitettuja arkaluonteisia henkilötietoja saa kerätä ja tallettaa sotilastiedustelun tietojärjestelmään ja muuhun henkilörekisteriin ja muutoin käsitellä silloin, kun tiedot ovat rekisterin käyttötarkoituksen kannalta tarpeellisia.

Henkilötietolain 11 §:n 1, 2 ja 4–6 kohdassa tarkoitettuja tietoja saa kerätä ja tallettaa sotilastiedustelun tietojärjestelmään ja muuhun henkilörekisteriin ja muutoin käsitellä ainoastaan silloin, kun se on tiedustelutehtävän suorittamiseksi välttämätöntä.

Mainitun pykälän 4 kohdassa tarkoitettuja tietoja saa lisäksi kerätä ja tallettaa sotilastiedustelun tietojärjestelmään ja muuhun henkilörekisteriin ja muutoin käsitellä silloin, kun se on rekisteröidyn oman turvallisuuden tai viranomaisen työturvallisuuden varmistamiseksi välttämätöntä.

Arkaluonteiset tiedot on poistettava rekisteristä välittömästi sen jälkeen, kun käsittelylle ei ole 1-3 momentissa mainittua perustetta.

106 §

Henkilön fyysisiin ominaisuuksiin perustuvien tunnistetietojen tietoturva

Tallettaessaan tai muutoin käsitellessään sähköisessä muodossa olevia henkilön fyysisiin ominaisuuksiin perustuvia tunnistetietoja rekisterinpitäjän tulee erityisesti huolehtia näiden tunnistetietojen tallettamisen ja muun käsittelyn tietoturvasta.

Henkilön fyysisiin ominaisuuksiin perustuvia tunnistetietoja talletettaessa ja muutoin käsiteltäessä on huolehdittava, että:

1) tunnistamisessa ja tunnistetietojen käsittelyssä käytettävät tietojärjestelmät, laitteet ja ohjelmistot ovat turvallisia;

2) tunnistetiedot on suojattu asiattomalta pääsyltä, luottamuksellisuuteen ja eheyteen kohdistuvilta loukkauksilta, muutoksilta ja väärentämiseltä sekä muulta vahingossa tai laittomasti tapahtuvalta käsittelyltä;

3) tunnistamisessa ja tunnistetietojen käsittelyssä toteutetaan tarpeelliset tekniset ja organisatoriset toimenpiteet sen varmistamiseksi, että tunnistaminen ja tunnistetietojen käsittely voidaan toteuttaa tietoturvallisella ja yksityisyyden suojan turvaavalla tavalla.

Rekisterinpitäjä vastaa edellä tarkoitetusta tietoturvasta myös sellaisen kolmannen osapuolen osalta, joka rekisterinpitäjän toimeksiannosta tallentaa fyysisiin ominaisuuksiin perustuvia tunnistetietoja.

107 §

Yksittäiseen tehtävään liittymättömien henkilötietojen käsittely ja käyttäminen

Sotilastiedusteluviranomaisen yksittäisessä tiedustelutehtävässä saatuja, tiedustelutehtävien suorittamiseksi tarpeellisia henkilötietoja, jotka eivät liity kyseiseen tai muuhun suoritettavana olevaan tiedustelutehtävään, mutta ovat tarpeen todennäköisesti tulevassa muussa tiedustelutehtävässä, saa kerätä ja tallettaa 101 §:ssä tarkoitettuun sotilastiedustelun tietojärjestelmään ja 104 §:ssä tarkoitettuun tilapäiseen henkilörekisteriin mainituissa lainkohdissa säädetyin edellytyksin.

Tämän lain 3 luvun mukaisilla tiedustelumenetelmillä saatua 1 momentissa tarkoitettua henkilötietoa saadaan kuitenkin käyttää vain sellaiseen tiedustelutehtävään, jonka toteuttamiseksi olisi saatu käyttää sitä tiedustelumenetelmää, jolla tieto on saatu. Tällaisen tiedon käyttämisestä päättää tuomioistuin silloin, jos sillä olisi ollut toimivalta päättää tiedustelumenetelmän käytöstä, jolla tieto on saatu.

Tietojen käsittelyn perustetta ja tarpeellisuutta on arvioitava vähintään kolmen vuoden välein. Tiedot on poistettava, kun tieto on todettu sen käyttötarkoituksen kannalta tarpeettomaksi.

108 §

Oikeus saada tietoja rekistereistä ja tietojärjestelmistä

Sotilastiedusteluviranomaisella on tässä laissa tarkoitettujen tehtävien suorittamiseksi ja henkilörekisteriensä ylläpitämistä varten oikeus saada maksutta ja salassapitosäännösten estämättä seuraavasti:
1) väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain (661/2009) 13—17 §:ssä tarkoitettuja tietoja;
2) sakkorekisteristä tietoja sakoista ja niiden täytäntöönpanosta sekä oikeushallinnon valtakunnallisen tietojärjestelmän diaari- ja asianhallintatietojen valtakunnalliseen käsittelyjärjestelmään sisältyviä tietoja syyttäjäviranomaisessa tai tuomioistuimessa vireillä olevista tai olleista rikosasioista ja ratkaisu- ja päätösilmoitusjärjestelmään sisältyviä tietoja rikosasioissa annetuista ratkaisuista ja niiden lainvoimaisuudesta, jos sellainen tieto on saatavissa;
3) ulkoasiainministeriön tietojärjestelmistä Suomessa lähettäjävaltiota edustavan diplomaatti- ja konsuliedustuston, kansainvälisen järjestön Suomessa olevan toimielimen ja muun samassa asemassa olevan kansainvälisen toimielimen henkilökuntaan kuuluvista ja näiden perheenjäsenistä sekä yksityisessä palveluksessa olevista henkilöistä, sekä ulkomaalaisrekisteristä annetussa laissa (1270/1997) säädettyyn ulkomaalaisrekisteriin kuuluvasta viisumiasioiden osarekisteristä tietoja viisumihakemuksista ja -päätöksistä;
4) poliisin henkilörekistereistä;
5) tietoja laissa henkilötietojen käsittelystä tullissa (639/2015) säädetyistä tullin rekistereistä;
6) tietoja ulosottokaaressa (705/2007) säädetystä ulosottorekisteristä;
7) ajoneuvoliikennerekisteristä annetussa laissa (541/2003) säädetystä ajoneuvoliikennerekisteristä omistajaa tai haltijaa koskevia tietoja;
8) tietoja matkustaja-aluksen henkilöluetteloista annetun lain (1038/2009) mukaisista matkustajia koskevista henkilöluetteloista;
9) majoitus- ja ravitsemistoiminnasta annetun lain (308/2006) mukaisia tarpeellisia matkustajatietoja majoitustoiminnan harjoittajilta;
10) tietoyhteiskuntakaaressa (917/2014) tarkoitettuja radiotaajuuksien käyttöä koskevia tietoja;
11) tietoja Puolustusvoimien henkilörekistereistä;
12) tietoja vapaaehtoisesta maanpuolustuksesta annetussa laissa säädetystä Maanpuolustuskoulutusyhdistyksen rekisteristä;
13) puolustusministeriöltä tietoja puolustustarvikkeiden viennistä annetussa laissa (282/2012) tarkoitetuista lupa-asioista;
14) ulkoasiainministeriöltä tietoja kaksikäyttötuotteiden vientivalvonnasta annetussa laissa (562/1996) tarkoitetuista lupa-asioista;
15) vesikulkuneuvorekisteristä annetussa laissa (424/2014) tarkoitetusta vesikulkuneuvorekisteristä sekä Ahvenanmaan huvivenerekisteristä veneitä ja niiden omistajia ja haltijoita koskevat tarpeelliset tiedot;
16) Maahanmuuttoviraston tietojärjestelmistä matkustusasiakirjaa, viisumia, oleskelua, kansainvälistä suojelua, maasta poistamista, maahantulokieltoa ja kansalaisuutta koskevasta asiasta;
17) ilmailulaissa (864/2014) tarkoitetusta ilma-alusrekisteristä ilma-aluksia, niiden haltijoita ja omistajia koskevia tietoja;
18) alusrekisterilaissa (512/1993) tarkoitetusta alusrekisteristä, rakenteilla olevien alusten rekisteristä ja historiarekisteristä tarpeelliset tiedot aluksista, niiden omistajista ja haltijoista;
19) tietoja liikenne- ja viestintäministeriön liikenneluparekisteristä;
20) tietoja laissa henkilötietojen käsittelystä rajavartiolaitoksessa annetussa laissa tarkoitetuista rekistereistä (579 /2005);

21) Rikosseuraamuslaitoksen henkilörekistereistä tuomitusta, vangista ja Rikosseuraamuslaitoksen yksikköön otetusta henkilöstä;
24) liikenne-, kalastus- ja ympäristöviranomaisilta tietoja kulkuneuvoista ja niiden sijainnista sekä liikenteestä;
25) tietoja Verohallinnolta verotuksen tietojärjestelmästä
26) Patentti- ja rekisterihallituksen kaupparekisteristä tiedot elinkeinonharjoittajia koskevista ilmoituksista ja tiedonannoista.

Tiedot voidaan luovuttaa myös teknisen käyttöyhteyden avulla tai muuten sähköisesti, siten kuin siitä rekisterinpitäjän kanssa sovitaan.

109 §

Tietojen saanti viranomaiselta

Sotilastiedusteluviranomaisella on oikeus saada viranomaiselta ja julkista tehtävää hoitamaan asetetulta yhteisöltä ja henkilöltä tässä laissa tarkoitetun tehtävän suorittamiseksi tarpeelliset tiedot ja asiakirjat maksutta ja salassapitovelvollisuuden estämättä, jollei sellaisen tiedon tai asiakirjan antamista sotilastiedusteluviranomaiselle tai tietojen käyttöä todisteena ole laissa kielletty tai rajoitettu.

110 §

Liikenteenharjoittajan velvollisuus lentomatkustajia koskevien tietojen antamiseen

Sen lisäksi, mitä 100 §:ssä säädetään, on lentoliikenteen harjoittajan toimitettava sotilastiedusteluviranomaiselle tämän pyynnöstä lentoliikenteen matkustajatiedot.

Lentoliikenteen matkustajatietoihin on sisällyttävä käytetyn matkustusasiakirjan numero ja tyyppi, kansalaisuus tai kansalaisuudettomuus, koko nimi, syntymäaika, rajanylityspaikka, jonka kautta henkilö saapuu jäsenvaltioiden alueelle tai lähtee jäsenvaltioiden alueelta, kuljetuksen koodi, kuljetuksen lähtö- ja saapumisaika, asianomaisella kuljetuksella kuljetettujen henkilöiden kokonaismäärä sekä alkuperäinen lähtöpaikka. Tiedot on luovutettava sähköisesti tai, jos se ei ole mahdollista, muulla asianmukaisella tavalla.

111 §

Tietojen luovuttaminen sotilasviranomaiselle

Rekisterinpitäjällä on oikeus salassapitosäännösten estämättä luovuttaa sotilasviranomaiselle sen laissa säädettyjen tehtävien suorittamiseksi tässä luvussa tarkoitettujen sotilastiedustelun tietojärjestelmän ja muiden henkilörekisterien tietoja, jos tiedot ovat tarpeen:
1) valtion turvallisuuden varmistamiseksi;
2) välittömän ja vakavan yleistä turvallisuutta uhkaavan vaaran torjumiseksi;

Tiedot saa myös luovuttaa teknisen käyttöyhteyden avulla tai muuten sähköisesti.

112 §

Tietojen luovuttaminen suojelupoliisille

Rekisterinpitäjä saa salassapitosäännösten estämättä luovuttaa tässä luvussa tarkoitetuista rekistereistä henkilötietoja suojelupoliisille, jos tiedot ovat tarpeen poliisilain 5 a luvussa (/) tai

siviilitiedusteluviranomaisen tietoliikennetiedustelusta annetussa laissa (/) tarkoitettua tiedustelua varten.

Tiedot saa luovuttaa myös teknisen käyttöyhteyden avulla tai muuten sähköisesti siten, kuin siitä rekisterinpitäjän kanssa sovitaan.

113 §

Tietojen luovuttaminen vaaran tai vahingon estämiseksi

Rekisterinpitäjä saa salassapitosäännösten estämättä luovuttaa tässä luvussa tarkoitetuista rekistereistä henkilötietoja hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi.

Toiselta viranomaiselta saatuja tietoja saa luovuttaa vain tiedot luovuttaneen viranomaisen suostumuksella.

114 §

Tietojen luovuttamisesta päättäminen

Oikeudesta luovuttaa 101 §:ssä tarkoitetun sotilastiedustelun tietojärjestelmän ja 104 §:ssä tarkoitetun tilapäisen henkilörekisterin tietoja teknisen käyttöyhteyden avulla tai tietojoukkona päättää pääesikunta.

Luovuttamisesta päätettäessä on rekisteröidyn tietosuojan ja tietoturvan varmistamiseksi otettava huomioon luovutettavien tietojen laatu.

115 §

Tietojen poistaminen sotilastiedustelun tietojärjestelmästä

Sotilastiedustelun tietojärjestelmästä poistetaan henkilötiedot 50 vuoden kuluttua viimeisen tiedon merkitsemisestä.

Tietojen käsittelyn perustetta ja tarpeellisuutta on arvioitava vähintään viiden vuoden välein.

116 §

Tietojen poistaminen tilapäisestä henkilörekisteristä

Tilapäisestä henkilörekisteristä poistetaan henkilötiedot, kun tieto on todettu rekisterin käyttötarkoituksen kannalta tarpeettomaksi.

Tietojen käsittelyn perustetta ja tarpeellisuutta on arvioitava vähintään kolmen vuoden välein.

Tarpeettomaksi käynyt tilapäinen henkilörekisteri on hävitettävä, jollei sitä siirretä arkistoitavaksi.

117 §

Henkilötunnuksen käsittely

Henkilötunnusta saa käsitellä rekisteröidyn antamalla suostumuksella tai silloin, kun se on välttämätöntä sotilastiedusteluviranomaisen tiedonhankintatehtävän kannalta.

Rekisterinpitäjän on huolehdittava siitä, että henkilötunnusta ei merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

118 §

Tarkastusoikeuden rajoitus

Rekisteröidyllä ei ole oikeutta tarkastaa 101 §:ssä tarkoitetun sotilastiedustelun tietojärjestelmän eikä 104 §:ssä tarkoitetun tilapäisen henkilörekisterin tietoja.

Tietosuojavaltuutettu voi rekisteröidyn pyynnöstä tai omasta aloitteestaan tarkastaa edellä mainittuun tietojärjestelmään ja rekistereihin talletettujen rekisteröityä koskevien tietojen lainmukaisuuden.

119 §

Tietojen luovuttaminen kansainvälisessä yhteistyössä

Sotilastiedusteluviranomainen saa 18 §:ssä säädetyssä kansainvälisessä yhteistyössä salassapitosäännösten estämättä luovuttaa tässä laissa säädetyn henkilörekisterin tietoja ulkomaan tiedustelu- ja turvallisuuspalveluille, jos se on välttämätöntä kansallisen turvallisuuden varmistamiseksi.

Luovutettavien tietojen laatu on varmennettava ja niihin on mahdollisuuksien mukaan lisättävä tietoja, joiden avulla vastaanottaja voi arvioida tietojen oikeellisuutta, täydellisyyttä, ajantasaisuutta ja luotettavuutta. Jos ilmenee, että on luovutettu virheellisiä tietoja tai että tietoja on luovutettu lainvastaisesti, asiasta on ilmoitettava viipymättä vastaanottajalle.

Tiedot saadaan luovuttaa myös teknisen käyttöyhteyden avulla tai tietojoukkona.

120 §

Kansainvälisessä yhteistyössä saatujen tietojen käsittely

Toisen valtion tiedustelu- tai turvallisuuspalvelulta saatujen tietojen käsittelyssä on noudatettava, mitä tietojen luovuttajan asettamissa ehdoissa määrätään salassapidosta, vaitiolovelvollisuudesta, tietojen käytön rajoituksista, tietojen edelleen luovutuksesta tai luovutetun aineiston palauttamisesta.

11 luku

Sotilastiedustelun valvonta puolustushallinnossa

121 §

Sotilastiedustelun oikeudellinen ja parlamentaarinen valvonta

Tiedustelutoiminnan laillisuusvalvontaan suorittaa tiedustelun valvontaviranomainen.

Parlamentaarista valvontaa suorittaa eduskunta.

122 §

Sisäinen valvonta

Pääesikunnan päällikkö valvoo sotilastiedustelua. Lisäksi Puolustusvoimien asessori vastaa sotilastiedustelun sisäisestä laillisuusvalvonnasta.

123 §

Puolustusministeriön suorittama valvonta

Puolustusministeriöllä on oikeus tarkastaa tässä laissa tarkoitettujen tiedonhankintakeinojen käytöstä laadittu pöytäkirja.

Puolustusministeriöllä on oikeus saada salassapitosäännösten estämättä tiedot yhteiskunnallisesti, taloudellisesti tai vakavuudeltaan merkittävistä sotilastiedusteluun liittyvistä asioista.

124 §

Kertomus eduskunnan oikeusasiamiehelle

Puolustusministeriön on annettava eduskunnan oikeusasiamiehelle vuosittain kertomus tiedustelumenetelmien ja niiden suojaamisen käytöstä ja valvonnasta.

125 §

Tarkemmat säännökset

Valtioneuvoston asetuksella voidaan antaa tarkempia säännöksiä tässä laissa tarkoitettujen tiedustelumenetelmien käytön järjestämisestä ja valvonnasta sekä toimenpiteiden kirjaamisesta ja valvontaa varten annettavista selvityksistä.

12 luku

Erinäiset säännökset

126 §

Määräaikojen laskeminen

Tässä laissa tarkoitettujen määräaikojen laskemiseen ei sovelleta säädettyjen määräaikain laskemisesta annettua lakia.

Aika, joka on määrätty kuukausina, päättyy sinä määräkuukauden päivänä, joka järjestysnumeroltaan vastaa sanottua päivää. Jos vastaavaa päivää ei ole siinä kuussa, jona määräaika päättyy, määräaika päättyy kuukauden viimeisenä päivänä.

127 §

Tiedustelukiellot

Telekuuntelua, telekuuntelun sijasta toimitettavaa tietojen hankkimista, teknistä havainnointia tai tietoliikennetiedustelua ei saa kohdistaa sellaiseen viestintään tai viestiin, josta viestinnän osapuoli ei saisi todistaa oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n nojalla.

Jos telekuuntelun, telekuuntelun sijasta tapahtuvan tietojen hankkimisen tai teknisen havainnoinnin aikana tai muulloin ilmenee, että kyseessä on viesti, jonka kuuntelu ja katselu on kielletty, toimenpide on keskeytettävä ja sillä saadut tallenteet ja sillä saatuja tietoja koskevat muistiinpanot on hävitettävä välittömästi.

Jollei toisin tässä laissa säädetä, tässä pykälässä tarkoitetut tiedustelukiellot eivät kuitenkaan koske tapauksia, joissa 1 momentissa tarkoitetun henkilön toiminta vaarantaa maanpuolustusta tai muuten vakavasti vaarantaa kansallista turvallisuutta ja myös hänen osaltaan on tehty päätös tele-

kuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, teknisestä kuuntelusta tai teknisestä katselusta.

128 §

Tallenteiden tarkastaminen

Tiedustelumenetelmän käyttöä johtavan ja tiedustelumenetelmää käyttävän virkamiehen on ilman aiheetonta viivytystä tarkastettava 3 tai 4 luvun tiedustelumenetelmien käytössä kertyneet tallenteet ja asiakirjat.

129 §

Tallenteiden tutkiminen

Tämän lain 3 ja 4 luvussa tarkoitettujen tiedustelumenetelmien käytössä kertyneitä tallenteita saa tutkia vain tuomioistuin ja pääesikunnan tiedustelupäällikkö, sotilastiedusteluviranomaisen tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies tai muu tiedustelutehtävään määrätty sotilastiedusteluviranomaisen virkamies.

Lisäksi tallenteita voi tutkia pääesikunnan tiedustelupäällikön määräyksestä sotilastiedusteluviranomaisen ulkopuolinen asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankintaa toteutettaessa.

130 §

Pöytäkirja

Tiedustelumenetelmän käytöstä on laadittava ilman aiheetonta viivytystä pöytäkirja.

Valtioneuvoston asetuksella annetaan tarkemmat säännökset tiedustelutehtävän toimenpiteiden kirjaamisesta.

131 §

Vaitiolovelvollisuus

Sotilastiedustelun viranomaisten henkilöstöön kuuluvan virkamiehen vaitiolovelvollisuudesta on voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa ja muussa laissa sekä tässä luvussa jäljempänä säädetään. Sama vaitiolovelvollisuus on sillä, joka suorittaa tiedustelutehtävää sotilastiedusteluviranomaisen johdon ja valvonnan alaisena tai avustaa tiedustelutehtävän suorittamisessa.

Sotilastiedusteluviranomaisen henkilöstöön kuuluva virkamies ei saa ilmaista luottamuksellisesti tietoja antaneen taikka peitehenkilönä toimineen henkilöllisyyttä koskevaa tietoa, jos tiedon ilmaiseminen vaarantaisi luottamuksellisesti tietoja antaneen tai peitehenkilönä toimineen tai hänen läheistensä turvallisuuden.

Vaitiolovelvollisuus on voimassa myös, jos henkilöllisyyttä koskevan tiedon ilmaiseminen vaarantaisi jo päättyneen, käynnissä olevan tai tulevan tiedonhankinnan.

Edellä 1 ja 2 momentissa tarkoitettu vaitiolovelvollisuus on myös sillä, joka suorittaa tiedustelutehtävää sotilastiedusteluviranomaisen johdon ja valvonnan alaisena tai avustaa tiedustelutehtävän suorittamisessa.

Vaitiolovelvollisuus on voimassa myös palvelussuhteen sotilastiedusteluviranomaisessa päätyttyä.

132 §

Vaitiolo-oikeus

Sotilastiedustelun viranomaisten henkilöstöön kuuluva ei ole velvollinen ilmaisemaan hänelle hänen palvelussuhteensa aikana luottamuksellisesti tietoja antaneen henkilöllisyyttä koskevaa tietoa eikä tietoa salassa pidettävistä taktisista tai teknisistä menetelmistä.

Sama vaitiolo-oikeus on sillä, joka suorittaa tiedustelutehtävää sotilastiedustelun viranomaisen johdon ja valvonnan alaisena tai avustaa tiedustelutehtävän suorittamisessa.

133 §

Virkamerkki

Sotilastiedusteluviranomaisen virkamiehellä on puolustusministeriön asetuksella säädettävä virkamerkki.

Sotilastiedusteluviranomaisen virkamiehen on tarvittaessa pidettävä virkamerkki mukana virkatehtävää suorittaessa. Sotilastiedusteluviranomaisen virkamiehen on tarvittaessa ilmaistava toimenpiteen kohteena olevalle henkilölle olevansa sotilastiedusteluviranomaisen virkamies ja pyynnöstä esitettävä virkamerkkinsä, jos ilmaiseminen tai esittäminen on mahdollista toimenpiteen suorittamista vaarantamatta.

Sotilastiedusteluviranomaisen on huolehdittava siitä, että virkatoimen suorittanut sotilastiedusteluviranomaisen virkamies on tarvittaessa yksilöitävissä.

134 §

Menettely tuomioistuimessa

Tiedustelumenetelmää koskeva lupa-asia käsitellään Helsingin käräjäoikeudessa. Käräjäoikeus on päätösvaltainen, kun siinä on yksin puheenjohtaja. Istunto voidaan pitää myös muuna aikana ja muussa paikassa kuin yleisen alioikeuden istunnosta säädetään.

Vaatimus tiedustelumenetelmän käytöstä on tehtävä kirjallisesti. Tiedustelumenetelmän käyttöä koskeva vaatimus on otettava viipymättä tuomioistuimessa käsiteltäväksi vaatimuksen tehneen tai hänen määräämänsä asiaan perehtyneen virkamiehen läsnä ollessa.

Asia on ratkaistava kiireellisesti. Käsittely voidaan pitää myös käyttäen videoneuvottelua tai muuta soveltuvaa teknistä tiedonvälitystapaa, jos käsittelyyn osallistuvilla on puhe- ja näköyhteys keskenään.

Tiedustelumenetelmää koskevan päätöksen sisällöstä säädetään tämän lain 3 ja 4 luvussa. Päätös on annettava heti tai viimeistään samaan tiedustelua koskevaan kokonaisuuteen liittyvien tiedustelumenetelmiä koskevien asioiden käsittelyn päätyttyä.

Jos tuomioistuin on myöntänyt luvan telekuunteluun tai televalvontaan, se saa tutkia ja ratkaista luvan myöntämistä uuteen henkilöön, teleosoitteeseen tai telepäätelaitteeseen koskevan asian vaatimuksen tehneen tai hänen määräämänsä virkamiehen läsnä olematta, jos on kulunut vähemmän kuin kuusi kuukautta aiemman lupa-asian käsittelystä. Asia voidaan käsitellä mainitun virkamiehen läsnä olematta myös, jos tiedustelumenetelmän käyttö on jo lopetettu.

Lupa-asiassa annettuun päätökseen ei saa hakea muutosta valittamalla. Päätöksestä saa ilman määräaikaa kannella Helsingin hovioikeudelle. Kantelu on käsiteltävä kiireellisenä.

Tiedustelumenetelmää koskevan asian käsittelyssä on kiinnitettävä erityistä huomiota salassapitovelvollisuuden toteutumiseen ja siihen, että asiakirjoihin ja tietojärjestelmiin sisältyvien tietojen suoja turvataan tarvittavin menettelytavoin ja tietoturvallisuusjärjestelyin.

135 §

Asianosaisjulkisuuden rajoittaminen eräissä tapauksissa

Henkilöllä, jonka oikeutta tai velvollisuutta asia koskee, ei ole viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 11 §:ssä säädetystä huolimatta oikeutta saada tietoa tässä laissa tarkoitetusta tiedonhankinnasta, ennen kuin 86 §:ssä tarkoitettu ilmoitus on tehty.

Siviilitiedusteluun liittyvistä rajoituksista säädetään poliisilain 5 a luvussa.

13 luku

Voimaantulo

136 §

Voimaantulo

Laki tulee voimaan päivänä 20 .

Lagförslag

Lag
om militär underrättelseverksamhet

1 kap.

Allmänna bestämmelser

1 §

Lagens tillämpningsområde

I denna lag föreskrivs om syftet med Försvarsmaktens underrättelseverksamhet (militär underrättelse), om myndigheternas uppgifter och befogenheter, beslutsfattande samt om styrningen och övervakningen av underrättelseverksamheten.

2 §

Förhållande till annan lagstiftning

Bestämmelser om civil underrättelseverksamhet finns i 5 a kap. i polislagen (xxx/xxxx) och i lagen om civil underrättelseinhämtning avseende datatrafik (/). Bestämmelser om övervakning av underrättelseverksamheten finns i lagen (/).

Bestämmelser om försvarsmaktens brottsbekämpning finns i lagen om militär disciplin och brottsbekämpning inom försvarsmakten (255/2014).

Bestämmelser om behandlingen av personuppgifter finns i personuppgiftslagen (523/1999) och lagen om offentlighet i myndigheternas verksamhet (621/1999) om inget annat bestäms i denna lag.

3 §

Den militära underrättelseverksamhetens syfte

Syftet med den militära underrättelseverksamheten är att inhämta och behandla information om yttre hot som stöd för den högsta statsledningens beslutsfattande och för att de uppgifter som avses i 2 § i lagen om försvarsmakten (551/2007) ska kunna fullgöras.

4 §

Föremål för den militära underrättelseverksamheten

Med militär underrättelseverksamhet kan man inom landet och utomlands inhämta information om

1) militär verksamhet,
2) utländsk underrättelseverksamhet,
3) verksamhet som hotar stats- och samhällsordningen,
4) massförstörelsevapen,

5) utvecklande och spridning av krigsmateriel,
6) allvarliga hot som riktas mot staten eller mot samhällets vitala funktioner,
7) en främmande stats planer eller verksamhet som kan orsaka skada för Finlands internationella relationer eller andra viktiga intressen,
8) kriser som hotar internationell fred och säkerhet,
9) hot som riktas mot säkerheten vid internationella krishanteringsoperationer,
10) hot som riktas mot säkerheten när försvarsmakten ger internationellt bistånd och i annan internationell verksamhet.

5 §

Proportionalitetsprincipen

Den militära underrättelseverksamhetens åtgärder ska vara försvarbara i förhållande till hur viktiga och nödvändiga de uppgifter är som erhålls genom informationsinhämtning och till hur brådskande det är att erhålla uppgifterna, till det eftersträvade målet med den militära underrättelseverksamheten, till föremålet för den militära underrättelseverksamheten, till den kränkning av rättigheter som andra orsakas av att en underrättelseåtgärd används samt till andra omständigheter som påverkar saken.

6 §

Principen om minsta olägenhet

Då den militära underrättelseverksamhetens befogenheter används får det inte ingripas i någons rättigheter i större utsträckning och ingen får orsakas större skada eller olägenheter än vad som är nödvändigt för att uppdraget ska kunna fullgöras.

7 §

Principen om ändamålsbundenhet

Den militära underrättelseverksamhetens befogenheter får endast användas för det syfte som föreskrivs i denna lag.

8 §

Förbud mot diskriminering

Inriktningen av åtgärderna inom den militära underrättelseverksamheten ska göras på ett icke-diskriminerande sätt. Inriktningen av en åtgärd inom den militära underrättelseverksamheten får inte enbart grunda sig på uppgifter om en persons ursprung, nationalitet, språk, religion, övertygelse, åsikt, politiska verksamhet, fackföreningsverksamhet, familjerelationer, sexuella inriktning, om inget annat följer av nödvändigheten med informationsinhämtningen.

9 §

Definitioner

I denna lag avses med
1) den som utför en koppling en sådan tillhandahållare av nät- och infrastrukturtjänster som avses i 6 § i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015) eller ett företag som helt och hållet ägs av den,

2) lokaliseringsuppgift information från ett kommunikationsnät eller en terminalutrustning som anger ett abonnemangs eller en terminalutrustnings geografiska position och som används för annat än för att förmedla meddelanden,
3) teleföretag en aktör som tillhandahåller nättjänster eller kommunikationstjänster för en grupp av användare som inte har avgränsats på förhand, dvs. bedriver allmän televerksamhet,
4) dataöverförare den part som äger eller innehar en kommunikationsnätsdel som överskrider Finlands gräns,
5) underrättelseinhämtningsmetoder militärunderrättelsemyndighetens befogenheter om vilka föreskrivs i 4 och 5 kap.,
6) datatrafikens tekniska data andra uppgifter om datatrafiken än de som hör till innehållet i ett meddelande,
7) identifieringsuppgifter uppgifter om ett meddelande som kan förknippas med en abonnent som avses i 3 § 7 punkten i informationssamhällsbalken (917/2014) eller med en användare som avses i 30 punkten i nämnda paragraf,
8) statlig aktör en främmande stats myndighet eller en aktör som kan jämställas med en sådan,
9) kommunikationsnät ett system som består av sammankopplade ledningar och av anordningar, och som är avsett för överföring eller distribution av meddelanden via ledning, med radiovågor, optiskt eller på något annat elektromagnetiskt sätt,
10) sammanslutningsabonnent en sammanslutningsabonnent som avses i 3 § 41 punkten i informationssamhällsbalken.

10 §

Förutsättningar för användning av underrättelseinhämtningsmetoderna

En förutsättning för att en underrättelseinhämtningsmetod ska få användas är att man med den kan antas få information som behövs med tanke på ett underrättelseuppdrag.

De underrättelseinhämtningsmetoder om vilka föreskrivs i denna lag får användas i hemlighet för dem som är föremål för metoderna.

Användningen av en underrättelseinhämtningsmetod ska avslutas före utgången av den tid som anges i beslutet eller tillståndet, genast när syftet med användningen har nåtts eller om det inte längre finns förutsättningar för att använda metoden.

2 kap.

Den militära underrättelseverksamhetens myndigheter samt styrning och tillsyn

11 §

Styrning och ledning av den militära underrättelseverksamheten

Det ministerutskott som behandlar utrikes- och säkerhetspolitik och republikens president behandlar vid ett gemensamt sammanträde förberedande de prioriteringar som ska gälla föremålen för den militära underrättelseverksamheten.

Försvarsministeriet styr den militära underrättelseverksamheten administrativt och ger Försvarsmakten de i 1 mom. avsedda prioriteringarna som har behandlats i förberedande syfte.

Huvudstaben leder den militära underrättelseverksamheten och iakttar då prioriteringarna för den militära underrättelseverksamheten.

12 §

Militärunderrättelsemyndigheter

Militärunderrättelsemyndigheter är huvudstaben och Försvarsmaktens underrättelsetjänst, som kan inhämta information för att utföra ett underrättelseuppdrag på det sätt som föreskrivs nedan.

Bestämmelser om militär underrättelseverksamhet i försvarsgrenarna finns i 60 §. Försvarsgrenarna är underställda militärunderrättelsemyndigheten i den militära underrättelseverksamheten.

13 §

Underrättelseuppdrag

Med ett underrättelseuppdrag avses ett uppdrag för informationsinhämtning som huvudstabens underrättelsechef ger militärunderrättelsemyndigheten och som gäller ett föremål för militär underrättelseverksamhet enligt 4 §. Ett underrättelseuppdrag ska basera sig på det syfte med den militära underrättelseverksamheten om vilket föreskrivs i 3 § eller på en begäran om information enligt 16 §.

14 §

Tillsynen över den militära underrättelseverksamheten

Försvarsministeriet ger det gemensamma sammanträdet mellan det ministerutskott som behandlar utrikes- och säkerhetspolitik och republikens president en utredning om de prioriteringar som det gemensamma sammanträdet mellan det ministerutskott som behandlar utrikes- och säkerhetspolitiken och republikens president har behandlat förberedande en gång per år eller på begäran av det gemensamma sammanträdet mellan det ministerutskott som behandlar utrikes- och säkerhetspolitiken och republikens president eller på initiativ av försvarsministeriet.

Huvudstaben ger försvarsministeriet årligen en utredning om den militära underrättelseverksamhetens art och omfattning samt hur den har inriktats. En utredning ska dessutom ges utan dröjsmål när försvarsministeriet ber om det.

3 kap.

Samverkan med andra myndigheter och internationellt samarbete

15 §

Samarbete med skyddspolisen och andra myndigheter

Militärunderrättelsemyndigheterna ska agera i samarbete med skyddspolisen för att sköta underrättelseinhämtningen på ett ändamålsenligt sätt och i detta syfte, trots det som föreskrivs om sekretess, ge skyddspolisen nödvändiga uppgifter.

Övriga myndigheter kan vid behov bistå militärunderrättelsemyndigheten i fullgörandet av ett underrättelseuppdrag.

Närmare bestämmelser om samarbetet mellan militärunderrättelsemyndigheterna och skyddspolisen får utfärdas genom förordning av statsrådet.

16 §

Begäran om upplysningar

Republikens president, statsrådets kansli, utrikesministeriet och försvarsministeriet kan hos huvudstaben begära upplysningar om föremålen för den militära underrättelseverksamheten, vilka stämmer överens med de prioriteringar som utrikes- och säkerhetspolitiska ministerutskottets och republikens presidents gemensamma sammanträde har behandlat i förberedande syfte.

17 §

Samordning av underrättelseverksamheten

Den militära och den civila underrättelseverksamheten samordnas mellan republikens president, statsrådets kansli, utrikesministeriet, försvarsministeriet och inrikesministeriet samt vid behov mellan andra ministerier och myndigheter.

Om det bedöms att den militära underrättelseverksamheten är utrikes- och säkerhetspolitiskt betydelsefull, ska ärendet i förberedande syfte behandlas mellan de myndigheter som nämns i 1 mom.

18 §

Internationellt samarbete

För att trygga Finlands nationella säkerhet får militärunderrättelsemyndigheterna i anknytning till sina uppgifter

1) byta underrättelseuppgifter med utländska underrättelse- och säkerhetstjänster trots sekretessbestämmelserna,

2) delta i internationellt samarbete i anknytning till inhämtandet och bedömningen av underrättelseuppgifter.

Huvudstabens underrättelsechef beslutar om internationellt samarbete i Finland eller utomlands samt om användningen av de befogenheter som sammanhänger med detta.

Vid överlåtelse och mottagande av uppgifter följs dessutom vad som särskilt bestäms om detta i internationella fördrag som är förpliktande för Finland eller föreskrivs i lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004).

4 kap.

Befogenheter till informationsinhämtning

19 §

Observation och systematisk observation

Med *observation* avses iakttagelser i underrättelsesyfte som i hemlighet riktas mot en viss person eller grupp av personer eller mot ett föremål, ämne, egendom, lokal eller område.

Med *systematisk observation* avses annan än kortvarig observation av en person eller grupp av personer som med fog kan antas ha samband med ett underrättelseuppdrag.

Militärunderrättelsemyndigheterna får inrikta systematisk observation på ett objekt som avses i 2 mom., om detta kan antas vara av ytterst stor betydelse för att få information med tanke på ett underrättelseuppdrag.

Observation som avses i denna paragraf får inte riktas mot utrymmen som används för stadigvarande boende.

20 §

Beslut om systematisk observation

En militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna beslutar om systematisk observation.

Beslutet om systematisk observation får meddelas för högst sex månader åt gången.

Beslutet om systematisk observation ska fattas skriftligen. I beslutet ska följande nämnas:

1) det underrättelseuppdrag som ligger till grund för åtgärden,
2) den person eller grupp av personer som åtgärden riktas mot,
3) de fakta som förutsättningarna för systematisk observation och inriktningen grundar sig på,
4) beslutets giltighetstid,
5) den tjänsteman som leder och övervakar den systematiska observationen och som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna,
6) eventuella begränsningar i och villkor för den systematiska observationen.

21 §

Förtäckt inhämtande av information

Med *förtäckt inhämtande* av information avses inhämtande av information genom kortvarig interaktion med en viss person där falska, vilseledande eller förtäckta uppgifter används för att hemlighålla militärunderrättelsemyndighetens tjänstemans uppdrag.

Militärunderrättelsemyndigheten får använda förtäckt inhämtande av information för att utföra ett underrättelseuppdrag.

Förtäckt inhämtande av information är inte tillåtet i bostäder ens med bostadsinnehavarens medverkan.

22 §

Beslut om förtäckt inhämtande av information

En militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna beslutar om förtäckt inhämtande av information.

Beslutet om förtäckt inhämtande av information ska fattas skriftligen. I beslutet ska följande nämnas:

1) det underrättelseuppdrag som ligger till grund för åtgärden,
2) den person eller grupp av personer som åtgärden riktas mot,
3) de fakta som förutsättningarna för förtäckt inhämtande av information och inriktningen grundar sig på,
4) den tjänsteman som leder och övervakar det förtäckta inhämtandet av information och som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna,
5) den planerade tidpunkten för genomförandet av åtgärden,
6) eventuella begränsningar i och villkor för det förtäckta inhämtandet av information.

Vid förändrade omständigheter ska beslutet vid behov ses över.

Om åtgärden inte tål uppskov, behöver ett beslut som avses i 1 mom. inte upprättas i skriftlig form före det förtäckta inhämtandet av information. Beslutet ska dock upprättas i skriftlig form utan dröjsmål efter att åtgärden har vidtagits.

23 §

Teknisk avlyssning

Med *teknisk avlyssning* avses att en viss persons eller persongrupps samtal eller meddelande som inte är avsett för utomstående och i vilket avlyssnaren inte deltar, trots 24 kap. 5 § i strafflagen (39/1889) avlyssnas, upptas eller behandlas på något annat sätt med hjälp av en teknisk anordning, metod eller programvara i syfte att ta reda på innehållet i samtalet eller meddelandet eller utreda deltagarnas verksamhet.

Militärunderrättelsemyndigheten får utanför ett utrymme som används för stadigvarande boende inrikta teknisk avlyssning på en person eller grupp av personer, om detta kan antas vara av ytterst stor betydelse för att få information med tanke på ett underrättelseuppdrag. Avlyssningen kan riktas mot utrymmen eller andra platser där det kan antas att en person eller grupp av personer som har samband med ett underrättelseuppdrag sannolikt befinner sig eller som de besöker.

24 §

Beslut om teknisk avlyssning

En domstol beslutar om teknisk avlyssning av en person som har berövats sin frihet på yrkande av en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna. Om ärendet inte tål uppskov, får en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna besluta om teknisk avlyssning till dess domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

En militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna beslutar om annan teknisk avlyssning än den som avses i 1 mom.

Tillstånd kan ges och beslut fattas för högst sex månader åt gången.

I ett beslut om teknisk avlyssning ska följande nämnas:

1) det underrättelseuppdrag som ligger till grund för åtgärden,
2) den person eller grupp av personer eller det utrymme eller någon annan plats som åtgärden riktas mot,
3) de fakta som förutsättningarna för och inriktningen av teknisk avlyssning grundar sig på,
4) hur länge tillståndet är i kraft med angivande av klockslag,
5) den tjänsteman som leder och övervakar den tekniska avlyssningen och som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna,
6) eventuella begränsningar i och villkor för den tekniska avlyssningen.

25 §

Optisk observation

Med *optisk observation* avses att man trots 24 kap. 6 § i strafflagen iakttar eller gör upptagningar av en viss person eller grupp av personer eller av ett utrymme eller någon annan plats med en kamera eller andra utplacerade tekniska anordningar, metoder eller programvaror.

Militärunderrättelsemyndigheten får utanför ett utrymme som används för stadigvarande boende inrikta optisk observation på en person eller grupp av personer, om detta kan antas vara av ytterst stor betydelse för att få information med tanke på ett underrättelseuppdrag. Observationen kan riktas mot utrymmen eller andra platser där det kan antas att den person eller grupp av personer som är föremål för observationen sannolikt befinner sig eller som de besöker.

26 §

Beslut om optisk observation

En domstol beslutar om optisk observation av en person som har berövats sin frihet på yrkande av en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna. Om ärendet inte tål uppskov, får en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna besluta om optisk observation till dess domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

En militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna beslutar om annan optisk observation än den som avses i 1 mom.

Tillstånd kan ges och beslut fattas för högst sex månader åt gången.

I ett beslut om optisk observation ska följande nämnas:

1) det underrättelseuppdrag som ligger till grund för åtgärden,
2) den person eller grupp av personer eller det utrymme eller någon annan plats som åtgärden riktas mot,
3) de fakta som förutsättningarna för och inriktningen av optisk observation grundar sig på,
4) hur länge tillståndet är i kraft med angivande av klockslag,
5) den tjänsteman som leder och övervakar den optiska observationen och som är särskilt förtrogen med användningen av Försvarsmaktens underrättelsetjänsts underrättelseinhämtningsmetoder,
6) eventuella begränsningar i och villkor för den optiska observationen.

27 §

Teknisk spårning

Med *teknisk spårning* avses att förflyttning av person, föremål, ämnen eller egendom spåras med hjälp av radiosändare som fästs eller som redan finns på objektet eller med hjälp av någon annan liknande teknisk anordning, metod eller programvara.

Militärunderrättelsemyndigheten får rikta teknisk spårning mot föremål, ämnen eller egendom eller mot föremål, ämne eller egendom som en person antas inneha eller använda.

Om syftet med teknisk spårning är att följa hur en person förflyttar sig genom att en spårningsanordning fästs i de kläder som personen bär eller i ett föremål som han eller hon bär med sig (teknisk spårning av en person), får åtgärden genomföras bara om detta med fog kan antas vara av synnerligen stor betydelse för erhållande av information med tanke på ett underrättelseuppdrag.

28 §

Beslut om teknisk spårning

En domstol beslutar om teknisk spårning av en person på yrkande av en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna. Om ärendet inte tål uppskov, får en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av militärunderrättelsemyndighetens underrättelseinhämtningsmetoder besluta om teknisk spårning av en person till dess att domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att underrättelseinhämtningsmetoden började användas.

En militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av militärunderrättelsemyndighetens underrättelseinhämtningsmetoder beslutar om annan teknisk spårning än den som avses i 1 mom.

Tillstånd kan ges och beslut fattas för högst sex månader åt gången.

I ett yrkande och i ett beslut om teknisk spårning ska följande nämnas:

1) det underrättelseuppdrag som ligger till grund för åtgärden,
2) den person, det föremål, det ämne eller den egendom som åtgärden riktas mot,
3) de fakta som förutsättningarna för och inriktningen av teknisk spårning grundar sig på,
4) tillståndets giltighetstid med angivande av klockslag,
5) den tjänsteman som leder och övervakar den tekniska spårningen och som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna,
6) eventuella begränsningar i och villkor för den tekniska spårningen.

29 §

Teknisk observation av utrustning

Med teknisk observation av utrustning avses att en funktion, informationsinnehållet eller identifieringsuppgifterna i en dator eller i en liknande teknisk anordning eller i dess programvara på något annat sätt än enbart genom sinnesförnimmelser observeras, upptas eller behandlas för att utreda omständigheter som är av betydelse med tanke på ett underrättelseuppdrag.

Teknisk observation av utrustning får inte användas för att skaffa information om innehållet i ett meddelande eller om dess identifieringsuppgifter.

Militärunderrättelsemyndigheten får ges tillstånd till teknisk observation av utrustning, om detta kan antas vara av synnerligen stor betydelse för inhämtning av information med tanke på ett underrättelseuppdrag. Militärunderrättelsemyndigheten får rikta teknisk observation av utrustning mot en dator eller en liknande teknisk anordning som personen i fråga sannolikt använder, eller mot dess programvara.

30 §

Beslut om teknisk observation av utrustning

En domstol beslutar om teknisk observation av utrustning på yrkande av en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna. Om ärendet inte tål uppskov, får en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna besluta om teknisk observation av utrustning till dess domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart som möjligt, dock senast 24 timmar efter det att underrättelseinhämtningsmetoden började användas.

Tillstånd får beviljas för högst sex månader åt gången.

I ett yrkande och i ett beslut om teknisk observation av utrustning ska följande nämnas:

1) det underrättelseuppdrag som ligger till grund för åtgärden,
2) den tekniska anordning eller programvara som åtgärden riktas mot,
3) de fakta som förutsättningarna för och inriktningen av teknisk observation av utrustning grundar sig på,
4) tillståndets giltighetstid med angivande av klockslag,
5) den tjänsteman som leder och övervakar den tekniska observationen av utrustning och som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna,
6) eventuella begränsningar i och villkor för den tekniska observationen av utrustning.

31 §

Installation och avinstallation av anordningar, metoder eller programvara

En tjänsteman som är anställd vid militärunderrättelsemyndigheten har rätt att fästa en anordning, metod eller programvara som används för teleavlyssning, inhämtning av information i stället för teleavlyssning, teleövervakning, teknisk avlyssning, optisk observation, teknisk spårning eller teknisk observation av utrustning på föremål, ämnen, egendom, i utrymmen och andra platser eller informationssystem som åtgärden riktas mot, om det behövs för den tekniska avlyssningen, den optiska observationen, den tekniska observationen av utrustning eller den tekniska spårningen. För att installera, ta i bruk och avinstallera anordningen, metoden eller programvaran har en tjänsteman vid militärunderrättelsemyndigheten då rätt att i hemlighet ta sig in i ovan nämnda objekt eller i ett ovan nämnt informationssystem samt att kringgå, låsa upp eller på något annat motsvarande sätt tillfälligt passera eller störa objektens eller informationssystemets säkerhetssystem.

32 §

Teleavlyssning

Med *teleavlyssning* avses att ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning genom ett allmänt kommunikationsnät som avses i 3 § 43 punkten i informationssamhällsbalken eller ett därtill anslutet kommunikationsnät avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och identifieringsuppgifterna i anslutning till det. Teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en sådan person som med fog kan antas ha samband med ett underrättelseuppdrag.

Militärunderrättelsemyndigheten får ges tillstånd till teleavlyssning av en statlig aktör.
Militärunderrättelsemyndigheten får ges tillstånd till teleavlyssning av någon annan än en statlig aktör, om detta kan antas vara av synnerligen stor betydelse för erhållandet av information med tanke på ett underrättelseuppdrag.

33 §

Inhämtning av information i stället för teleavlyssning

Om det är sannolikt att ett meddelande som avses i 32 § och dess identifieringsuppgifter inte längre är tillgängliga genom teleavlyssning, kan militärunderrättelsemyndigheten beviljas tillstånd att inhämta informationen hos ett teleföretag eller en sammanslutningsabonnent, under de förutsättningar som anges i 32 §.

Om inhämtningen av information för utredning av innehållet i ett meddelande riktas mot en personlig teknisk anordning som lämpar sig för att sända och ta emot meddelanden och finns i direkt anslutning till en teleterminalutrustning eller mot förbindelsen mellan en sådan anordning och en teleterminalutrustning, kan militärunderrättelsemyndigheten beviljas tillstånd till inhämtning av information i stället för teleavlyssning, om de förutsättningar som anges i 32 § föreligger.

34 §

Beslut om teleavlyssning och motsvarande inhämtning av information

En domstol beslutar om teleavlyssning och om inhämtning av information i stället för teleavlyssning på yrkande av en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna.

Tillstånd till teleavlyssning eller inhämtning av information i stället för teleavlyssning kan ges för högst sex månader åt gången.

I yrkandet och i beslutet om teleavlyssning och inhämtning av information i stället för teleavlyssning ska följande nämnas:

1) det underrättelseuppdrag som ligger till grund för åtgärden,
2) den person, teleadress eller teleterminalutrustning som åtgärden riktas mot,
3) de fakta som förutsättningarna för och inriktningen av teleavlyssningen eller inhämtningen av information i stället för teleavlyssning grundar sig på,
4) giltighetstiden med angivande av klockslag för tillståndet till teleavlyssning eller inhämtning av information i stället för teleavlyssning,
5) den tjänsteman som leder och övervakar utförandet av teleavlyssningen eller inhämtningen av information i stället för teleavlyssning och som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna,
6) eventuella begränsningar i och villkor för teleavlyssningen eller inhämtningen av information i stället för teleavlyssning.

35 §

Teleövervakning

Med *teleövervakning* avses att förmedlingsuppgifter inhämtas om ett meddelande som har sänts från en teleadress eller teleterminalutrustning som är kopplad till ett kommunikationsnät eller som har mottagits till en sådan adress eller utrustning samt att uppgifter om en teleadress eller teleterminalutrustnings läge inhämtas. Med förmedlingsuppgift avses uppgift som kan förknippas med en abonnent eller användare och som behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden.

Militärunderrättelsemyndigheten får ges tillstånd till teleövervakning av en teleadress eller en teleterminalutrustning som innehas av en statlig aktör.

Militärunderrättelsemyndigheten får ges tillstånd till teleövervakning av en teleadress eller teleterminalutrustning som innehas eller annars används av någon annan än en statlig aktör, om detta kan antas vara av synnerligen stor betydelse för informationsinhämtning med tanke på ett underrättelseuppdrag.

36 §

Beslut om teleövervakning

En domstol beslutar om teleövervakning på yrkande av en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna. Om ett ärende som gäller teleövervakning inte tål uppskov, får en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna besluta om teleövervakning till dess domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

Militärunderrättelsemyndigheten får för informationsinhämtning med tanke på ett underrättelseuppdrag med en persons samtycke inrikta teleövervakning på en teleadress eller teleterminalutrustning som personen innehar.

Huvudstabens underrättelsechef eller en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna beslutar om den teleövervakning som avses i 2 mom.

Tillstånd får beviljas och beslut fattas för högst sex månader åt gången, och tillståndet eller beslutet får gälla även en viss tid före tillståndet beviljades eller beslutet fattades, vilken kan vara längre än sex månader.

I ett yrkande och i ett beslut om teleövervakning ska följande nämnas:
1) det underrättelseuppdrag som ligger till grund för åtgärden samt syftet med åtgärden,
2) den person, teleadress eller teleterminalutrustning som åtgärden riktas mot,
3) de fakta som förutsättningarna för teleövervakning och inriktningen grundar sig på,
4) tillståndets giltighetstid med angivande av klockslag,
5) den tjänsteman som leder och övervakar teleövervakningen och som är särskilt förtrogen med användningen av Försvarsmaktens underrättelsetjänsts underrättelseinhämtningsmetoder,
6) eventuella begränsningar i och villkor för teleövervakningen.

37 §

Inhämtande av basstationsuppgifter

Med inhämtande av basstationsuppgifter avses inhämtande av information om teleterminalutrustningar och teleadresser som redan är eller kommer att bli registrerade i ett telesystem via en viss basstation.

Militärunderrättelsemyndigheten kan beviljas tillstånd att inhämta basstationsuppgifter som behövs med tanke på ett underrättelseuppdrag.

38 §

Beslut om inhämtande av basstationsuppgifter

En domstol beslutar om inhämtande av basstationsuppgifter på yrkande av en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna. Om ärendet inte tål uppskov, får en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna besluta om inhämtande av basstationsuppgifter till dess domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att underrättelseinhämtningsmetoden började användas.

Tillstånd beviljas för en viss tidsperiod.

I ett yrkande och i ett beslut om inhämtande av basstationsuppgifter ska följande nämnas:
1) det underrättelseuppdrag som ligger till grund för åtgärden samt syftet med åtgärden,
2) vilken basstation tillståndet gäller,
3) de fakta som ligger till grund för förutsättningarna för och inriktningen av inhämtandet av basstationsuppgifter,
4) den tidsperiod som tillståndet gäller,
5) den tjänsteman som leder och övervakar inhämtandet av basstationsuppgifter och som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna,
6) eventuella begränsningar i och villkor för inhämtandet av basstationsuppgifter.

39 §

Inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning

För att utföra ett underrättelseuppdrag får militärunderrättelsemyndigheten med en teknisk anordning inhämta identifieringsuppgifter för teleadresser eller teleterminalutrustning.

Beslut om inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning fattas av en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna.

40 §

Täckoperation

Med *täckoperation* avses planmässigt inhämtande av information om en viss person, dennes verksamhet eller en grupp av personer genom infiltration, där falska, vilseledande eller förtäckta uppgifter eller registeranteckningar används eller falska handlingar framställs eller används för att förvärva det förtroende som behövs för inhämtandet av information eller för att förhindra att inhämtandet av information avslöjas.

Militärunderrättelsemyndigheten får inrikta täckoperation på en person eller grupp av personer, om detta är nödvändigt för att inhämta uppgifter som är nödvändiga med tanke på ett underrättelseuppdrag, och informationsinhämtningen ska anses nödvändig med tanke på planenligheten, organiseringen eller yrkesmässigheten i verksamheten eller den kontinuitet eller upprepning som kan förutses i den verksamhet som är föremål för ett underrättelseuppdrag.

En täckoperation får företas i en bostad endast om tillträdet till eller vistelsen i bostaden sker under aktiv medverkan av den som använder bostaden.

Militärunderrättelsemyndigheterna får inrikta en täckoperation på en person eller grupp av personer i ett datanät, om detta kan antas vara av ytterst stor betydelse för att få information med tanke på ett underrättelseuppdrag.

41 §

Framställning om och plan för en täckoperation

I en framställning om täckoperation ska följande nämnas:
1) den som gjort framställningen om åtgärden,
2) den person eller grupp av personer, tillräckligt specificerad, som är föremål för informationsinhämtningen,
3) det underrättelseuppdrag som ligger till grund för åtgärden,
4) syftet med täckoperationen,
5) behovet av täckoperationen,
6) övriga uppgifter som behövs för att bedöma förutsättningarna för täckoperationen.

Över genomförandet av en täckoperation ska en sådan skriftlig plan göras upp som innehåller väsentlig och tillräckligt detaljerad information för beslutsfattandet om och genomförandet av täckoperationen. Vid förändrade omständigheter ska planen vid behov ses över.

42 §

Beslut om en täckoperation

Huvudstabens underrättelsechef beslutar om en täckoperation som avses i 40 §. Beslut om en täckoperation som enbart ska genomföras i ett datanät fattas av en militärjurist eller en annan tjänsteman som är särskilt förtrogen med underrättelseinhämtningsmetoderna.

Beslut om en täckoperation får meddelas för högst sex månader åt gången.

Beslut om en täckoperation ska fattas skriftligen. I beslutet ska följande nämnas:
1) den som gjort framställningen om åtgärden,
2) den tjänsteman som ansvarar för genomförandet av täckoperationen och som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna,
3) identifikationsuppgifterna för de tjänstemän som genomför täckoperationen,
4) det underrättelseuppdrag som ligger till grund för åtgärden,
5) den person eller grupp av personer, tillräckligt specificerad, som är föremål för informationsinhämtningen,
6) de fakta som förutsättningarna för täckoperationen och inriktningen grundar sig på,

7) täckoperationens syfte och genomförandeplan,
8) beslutets giltighetstid,
9) eventuella begränsningar i och villkor för täckoperationen.

Vid förändrade omständigheter ska beslutet vid behov ses över. Beslut om avslutande av en täckoperation ska fattas skriftligen.

43 §

Användning av informationskällor

Med *användning av informationskällor* avses annat än sporadiskt konfidentiellt mottagande av information av betydelse för skötseln av underrättelseuppdrag av personer som inte hör till en finsk myndighet (informationskälla).

Militärunderrättelsemyndigheten får be en informationskälla, som har godkänts för detta ändamål, är lämplig till sina personliga egenskaper, har registrerats och har samtyckt till informationsinhämtning, inhämta sådan information som avses i 1 mom. (styrd användning av informationskälla), om det kan antas att den styrda användningen av informationskällan är av synnerligen stor betydelse för att information ska fås med tanke på underrättelseuppdraget.

Vid styrd användning av informationskällor får en informationskälla inte ombes inhämta information på ett sådant sätt som förutsätter utövande av myndighetsbefogenheter eller som äventyrar informationskällans eller någon annans liv eller hälsa. Innan styrd användning av informationskälla inleds ska informationskällan upplysas om sina rättigheter och skyldigheter och i synnerhet om vad som är tillåten och förbjuden verksamhet enligt lag. Informationskällans säkerhet ska vid behov tryggas under och efter informationsinhämtningen.

44 §

Behandling av uppgifter om en informationskälla och betalning av arvode

Uppgifter om en informationskälla får registreras i ett personregister.

Till en registrerad informationskälla får arvode betalas. Av grundad anledning får arvode betalas även till en oregistrerad informationskälla. Särskilda bestämmelser gäller om skatteplikt för arvodet.

45 §

Beslut om styrd användning av informationskällor

Huvudstabens underrättelsechef beslutar om styrd användning av en informationskälla.

Beslut om styrd användning av en informationskälla kan meddelas för högst sex månader åt gången.

Beslut om styrd användning av en informationskälla ska fattas skriftligen. I beslutet ska följande nämnas:
1) den som gjort framställningen om åtgärden,
2) den tjänsteman som ansvarar för genomförandet av underrättelseuppdraget och som är särskilt förtrogen med användningen av Försvarsmaktens underrättelsetjänsts underrättelseinhämtningsmetoder,
3) identifikationsuppgifterna för informationskällan,
4) det underrättelseuppdrag som ligger till grund för åtgärden,
5) syftet med inhämtandet av information och genomförandeplanen,
6) beslutets giltighetstid,
7) eventuella begränsningar i och villkor för den styrda användningen av en informationskälla och skyddandet av den.

Vid förändrade omständigheter ska beslutet vid behov ses över. Beslut om att styrd användning av en informationskälla ska avslutas ska fattas skriftligen.

46 §

Tryggande av informationskälla

Militärunderrättelsemyndigheten kan med en informationskällas samtycke övervaka dennes bostad eller annan lokal som informationskällan använder för boende och dess omedelbara närmiljö med kamera eller en annan teknisk anordning, metod eller programvara som installerats på platsen, om det är nödvändigt för att avvärja en fara som hotar informationskällans liv eller hälsa. Utomstående behöver inte upplysas om att informationskällan tryggas.

En förutsättning för tryggandet av en informationskälla är dessutom att det har bedömts att informationskällan till sina personliga egenskaper är lämplig för detta.

Övervakningen ska avslutas utan dröjsmål, om den inte längre är nödvändig för att avvärja en fara som hotar informationskällans liv eller hälsa.

Upptagningar som samlats in enligt 1 mom. ska utplånas så snart de inte behövs för att trygga informationskällans säkerhet. Om upptagningarna trots allt behöver bevaras av orsaker som har samband med rättsskyddet för någon som har del i saken, får upptagningarna bevaras och användas i detta syfte. De ska i så fall utplånas när saken har avgjorts genom ett lagakraftvunnet beslut eller avskrivits.

47 §

Bevisprovokation genom köp

Med *bevisprovokation* genom köp avses ett köpeanbud eller köp av ett föremål, ett ämne, egendom eller en tjänst som militärunderrättelsemyndigheterna gör i syfte att ta om hand eller påträffa ett föremål, ett ämne eller egendom som har samband med ett underrättelseuppdrag.

Militärunderrättelsemyndigheten får utföra bevisprovokation genom köp, om det är nödvändigt för att få information med tanke på ett underrättelseuppdrag.

Den som genomför bevisprovokation genom köp får utföra bara sådan informationsinhämtning som är nödvändig för genomförandet av bevisprovokationen. Bevisprovokation genom köp ska genomföras så att den inte får den person som är föremål för åtgärden eller någon annan att begå ett brott som denne inte annars skulle begå.

Bevisprovokation genom köp är tillåten i en bostad bara om tillträdet till eller vistelsen i bostaden sker under aktiv medverkan av den som använder bostaden.

48 §

Beslut om bevisprovokation genom köp

Huvudstabens underrättelsechef beslutar om bevisprovokation genom köp. Beslut om bevisprovokation genom köp som gäller säljanbud uteslutande till allmänheten får fattas också av en till uppdraget förordnad militärjurist eller annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna.

Beslut om bevisprovokation genom köp får meddelas för högst sex månader åt gången.

Beslut om bevisprovokation genom köp ska fattas skriftligen. I beslutet ska följande nämnas:

1) det underrättelseuppdrag som ligger till grund för åtgärden,
2) den person som är föremål för bevisprovokationen,
3) de fakta som förutsättningarna för bevisprovokation genom köp och inriktningen grundar sig på,
4) de föremål, de ämnen, den egendom eller de tjänster som är föremål för bevisprovokationen,
5) syftet med bevisprovokationen,

6) beslutets giltighetstid,
7) den tjänsteman som leder och övervakar bevisprovokation genom köp och som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna,
8) eventuella begränsningar i och villkor för bevisprovokationen.

49 §

Plan för genomförande av bevisprovokation genom köp

Över genomförandet av bevisprovokation genom köp ska det upprättas en skriftlig plan, om detta behövs med hänsyn till operationens omfattning eller andra motsvarande skäl.

Vid förändrade omständigheter ska planen för genomförande av bevisprovokationen vid behov ses över.

50 §

Beslut om genomförande av bevisprovokation genom köp

Beslut om genomförande av bevisprovokation genom köp ska fattas skriftligen. Beslutet fattas av den tjänsteman som ansvarar för genomförandet av bevisprovokation genom köp och som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna,

I beslutet ska följande nämnas:
1) den militärjurist eller en annan tjänsteman som fattade beslut om bevisprovokation genom köp och som är särskilt förtrogen med användningen av militärunderrättelsemyndighetens underrättelseinhämtningsmetod samt datum då beslutet meddelades och dess innehåll,
2) identifikationsuppgifter på de tjänstemän vid militärunderrättelsemyndigheten vilka utför bevisprovokation genom köp,
3) en utredning av hur det har säkerställts att bevisprovokationen inte får den som är föremål för åtgärden eller någon annan att begå ett brott som denne annars inte skulle begå,
4) eventuella begränsningar i och villkor för bevisprovokationen.

Om åtgärden inte tål uppskov, behöver ett beslut som avses i 2 mom. inte upprättas i skriftlig form före bevisprovokationen. Beslutet ska dock upprättas i skriftlig form utan dröjsmål efter bevisprovokationen.

Vid förändrade omständigheter ska beslutet om genomförande av bevisprovokationen vid behov ses över.

51 §

Platsspecifik underrättelseinhämtning

Med *platsspecifik underrättelseinhämtning* avses underrättelseinhämtning som görs på en viss plats för att ett föremål, egendom, dokument, information eller en omständighet ska hittas.

Platsspecifik underrättelseinhämtning får inte genomföras på en plats där det finns anledning att anta att underrättelseinhämtningen kommer att omfatta information som de som avses i 17 kap. 23 § 1 mom. i rättegångsbalken inte får vittna om i rättegång eller som de som avses i 24 § 2 eller 3 mom. i nämnda kapitel får vägra röja. Platsspecifik underrättelseinhämtning får dock genomföras, om det finns anledning att anta att underrättelseinhämtningen kommer att omfatta information som en person kan åläggas att vittna om med stöd av 17 kap. 23 § 3 mom. i rättegångsbalken eller svara på frågor om med stöd av 17 kap. 24 § 4 mom. i rättegångsbalken.

Militärunderrättelsemyndigheten får beviljas tillstånd till platsspecifik underrättelseinhämtning utanför ett utrymme som används för stadigvarande boende, om detta kan antas vara av ytterst stor betydelse för att få information med tanke på ett underrättelseuppdrag.

52 §

Beslut om platsspecifik underrättelseinhämtning

En domstol beslutar om platsspecifik underrättelseinhämtning, om den riktas mot en plats, som man inte har allmänt tillträde till eller om det allmänna tillträdet till den har begränsats eller förhindrats under den tidpunkt då platsspecifik underrättelseinhämtning genomförs, på yrkande av en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna.

Om ett ärende som avses i 1 mom. inte tål uppskov, får huvudstabens underrättelsechef eller en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna besluta om platsspecifik underrättelseinhämtning till dess domstolen har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att metoden började användas.

Huvudstabens underrättelsechef eller en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna beslutar om annan platsspecifik underrättelseinhämtning än den som avses i 1 mom.

Tillstånd kan ges och beslut fattas för högst en månad åt gången.

I det yrkande eller beslut som gäller platsspecifik underrättelseinhämtning ska tillräckligt noggrant specificeras:

1) det underrättelseuppdrag som ligger till grund för åtgärden,
2) den plats som är föremål för den platsspecifika underrättelseinhämtningen,
3) de fakta på grundval av vilka förutsättningar för platsspecifik underrättelseinhämtning anses föreligga,
4) såvitt möjligt vad man försöker hitta genom den platsspecifika underrättelseinhämtningen,
5) eventuella begränsningar i den platsspecifika underrättelseinhämtningen.

När ärendets brådskande natur förutsätter det, får ett beslut om platsspecifik underrättelseinhämtning registreras efter att den platsspecifika underrättelseinhämtningen har genomförts.

Vid platsspecifik underrättelseinhämtning får inte sådan information som avses i 8 kap. 1 § 3 mom. i tvångsmedelslagen (806/2011) inhämtas. Om det vid platsspecifik underrättelseinhämtning visar sig att underrättelseinhämtningen har inriktats på sådan information, ska underrättelseinhämtningen till denna del avslutas genast och de anteckningar och kopior som gäller informationen genast förstöras.

53 §

Kopiering

Militärunderrättelsemyndigheten har för inhämtning av uppgifter med tanke på ett underrättelseuppdrag rätt att kopiera ett dokument eller ett annat föremål genom användning av en teknisk anordning.

54 §

Kopieringsförbud

Handlingar eller andra objekt som avses i 53 § får inte kopieras, om de innehåller sådant som en person med stöd av 17 kap. 10—14, 16, 20 eller 21 § i rättegångsbalken inte får vittna om eller har rätt att vägra vittna om.

Om tystnadsplikten eller tystnadsrätten grundar sig på 17 kap. 11 § 2 eller 3 mom. eller 13, 14, 16 eller 20 § i rättegångsbalken, är en förutsättning för förbudet utöver det som föreskrivs i 1 mom. dessutom att objektet innehas av en person som avses i bestämmelsen i fråga eller av någon som

står i ett sådant förhållande till honom eller henne som avses i 22 § 2 mom. i det kapitlet, eller av den till vars förmån tystnadsplikten eller tystnadsrätten har föreskrivits.

Kopieringsförbud gäller dock inte, om

1) den som avses i 17 kap. 11 § 2 eller 3 mom., 12 § 1 eller 2 mom., 13 § 1 eller 3 mom., 14 § 1 mom. eller 16 § 1 mom. i rättegångsbalken och till vars förmån tystnadsplikten har föreskrivits samtycker till kopiering,

2) en person som avses i 17 kap. 20 § 1 mom. i rättegångsbalken samtycker till kopiering.

55 §

Kopieringsförbud som anknyter till teleavlyssning, teleövervakning och basstationsuppgifter

Handlingar eller data som innehas av ett teleföretag eller en sammanslutningsabonnent och som innehåller information som anknyter till ett meddelande som avses i 4 kap. 32 § 1 mom. i denna lag eller identifieringsuppgifter som avses i 35 § 1 mom. i nämnda kapitel eller basstationsuppgifter som avses i 37 § 1 mom. får inte kopieras.

56 §

Kopiering av en försändelse

Ett brev eller en annan motsvarande försändelse får kopieras innan den anländer till mottagaren, om kopieringen av försändelsen kan antas vara av synnerligen stor betydelse för att få information med tanke på ett underrättelseuppdrag.

57 §

Kvarhållande av en försändelse för kopiering

Om det finns orsak att anta att ett brev eller en annan motsvarande försändelse, som får kopieras, är på väg till ett postkontor, en järnvägstrafikplats eller till ett verksamhetsställe där yrkesmässig transport av försändelser bedrivs, eller redan finns där, får en militärjurist eller en annan tjänsteman som förordnats till uppdraget och som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna besluta att försändelsen ska hållas kvar på postkontoret, trafikplatsen eller verksamhetsstället, tills man har hunnit kopiera den.

Beslutet som avses i 1 mom. fattas för en tid av högst en månad, som börjar när chefen för postkontoret, trafikplatsen eller verksamhetsstället har fått kännedom om beslutet. En försändelse får inte utan tillstånd av den tjänsteman som avses i 1 mom. överlåtas till någon annan än tjänstemannen eller en person som han eller hon har bestämt.

Chefen för postkontoret, trafikplatsen eller verksamhetsstället ska genast meddela den som har fattat beslutet när försändelsen har anlänt. Denne ska utan ogrundat dröjsmål besluta om kopiering.

58 §

Beslut om kopiering

En militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna beslutar om kopiering.

Om ett ärende inte tål uppskov, får också någon annan än en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna i ett enskilt fall besluta om kopiering, tills den tjänsteman som avses i 1 mom. har avgjort saken. Ärendet

ska ges till den militärjurist eller tjänsteman som avses i 1 mom. för avgörande genast när det är möjligt, dock senast 24 timmar efter det att informationsinhämtningsmetoden började användas.

59 §

Registrering av kopieringen och förstöring av kopian

Över kopieringen av en handling eller ett annat objekt ska utan ogrundat dröjsmål upprättas ett protokoll. I det ska tillräckligt noggrant nämnas syftet med kopieringen, redogöras för det förfarande som lett till kopieringen samt specificeras föremålet för kopieringen.

En kopia som visat sig onödig ska genast förstöras.

60 §

Radiosignalspaning

Med *radiosignalspaning* avses informationsinhämtning som riktas mot elmagnetiska vågor på radiofrekvenser (radiovågor).

Försvarsmaktens underrättelsetjänst eller försvarsgrenar kan rikta radiosignalspaning mot radiovågor som sänds från en anordning utanför finskt territorium eller som anländer till en sådan anordning.

Radiosignalspaning får inte riktas mot förtrolig kommunikation mellan personer.

61 §

Beslut om radiosignalspaning

Huvudstabens underrättelsechef beslutar om radiosignalspaning.

62 §

Underrättelseinhämtning som avser utländska datasystem

Med *underrättelseinhämtning* som avser utländska datasystem avses inhämtning av information med datatekniska metoder från ett datasystem utanför Finland.

Försvarsmaktens underrättelsetjänst får inrikta underrättelseinhämtning som avser utländska datasystem på ett datasystem, om detta kan antas vara av synnerligen stor betydelse för inhämtning av information med tanke på ett underrättelseuppdrag.

Underrättelseinhämtning som avser utländska datasystem får inte riktas mot förtrolig kommunikation mellan personer.

63 §

Beslut om underrättelseinhämtning som avser utländska datasystem

Huvudstabens underrättelsechef beslutar om underrättelseinhämtning som avser utländska datasystem.

Militärunderrättelsemyndigheten ska hålla försvarsministeriet informerat om pågående underrättelseinhämtning som avser utländska datasystem.

64 §

Beslut om militär underrättelseverksamhet utomlands

Beslut om militär underrättelseverksamhet och användning av underrättelseinhämtningsmetoder någon annanstans än i Finland fattas av huvudstabens underrättelsechef.

Beslutet ska fattas skriftligen. I fråga om innehållet i beslut, framställning och plan som gäller användning av en underrättelseinhämtningsmetod iakttas vad i denna lag föreskrivs om framställning, plan, yrkande eller beslut.

Utöver vad som föreskrivs om förbud som gäller ett utrymme som används för stadigvarande boende, tillämpas bestämmelserna i 55, 76, 77, 85, 86, 126 och 127 § i denna lag inte på den militära underrättelseverksamhet och den användning av underrättelseinhämtningsmetod som avses i 1 mom.

5 kap.

Informationsinhämtning som avser datatrafik

65 §

Tillämpningsområde

I detta kapitel föreskrivs om teknisk informationsinhämtning som riktas mot datatrafik i ett kommunikationsnät som överskrider Finlands gräns, vilken baserar sig på automatiserad avskiljning av datatrafik samt om behandling av den inhämtade informationen (underrättelsesinhämtning som avser datatrafik).

66 §

Behandling av tekniska data

För inriktning av underrättelseinhämtning som avser datatrafik får Försvarsmaktens underrättelsetjänst i datatrafiken i ett kommunikationsnät kortvarigt samla in och lagra tekniska data om datatrafiken och med hjälp av automatisk databehandling behandla dem för statistisk analys.

I resultatet av den statistiska analysen får inte ingå sådan information genom vilken en enskild fysisk person kan identifieras.

Försvarsmaktens underrättelsetjänst ska förstöra insamlade och lagrade tekniska data om datatrafiken omedelbart efter att resultatet av den statistiska analysen har blivit klart.

67 §

Beslut om behandling av tekniska data

En domstol beslutar om behandlingen av tekniska data på yrkande av en militärjurist eller en annan tjänsteman vid Försvarsmaktens underrättelsetjänst, vilken är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna.

Tillstånd får beviljas för högst tre månader åt gången.

Av det yrkande och beslut som gäller behandlingen av tekniska data ska följande framgå:

1) det geografiska område i fråga om vilket tekniska data i inkommande eller utgående datatrafik ska behandlas,

2) de delar av kommunikationsnätet där data söks,

3) den tjänsteman som leder och övervakar behandlingen av tekniska data och som är särskilt förtrogen med användningen av Försvarsmaktens underrättelsetjänsts underrättelseinhämtningsmetoder,
4) en plan för hur behandlingen av tekniska data ska genomföras.

68 §

Underrättelseinhämtning som avser en statlig aktörs datatrafik

Försvarsmaktens underrättelsetjänst kan med hjälp av automatisk databehandling i den datatrafik i kommunikationsnät som överskrider Finlands gräns inhämta en med tanke på underrättelseuppdraget väsentlig statlig aktörs datatrafik samt behandla den statliga aktörens kommunikation. Inhämtningen av information i datatrafiken grundar sig på användningen av sökbegrepp.

Försvarsmaktens underrättelsetjänst får behandla den information som inhämtats i datatrafiken automatiskt och manuellt.

Som sökbegrepp får inte användas uppgifter som specificerar terminalutrustning eller teleadress som en person, som vistas i Finland, innehar eller som denne annars förmodligen använder.

69 §

Beslut om underrättelseinhämtning som avser en statlig aktörs datatrafik

En domstol beslutar om underrättelseinhämtning som avser en statlig aktörs datatrafik på yrkande av huvudstabens underrättelsechef. Om ärendet inte tål uppskov, får huvudstabens underrättelsechef besluta om underrättelseinhämtning som avser en statlig aktörs datatrafik till dess domstolen har avgjort yrkandet om beviljande av tillstånd. Beslutet ska upprättas skriftligen. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att underrättelseinhämtning som avser datatrafik började användas.

Tillstånd får beviljas för högst sex månader åt gången.

I ett yrkande och beslut som gäller underrättelseinhämtning som avser en statlig aktörs datatrafik ska framgå:
1) det underrättelseuppdrag för vilket datatrafik inhämtas,
2) de sökbegrepp eller kategorier av sökbegrepp som ska användas i verksamheten och motiveringarna till dem,
3) den del av kommunikationsnätet som underrättelseinhämtningen inriktas på samt motiveringarna till inriktningen,
4) tillståndets giltighetstid med angivande av klockslag,
5) den tjänsteman som leder och övervakar underrättelseinhämtningen som avser datatrafik och som är särskilt förtrogen med användningen av Försvarsmaktens underrättelsetjänsts underrättelseinhämtningsmetoder,
6) eventuella begränsningar i och villkor för underrättelseinhämtning som avser en statlig aktörs datatrafik.

70 §

Underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer

Försvarsmaktens underrättelsetjänst får med hjälp av automatisk databehandling i den datatrafik i kommunikationsnät som överskrider Finlands gräns inhämta information om datatrafiken hos andra än statliga aktörer, vilken är väsentlig med tanke på underrättelseuppdraget, om den underrättelseinhämtning som riktas mot datatrafiken hos andra än statliga aktörer kan antas vara nödvändig för erhållande av information med tanke på ett underrättelseuppdrag. Inhämtningen av information i datatrafiken grundar sig på användningen av sökbegrepp.

Som sökbegrepp får inte användas uppgifter som specificerar terminalutrustning eller teleadress som en person, som vistas i Finland, innehar eller som denne annars förmodligen använder.

Underrättelseinhämtningen i datatrafik från andra än statliga aktörer får inte inriktas utgående från ett meddelandes innehåll, om det inte vid inriktningen används information som beskriver innehållet i ett sabotageprogram.

Försvarsmaktens underrättelsetjänst får behandla den information som inhämtats i datatrafiken automatiskt och manuellt.

71 §

Beslut om underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer

En domstol beslutar om underrättelseinhämtning som avser datatrafik hos andra än statliga aktörer på yrkande av huvudstabens underrättelsechef. Om ärendet inte tål uppskov, får huvudstabens underrättelsechef besluta om inledande av underrättelseinhämtning som avser datatrafiken hos andra än statliga aktörer till dess domstolen har avgjort yrkandet om beviljande av tillstånd. Beslutet ska upprättas skriftligen. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att underrättelseinhämtning som avser datatrafik började användas.

Tillstånd får beviljas för högst sex månader åt gången.

I ett yrkande och beslut som gäller underrättelseinhämtning som avser datatrafiken hos andra än statliga aktörer ska framgå:

1) det underrättelseuppdrag för vilket datatrafik inhämtas,
2) fakta som gäller föremålet för underrättelseinhämtningen,
3) de fakta som ligger till grund för förutsättningarna för underrättelseinhämtning som avser datatrafik,
4) de sökbegrepp eller kategorier av sökbegrepp som ska användas i underrättelseinhämtningen och motiveringarna till dem,
5) den del av kommunikationsnätet som underrättelseinhämtningen inriktas på samt motiveringarna till inriktningen,
6) tillståndets giltighetstid med angivande av klockslag,
7) den tjänsteman vid militärunderrättelsemyndigheten som övervakar och leder insamlingen och lagringen av kommunikationen,
8) eventuella begränsningar i och villkor för underrättelseinhämtning som avser datatrafik.

72 §

Genomförande av den koppling som underrättelseinhämtning som avser datatrafik förutsätter

Den som utför kopplingen i underrättelseinhämtning som avser datatrafik verkställer de tillstånd som avses i detta kapitel och styr datatrafiken i den kommunikationsnätsdel som avses i tillståndet till Försvarsmaktens underrättelsetjänst.

Den som utför kopplingen överlåter vidare till Försvarsmaktens underrättelsetjänst datakommunikationen i den kommunikationsnätsdel som stämmer överens med den anslutning som avses i tillståndet.

73 §

Tekniskt genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning

Med tekniskt genomförande av underrättelseinhämtning som avser datatrafik för skyddspolisens räkning avses:

1) statistisk analys av tekniska data utgående från ett uppdrag som skyddspolisen har gett Försvarsmaktens underrättelsetjänst och sändande av analysen till skyddspolisen, samt
2) inhämtande av datatrafik i en kommunikationsnätsdel som överskrider Finlands gräns i enlighet med det tillstånd som en domstol har beviljat skyddspolisen med hjälp av automatiserad databehandling och överlåtelse av de inhämtade uppgifterna vidare till skyddspolisen.

Bestämmelser om det tekniska genomförandet av underrättelseinhämtning som avser datatrafiken för skyddspolisens räkning finns i 10 § i lagen om civil underrättelseinhämtning avseende datatrafik.

Försvarsmaktens underrättelsetjänst får inte för skyddspolisens räkning ta reda på ett meddelandes innehåll i samband med det tekniska genomförandet av underrättelseinhämtning som avser datatrafik.

74 §

Utplåning av uppgifter

De uppgifter som har inhämtats med hjälp av underrättelseinhämtning som avser datatrafik ska utan dröjsmål utplånas, om
1) det visar sig att båda parterna i förtrolig kommunikation befann sig i Finland när kommunikationen försiggick,
2) avsändaren eller mottagaren har skyldighet eller rätt att vägra vittna om uppgifterna i fråga med stöd av 17 kap. 13, 14, 16 eller 20 § i rättegångsbalken.

75 §

Utlämnande av uppgifter om ett skadligt datorprogram till företag och sammanslutningar

Trots sekretessbestämmelserna får militärunderrättelsemyndigheterna lämna ut uppgifter om ett skadligt datorprogram och dess verksamhet, vilka inhämtats med hjälp av underrättelseinhämtning som avser datatrafik, till ett företag, en sammanslutning eller en myndighet, om överlåtelse av uppgifterna behövs för att trygga försvaret av landet, skydda den nationella säkerheten eller trygga företagets eller sammanslutningens intressen.

6 kap.

Anmälan om underrättelseuppgifter i vissa situationer

76 §

Anmälan om brottsmisstanke

Militärunderrättelsemyndigheterna ska utan ogrundat dröjsmål till den behöriga förundersökningsmyndigheten anmäla de uppgifter som behövs för att en förundersökning ska kunna inledas, om det medan en metod för underrättelseinhämtning används framkommer att det finns skäl att misstänka ett brott enligt 15 kap. 10 § i strafflagen.

Militärunderrättelsemyndigheten får anmäla ett misstänkt brott till förundersökningsmyndigheten, om det strängaste straffet som har föreskrivits för brottet är fängelse i minst tre år och anmälan kan antas ha synnerligen stor betydelse för utredningen av brottet.

En militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna beslutar om den anmälan som avses i denna paragraf.

77 §

Anmälan i vissa fall

Militärunderrättelsemyndigheten ska utan ogrundat dröjsmål till brottsbekämpningsmyndigheten anmäla, om det medan en underrättelseinhämtningsmetod används framkommer ett brott som avses i 15 kap. 10 § i strafflagen och som ännu kan förhindras.

Militärunderrättelsemyndigheten får för brottsbekämpningsmyndigheten röja en uppgift som inhämtats när en underrättelseinhämtningsmetod användes för att förhindra ett sådant brott för vilket det föreskrivna strängaste straffet är fängelse i minst två år.

Information som inhämtats genom användning av en underrättelseinhämtningsmetod får alltid röjas som en utredning som stöder att någon är oskyldig samt för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada.

Huvudstabens underrättelsechef beslutar om att göra en sådan anmälan som avses i denna paragraf.

78 §

Anmälan om att förundersökning eller brottsbekämpning inleds

Om en förundersökningsmyndighet utgående från en anmälan som avses i detta kapitel inleder en förundersökning eller vidtar en förundersökningsåtgärd eller om en brottsbekämpande myndighet inleder en åtgärd som syftar till att förhindra ett brott, ska förundersökningsmyndigheten eller den brottsbekämpande myndigheten i tillräckligt god tid innan förundersökning inleds, förundersökningsåtgärden vidtas eller den brottsbekämpande åtgärden vidtas till militärunderrättelsemyndigheten anmäla detta.

79 §

Anmälan om domstolens tillstånd

Militärunderrättelsemyndigheten ska informera tillsynsmyndigheten för underrättelseinhämtning om de tillstånd som domstolen har beviljat med stöd av 4 och 5 kap. i denna lag så snart som möjligt efter domstolens beslut.

7 kap.

Skyddande och tryggande av militär underrättelseverksamhet, utplåning av uppgifter samt anmälan om underrättelseinhämtning

80 §

Skyddande av militär underrättelseverksamhet

Militärunderrättelsemyndigheten får använda falska, vilseledande eller förtäckta uppgifter, göra och använda falska, vilseledande eller förtäckta registeranteckningar samt upprätta och använda falska handlingar, när det är nödvändigt för att förhindra att den militära underrättelseverksamheten avslöjas.

En registeranteckning som avses i 1 mom. ska rättas när förutsättningarna enligt det momentet inte längre finns.

81 §

Beslut om skyddande av militär underrättelseverksamhet

Beslut om registeranteckningar och upprättande av handlingar enligt 80 § ska fattas av huvudstabens underrättelsechef.

En militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna beslutar om annat skyddande än det som avses i 1 mom.

Den myndighet som har fattat beslut om registeranteckningar och upprättande av handlingar ska föra en förteckning över anteckningarna och handlingarna, övervaka användningen av dem samt se till att anteckningarna rättas.

82 §

Tryggande av en tjänsteman som använder en underrättelseinhämtningsmetod

En militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna får besluta att en tjänsteman som ska genomföra förtäckt inhämtande av information, en täckoperation eller bevisprovokation genom köp ska förses med en teknisk anordning som möjliggör avlyssning och observation, om utrustningen är motiverad för att tjänstemannens säkerhet ska kunna tryggas.

Avlyssningen och observationen får upptas. Upptagningarna ska utplånas så snart de inte behövs för att trygga tjänstemannens säkerhet. Om upptagningarna trots allt behöver bevaras av orsaker som har samband med rättsskyddet för någon som har del i saken, får upptagningarna bevaras och användas i detta syfte. De ska i så fall utplånas när saken har avgjorts genom ett lagakraftvunnet beslut eller avskrivits.

83 §

Utplåning av underrättelseuppgifter

En uppgift som inhämtats med stöd av denna lag ska utplånas utan dröjsmål efter att det framgått att den inte behövs eller inte får användas för att sköta uppdrag inom den militära underrättelseverksamheten.

84 §

Användning av en uppgift som inte ansluter sig till ett underrättelseuppdrag

En uppgift som inte ansluter sig till ett underrättelseuppdrag får användas vid utförandet av ett pågående eller kommande underrättelseuppdrag, om uppgiften hade fått inhämtas med samma underrättelseinhämtningsmetod som den uppgift som inte ansluter sig till ett underrättelseuppdrag inhämtades med. Beslut om användning av en uppgift som inte ansluter sig till ett underrättelseuppdrag ska fattas av domstolen, om den är behörig att fatta beslut om den informationsinhämtningsmetod med vilken uppgiften har fåtts.

Bestämmelser om anmälan om militära underrättelseuppgifter i vissa situationer finns i 6 kap.

85 §

Avslutande av användningen av en underrättelseinhämtningsmetod i en brådskande situation och utplåning av en uppgift som inhämtats med den

Om huvudstabens underrättelsechef eller en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna i en brådskande situation enligt 24, 26, 28, 30, 36, 38, 52, 58, 69, eller 71 § har beslutat att inhämtande av basstationsuppgifter, teknisk spårning av en person, teknisk avlyssning, optisk observation eller teknisk observation av utrustning, underrättelseinhämtning i datatrafiken hos en statlig aktör eller underrättelseinhämtning i datatrafiken hos någon annan än en statlig aktör ska inledas, men domstolen anser att det inte har funnits förutsättningar för åtgärden, ska användningen av underrättelseinhämtningsmetoden avslutas och det material som fåtts på detta sätt och anteckningarna om de uppgifter som fåtts på detta sätt genast utplånas.

86 §

Meddelande om underrättelseinhämtning

Den som varit föremål för teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, systematisk observation, förtäckt inhämtande av information och optisk observation ska utan dröjsmål meddelas om detta skriftligen efter det att syftet med informationsinhämtningen har nåtts, om föremålet för åtgärden är en person.

Underrättelseinhämtning som avser datatrafiken hos någon annan än en statlig aktör ska meddelas skriftligen till den person som varit föremål för underrättelseinhämtningen efter det att syftet med inhämtningen har nåtts och om innehållet i ett förtroligt meddelande från en viss person som befinner sig i Finland har retts ut vid behandlingen. Skyldighet att meddela föreligger emellertid inte, om den information som inhämtats med underrättelseinhämtning som avser datatrafik har utplånats med stöd av 74 §.

Den domstol som beviljat tillståndet ska samtidigt skriftligen informeras om meddelandet till föremålet.

På yrkande av huvudstabens underrättelsechef eller en militärjurist eller annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna får domstolen besluta att meddelande enligt 1 eller 2 mom. till den som varit föremål för en åtgärd får skjutas upp med högst två år åt gången, om det är motiverat för att trygga pågående informationsinhämtning, skydda landets försvar eller den nationella säkerheten eller skydda liv eller hälsa. Domstolen får besluta att inget meddelande ska ges, om det är nödvändigt för att trygga det militära försvaret eller den nationella säkerheten eller skydda liv eller hälsa.

Om den som är föremål för underrättelseinhämtningen inte är identifierad vid utgången av den föreskrivna tid eller det uppskov som avses i 1, 2 eller 4 mom., ska han eller hon utan ogrundat dröjsmål skriftligen meddelas om underrättelseinhämtningen när identiteten har utretts.

Den som varit föremål för en underrättelseinhämtningsmetod behöver inte meddelas om en täckoperation, bevisprovokation genom köp, styrd användning av informationskällor eller platsspecifik underrättelseinhämtning, om förundersökning inte har inletts i ärendet. Om förundersökning inleds, ska bestämmelserna i 10 kap. 60 § i tvångsmedelslagen iakttas.

I fråga om handläggning i domstol av ett ärende som gäller meddelande ska 134 § iakttas.

8 kap.

Deltagande av en annan tjänsteman vid Försvarsmakten och av värnpliktiga i militär underrättelseverksamhet samt internationell verksamhet

87 §

Deltagande av en annan tjänsteman vid Försvarsmakten i militär underrättelseverksamhet

En tjänsteman vid Försvarsmakten som har fått tillräcklig utbildning i användningen av underrättelseinhämtningsmetoderna får under styrning och övervakning av militärunderrättelsemyndigheten använda de underrättelseinhämtningsmetoder som avses i 4 kap. för att inhämta information för ett underrättelseuppdrag. Dessa tjänstemän är underställda den militärunderrättelsemyndighet som utför ett underrättelseuppdrag.

88 §

Befogenheter för en reservist som tjänstgör i enlighet med värnpliktslagen

En reservist som deltar i en repetitionsövning i enlighet med värnpliktslagen och som har fått tillräcklig utbildning får bistå militärunderrättelsemyndigheten i radiosignalspaning, underrättelseinhämtning som avser utländska datasystem, behandlingen av tekniska data och vid inriktningen av underrättelseinhämtning som avser datatrafik.

En reservist som deltar i en repetitionsövning i enlighet med 32 § 3 mom. i värnpliktslagen, i extra tjänstgöring i enlighet med 82 § eller som har förordnats till tjänstgöring under mobilisering i enlighet med 86 § i samma lag och som har fått tillräcklig utbildning får utöver det som föreskrivs i 1 mom. också använda systematisk observation, teknisk avlyssning, optisk observation, teknisk spårning och teknisk observation av utrustning samt underrättelseinhämtning som avser utländska datasystem för att utföra ett underrättelseuppdrag.

En reservist som i enlighet med 47 § i lagen om försvarsmakten har tagit avsked från militärunderrättelsemyndigheten och deltar i en repetitionsövning enligt värnpliktslagen får använda befogenheterna i 4 kap.

Reservisten får använda de befogenheter som avses i denna paragraf endast under styrning och övervakning av en tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna.

89 §

En reservists deltagande i internationell verksamhet

Någon som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna, som har tagit avsked från militärunderrättelsemyndigheten i enlighet med 47 § i lagen om försvarsmakten, som deltar i givandet av internationellt bistånd och annan internationell verksamhet och har tagits i ett anställningsförhållande till Försvarsmakten eller står i ett tjänstgöringsförhållande enligt lagen om militär krishantering, beslutar om användningen av de underrättelseinhämtningsmetoder om vilka föreskrivs i 4 kap. när Försvarsmakten ger internationellt bistånd och i annan internationell verksamhet samt vid en militär krishanteringsoperation.

En reservist som har fått tillräcklig utbildning i användningen av underrättelseinhämtningsmetoderna och som har tagits i ett anställningsförhållande till Försvarsmakten får använda de underrättelseinhämtningsmetoder om vilka föreskrivs i 4 kap. under styrning och övervakning av en tjänsteman som är särskilt förtrogen med användningen av underrättelsemetoderna eller en reservist som avses i 1 mom.

Huvudstabens underrättelsechef fattar beslut om en i denna paragraf avsedd persons medverkan i givandet av internationellt bistånd eller i militär krishantering samt om de underrättelseinhämtningsmetoder som ska användas i den internationella verksamheten.

90 §

Tjänsteansvar för den som tjänstgör i enlighet med värnpliktslagen

På den som tjänstgör i enlighet med värnpliktslagen och använder sådan befogenhet som avses i 88 § tillämpas de bestämmelser som gäller straffrättsligt tjänsteansvar.

91 §

Skadeståndsansvar för den som tjänstgör i enlighet med värnpliktslagen

För en skada som en reservist i tjänstgöring i enlighet med värnpliktslagen har orsakat svarar staten i enlighet med vad som föreskrivs i skadeståndslagen (412/1974).

På skadeståndsansvaret för en reservist i tjänstgöring i enlighet med värnpliktslagen tillämpas bestämmelserna om en värnpliktigs skadeståndsansvar i 4 kap. i skadeståndslagen.

9 kap.

Yppandeförbud, skyldigheter och rättigheter som gäller teleföretag och dataöverförare samt erhållande av information från vissa parter

92 §

Yppandeförbud

En utomstående eller en som tjänstgör i enlighet med värnpliktslagen och som har bistått vid utförandet av ett underrättelseuppdrag får inte yppa en uppgift eller omständighet som kommit till dennes kännedom om underrättelseuppdraget.

Till straff för överträdelse av yppandeförbudet döms enligt 38 kap. 1 eller 2 § i strafflagen, om inte strängare straff för gärningen föreskrivs någon annanstans i lag.

93 §

Teleföretags biståndsskyldighet

Ett teleföretag ska utan ogrundat dröjsmål göra de kopplingar i ett telenät som behövs för teleavlyssning och teleövervakning samt tillhandahålla militärunderrättelsemyndigheten de uppgifter och den utrustning samt den personal som behövs för utförande av teleavlyssningen. Detsamma gäller de situationer där militärunderrättelsemyndigheten genomför teleavlyssning eller teleövervakning med hjälp av tekniska anordningar.

94 §

Dataöverförares biståndsskyldighet

Dataöverföraren är skyldig att medverka till att den accesspunkt som underrättelseinhämtning som avser datatrafik kräver kan realiseras genom att ge Försvarsmaktens underrättelsetjänst de uppgifter som är nödvändiga för detta syfte och tillträde till de utrymmen där man har för avsikt att genomföra accesspunkten. Försvarsmaktens underrättelsetjänst ska genomföra accesspunkten så

att detta orsakar så liten olägenhet som möjligt för dataöverföraren. Dataöverföraren har rätt att delta i åtgärderna som syftar till att genomföra accesspunkten.

Om en accesspunkt som avses i 1 mom. inte kan realiseras genom medverkan av dataöverföraren, har Försvarsmaktens underrättelsetjänst rätt att realisera accesspunkten till den kommunikationsnätsdel som administreras av dataöverföraren. Såvitt möjligt ska dataöverföraren vara på plats när den accesspunkt som förutsätts för underrättelseinhämtning realiseras.

Dataöverföraren ska utan oskäligt dröjsmål på en specificerad begäran av Försvarsmaktens underrättelsetjänst ge den de uppgifter överföraren har, vilka är nödvändiga för att kommunikationsnätsdelen ska kunna specificeras för det tillståndsyrkande och tillståndsbeslut som avses i 5 kap. och som ska ställas till domstolen.

95 §

Ersättning till teleföretag

Ett teleföretag har rätt att få ersättning av statens medel för direkta kostnader som orsakats av att företaget i enlighet med denna lag har bistått militärunderrättelsemyndigheten och lämnat uppgifter, så som föreskrivs i 299 § i informationssamhällsbalken. Den militärunderrättelsemyndighet som vidtagit åtgärden beslutar om utbetalning av ersättningen.

96 §

Ersättning till dataöverföraren

En dataöverförare har rätt att få ersättning av statens medel för direkta kostnader som orsakats av att överföraren i enlighet med denna lag har bistått militärunderrättelsemyndigheten och lämnat uppgifter. Försvarsmaktens underrättelsetjänst beslutar om utbetalning av ersättningen.

97 §

Ansökan om ändring i ett ersättningsbeslut

Omprövning av ett beslut om ersättning till ett teleföretag eller en dataöverförare får begäras på det sätt som föreskrivs i förvaltningslagen (434/2003).

Det beslut som meddelas med anledning av begäran om omprövning får överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges i förvaltningsprocesslagen (586/1996).

Förvaltningsdomstolens beslut får överklagas genom besvär endast om högsta förvaltningsdomstolen beviljar besvärstillstånd.

Förvaltningsdomstolen ska ge Kommunikationsverket tillfälle att bli hört.

98 §

Avgifter för utförandet av kopplingen

Den som utför en koppling får ta ut avgifter av Försvarsmaktens underrättelsetjänst för tjänster som den har producerat utgående från 5 kapitlet. Avgifterna får inte överstiga beloppet av de totala kostnader som utförandet av kopplingen medför för den som utför kopplingen.

99 §

Användning av uppgifter som teleföretagen lagrar

Uppgifter som avses i 157 § 1 mom. i informationssamhällsbalken får användas för att utföra ett militärt underrättelseuppdrag.

100 §

Rätt att få information av privata sammanslutningar och personer

På begäran av en militärjurist eller en annan tjänsteman som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoderna har militärunderrättelsemyndigheten trots den företags-, bank- eller försäkringshemlighet som förpliktar en sammanslutnings medlem, revisor, verkställande direktör, styrelsemedlem eller anställd få sådana uppgifter som i ett enskilt fall kan antas vara nödvändiga vid utredningen av verksamhet som avses i 4 §, och vilka kan antas vara av betydelse
1) för att identifiera, få tag på eller reda ut kontaktuppgifterna till en fysisk eller juridisk person eller för att reda ut hur en person som är föremål för militär underrättelseverksamhet rör sig,
2) för att inrikta användningen av en underrättelseinhämtningsmetod på en viss person, eller
3) för att reda ut en fysisk eller juridisk persons ekonomiska verksamhet.

Militärunderrättelsemyndigheterna har i enskilda fall på begäran rätt att av teleföretag och av sammanslutningsabonnenter få kontaktuppgifter för teleadresser som inte är upptagna i en offentlig katalog eller information som specificerar en teleadress eller teleterminalutrustning, om informationen behövs för ett underrättelseuppdrag. Militärunderrättelsemyndigheterna har motsvarande rätt att få information om utdelningsadresser av en sammanslutning som bedriver postverksamhet.

10 kap.

Den militära underrättelseverksamhetens informationssystem och övriga personregister

101 §

Den militära underrättelseverksamhetens informationssystem

Informationssystemet för militär underrättelseverksamhet är ett permanent personregister som är avsett att användas av militärunderrättelsemyndigheten och som förs med hjälp av automatisk databehandling. Registeransvarig för informationssystemet för militär underrättelseverksamhet är huvudstaben. Till informationssystemet kan dessutom höra delar som upprätthålls manuellt.

Av informationssystemet ska framgå vem som har registrerat en uppgift.

102 §

Datainnehållet i informationssystemet för militär underrättelseverksamhet

Informationssystemet för militär underrättelseverksamhet kan innehålla uppgifter som det är nödvändigt att behandla och kombinera för att de uppdrag som i denna lag föreskrivs för militärunderrättelsemyndigheten ska kunna fullgöras.

I informationssystemet för militär underrättelseverksamhet får följande behövliga uppgifter om en person registreras:
1) personbeteckning,

2) identifieringsuppgifter som grundar sig på personens fysiska egenskaper och andra identifieringsuppgifter samt ljud- och bildupptagningar,
3) uppgifter om medborgarskap och familjeförhållanden,
4) uppgifter om bosättningsort,
5) uppgifter om utbildning och yrke samt arbets- och anställningshistoria,
6) kontaktuppgifter,
7) uppgifter om resande,
8) andra uppgifter som behövs för identifiering av en fysisk eller juridisk person eller med tanke på personens säkerhet eller uppgifter som behövs med tanke på arbetarskyddet vid försvarsmakten,
9) identifieringsuppgifter,
10) andra uppgifter som gäller en persons verksamhet och beteende.

I registret får dessutom föras in uppgifter som behövs för utredning av tillförlitligheten hos en person eller ett företag.

103 §

Rätt att använda informationssystemet för militär underrättelseverksamhet

Informationssystemet för militär underrättelseverksamhet får användas av de tjänstemän som har förordnats till uppdrag som avses i denna lag. Rätt att använda informationssystemet får också beviljas reservister som deltar i en repetitionsövning enligt värnpliktslagen för fullgörande av uppdrag om vilka föreskrivs i 88 §. Användningen av informationssystemet ska då ske under ledning och övervakning av en tjänsteman som förordnats till ett militärt underrättelseuppdrag.

104 §

Tillfälliga personregister

Militärunderrättelsemyndigheten får ha i riksomfattande användning eller en eller flera förvaltningsenheter inom myndigheten får ha i användning tillfälliga personregister.

I ett tillfälligt personregister får införas och i det får hanteras endast sådana personuppgifter som är nödvändiga för att ett uppdrag eller en uppdragshelhet som avses i denna lag ska kunna fullgöras. Rätt att använda ett tillfälligt personregister har de tjänstemän för vilkas bruk registret har inrättats. Av registret ska framgå vem som har registrerat en uppgift.

Registeransvarig för ett riksomfattande tillfälligt personregister är huvudstaben. Registeransvarig för ett annat tillfälligt personregister än ett riksomfattande är den förvaltningsenhet som ansvarar för verksamheten.

Huvudstaben beslutar om inrättande av ett riksomfattande tillfälligt personregister. Den förvaltningsenhet som ansvarar för verksamheten beslutar om inrättande av ett annat tillfälligt personregister än ett riksomfattande. Ett skriftligt beslut fattas om inrättande av ett register. Ett beslut om inrättande av ett tillfälligt personregister som är i riksomfattande användning och en väsentlig ändring av registret ska senast en månad innan registret inrättas eller ändras anmälas till dataombudsmannen. I beslutet om inrättande ska ändamålet med personregistret anges.

105 §

Behandling av känsliga uppgifter

Sådana känsliga personuppgifter som nämns i 11 § 3 punkten i personuppgiftslagen får samlas in och lagras i informationssystemet för militär underrättelseverksamhet och i ett annat personregister och annars behandlas då uppgifterna är behövliga med tanke på syftet med registret.

Uppgifter som nämns i 11 § 1, 2 och 4—6 punkten i personuppgiftslagen får samlas in och registreras i informationssystemet för militär underrättelseverksamhet och i ett annat personregister

och i övrigt behandlas endast om det är nödvändigt för att ett underrättelseuppdrag ska kunna fullgöras.

De uppgifter som nämns i 4 punkten i nämnda paragraf får dessutom samlas in och registreras i informationssystemet för militär underrättelseverksamhet och i ett annat personregister och i övrigt behandlas om det är nödvändigt för att säkerställa den registrerades egen säkerhet eller myndighetens arbetarskydd.

Känsliga uppgifter ska utplånas ur registret så snart det inte finns någon i 1–3 mom. nämnd grund att behandla dem.

106 §

Dataskydd för identifieringsuppgifter som grundar sig på fysiska egenskaper

Vid registrering eller annan hantering av sådana identifieringsuppgifter i elektronisk form som grundar sig på en persons fysiska egenskaper ska den registeransvariga särskilt sörja för dataskyddet för dessa identifieringsuppgifter.

Vid registrering eller annan hantering av identifieringsuppgifter som grundar sig på en persons fysiska egenskaper ska det ses till att

1) de informationssystem, maskinvaror och programvaror som används för identifiering och för hantering av identifieringsuppgifterna är säkra,

2) identifieringsuppgifterna är skyddade mot obehörig åtkomst och mot kränkningar, modifieringar och förfalskningar som avser identifieringsuppgifternas konfidentiella karaktär och integritet samt annan hantering som sker av misstag eller i strid med lag,

3) det vid identifiering och vid hantering av identifieringsuppgifter genomförs behövliga tekniska och organisatoriska åtgärder för att säkerställa att identifieringen och hanteringen kan genomföras på ett sätt som tryggar dataskyddet och integritetsskyddet.

Den registeransvariga svarar för det ovan avsedda dataskyddet också i fråga om en tredje part som på uppdrag av den registeransvariga registrerar identifieringsuppgifter som grundar sig på en persons fysiska egenskaper.

107 §

Hantering och användning av personuppgifter som inte hänför sig till ett enskilt uppdrag

Personuppgifter som militärunderrättelsemyndigheten har fått i ett enskilt underrättelseuppdrag och som är nödvändiga för fullgörandet av underrättelseuppdrag men som inte hänför sig till uppdraget i fråga eller något annat underrättelseuppdrag som fullgörs, men som sannolikt behövs i ett annat kommande underrättelseuppdrag, får samlas och föras in i det informationssystem för militär underrättelseverksamhet som avses i 101 § och i det tillfälliga personregister som avses i 104 § under de förutsättningar om vilka föreskrivs i nämnda paragrafer.

En personuppgift som avses i 1 mom. och som inhämtats med underrättelseinhämtningsmetoder enligt 4 kap. i denna lag får dock användas endast i ett sådant underrättelseuppdrag för vars genomförande den underrättelseinhämtningsmetod med vilken uppgiften har inhämtats skulle ha fått användas. Beslut om användning av en sådan uppgift fattas av domstolen, om den är behörig att fatta beslut om den informationsinhämtningsmetod med vilken informationen har fåtts.

Hur befogad och nödvändig hanteringen av uppgifterna är ska bedömas minst vart tredje år. Uppgifterna ska utplånas när de har konstaterats vara onödiga med tanke på användningsändamålet.

108 §

Rätt att få uppgifter ur register och informationssystem

Militärunderrättelsemyndigheten har för att fullgöra sina uppdrag som avses i denna lag och upprätthålla sina personregister rätt att utan avgift och trots sekretessbestämmelserna få följande:
1) uppgifter enligt 13–17 § i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009),
2) ur bötesregistret de uppgifter om bötesstraff och verkställigheten av dem som införts i registret samt ur det i justitieförvaltningens riksomfattande informationssystem ingående rikssystemet för behandling av diarie- och ärendehanteringsuppgifter uppgifter om brottmål som är eller har varit anhängiga hos åklagarmyndigheterna eller vid domstol och ur registret över avgöranden och meddelanden om avgöranden uppgifter om avgöranden i brottmål och om avgörandenas laga kraft, om sådan information kan fås,
3) ur utrikesministeriets informationssystem uppgifter om dem som hör till personalen vid diplomatiska beskickningar och konsulat som representerar den utsändande staten i Finland och om dem som hör till personalen vid en internationell organisations organ i Finland eller något annat internationellt organ i samma ställning samt om dessa personers familjemedlemmar och om dem som är i privat tjänst hos dessa personer, samt uppgifter om visumansökningar och visumbeslut ur delregistret för visumärenden som ingår i utlänningsregistret om vilket föreskrivs i lagen om utlänningsregistret (1270/1997),
4) uppgifter ur polisens personregister,
5) uppgifter ur tullens register om vilka föreskrivs i lagen om behandling av personuppgifter inom Tullen (639/2015),
6) uppgifter ur utsökningsregistret om vilket föreskrivs i utsökningsbalken (705/2007),
7) uppgifter om ägare eller innehavare av ett fordon ur fordonstrafikregistret enligt lagen om fordonstrafikregistret (541/2003),
8) uppgifter om de personlistor som gäller passagerare enligt lagen om passagerarfartygs personlistor (1038/2009),
9) nödvändiga uppgifter om resande enligt lagen om inkvarterings- och förplägnadsverksamhet (308/2006) av utövare av inkvarteringsverksamhet,
10) uppgifter om användning av radiofrekvenser som avses i informationssamhällsbalken,
11) uppgifter ur försvarsmaktens personregister,
12) uppgifter ur Försvarsutbildningsföreningens register om vilket föreskrivs i lagen om frivilligt försvar (556/2007),
13) uppgifter från försvarsministeriet om de tillståndsärenden som avses i lagen om export av försvarsmateriel (282/2012),
14) uppgifter från utrikesministeriet om de tillståndsärenden som avses i lagen om kontroll av export av produkter med dubbel användning (562/1996),
15) ur farkostregistret som avses i lagen om farkostregistret (424/2014) och ur Ålands fritidsbåtsregister uppgifter som behövs om båtar samt om ägare och innehavare av sådana,
16) ur Migrationsverkets informationssystem uppgifter om ärenden som gäller resedokument, visum, vistelse, internationellt skydd, avlägsnande ur landet, inreseförbud och medborgarskap,
17) ur luftfartygsregistret som avses i luftfartslagen (864/2014) uppgifter om luftfartyg samt om innehavare och ägare av sådana,
18) ur fartygsregistret, registret över fartyg under byggnad och historikregistret som avses i fartygsregisterlagen (512/1993) sådana uppgifter som behövs om fartyg samt om ägare och innehavare av sådana,
19) uppgifter ur kommunikationsministeriets trafiktillståndsregister,
20) uppgifter ur de register som avses i lagen om behandling av personuppgifter vid gränsbevakningsväsendet (579/2005),
21) ur Brottspåföljdsmyndighetens personregister uppgifter om en person som dömts, fängslats och tagits in på en enhet vid Brottspåföljdsmyndigheten,

22) av trafik-, fiske- och miljömyndigheterna uppgifter om fordon och deras position samt om trafik,
25) uppgifter ur Skatteförvaltningens informationssystem för beskattningen,
26) ur Patent- och registerstyrelsens handelsregister uppgifter om anmälningar och meddelanden som gäller näringsidkare.

Uppgifterna kan också lämnas ut genom teknisk anslutning eller annars elektroniskt på det sätt som om detta överenskoms med den registeransvariga.

109 §

Rätt att få information av myndigheter

Militärunderrättelsemyndigheten har rätt att för ett uppdrag som avses i denna lag av myndigheter och sammanslutningar och personer som tillsatts för att sköta ett offentligt uppdrag avgiftsfritt och trots sekretessbestämmelser få de uppgifter och handlingar som behövs, om inte givandet av en sådan uppgift eller handling till militärunderrättelsemyndigheten eller användning av uppgifterna som bevis har förbjudits eller begränsats i lag.

110 §

Transportörers skyldighet att lämna uppgifter om flygpassagerare

Utöver det som föreskrivs i 100 § ska ett lufttrafikföretag på begäran av militärunderrättelsemyndigheten tillställa myndigheten uppgifter om passagerare i flygtrafik.

I uppgifterna om passagerare i flygtrafik ska inbegripas numret på och typen av det resedokument som använts, medborgarskap eller avsaknad av medborgarskap, fullständigt namn, födelsetid, det gränsövergångsställe där personen anländer till medlemsstaternas territorium eller lämnar medlemsstaternas territorium, transportkod, transportens avgångs- och ankomsttider, det totala antalet personer som ingår i transporten i fråga samt den ursprungliga avgångsorten. Uppgifterna ska överlåtas elektroniskt eller, om detta inte är möjligt, på något annat adekvat sätt.

111 §

Utlämnande av uppgifter till en militär myndighet

Trots sekretessbestämmelserna har den registeransvariga rätt att till en militär myndighet lämna ut uppgifter i informationssystemet för militär underrättelseverksamhet och andra personregister, vilka avses i detta kapitel, för att de i lag föreskrivna uppdragen ska kunna fullgöras, om uppgifterna behövs för att
1) trygga statens säkerhet,
2) avvärja en omedelbart förestående allvarlig fara som hotar den allmänna säkerheten.

Uppgifterna får också lämnas ut genom teknisk anslutning eller annars elektroniskt.

112 §

Utlämnande av uppgifter till skyddspolisen

Den registeransvariga får trots sekretessbestämmelserna till skyddspolisen lämna ut personuppgifter ur de register som avses i detta kapitel, om uppgifterna behövs för sådan underrättelseinhämtning som avses i 5 a kap. i polislagen eller i lagen om civil underrättelseinhämtning avseende datatrafik.

Uppgifterna får också lämnas ut genom teknisk anslutning eller annars elektroniskt på det sätt som om detta överenskoms med den registeransvariga.

113 §

Utlämnande av uppgifter för att förhindra en fara eller skada

Trots sekretessbestämmelserna får den registeransvariga lämna ut personuppgifter ur de register som avses i detta kapitel för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada.

Uppgifter som erhållits av en annan myndighet får endast lämnas ut med samtycke av den myndighet som lämnat uppgifterna.

114 §

Beslut om utlämnande av uppgifter

Beslut om rätten att lämna ut uppgifter ur informationssystemet för militär underrättelseverksamhet enligt 101 § och ur ett tillfälligt personregister enligt 104 § genom teknisk anslutning eller som en datamängd fattas av huvudstaben.

När beslut om utlämnande fattas ska uppgifternas art beaktas för att den registrerades integritetsskydd och datasäkerhet ska kunna tryggas.

115 §

Utplåning av uppgifter i informationssystemet för militär underrättelseverksamhet

I informationssystemet för militär underrättelseverksamhet utplånas personuppgifterna 50 år efter att den sista uppgiften införts.

Hur befogad och nödvändig hanteringen av uppgifterna är ska bedömas minst vart femte år.

116 §

Utplåning av uppgifter i tillfälliga personregister

I ett tillfälligt personregister utplånas personuppgifterna när det har konstaterats att uppgifterna är onödiga med tanke på registrets ändamål.

Hur befogad och nödvändig hanteringen av uppgifterna är ska bedömas minst vart tredje år.

Ett tillfälligt personregister som blivit onödigt ska förstöras, om det inte flyttas över för arkivering.

117 §

Hantering av personbeteckning

En personbeteckning får hanteras med samtycke av den registrerade eller när det är nödvändigt med tanke på ett informationsinhämtningsuppdrag som militärunderrättelsemyndigheten har.

Den registeransvariga ska se till att personbeteckningen inte onödigt antecknas i handlingar som skrivs ut eller upprättas på basis av personregistret.

118 §

Begränsning av granskningsrätten

En registrerad har inte rätt att granska uppgifterna i informationssystemet för militär underrättelseverksamhet som avses i 101 § eller i ett tillfälligt personregister som avses i 104 §.

Dataombudsmannen kan på begäran av en registrerad eller på eget initiativ granska lagenligheten i de uppgifter om den registrerade som har införts i ovan nämnda informationssystem och register.

119 §

Överlåtelse av uppgifter i internationellt samarbete

Militärunderrättelsemyndigheten får i internationellt samarbete enligt 18 § trots sekretessbestämmelserna till utländska underrättelse- och säkerhetstjänster överlåta uppgifter ur ett personregister som det föreskrivs om i denna lag, om detta är nödvändigt för att säkerställa den nationella säkerheten.

Kvaliteten på de uppgifter som lämnas ut ska bekräftas och uppgifterna ska om möjligt förses med information som gör det möjligt för mottagaren att bedöma hur korrekta, fullständiga, aktuella och tillförlitliga uppgifterna är. Om det framgår att felaktiga uppgifter har lämnats ut eller att uppgifter lämnats ut i strid med lag, ska detta utan dröjsmål meddelas mottagaren.

Uppgifterna får också lämnas ut genom teknisk anslutning eller som en datamängd.

120 §

Behandling av uppgifter som erhållits i internationellt samarbete

Vid behandlingen av uppgifter som erhållits från en annan stats underrättelse- eller säkerhetstjänst ska i fråga om sekretess, tystnadsplikt, begränsningar i användningen av uppgifter, vidareöverlåtelse av uppgifter eller återsändande av utlämnat material iakttas vad som anges i de villkor som den som lämnat ut uppgifterna ställt.

11 kap.

Övervakningen av den militära underrättelseverksamheten inom försvarsförvaltningen

121 §

Rättslig och parlamentarisk övervakning av den militära underrättelseverksamheten

Laglighetsövervakningen av underrättelseverksamheten utförs av tillsynsmyndigheten för underrättelseverksamheten.

Den parlamentariska övervakningen utförs av riksdagen.

122 §

Intern kontroll

Chefen för huvudstaben övervakar den militära underrättelseverksamheten. Vidare svarar försvarsmaktens assessor för den interna laglighetsövervakningen av den militära underrättelseverksamheten.

123 §

Tillsyn som försvarsministeriet utövar

Försvarsministeriet har rätt att granska protokoll som upprättats över användningen av de underrättelseinhämtningsmetoder som avses i denna lag.

Trots sekretessbestämmelserna har försvarsministeriet rätt att få uppgifter om omständigheter som anknyter till den militära underrättelseverksamheten och som är av betydelse samhälleligt, ekonomiskt eller till sin allvarlighetsgrad.

124 §

Berättelse till riksdagens justitieombudsman

Försvarsministeriet ska årligen till riksdagens justitieombudsman avge en berättelse om hur underrättelseinhämtningsmetoderna och skyddandet av dem har använts och övervakats.

125 §

Närmare bestämmelser

Genom förordning av statsrådet kan närmare bestämmelser utfärdas om ordnandet och övervakningen av användningen av i denna lag avsedda underrättelseinhämtningsmetoder samt om dokumentering av åtgärderna och om de rapporter som ska lämnas för övervakningen.

12 kap.

Särskilda bestämmelser

126 §

Uträkning av tidsfrister

Vid uträkning av tidsfrister enligt denna lag ska inte lagen om beräknande av laga tid (150/1930) tillämpas.

En i månader uttryckt tid går ut den dag i den bestämda månaden som till sitt ordningsnummer motsvarar den dag då den utsatta tiden börjar löpa. Om motsvarande dag inte finns i den månad då den bestämda tiden löper ut, löper den bestämda tiden ut på månadens sista dag.

127 §

Förbud mot underrättelseinhämtning

Teleavlyssning, inhämtande av information i stället för teleavlyssning, optisk observation eller underrättelseinhämtning som avser datatrafik får inte riktas mot sådan kommunikation eller ett sådant meddelande, som parterna i kommunikationen inte får vittna om med stöd av 17 kap. 13, 14, 16 eller 20 § i rättegångsbalken.

Om det under teleavlyssningen, inhämtandet av information i stället för teleavlyssning eller den optiska observationen eller vid något annat tillfälle framkommer att det är fråga om ett meddelande som inte får avlyssnas eller observeras, ska åtgärden avbrytas och de upptagningar som fåtts genom den och anteckningarna om de uppgifter som fåtts genom den genast utplånas.

Om inget annat föreskrivs i denna lag, gäller de förbud mot underrättelseinhämtning som avses i denna paragraf dock inte sådana fall där en person som avses i 1 mom. med sin verksamhet äventyrar försvaret eller annars allvarligt äventyrar den nationella säkerheten och det också i fråga om denne har fattats beslut om teleavlyssning, inhämtande av information i stället för teleavlyssning, teknisk avlyssning eller optisk observation.

128 §

Granskning av upptagningar

Den tjänsteman som leder användningen av en underrättelseinhämtningsmetod och använder en underrättelseinhämtningsmetod ska utan ogrundat dröjsmål granska de upptagningar och handlingar som uppkommit vid användningen av underrättelseinhämtningsmetoderna i 4 eller 5 kap.

129 §

Undersökning av upptagningar

De upptagningar som uppkommit vid användningen av de underrättelseinhämtningsmetoder som avses i 4 och 5 kap. i denna lag får undersökas endast av domstol och huvudstabens underrättelsechef, en tjänsteman vid militärunderrättelsemyndigheten som är särskilt förtrogen med användningen av underrättelseinhämtningsmetoder eller en annan tjänsteman vid militärunderrättelsemyndigheten som har förordnats till ett underrättelseuppdrag.

Dessutom får upptagningar på förordnande av huvudstabens underrättelsechef också undersökas av en sakkunnig som står utanför militärunderrättelsemyndigheten eller en annan person som bistår vid underrättelseinhämtningen.

130 §

Protokoll

Över användningen av en underrättelseinhämtningsmetod ska utan ogrundat dröjsmål upprättas ett protokoll.

Genom förordning av statsrådet utfärdas närmare bestämmelser om registreringen av åtgärderna i ett underrättelseuppdrag.

131 §

Tystnadsplikt

I fråga om tystnadsplikten för tjänstemän som är anställda vid militärunderrättelsemyndigheten gäller vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet, annanstans i lag och nedan i detta kapitel. Samma tystnadsplikt har den som utför ett underrättelseuppdrag under ledning och övervakning av militärunderrättelsemyndigheten eller bistår vid fullgörandet av ett underrättelseuppdrag.

Tjänstemän som är anställda vid militärunderrättelsemyndigheten får inte lämna ut uppgifter som avslöjar identiteten hos en person som har lämnat information konfidentiellt eller deltagit i en täckoperation, om utlämnandet av informationen kan äventyra den persons säkerhet som gett uppgifterna eller deltagit i en täckoperation, eller en närstående persons säkerhet.

Tystnadsplikten gäller också när utlämnandet av uppgifterna om identiteten kan äventyra redan avslutad, pågående eller framtida underrättelseinhämtning.

Tystnadsplikt enligt 1 och 2 mom. har också den som utför ett underrättelseuppdrag under ledning och övervakning av militärunderrättelsemyndigheten eller bistår vid fullgörandet av ett underrättelseuppdrag.

Tystnadsplikten gäller också efter det att anställningsförhållandet till militärunderrättelsemyndigheten har upphört.

132 §

Rätt att förtiga uppgifter

De som är anställda vid militärunderrättelsemyndigheterna är inte skyldiga att lämna ut information om identiteten hos en person av vilken de i sitt anställningsförhållande har fått konfidentiell information och inte heller om sekretessbelagda taktiska eller tekniska metoder.

Samma rätt att förtiga uppgifter har den som utför ett underrättelseuppdrag under ledning och övervakning av militärunderrättelsemyndigheten eller bistår vid fullgörandet av ett underrättelseuppdrag.

133 §

Tjänstetecken

En tjänsteman vid militärunderrättelsemyndigheten har ett tjänstetecken om vilket föreskrivs genom förordning av försvarsministeriet.

En tjänsteman vid militärunderrättelsemyndigheten ska vid behov ha med sig tjänstetecknet när tjänstemannen utför ett tjänsteuppdrag. En tjänsteman vid militärunderrättelsemyndigheten ska vid behov presentera sig som tjänsteman vid militärunderrättelsemyndigheten för den som är föremål för en åtgärd och på begäran visa upp sitt tjänstetecken, om presentationen eller uppvisandet kan ske utan att åtgärden äventyras.

Militärunderrättelsemyndigheten ska se till att en tjänsteman vid myndigheten som har utfört ett tjänsteuppdrag vid behov kan identifieras.

134 §

Förfarandet vid domstol

Ett tillståndsärende som gäller en underrättelseinhämtningsmetod behandlas vid Helsingfors tingsrätt. Tingsrätten är domför med ordföranden ensam. Ett sammanträde kan hållas även vid en annan tidpunkt och på en annan plats än vad som bestäms om allmän underrätts sammanträde.

Ett yrkande på användning av en underrättelseinhämtningsmetod ska göras skriftligen. Ett yrkande som gäller användning av en underrättelseinhämtningsmetod ska utan dröjsmål tas upp till behandling i domstol i närvaro av den tjänsteman som framställt yrkandet eller en av denne förordnad tjänsteman som är insatt i ärendet.

Ärendet ska avgöras skyndsamt. Behandlingen kan också ske med anlitande av videokonferens eller någon annan lämplig teknisk dataöverföring där de som deltar i behandlingen har sådan kontakt att de kan tala med och se varandra.

Bestämmelser om innehållet i det beslut som gäller en underrättelseinhämtningsmetod finns i 4 och 5 kap. i denna lag. Beslutet ska meddelas omedelbart eller senast när behandlingen av ärenden som gäller underrättelseinhämtningsmetoder, vilka anknyter till samma underrättelsehelhet, har avslutats.

Om domstolen har beviljat tillstånd till teleavlyssning eller teleövervakning, får den pröva och avgöra ett ärende som gäller beviljande av tillstånd i fråga om en ny person, teleadress eller teleterminalutrustning utan att den tjänsteman som framställt yrkandet eller en av denne förordnad tjänsteman är närvarande, om det har förflutit mindre än sex månader från behandlingen av det

tidigare tillståndsärendet. Ärendet kan behandlas utan att tjänstemannen är närvarande också om användningen av underrättelseinhämtningsmetoden redan har avslutats.

Ett beslut i ett tillståndsärende får inte överklagas genom besvär. Klagan mot beslutet får anföras utan tidsbegränsning vid Helsingfors hovrätt. Klagan ska behandlas i brådskande ordning.

Vid handläggningen av ett ärende som gäller en underrättelseinhämtningsmetod ska det fästas särskild vikt vid att sekretessen iakttas och att informationen i handlingar och informationssystem skyddas genom behövliga förfaranden och datasäkerhetsarrangemang.

135 §

Begränsning av partsoffentlighet i vissa fall

En person vars rättigheter eller skyldigheter saken gäller har inte, trots 11 § i lagen om offentlighet i myndigheternas verksamhet, rätt att få vetskap om underrättelseinhämtning enligt denna lag förrän ett meddelande enligt 86 § har avgetts.

Bestämmelser om begränsningar som hänför sig till civil underrättelseverksamhet finns i 5 a kap. i polislagen.

13 kap.

Ikraftträdande

136 §

Ikraftträdande

Lagen träder i kraft den 20 .

Puolustusministeriö
Eteläinen Makasiinikatu 8
PL 31, 00131 HELSINKI

www.defmin.fi

ISBN: 978-951-25-2898-1 nid.
ISBN: 978-951-25-2899-8 pdf